Digital Forensic Laboratory (DFL) Guidelines 2021[1]

[Ref: section 10 of Digital Security Act 2018]

1. Background Information

1.1 Scientific Evidence in criminal investigation

"EVERY contact leaves a trace'' in both physical and virtual world which led scientists to develop forensic science. The need for scientific evidence arise when investigation officer (IO) cannot conclude a criminal investigation solely on the basis of oral testimony or documentary evidence of an witness or confession of an accused. Forensic science enters the investigation process to fill up the gap. It strives to find out truth surrounding a crime scene using scientific principles and procedure to support decision makers in criminal justice system.. The word "Forensic" derived from a Latin word "forensis" which means "a forum" where in Roman times, senators and others debated and held judicial proceedings as multi-dimensional space of negotiation and truth-finding.

Forensics or forensic science is defined as (i) the use of scientific principles in issues of law, (ii) the use of science in a legal setting. Forensic scientists can not only aid in investigations into a crime, but also help determine who the victim and suspect are, what crime was actually committed, and if the suspect is able to stand trial.

In Bangladesh, criminal investigation is mainly governed by three legislation — the Code of Criminal Procedure 1898, the Evidence Act 1872 and the Police Regulations of Bengal 1943. These three instruments, however, do not provide any direct provisions governing the collection and management of forensic evidence. They provide some relevant regulations regarding criminal investigations. The technological advancements in the last century has opened the door for forensic science to our justice system. This led to establishment of specialist set-up under Police administration for handwriting identification or finger impression or DNA and lastly digital forensics under ICTD and Police.

1.2 Electronic/Digital Evidence

'Information and Communication Technology (ICT) Act, 2006' (amended in 2013 and 2018) and the Digital Security Act 2018 recognise digital record and evidence and regulate all activities in the digital space. Speedy Trial Tribunal Ain 2002, Ain Sringkhola Bighnokari Aporadh Ain 2002, Pornography Niyontron Ain2012 also take cognizance of electronic

[1]established or to be established under Digital Forensic Act 2018 and Digital Forensic Rules 2020. *Approved for immediate release by National Security Council on 00.00.2021 under section 10 of Digital Security Act 2018 and rule 13 of Digital Forensic Rules 2020.*

evidence. etc. Although "the Evidence Act itself does not include specific information on what encompasses electronic evidences or how to use these evidences in various suits, creating uncertainty among the lawyers and the judges about using and interpreting them under the scope of the Act."[2]Evidence according to section 3 of Evidence Act 1872 comprises 'oral evidence by witness upon inquiry before the court and documentary evidence produced before the court for inspection'. The sole reference on forensic investigation is section 45 of the Evidence Act, 1872. "If the court put forward the necessity to form an opinion as to determine the fact of science or art or handwriting identification or finger impression etc., then the court may summon the assistance of specially skilled person/s in that particular field".

1.3 Digital Forensics

The latest addition in forensic science is Digital Forensics. Until 2020, there was no well-founded rule to consider evidence from the cyberspace or digital devices. Digital Security Rules 2021 has been enacted to fillup the gap and guide criminal investigation in digital space or digital devices to gather digital/electronic evidence.

Digital forensics investigates material found on digital devices. While its primary focus is on computers, it can and does include any device that stores digital data, including mobile devices, databases and networks. The type of investigations done by digital forensics varies, though they typically include evidence needed in criminal courts that is obtained from a computer, evidence derived from the internet, or investigations into network intrusions. It can be used to identify a crime, identify culprits, confirm statements and even prove the authenticity of documents. Now globally digital forensics is one of the largest and most complex part of forensic science.

2. Establishment of Digital Forensic Lab

The Digital Security Agency (DSA) with the approval of National Security Council will establish one or more digital forensic laboratory (DFL[3]) to implement the mandate of section 10(1) of the Digital Security Act (Act). The functions and activities of the laboratory will be conducted under overall guidance and supervision of DSA.The case management of any digital forensic

[2]Md. Mahmudul Islam Shakilhttps://thefinancialexpress.com.bd/public/index.php/views/need-for-amending-evidence-law-1872-1577458405 Published: December 27, 2019, retrieved on 16 May 2021.

[3] CIRT, BCC [https://www.cirt.gov.bd/], CID of Bangladesh Police,Cyber Crime Investigation Division, Dhaka Metropolitan Police, and CCA, BCC [http://www.cca.gov.bd/] are pioneers in Bangladesh. They are yet to be recognised under sec 10(2) of DSA 2018.

case, laboratory analysis and quality assurance of any digital forensic lab will be done following the seven BSTI and ISO standards mentioned in Rule 14(1). In this regard the Lab will ensure:

(a) Efficacy of its work procedure;

(b) Use appropriate standard forensic sample;

(c) Maintain and calibrate all equipment and machinery used in forensic examination; and

(d) The personnel engaged in the digital forensic lab (i) receive appropriate training on forensic tools and other relevant skills, (ii) are duly certified user of hardware and software and(iii) also duly certified to present evidence as expert witness before a court of law.

3. Definitions

(1) In this Guideline, unless there is anything repugnant in the subject or context -

(i) "Digital Evidence" means Information or data stored or transmitted in binary form that may be relied on as evidence[4];

(ii) "Digital Evidence first responder (DEFR)" meansPerson who is authorized, trained and qualified to act first at an incident scene in performing digital evidence collection and acquisition with the responsibility for handling that evidence. The post is called Digital Forensic Investigator (Hardware) and includes Assisant Digital Forensic investigator;

(iii) "Digital Evidence Specialist (DES)" meansPerson who can carry out the tasks of a DEFR and has specialized knowledge, skills and abilities to handle a wide range of technical issues. The post is called Analyst and includes Digital Forensic Examiner or Assistant Digital Forensic Examiner.

(iv) "Digital Forensic" meansDigital forensic is a branch of forensic science that focuses on identifying, acquiring, processing, analysing and reporting on data stored on a computer, digital devices or other digital storage media. The main goal of digital forensics is to extract data from the electronic evidence, process the data into useful information and present the findings for prosecution[5].

(v) "Digital Forensic Laboratory Supervisor" means an officer responsible to exercise the powers and functions defined in this guideline and in rule 16(3) of the Digital Security Rules[6];

[4]p2 BDS ISO/IEC 27037

[5]p12 Global guideline, Interpol, 2019

[6] Bangladesh Gazettee page 3229, 8.3.2020 Digital Security Rules 2020

(vi) "Digital Forensic Laboratory Expert" meansAn officer responsible to exercise the powers and functions defined in this guideline and in rule 16(4) of the Digital Security Rules[6];

(vii) "digital investigation" meansuse of scientifically derived and proven methods towards the identification, collection, transportation, storage, analysis, interpretation, presentation, distribution, return, and/or destruction of digital evidence derived from digital sources, while obtaining proper authorizations for all activities, properly documenting all activities, interacting with the physical investigation, preserving digital evidence, and maintaining the chain of custody, for the purpose of facilitating or furthering the reconstruction of events found to be incidents requiring a digital investigation, whether of criminal nature or not;

(viii) "electronic evidence" meansThe computer, digital device or other digital storage system which holds valuable data for investigation is known as electronic evidence[5];

(ix) "electronic discovery" means*discovery* that includes the identification, preservation, collection, processing, review, analysis, or production of *Electronically Stored Information.*[7]*;*

