Draft

Leveraging ICT for Growth, Employment and Governance Project
Bangladesh Computer Council (BCC)
Information and Communication Technology Division
Ministry of Posts, Telecommunications and Information Technology
ICT Tower, Plot # E-14/X, Agargaon, Dhaka-1207,
Bangladesh

Terms of Reference

For

Digital Forensic Analyst

(Contract Package # S32A-32B)
(Credit #5911-BD)

January 2018

Terms of Reference (TOR)
For
Digital Forensic Analyst
(Contract Package # S32A-32B)

1. Background

Bangladesh Computer Council (BCC), an organization of Information & Communication Technology Division, Ministry of Posts, Telecommunications and Information Technology has received financing from the World Bank toward the cost of the Leveraging ICT for Growth, Employment and Governance (LICT) Project (IDA credit no.: 5911-BD) and intends to apply part of the proceeds for payment of services related to Consultancy for Digital Forensic Analyst.

The project consists of three components: (i) IT/ITES Industry Development, (ii) E-Government and (iii) Project Management Support.

The project development objectives are to: (i) Catalyze the growth of Bangladesh's IT/ITES industry for employment creation and export diversification; and (ii) Strengthen IT/ITES facilities, policies, standard and guidelines for public sector modernization.

2. Objective of the Assignment

The objective is to recruit a person for the position of Digital Forensic Analyst in order to achieve organization goals by defining, integrating, and upgrading comprehensive information system architecture; managing projects and computer security.

3. Scope of Work

3.1 Description

A Digital Forensic Analyst within Bangladesh e-government Response Team, the candidate will be expected to serve as a tactical arm of the team, conducting computer forensic analysis, data recovery, eDiscovery, and other IT investigative work. Due to the inherent volatility of investigative response work, the candidate will be expected to discharge the various responsibilities assigned to their role while successfully managing a variable caseload. The candidate will be responsible for integrity in analysis, quality in client deliverables, as well as gathering caseload intelligence. The position will operate within a close team of computer forensics, fraud examiners, and other IT investigative experts, as well as customer management, counsel, human resources, and other IT technical personnel. The candidate will be expected to possess solid IT technical experience, strong communication skills, and must be technically able to hit the ground running in most any back office environment. The candidate must be well-versed and capable of leading an engagement in at least 2 of our core offerings: PCI-related IR/Forensics investigations, Financial Services, Intellectual Property, Computer Security Incident Response Team (CSIRT), Expert Witness/Litigation Support, IR Training, eDiscovery, Mobile Phone Forensics.

3.2 Responsibilities

Digital Forensic Specialist would be responsible for the following:

- Perform forensic analysis of electronic data sources (workstations, laptops, servers, mobile devices, etc.) in response to cyber incidents.
- Investigate network intrusions to determine the cause and extent of the breach.

- Preserve, harvest, and process electronic data according to the relevant policies and practices.
- Develop technical solutions to complex problems that require the regular use of ingenuity and creativity, work without appreciable direction, and exercise considerable latitude in determining the technical objectives of the assignment.
- Research and maintain proficiency in tools, techniques, countermeasures, and trends in data hiding and network security and encryption.
- Produce high quality written work products, presenting complex technical matters clearly and concisely.
- Represent the organization as and interact with senior external personnel on significant technical matters often requiring coordination between organizations

3.3 Competencies

- ➢ **Analysis:** Identify and understand issues, problems and opportunities; compare data from different sources to draw conclusions.
- ➢ **Communication:** Clearly convey information and ideas through a variety of media to individuals or groups in a manner that engages the audience and helps them understand and retain the message.
- ➢ **Exercising Judgment and Decision Making:** Use effective approaches for choosing a course of action or developing appropriate solutions; recommend or take action that is consistent with available facts, constraints and probable consequences.
- ➢ **Technical and Professional Knowledge:** Demonstrate a satisfactory level of technical and professional skill or knowledge in position-related areas; remains current with developments and trends in areas of expertise.
- ➢ **Building Effective Relationships:** Develop and use collaborative relationships to facilitate the accomplishment of work goals.
- ➢ **Client Focus:** Make internal and external clients and their needs a primary focus of actions; develop and sustain productive client relationships
- ➢ **Demonstrated ability to describe non-functional requirements** and translate into architecture constraints
- ➢ Experience with government systems (operating systems, applications, databases, networks, etc) and business processes.

4. Qualifications & Experience

4.1. Educational Qualification:

Bachelor's degree in Computer Science, Information Security, or Information Systems Management

4.2. Work Experience:

- Minimum Seven (7) years of experience in digital forensics
- Proficient in the latest forensic, response, and reverse engineering skills and astute in the latest exploit methodologies.
- Must be proficient in using tools like Encase, FTK, Helix, Wireshark, X Ways Forensic for memory analysis, malware analysis and forensic analysis
- Knowledge of OS internals
- Experience parsing and analyzing memory snapshots
- Programming skills in Python, Perl, Ruby
- Reverse engineering skills and experience is a plus

- Knowledge of Army/Joint digital media forensics procedures, doctrine, and practices is a plus.
- Background in counterintelligence/counterterrorism and/or law enforcement is a plus.
- Experience with intelligence and/or law enforcement databases and systems is a plus.
- digital evidence handling
- malicious code behavioral analysis
- scripting and programming

Knowledge of:

  - intelligence or counterintelligence principles
  - Mac OS or Linux forensics
  - mobile forensics

- Excellent technical writing skills and oral presentation skills

4.3. Certification:

- At least one of the following certifications: GCIH, GCFE, EnCE, ACE, CFCE, GREM, GCFA , CHFI, SANS Institute Forensic Toolkit (SIFT), FTK, X Ways Forensics

5. Reporting Arrangements

The Digital Forensic Analyst will assist and report to the Project Director, under the general supervision and guidance of the e-Government Team Leader and CIRT Team Leader.

6. Duration of the Assignment:

The duration of the assignment will be about 16 months and may extend subject to satisfactory performance of the Consultants & Project Extension.

7. Facilities to be provided by the Client:

Project will provide appropriate office space and other associated (data, information, furniture, stationeries, etc.) necessary to carry out the assignment.

8. Reporting requirements/deliverable:

The Digital Forensic Analyst will need the following reporting requirements/deliverables, but not limited to:

- ➢ Chain of custody
- ➢ Monthly work plan and progress report;
- ➢ Yearly Report
- ➢ Any other Report, as required.