(x) Electronically Stored Information (ESI)meansdata or information of any kind and from any source, whose temporal existence is evidenced by being stored in or on any electronic medium. ESI includes traditional e-mail, memos, letters, spreadsheets, databases, office documents, presentations and other electronic formats commonly found on a computer. ESI also includes system, application and file-associated metadata such as timestamps, revision history, file type, etc.[8]

(xi) "examination" meansset of processes applied to identify and retrieve relevant potential digital evidence from one or more sources[SOURCE: ISO/IEC 27042:2015, 3.7]

(xii) "Examiner" means an officerresponsible for conducting digital forensic examination or providing expert opinion on digital/electronic evidence before any court or other authority and the appointment is notified in the official gazettee;

(xiii) "incident" meanssingle or a series of unwanted or unexpected information security breaches or events, whether of criminal nature or not, that have a significant probability of compromising business operations or threatening information security;

(xiv) "investigation" meansapplication of *examinations*, analyses, and interpretation to aid understanding of an incident[9];

[7]ISO/IEC 27050-1:2019 Part 1, 3.7
[8]ISO/IEC 27050-1:2019 Part 1, 3.8
[9]ISO/IEC 27042:2015, 3.10

(xv) "investigative team" all persons involved directly in the conduct of the investigation[10];

(xvi) "Requisition" meansRequest in prescribed format by a police officer or an organisation to conduct a digital forensic investigation;

(2) The words and expressions used in this guideline but not defined shall have the same meaning as are used in the Information and Communication Technology Act 2006 or Digital Security Act 2018 or Digital Security Rules 2020 or seven BDS-ISO/IEC standards mentioned in rule 14 (para 6 below).

4. Abbreviation

DFL Digital Forensic laboratory

ISOInternational Standard Organisation

IECInternational Electrotechnical Commission

BDSBangladesh Standard

BSTI Bangladesh Standard Testing Institution

5. Requisition and processing requests

5.1A police officer or chief executive of an organisation may sign and forward a requisition addressed to DFL supervisor for collection of digital evidence for an offence or incident under section 53(a)& 53(d) of the Act and he may do so with the approval of the court/tribunal under section 53(b)-(c);

5.2 The DFL supervisor on receipt of such requisition shall refer it to the DFL expert under whose supervision and guidance the examination will be carried out. The expert shall ascertain with the help of requisition officer the digital storage media and processing devices that may contain the potential digital evidence relevant to the incident.Thereafter the expert shall proceed with the acquisition, examination, preservation, documentation and reporting following the provisions mentioned hereunder.

6. Operational guidelines

[10]ISO/IEC 27042:2015, 3.12

DFL will providequality services andin doing so shall generallyfollow the recognised BSTI standards namely ISO/IEC/BDS 17025, ISO/IEC/BDS 15489, ISO/IEC/BDS 27037, ISO/IEC/BDS 27041, ISO/IEC/BDS 27042, ISO/IEC/BDS 27043, ISO/IEC/BDS 27050 in all stages of the digital forensic work. It shall also follow the provisions detailed in rule 14-16 and schedule of Digital Security Rules 2020. Salient features of BSTI adopted standards are:

6.1 ISO/IEC/BDS 15489 – Records management – Part 1 Concepts and principles [Annexure 1/1] and Part 2 Guidelines [Annexure 1/2]

Part 1 of this standard establishes the core concepts and principles for the creation, capture and management of paper and digital records. Part 2 is the guideline which is supplementary to Part 1. Increasingly, records are made and kept in digital environments, offering a range of opportunities for new kinds of use and reuse. Digital environments also allow greater flexibility in the implementation of records controls, within and between systems that manage records.

6.2 ISO/IEC/BDS 17025 -General requirements for the competence of testing and calibration laboratories [Annexure 2]

This standard specifies the general requirements for the competence, impartiality and consistent operation of laboratories. It is applicable to all organizations performing laboratory activities, regardless of the number of personnel.Laboratory customers, regulatory authorities, organizations and schemes using peer-assessment, accreditation bodies, and others use this document in confirming or recognizing the competence of laboratories.

6.3 ISO/IEC/BDS 27037 – Guidelines for identification, collection, acquisition, and preservation of digital evidence [Annexure 3]

This ISO/IEC/BDS Standard provides guidelines for specific activities in handling potential digital evidence; these processes are: identification, collection, acquisition and preservation of potential digital evidence. These processes are required in an investigation that is designed to maintain the integrity of the digital evidence – an acceptable methodology in obtaining digital evidence that will contribute to its admissibility in legal and disciplinary actions as well as other required instances. This Standard also provides general guidelines for the collection of non-digital evidence that may be helpful in the analysis stage of the potential digital evidence.

This Standard intends to provide guidance to those individuals responsible for the identification, collection, acquisition and preservation of potential digital evidence. These

individuals include Digital Evidence First Responders (DEFRs), Digital Evidence Specialists (DESs), incident response specialists and forensic laboratory managers. This Standard ensures that responsible individuals manage potential digital evidence in practical ways that are acceptable worldwide, with the objective to facilitate investigation involving digital devices and digital evidence in a systematic and impartial manner while preserving its integrity and authenticity.

This Standard also intends to inform decision-makers who need to determine the reliability of digital evidence presented to them. It is applicable to organizations needing to protect, analyze and present potential digital evidence. It is relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence.

Application of this Standard requires compliance with national laws, rules and regulations. It should not replace specific legal requirements of any jurisdiction. Instead, it may serve as a practical guideline for any DEFR or DES in investigations involving potential digital evidence. It does not extend to the analysis of digital evidence and it does not replace jurisdiction-specific requirements that pertain to matters such as admissibility, evidential weighting, relevance and other judicially controlled limitations on the use of potential digital evidence in courts of law. This Standard may assist in the facilitation of potential digital evidence exchange between jurisdictions. In order to maintain the integrity of the digital evidence, users of this Standard are required to adapt and amend the procedures described in this Standard in accordance with the specific jurisdiction's legal requirements for evidence.

The potential digital evidence referred to in this Standard may be sourced from different types of digital devices, networks, databases, etc. It refers to data that is already in a digital format.This Standard gives guidance for the following devices[11] and/or functions that are used in various circumstances:

Digital storage media used in standard computers like hard drives, floppy disks, optical and magneto optical disks, data devices with similar functions,

Mobile phones, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards,

Mobile navigation systems,

Digital still and video cameras (including CCTV),

Standard computer with network connections,

Networks based on TCP/IP and other digital protocols, and

[11] The List is indicative and not exhaustive.

Devices with similar functions as above.

This standard details the context of collection, principles, handling requirements, processes of handling of digital evidence.

The key components of identification, collection, acquisition and preservation of digital evidence are:

Chains of custody

Precautions at the site of incident

Roles and responsibilities

Competency

Use of reasonable care

Documentation

Briefing

Proritizing collection and acquisition

Preservation of potential digital evidence

The standard provide detail instances of identification, collection, acquisition and preservation of digital evidence including non digital evidence in powered and powered of digital devices namely: (i) computer, peripheral devices and digital storage media, (ii) network devices and (iii) CCTV.

Finally the standard laid down the minimum documentation requirements for evidence transter.

6.4 ISO/IEC/BDS 27041 Guidance on assuring suitability and adequacy of incident investigative method [Annexure 4]

This Standard provides guidance on mechanisms for ensuring that methods and processes used in the investigation of information security incidents are "fit for purpose". It encapsulates best practice on defining requirements, describing methods, and providing evidence that implementations of methods can be shown to satisfy requirements. It includes consideration of how vendor and third-party testing can be used to assist this assurance process.

6.5 ISO/IEC/BDS 27042 – Guidelines for the analysis and interpretation of digital evidence [Annexure 5]

This Standard provides guidance on the conduct of the analysis and interpretation of potential digital evidence in order to identify and evaluate digital evidence which can be used to aid understanding of an incident. The exact nature of the data and information making up the potential digital evidence will depend on the nature of the incident and the digital evidence sources involved in that incident.

Analysis and interpretation of digital evidence can be a complex process. In some circumstances, there can be several methods which could be applied and members of the investigative team will be required to justify their selection of a particular process and show how it is equivalent to another process used by other investigators. In other circumstances, investigators may have to devise new methods for examining digital evidence which has not previously been considered and should be able to show that the method produced is "fit for purpose".

Application of a particular method can influence the interpretation of digital evidence processed by that method. The available digital evidence can influence the selection of methods for further analysis of digital evidence which has already been acquired.

This Standard provides a common framework, for the analytical and interpretational elements of information systems security incident handling, which can be used to assist in the implementation of new methods and provide a minimum common standard for digital evidence produced from such activities.

This standard details investigation, analysis, live analysis, interpretation, Reporting and competence and proficiency of the persons carrying out the analysis and interpretation of digital evidence.

6.6ISO/IEC/BDS 27043 – Incident investigation principles and processes [Annexure 6]

This Standard provides guidelines that encapsulate idealized models for common investigation processes across various investigation scenarios. This includes processes from pre-incident preparation up to and including returning evidence for storage or dissemination, as well as general advice and caveats on processes and appropriate identification, collection, acquisition, preservation, analysis, interpretation, and presentation of evidence. A basic principle of digital investigations is repeatability, where a suitably skilled investigator has to be able to obtain the same result as another similarly skilled investigator, working under similar conditions. This principle is exceptionally important to any general investigation. Guidelines for many investigation processes have been provided to ensure that there is clarity and transparency in obtaining the produced result for each particular process. The motivation

to provide guidelines for incident investigation principles and processes follows.

Established guidelines covering incident investigation principles and processes would expedite investigations because they would provide a common order of the events that an investigation entails. Using established guidelines allows smooth transition from one event to another during an investigation. Such guidelines would also allow proper training of inexperienced investigators. The guidelines, furthermore, aim to assure flexibility within an investigation due to the fact that many different types of digital investigations are possible. Harmonized incident investigation principles and processes are specified and indications are provided of how the investigation processes can be customized in different investigation scenarios.

A harmonized investigation process model is needed in criminal and civil prosecution settings, as well as in other environments, such as corporate breaches of information security and recovery of digital information from a defective storage device. The provided guidelines give succinct guidance on the exact process to be followed during any kind of digital investigation in such a way that, if challenged, no doubt should exist as to the adequacy of the investigation process followed during such an investigation.

6.6.1 Digital investigations

(a) General principles

Digital investigations are in practice applied whenever it is needed to investigate digital evidence as a result of an incident, whether an incident is of criminal nature or not. There are many kinds of digital investigations, such as on desktop computers, laptops, servers, data repositories, handheld/mobile device investigations, investigations on live data (e.g. network and volatile data investigations), and investigations on digital appliances such as DVRs, game consoles, and control systems. The digital investigation process, however, is formulated in such a way that it is applicable to any kind of digital investigation.

(b) Legal principles

In this standard an overview is given of the legal requirements pertaining to digital investigations and especially the admissibility of digital evidence in a court of law. It should be noted that legal requirements may differ extensively in different jurisdictions across the world. It records the generic requirements in terms of legal issues that can be adopted by the legal system of a specific jurisdiction.

(c) Digital investigation processes

The digital investigation processes constitute a long list In order to abstract digital investigation processes at a higher level, they can be categorized into the following digital

investigation process classes:

readiness processes: That class of processes dealing with pre-incident investigation processes. This class deals with defining strategies which can be employed to ensure systems are in place, and that the staff involved in the investigative process are proficiently trained prior to dealing with an incident occurring. The readiness processes are optional to the rest of the digital investigation processes.

initialization processes: This class of processes dealing with the initial commencement of the digital investigation. Initialization processes include: (i) incident detection; (ii) first response; (iii) planning; and (iv) preparation.

acquisitive processes: They deal with the physical investigation of a case where potential digital evidence is identified and handled. Acquisitive processes includ(i) potential digital evidence identification; (ii) potential digital evidence acquisition;(iii) potential digital evidence transportation; and (iv) potential digital evidence storage.

investigative processes: They deal with uncovering the potential digital evidence. Investigative processes include (i) potential digital evidence examination and analysis; (ii) digital evidence interpretation; (iii) reporting; (iv) presentation; and (v) investigation closure.

concurrent processes: That class of processes that continues concurrently alongside the other processes. This class of processes differ from the previous classes in the sense that they happen in tandem with the other processes instead of linear. In addition, the particular order in which the concurrent processes execute is irrelevant as opposed to the other non-concurrent processes. Concurrent processes include (i) obtaining authorization; (ii) documentation; (iii) managing information flow; (iv) preserving chain of custody; (v) preserving digital evidence; and (v) interaction with the physical investigation.

6.7 ISO/IEC/BDS 27050 Electronic discovery - Part 1:Overview and concepts; Part 2: Guidance for governance and management of electronic discovery; Part 3: Code of practice for electronic discovery.

Electronic discovery is the process of discovering pertinent Electronically Stored Information (ESI) or data by one or more parties involved in an investigation or litigation, or similar proceeding. This standard consists of three parts: (i) overview and concepts, (ii) guidance for governance and management of electronic discovery, and (iii) code of practice for electronic discovery. These three parts are relevant for both technical and non-technical persons involved at any stage from identification to presentation of the results to the requisition or judicial or relevant authority.

Part 1: Overview and concepts[Annexure 7(1)]

This document provides an overview of electronic discovery. In addition, it defines related terms and describes the concepts, including, but not limited to, identification, preservation, collection, processing, review, analysis, and production of ESI. This document also identifies other relevant standards (e.g. ISO/IEC 27037) and how they relate to, and interact with, electronic discovery activities.

Part 2: Guidance for governance and management of electronic discovery[Annexure 7(2)]

This document provides guidance for technical and non-technical personnel at senior management levels within an organization, including those with responsibility for compliance with statuary and regulatory requirements, and industry standards.

It describes how such personnel can identify and take ownership of risks related to electronic discovery, set policy and achieve compliance with corresponding external and internal requirements. It also suggests how to produce such policies in a form which can inform process control. Furthermore, it provides guidance on how to implement and control electronic discovery in accordance with the policies.

Part 3: Code of practice for electronic discovery [Annexure 7 (3)]

This document provides requirements and recommendations on activities in electronic discovery, including, but not limited to, identification, preservation, collection, processing, review, analysis and production of electronically stored information (ESI). In addition, this document specifies relevant measures that span the lifecycle of the ESI from its initial creation through to final disposition.

This document is relevant to both non-technical and technical personnel involved in some or all of the electronic discovery activities. It is important to note that the user is expected to be aware of any applicable jurisdictional requirements.

7. Digital Forensic examination procedures

TheISO/IEC/BDS 27037 [Annexure 3] and (ii) ISO/IEC/BDS 27042 [Annexure 5] details the recognized protocol that guide the assessment, acquisition, examination, documentation, reporting and archiving digital evidence. The former deals with indentification, collection,

acquisition, and preservation of digital evidence. The later one with analysis and interpretation of digital evidence.

The schedule of Digital Security Rules 2020 details the proceduresof digital examination . The principles, processes, suitability and adequacy of digital investigation are laid down in (i) ISO/IEC/BDS 27041 [Annexure 4] and (ii) ISO/IEC/BDS 27043 [Annexure 6]. The four steps for digital forensic examination are: (1) digital evidence assessment, (2) acquisition of digital evidence, (3) examination of digital evidence and (4) documentation of and reporting on digital evidence.

7.1 Digital Evidence Assessment

Digital evidence is represented in physical and logical form. The physical form includes the representation of data within a tangible device. The logical form of the potential digital evidence refers to the virtual representation of data within a device.

7.1.1Procedure: The steps detailed below shall be closely observed while receiving the forensic sample ~~or alamat~~ and the receiver shall record observations thereon, e.g. :-

(i) Legal basis for collection of the evidence;
(ii) Whether the forensic sample (digital evidence) received as sealed or not;
(iii) Description of forensic evidence or case history;
(iv) The relevant HW, SW and other evidences along with the file;
(v) State of forensic sample or evidence;
(vi) surrounding circumstances of evidence collection

7.1.2 The DFL assigned officer will review the following issues in connection with the requisition for forensic examination:

(i) Legal authority of the requisition officer;

(ii) Ascertain complete documentation of forensic examination requisition; and

(iii) Complete documentation of chain of custody.

7.1.3 The DFL assigned officer shall consult the requisition officer regarding his request and share possible results of the examination. In this consultation the following issues will be considered:

(i) Necessity of any additional special test (e.g. Search key words, Tool marks, Trace and questioned documents etc.) in connection with forensic examination of the given forensic sample or digital evidence;

(ii) Collect supplementary forensic sample or digital evidence (e.g. order to preserve and provide log of the internet service provider, identify remote location data archive/storage, email acquisition etc.)

(iii) Collection of any other sample or evidence to consider nexus between forensic sample or digital evidence and vicinal components in the interest of the investigation (for example: in a fraud or cheating case other items like laminator, deactivated credit card, cheque book, scanner, printer etc except the computer);

(iv) identify forensic sample or digital evidence (e.g. spreadsheet, file, database, financial record etc.)

(v) Determine necessity of additional information collection from the infected system (for example: pseudonym or alias, email address, name of internet service provider, user and network configuration, system log, password, used name etc) and acquisition from user and the officer of the infected system service provider;

(vi) Evaluate user skills of the infected system;

(vii) Determine order of examination of forensic sample or digital evidence or authentic information;

(viii) Determine necessity of additional expert to conduct the forensic examination;

(ix) Identify necessary equipment to conduct the forensic examination.

7.2 Acquisition of digital evidence

7.2.1. The following steps to be taken during acquisition of forensic sample or digital evidence:

(a) procedure:- The collection of forensic sample or digital evidence will be done considering the issues detailed below:-

(i) Prepare copy/replica for forensic test using bit by bit imaging for protection and preservation of main forensic sample or digital evidence;

(ii) Document configuration system of selected or used hardware and software;

(iii) Verify the hardware and software activities of the slected or used computer system;

(iv) Ensure access from outside to the storage media by removing casing of the digital device;

(v) Protect the selected digital device from static electricity and magnetic field and humidity;

(vi) Identify the external or internal and type of (ROM/SSD/IDE/SATA/SCSI) storage media of the digital device or both;

(vii) Record specification and configuration of the internal storage device and hardware of the digital device;

(viii) Record specification, interface and configuration of the drive (for example model, size, jumper settings, location, drive interface);

(ix) Examine internal and external component or machine parts of the selected digital device (e.g. mouse, keyboard, media access control address (MAC) including sound card, graphics card, network card, memory card of the personal computer, PCMCIA card, external drive etc;

(x) Disconnet power supply of motherboard and data cable to prevent deletion, loss or change of data of the seleted digital device;

(xi) Acquire configuration data by separate or controlled booting system from the system of suspected digital device;

(xii) Acquire CMOS/BIOS/Firmware data by separate controlled booting from the system of suspected digital device;

(xiii) Examine boot sequence of suspected digital device (e.g. BIOS/Firmware may be changed by system boot from floppy or CD-ROM drive);

(b) Procedure to be followed to record and preserve system date and time of the digital device accepted for forensic examination:

(i) Recover/revitalize booting system from forensic boot disk to determine functionality of the suspected digital device accepted for forensic examination (in case of failure of booting system);

(ii) Disconnect hard-disk and confirm connection of floppy or USB port or CD-ROM or DVD ROM drive or other booting system devices;

(iii) Load forensic boot disk in floppy or USB port or CD-ROM drive and ensure booting of the computer from forensic boot disk;

(iv) Collect CMOS or BIOS drive configuraton information from 3rd controlled boot after connectiong all storage devices;

(v) Ensure booting the digital device using forensic boot disk from the floppy or USB port or CD-ROM drive to avoid accidental booting and data loss of the computer

using affected storage device of the system device accepted for forensic examination;

(vi) In BIOS drive configuration select the drive configuration data to logical block address (LBA) or Large Disk or Cylinder, Head, Sector (CHS) preferably auto detection;

(C) **Power system down** |- (1) Remove the storage device from the digital device accepted for forensic examination and connect it to the system of the examiner to acquire information. Appropriate measures to be taken to connect the seized device in the examiner's system and in exceptional situation the storage device will not be disconnected from seized digital device when the following issues to be considered, e.g.:-

(i) The expected result may be uncertain or destroyed forever if the disks are separated in case of RAID (Redundant Array of Independent Disk) system;

(ii) It will be diffcult to access the laptop drive as the laptop may become useless if the drive is separated from the main system;

(iii) Hardware dependence (Legacy accessories) e.g. old drive may be `unusable` in the new system;

(2) Data acquisition can be made using forensic network or communication device as the digital device used for committing the crime;

(3) Data will be transferred from seized storage device to a device which is virus free, clean and free from any bug so that the originality of the transferred data remain intact. For that the Independent Cyclic Redundancy check (CRC), Hashing technology will be used after observing the measures detailed below:

(a) The process will be deemed complete if hardware right protection is applied based on selected acquisition procedure;

(b) Install right protection in the seized device;

(c) The Forensic lab's booting system will be used to boot (the device will remain attached in non-bootable mode);

(d) The affected device/drive can boot from the Forensic lab's system only when the right protection is active and enabled;

(e) The total, used and unused storage capacity of the seized device (has to be recorded/) will be marked using appropriate software;

(f) An exact copy/image from the storage device to be archived in the Forensic lab storage using the electronic serial number, evidence, standalone software, forensic software analysis suite, dedicated hardware device etc.

(g) Originality of the acquired data will be ascertained through bit to bit and sector-by-sector comparison between the original and the copy.

7.3Examination of Forensic sample or digital evidence

The digital evidence will be examined using appropriate forensic procedure and if appropriate, refrain from examination of the original forensic sample or digital evidence. The steps to be followed during examination of forensic sample or digital evidence are, e.g.:-

(1) **Preparation** |- The digital evidence will be recovered or extracted using separate device/ media after creating directory/directories.

(2) **Data extraction**:- The following two separate physical and logical extraction procedure can be used for data extraction. All data can be recovered from the physical drive using logical extraction procedure after classifying operating system, file system and the application, e.g. :-

(a) **Physical extraction**: In this procedure, whatever be the file system, data can be extracted from physical layer, e.g.:-

(i) Find out keyword, file detection, un-allocated space of physical drive and locate partition table;

(ii) Find data or information through Keyword which are not part of operating system or file system;

(iii) Find/Undelete Data or information through data recovery, which are not part of operating system or file system;

(iv) Find out the file system format after examining and determining the partition table and physical size of the hard drive;

(b) **Logical extraction**: Data (e.g. active files, deleted files, space in between the file, unallocated space etc) can be extracted in this system on the basis of file system of the drive. In order to extract data from the file, the following steps will be implemented based on the system's various features e.g.: file structure, file type, file name, size, location, date, time and other issues, e.g:-

(i) Ascertain and determine known file by comparing authentic hash value with derived hash value;

(ii) Extract relevant files in the drive after examining location, file header, file name and type;

(iii) Extract deleted files;

(iv) Extract files protected by password, encryption and compression;

(v) Identify unallocated space of the files

(vi) identify unallocated space.

(3) **Analysis of extracted file** |- The relative importance of the extracted data at the time of occurrence will be ascertained through analysis of time frame, hidden data, application and file, owner and jurisdiction etc by considering the time displayed in the BIOS of the computer and the displayed time, e.g.:-

(a) **Time frame analysis of the digital device**: The association between digital device and the user may be established by time frame analysis. Review and analysis of time can be made of the digital device in any of the following two procedure, for example:

(i) File system data relating to time can help establish relations between the user and the relevant file through inquiry (e.g. changes in read or write or execute or protect of the latest file, last use, creation of file and last changes in the file etc);

(ii) Analyze system and application logs considering error log, application installation log, connection log, security log etc from OS registry.

(b) **Hidden data analysis**|- The processes detailed hereunder will be applied to locate and extract hidden computer data through hidden data analysis, e.g.:

(i) inconsistency to be noted if user deliberately or intentionally modified data by correlating file header with file extension;

(ii) Ascertain unauthorized access by enabling access to password protected, encrypted and compressed file;

(iii) Presence of Data in host protected area will prove attempt to conceal data through access to host protected area;

(c) Application and file analysis: Procedure detailed below will be considered to form an opinion on system including relevant data and the user's capacity during examination of programs and files of the digital device, e.g.:-

(i) consider renaming of the files for relevance and pattern analysis;

(ii) Content analysis of the file;

(iii) Mark type and number of the operating systems of the digital devices;

(iv) Mark consistency between file and existing applications of the digital device;

(v) Mark consistency among files of the digital device (e.g. mark consistency between browser cache file and internet history log and between attachments sent with email with the relevant email of the seized digital device);

(vi) Mark relevance of the unknown files of the digital device with the on-going investigation;

(vii) Examine user default storage location to determine location for saving relevant files in a specified location or any other place reserved for application of the digital devices;

(viii) Examine and verify the users digital device configuration;

(ix) Analyze and review metadata file of the digital device to ascertain no of revision/editing made by the author of the metadata to include that data and related other data.

(d) **Ownership and use**: When it is required to determine creator, editor, accessor, data owner, and known users of files of the digital device, the following characteristics will be considered at the time of analysis, e.g.:

(i) **Time frame analysis**: Identify the owner and user of the file of the digital device through specific date and time;

(ii) **Application and file analysis**: store file of digital device at non-default location (e.g. create a directory titled “Child Porn” by user of the digital device);

(iii) **Application and file analysis**: Form opinion on file content and its evidentiary value from the file name of the digital device;

(iv) **Hidden data analysis**: Hide data deliberately to avoid detection;

(v) **Hidden data analysis**: In case of recovery of a file protected by password and encrypted, the password caretaker may be identified as owner and user;

(vi) **Application and file analysis**: Owner or user may be identified from the content of the file of the digital device.

(4) **Result obtained**: Full report to be prepared after considering results obtained.

7.4 Documentation and Reporting

The steps detailed below will guide preparation of record and report, e.g.:-

(a) **Procedure** |- The report must be self-explanatory and error-free and understandable to the relevant authority, prepared and preserved following the current policy and technology. The examiner's report shall include the following issues namely:-

(i) Discussion notes with investigation officer and if applicable with the relevant advocate;

(ii) Preserve copy of alamat or digital sample collection procedure;

(iii) Preserve copy of forensic examination requisition document;

(iv) Preserve copy of chain of custody document

(v) Record detail description of actions taken in the case file;

(vi) Record results of action taken and date, time of taking notes and description thereof;

(vii) Record observed irregularities and actions taken thereon during forensic examination;

(viii) Additional information (namely: Network topology, Authorised user list, user agreement and include password);

(ix) Record changes made in the system or network on the direction/order of the examiner or government agency or government;

(x) Operating system and Record current version of the relevant software including installed patches;

(xi) Record data related to remote storage, remote user access and offsite backup.

DG DSA will be informed about such forensic sample or digital evidence for additional enquiry which cannot be examined under current legal framework.

(b) **Examiner's Report** |- The following information shall be included during preparation of the report:

(i) Identity of the examiner's organization;

(ii) Submission number or Investigation indentifier;

(iii) Identity of the Enquiry Officer;

(iv) depositor's identity;

(v) Receiving date;

(vi) Date of report;

(vii) Serial no, manufacturer, model including Details description of the forensic sample or case alamats received for examinations;

(viii) Identity and signature of the examiner;

(ix) Brief description of actions taken during examination (string enquiry, graphics search image, retrieval of deleted files etc.)

(x) Results and Conclusion.

(c) **Summary report of the results**|-The summary result of the forensic examination on received forensic alamat will be recorded in the report.

(d) **Detail report of the results**|-The following issues will be recorded after detail examination of forensic sample or digital alamat, namely:

(1) Seized files of digital device related to the requisition;

(2) Other Files including deleted files which may support result;

(3) String inquiry, key word search and results of text string enquiry;

(4) Analysis of evidences related to internet (namely web site traffic analysis, chat logs, cache files, email and news group activities);

(5) Analysis of graphic image;

(6) Information on program registry and ownership determination;

(7) Analysis of relevant information;

(8) Description of existing programs in forensic sample or digital alamats examined;

(9) Strategy used to hide or musking data, (namely Encryption or Steganography) features of hidden data, hidden partition and name of inconsistent files.

The name and signature of the expert giving opinion or conducting the analysis will be appended to the report as prescribed.

8. Quality assurance

To ensure service quality, the Digital Forensic Lab will –

(a) Manage all services and conduct forensic analyses by duly qualified and trained personnel in accordance with the BSTI standards and provisions of the above mentioned Rules [para 6.2 of ISO/IEC/BDS 17025];

(b) Apply recognised processes as detailed in ISO/IEC/BDS 27043 of Forensic analysis;

(c) Install and use appropriate equipment and machinery to maintain the technical standard of forensic analysis. The details of equipment and machinery will be documented and maintained [ref para 6.4 of ISO/IEC/BDS 17025] ;

(d) Maintain physical infrastructure facilities [para 6.3 of ISO/IEC/BDS 17025];

(f) Ensure security and confidentiality of all stored information. Provisions of ISO/IEC/BDS 15489 will guide storage, use and reuse of digital information both digital and paper based.

9. Manpower of Digital Forensic Lab

Subject to the approval of the Government, the professional manpower of DSA's Digital Forensic Lab shall be:

1. 1X Senior Manager
2. 1X Digital Forensic Lab Supervisor
3. 2X Analyst (Digital Forensic -Computer)
4. 1X Analyst (Digital Forensic – Mobile device)
5. 1X Analyst (Digital Forensic – Autonomous device)
6. 2X Analyst (Digital Forensic - Hardware)
7. 1X Digital Forensic Investigator (Hardware)
8. 1X Administrator (Forensic Lab)
9. 1X Digital Forensic examiner
10. 2X Assistant Analyst
11. 2x Assistant Administrator
12. 2X Assistant Digital Forensic Investigator
13. 2X Assistant Digital Forensic examiner

The age, qualification and experience, Charter of duties and pay grade are as follows:

Sl	Name, no, pay and Age[12]	Qualification and Experience	Charter of duties
1	2	3	4
1.	1X Senior Manager (Grade-3) Tk.56500-74400 Not more than45 years	By promotion from Digital Forensic Lab supervisor; Direct recruitment if no suitable candidate in feeder post. **For Promotion** Minimum 3 years satisfactory service record in the feeder post **For Direct Recruitment** Post graduate degree in computer Science/Computer Science and Engineering/ Electrical and Electronic Engineering/Electrical and Computer Engineering/Telecom Engineering/Information and Communication Technology with at least two publication in reputed and relevant international journal. Atleast 10 (ten) year work experience in the relevant field. No third division/class in academic life. Phd degree in the relevant field/at least 5 internationally recognized certification in the relevant field will get preference over other candidates.	1. Perform duties assigned by the supervising officer 2. Plan, Coordinate, set standard, Analysis and supervision of forensic assignments 3. Define Terms of Reference of all forensic teams 4. Electronic processing of all Forensic data and information 5. Coordinate all analytical works of the Forensic teams 6. Ensure timely submission of all issues connected with forensic analysis of evidence 7. Ensure security of all samples and evidence received by the lab 8. Ensure accuracy and calibration of all forensic tools 9. Perform any of duties assigned by the supervising authority
2.	1X Digital Forensic Lab Supervisor (Grade-4) Tk.50000-71200 Not more than40 years	By promotion from amongst Analyst/SOC Analyst (TIRE-3); Direct recruitment if no suitable candidate in feeder post. **For Promotion** Minimum3 years satisfactory service record in the feeder post **For Direct Recruitment**	1. Perform duties assigned by the supervising officer 2. Prepare maintenance strategy of the DFL and ensure conduct of regular routine maintenance work; 3. Supervise all maintenance work and ensure digital

[12]Age limit for direct recruitment

Sl	Name, no, pay and Age[12]	Qualification and Experience	Charter of duties
1	2	3	4
		Post graduate degree in computer Science/ Computer Science and Engineering/Electrical and Electronic Engineering/Electrical and Computer Engineering/ Telecom Engineering/Information and Communication Technology. Atleast 8 (eight) year work experience in the relevant field. No third division/class in academic life. Phd degree in the relevant field/at least 4 (four) internationally recognized technical certification in the relevant field will get preference over other candidates.	forensic training of all subordinate staff and officer; 4. Ensure timely utilisation of all maintenance tools and equipment; and 5. Perform any of duties assigned by the supervising authority **Additional Duties** The DFL supervisor will perform the following additional duties along with routine responsi-bilities mentioned above : (i) Act as senior forensic expert; (ii) Conduct, ensure, oversee and review for all lab personnel: (iii) BSTI-ISO standards compliant Training; (iv) Annual performance evaluation; (v) Technical and administrative review of all reports and evidences prepared; (vi) Skills and expertiseVerification; (vii) Usefulness and error free operation of installed hardware, software and other machineries; (viii) Validate quality operation of all installed hardware and software;

Sl	Name, no, pay and Age[12]	Qualification and Experience	Charter of duties
1	2	3	4
			(ix) Recommend appropriate hardware and software for the forensic lab.
3.	2X Analyst (Digital Forensic - Computer) (Grade-5) Tk.43000-69850 Not more than38 years	By promotion from amongst Administrator/ Program Manager/Application ProgrammerDigital Forensic Investigator/Digital Forensic Examiner; Direct recruitment if no suitable candidate in feeder post **For Promotion** Minimum 3 years satisfactory service record in the feeder post. **For Direct Recruitment** Post graduate degree in computer Science/ Computer Science and Engineering/Electrical and Electronic Engineering/Electrical and Computer Engineering/Telecom Engineering/ Information and Communication Technology/ Cyber Security/Information Security. Atleast 5 (five) year work experience in the relevant field. No third division/class in academic life. At least 3 (three) internationally recognized technical certification in the relevant field will get preference over other candidates.	1. Perform duties assigned by the supervising officer; 2. Ensure use of up-to-date version of the operating system; 3. Ensure database protection and retrieval of data; 4. Procure all computer spares, peripherals and establish the network of the agency 5. Take measures to prevent cyber crime and if necessary track ip and physical address 6. Assist password break and anlysis of trapdoor of the system; 7. Access protected database, perform data recovery and trouble shoot to recover alamat [digital evidence]; 8. Collect and recover data, information from electronic equipment; 9. Prepare unbiased report on basis of recovered digital data and information; 10. Perform any of duties assigned by the supervising authority **Additional Duties**

Sl	Name, no, pay and Age[12]	Qualification and Experience	Charter of duties
1	2	3	4
			The senior most analyst will act as digital forensic lab expert. S/Hewill perform the following additional duties along with routine responsibilities mentioned above : (a) Collect and recover data and information from electronic equipment and system; (b) Prepare impartial report on the basis of recovered or collected digital data; (c) Review all administrative and technical reports of pending cases (d) Support law enforcement agencies to identify crime scene forensic evidences; (e) Depose in a court of law to establish truth or otherwise of the verified authentic evidence; (f) Provide on-the-jobtraining, advise and guidance to the officers; (g) Ensure and validate quality operation of all installed hardware and software;

Sl	Name, no, pay and Age[12]	Qualification and Experience	Charter of duties
1	2	3	4
			(h) Ensure performance of all used hardware and software in forensic cases.
4.	1X Analyst (Digital Forensic – Mobile device) (Grade-5) Tk.43000-69850 Not more than38 years	By promotion from amongst Administrator/ Program Manager/Application Programmer/ Standard Certification and Accreditation Specialist/ Cryptographic Expert/ Penetration Tester/ Incident Handler/Big Data Architect/ Security Architect/Content Strategist/Digital Forensic Investigator/Digital Forensic Examiner; Direct recruitment if no suitable candidate in feeder post. **For Promotion** Minimum 3 years satisfactory service record in the feeder post. **For Direct Recruitment** Post graduate degree in computer Science/ Computer Science and Engineering/ Electrical and Electronic Engineering/Electrical and Computer Engineering/Telecom Engineering/ Information and Communication Technology/ Cyber Security/Information Security. Atleast 5 (five) year work experience in the relevant field. No third division/class in academic life. At least 3 (three) internationally recognized technical certification in the relevant field will get preference over other candidates.	1. Perform duties assigned by the supervising officer; 2. Track mobile IMEI; 3. Retrieve data from mobile database; 4. Access and troubleshoot operating system; 5. Arrange mobile password break and identify finger print; 6. Access protected database to recover alamat [digital evidence]; 7. Prepare strategy for Risk mitigation of mobile, data recovery and troubleshoot; 8. Collect and recover data, information from electronic equipment; 9. Prepare unbiased report on basis of recovered digital data and information; 10. Perform any of duties assigned by the supervising authority;
5.	1X Analyst (Digital	By promotion from amongst Administrator/Program	1. Perform duties assigned by the supervising officer;

Sl	Name, no, pay and Age[12]	Qualification and Experience	Charter of duties
1	2	3	4
	Forensic – Autonomous device) (Grade-5) Tk.43000-69850 Not more than38 years	Manager/Application Programmer/Standard Certification and Accreditation Specialist/ Cryptographic Expert/ Penetration Tester/ Incident Handler/Big Data Architect/Security Architect/Content Strategist/Digital Forensic Investigator/Digital Forensic Examiner; Direct recruitment if no suitable candidate in feeder post. **For Promotion** Minimum 3 years satisfactory service record in the feeder post **For Direct Recruitment** Post graduate degree in computer Science/Computer Science and Engineering/Electrical and Electronic Engineering/Electrical and Computer Engineering/Telecom Engineering/Information and Communication Technology/Cyber Security/Information Security. Atleast 5 (five) year work experience in the relevant field. No third division/class in academic life. At least 3 (three) internationally recognized technical certification in the relevant field will get preference over other candidates.	2. Assist in installing and uninstalling all autonomous devices and retrieve data therefrom; 3. Access protected database to retrieve alamat; 4. Train to find out the process in committing cyber crime using autonomous devices 5. Data recovery and trouble shoot autonomous devices using operating system; 6. Collect and recover data, information from electronic equipment; 7. Prepare unbiased report on basis of recovered digital data and information; 8. Perform any of duties assigned by the supervising authority;
6.	2X Analyst (Digital Forensic - Hardware) (Grade-5)	By promotion from amongst Administrator/Program Manager/Application Programmer/Standard Certification and Accreditation Specialist/ Cryptographic Expert/ Penetration Tester/ Incident	1. Perform duties assigned by the supervising officer; 2. Assist in procurement, customisation of hardware earmarked for use in the digital forensic lab;

Sl	Name, no, pay and Age[12]	Qualification and Experience	Charter of duties
1	2	3	4
	Tk.43000-69850 Not more than38 years	Handler/Big Data Architect/Security Architect/Content Strategist/Digital Forensic Investigator/Digital Forensic Examiner; Direct recruitment if no suitable candidate in feeder post. Atleast 5 (five) year work experience in the relevant field. No third division/class in academic life. **For Promotion** Minimum 3 years satisfactory service record in the feeder post. **For Direct Recruitment** Post graduate degree in computer Science/ Computer Science and Engineering/Electrical and Electronic Engineering/Electrical and Computer Engineering/Telecom Engineering/ Information and Communication Technology/ Cyber Security/Information Security.Direct recruitment if no suitable candidate in feeder post. At least 3 (three) internationally recognized technical certification in the relevant field will get preference over other candidates.	3. Design necessary software required for the installed hardware of the forensic lab; 4. Assess effectiveness of the hardware and computer peripherals; 5. Assess cyber threat level of the installed hardware; 6. Assist in data retrieval; 7. Assist in designing necessary hardware to conduct new type of forensic test; 8. Collect and recover data, information from electronic equipment; 9. Prepare unbiased report on basis of recovered digital data and information; 10. Perform any of duties assigned by the supervising authority;
7.	1X Digital Forensic Investigator (Hardware) (Grade-6) Tk.35500-63410	By promotion from amongst Assistant Digital Forensic Investigator; Direct recruitment if no suitable candidate in feeder post. **For Promotion** Minimum 9 (nine) years satisfactory service record in the feeder post; **For Direct Recruitment**	1. Perform duties assigned by the supervising officer; 2. Ensure smooth performance of all installed equipment; 3. Arrange repair and maintenance of all out of order equipment of the Forensic Laboratory;

Sl	Name, no, pay and Age[12]	Qualification and Experience	Charter of duties
1	2	3	4
	Not more than36 years	Post graduate degree in computer Science/ Computer Science and Engineering/ Electrical and Electronic Engineering/Electrical and Computer Engineering/Telecom Engineering/ Information and Communication Technology/ Cyber Security/Information Security. Atleast 3 (three) year work experience in the relevant field. No third division/class in academic life. At least 2 (two) internationally recognized technical certification in the relevant field will get preference over other candidates.	4. Determine types work to be performed in the lab; 5. Ensure backup power supply of all installed equipment of the lab 6. Troubleshoot and repair all equipment 7. Perform any of duties assigned by the supervising authority;
8.	1X Administrator (Forensic Lab) (Grade-6) Tk.35500-63410 Not more than36 years	By promotion from amongst Assistant Analyst/IT officer/IT Security Officer/Assistant Administrator; Direct recruitment if no suitable candidate in feeder post **For Promotion** Minimum 9 (nine) years satisfactory service record in the feeder post **For Direct Recruitment** Post graduate degree in computer Science/ Computer Science and Engineering/Electrical and Electronic Engineering/Electrical and Computer Engineering/Telecom Engineering/ Information and Communication Technology/ Cyber Security/Information Security. Atleast 3 (three) year work experience in the relevant field. No third division/class in academic life. Work experience in a cyber security organisation and At least 2 (two) internationally recognized technical	1. Perform duties assigned by the supervising officer; 2. Update software, anti-virus and all system deployed in the Forensic Laboratory; 3. Ensure cybersecurity of all equipment installed in the Forensic Laboratory; 4. Arrange repair and maintenance of all out of order equipment of the Forensic Laboratory; 5. Perform any of duties assigned by the supervising authority;

Sl	Name, no, pay and Age[12]	Qualification and Experience	Charter of duties
1	2	3	4
		certification in the relevant field will get preference over other candidates.	
9.	1X Digital Forensic examiner (Grade-6) Tk.35500-63410 Not more than36 years	By promotion from amongst Assistant Digital Forensic examiner; Direct recruitment if no suitable candidate in feeder post **For Promotion** Minimum 9 (nine) years satisfactory service record in the feeder post **For Direct Recruitment** Post graduate degree in computer Science/ Computer Science and Engineering/Electrical and Electronic Engineering/Electrical and Computer Engineering/Telecom Engineering/ Information and Communication Technology/ Cyber Security/Information Security. Atleast 3 (three) year work experience in the relevant field. No third division/class in academic life. At least 2 (two) internationally recognized technical certification in the relevant field will get preference over other candidates.	1. Perform duties assigned by the supervising officer; 2. Examine all equipment and media suspected of use in the commission of cybercrime; 3. Prepare and present Chart for analysis and preserve main evidence; 4. Disconnect digital devices if necessary; 5. Present and preserve used material and media to prove a case in a court of law; 6. Depose in a court of law on digital evidence and if necessary conduct enquiry on used system and materials; 7. Perform any of duties assigned by the supervising authority;
10.	2X Assistant Analyst (Grade-9) Tk.22000-53060 Not more than30 years	Direct Recruitment Graduate degree from a recognized university in computer Science/Computer Science and Engineering/Electrical and Electronics Engineering/Electrical and Computer Engineering/ Telecommunication Engineering /Information and Communication Technology. No third division/class in academic life.	1. Perform duties assigned by the supervising officer; 2. Assist relevant Analyst in discharge of official duties; 3. Perform any of duties assigned by the supervising authority;

Sl	Name, no, pay and Age[12]	Qualification and Experience	Charter of duties
1	2	3	4
		Candidate with Work experience in the relevant field will get preference over other candidates.	
11.	2x Assistant Administrator (Grade-9) Tk.22000-53060 Not more than30 years	25% by promotion from amongst computer operator/ Helpdesk Assistant and remaining 75% by direct recruitment. **For Promotion** 8 years satisfactory service record in feeder post along with training in COBAL/ FORTRAN/BASIC or high level computer language and successfully completed standard aptitude tesh Direct Recruitment Graduate degree from a recognized university in computer Science/Computer Science and Engineering/ Electrical and Electronics Engineering/ Telecommunication Engineering/ Electrical and Computer Engineering/ Information and Communication Technology. No third division/class in academic life. Candidate with Work experience in the relevant field will get preference over other candidates.	1. Perform duties assigned by the supervising officer; 2. Assist Administrator in discharge of official duties; 3. Perform any of duties assigned by the supervising authority;
12.	2X Assistant Digital Forensic Investigator (Grade-9) Tk.22000-53060	**Direct Recruitment** Graduate degree in computer Science/Computer Science and Engineering/Electrical and Electronic Engineering/Information and Communication Technology. No third division/class in academic life.	1. Perform duties assigned by the supervising officer; 2. Support procurement of necessary hardware, perform evaluation and customise hardware; 3. Conduct regular test and calibration of all forensic hardware

Sl	Name, no, pay and Age[12]	Qualification and Experience	Charter of duties
1	2	3	4
	Not more than30 years	Candidate with Work experience in the relevant field will get preference over other candidates.	4. Maintenance of all legacy hardware 5. Perform any of duties assigned by the supervising authority;
13.	2X Assistant Digital Forensic examiner (Grade-9) Tk.22000-53060 Not more than30 years	**Direct Recruitment** Graduate degree in computer Science/Computer Science and Engineering/Electrical and Electronic Engineering/Telecom Engineering/Information and Communication Technology. No third division/class in academic life. Candidate with Work experience in the relevant field will get preference over other candidates.	1. Perform duties assigned by the supervising officer; 2.Support procurement of necessary hardware, perform evaluation and customise hardware; 3. Conduct regular test and calibration of all forensic hardware 4. Maintenance of all legacy hardware 5. Perform any of duties assigned by the supervising authority;

Note: DFL will engage the above mentioned manpower on government approval of the organogram. The appointment shall be made following existing rules and regulations.

10. Hardware and Software

Form 1: DSA DFL Service Request Form/Requisition letter

Date:

1. Name of Organisation with address including telephone and email:

2. Name, designation and contact details of officer submitting:

3. Case Information

Case/Reference no	Police station/Upazila	District

4. Case detail/Nature of Crime

4.1 Nature of Crime:
4.2 Section of law:
4.3 Brief History:
4.4 Any other relevant detail:

5. Exhibits for examination

Sl#	Description of exhibits	How, when and by whom found	Source of exhibits:	Exhibit relates to Suspect/Victim/ Person of interest	Remarks (if any)
1	**2**	**3**	**4**	**5**	**6**

6. Information on Suspect/Victim/Person of interest:

6.1: Full name:

6.2 Occupation:

6.3 Gender:

6.4 Remarks:

7. Other information

Rank and signature of Investigating officer	
Name, rank and sign of forwarding officer:	
Enclosure details including specimen seal's impression on exhibits	

8. Return of the exhibits from DFL after examination

Ref. no Date Description of returned exhibits with results and specimen seal's impression on returned exhibits Sign and Designation of forwarding authority

Form-2: Chain of Custody Form [use one form for one item]

1. Case detail

Case no: name of IO:

Details of digital evidence with unique identification no

Date and time of seizure:

2. Technical Information

Manufacturer	Model	Serial no	Country of origin
1	2	3	4

3. Description

4. Chain of Custody

Reason/Action*	Received from	Received by	Date	Time	Remarks
1	2	3	4	5	6

* **IO shall ensure documentation of the reasons for transferring the seized evidence to other custodians in chronological order**

Form 3: Information/Evidence Preservation Notice

(sec 44-45 Digital Security Act 2018)

Memo no. Date:

To

(name and address of the person to whom the notice is served)

Subject: Information/Evidence Preservation Notice u/s 44-45 Digital Security Act 2018 read with section 94 of Code of Criminal Procedure

Ref: PS case no/Enquiry ref

Dear Sir/Madame

With reference to the case/enquiry referred to above, this is to inform you that the undersigned has been appointed IO/Enquiry Officer. Prima facie it appears that/established that, critical evidence in this matter exists in the form of electronic records in the computer/computer system/network system of ….. …… ……. (see note below). The undersigned has been directed/authorized by the Director General DSA to do the needful.

This is a notice to you and demand that such evidence indentified must be immediately preserved and retained by you until further written notice from the undersigned. The request is made as per sec 94 of the Code of Criminal Procedure 1898 read with sec 44 of Digital Security Act 2018. Failure to comply with this notice will make you liable for legal action as per Penal Code 1860 and other relevant laws.

Please contact the undersigned if you have any question regarding this notice.

See guidance note on the reverse page

(To be signed by the Enquiry officer/IO with Offical seal)

Guidance Note for notice receiver

For the purpose of this notice electronic record has the same meaning as defined in Information and Communication Technology Act 2006 and shall include, but not limited to, all text files (including word processing documents), spread sheets, email files and information concerning email (including logs of email history and usage, header information and deleted files), internet history files and preferences, GIF files, databases, calendar and scheduling information, computer system activity logs and all file fragments and backup files containging electronic data. The notice receiver will:

1. Preserve and retain all electronic records generated or received (relating to enquiry) (give details)
2. Preserve and retain all electronic records generated or received (relating to the enquiry)(give details)
3. Refrain from opreating (or removing or altering fixed or external drives and media attached thereto) standalone PC, network workstations, notebook and/or laptop computers operated by (accused) (give details)
4. Retain and preserve all backup tapes or other storage media, whether online or offline, and refrain from overwriting or deleting information contained thereon, which may contain electronic records identified above.

Form 4: Exhibit Registration form

Section 1: Exhibit receive

Sl	DFL Exhibit label	Manufacturer	Capacity	Description include any defect of the item	Manufacturer serial number
1	2	3	4	5	6

Requisition Officer	DFL
1	2
Sign here Name & Designation Date	Sign here Name & Designation Date

Section 2: Exhibit return

I have ageed that DFL has returned all the exhibits listed in section 1 to me. Upon signing the above column, both parties agreed that the work has been completed and the case is signed off

Requisition Officer	DFL
1	2
Sign here Name & Designation Date	Sign here Name & Designation Date

Form 5: Sample letter to Service provider

Sec 38 and 46 of the Digital Security Act 2018

Letter head

Date:

From: Name and address of the IO or OC with full contact information

To: Name,aAddress and full contact information of the service provider

Subject: Request to to furnish details or information about . . . . . .
Ref:

Dear Sir/Madame

Body of the letter

Official Seal	Signature