

Extraction, Recovery and Analysis of Data from MYSQL Database Proficiency Testing Program for Digital Forensics

INSTRUCTIONS TO TO PARTICIPANTS

Dear Participant,

Your unit has been invited to participate in proficiency testing (PT) program: *Extraction, Preservation and Recovery of Electronic Data* (CNAS-GA IT0002), which is hold by the China National Accreditation Service for Conformity Assessment (CNAS).

This program is supported by a quality assurance research in proficiency testing of CNAS and promoted by International Criminal Police Organization (INTERPOL) which attempts to assess the equivalence and effectiveness of digital evidence and address common problems of the forensic units/practitioners' results and performance. This program is open for participation to all laboratories/units engaged in Digital Forensics and it is **FREE OF CHARGE** to all related laboratories/units from the member countries of Asia Pacific Accreditation Cooperation Organization (APAC), International Laboratory Accreditation Cooperation (ILAC) and INTERPOL. If you would like to participate in this PT program please read the information below.

1. Introduction

At present, the number of reported network frauds is increasing all over the world and the technology of cybercrimes is also constantly upgrading. Digital forensics plays a more and more important role in solving network crimes. With the aim of enhancing the quality and comparability of digital forensics and investigation in various countries/regions, we propose this PT program. This PT program is designed based on the background of a network fraud which is intended to assist participants in demonstrating their professional capacity of extracting, preserving, recovering and analyzing of electronic data.

The PT items are designed and provided by Shanghai Stars Digital Data Forensics Center (SDFC) which gained the accreditation to ISO/IEC 17025 as well as ISO/IEC 17043 in the digital forensic area. CNAS will coordinate and invite multi-national experts to participate in this PT program. Based on the actual situation of the sample design, experts will jointly determine the criteria for participants' performance evaluation. This program will give evaluation and technical suggestions on the performance of all participants.

2. Objective

This proposed PT program is an interpretive test which is designed to reflect the actual casework of fraud. This program is intended to assist participants in demonstrating their professional capacity of extracting, preserving, recovering, and analyzing data from the MYSQL database, understanding the difference between the different laboratories, and identifying problems and opportunities for self-improvement.

3. Organizations of the PT Program

As the organizer of this PT program, CNAS is the national accreditation body of China, a full member of APAC, ILAC and International Accreditation Forum (IAF) and a signatory of the multilateral recognition agreements (MLA/MRA) of these organizations. In this program, CNAS is responsible for proposing the

PT program, inviting participants, circulating the PT report and acting as a contact point between participants and the PT Provider.

As the provider of this PT program, SDFC is an authoritative research institution in the field of digital forensics, and acquired the PT provider accreditation in accordance with ISO/IEC 17043. In this program, SDFC takes responsibility for all tasks in the development and operation, including preparation and distribution of proficiency test samples, results analysis and evaluation of the participants' performance, preparation of PT report.

4. Fee for participation

Free of charge to the participants from the member countries of APAC, ILAC and INTERPOL.

5. Call for participation

All the labs/units engaged in digital forensics (accredited or unaccredited against ISO/IEC 17025) are called for this PT program, including labs/units from law enforcement agencies, (e.g. police department) or other forensic laboratories from social agencies, universities, institutes, etc. The total number of participating laboratories shall be limited to about 200.

Participants should complete the Application Form and send it to the contact person listed below through email no later than **April 28, 2022**.

6. Confidentiality

All information furnished by participants as part of this PT program will be treated confidentially. The PT report issued at the completion of this PT program does not identify individual participant. Each participant is issued a unique identification code during enrolment that is used in the report to ensure confidentiality of performance.

7. Proficiency Testing Item (Sample)

- (1) The sample of this PT program provided to each participant will be a pack of digital files containing: 1) Guidance: Case Information and Answer Sheet; 2) An image file of the MySQL database server.
- (2) All the samples will be dispatched through internet. After confirming the application information, PT provider will send an email to the participants to inform the sample download link.
- (3) Participants shall promptly contact PT provider for any download difficulty or sample damages. Sample will be replaced for any damaged/download-failed claims.

8. Examination Request

- (1) Participants are required to examine the given database to extract, preserve and recover the data; analyze and identify the evidence for fraud from the data.
- (2) PT sample must be handled and analyzed with the participant's regular workflow, using routine methods/standards.

9. Result Feedback

- (1) Participants should use the Answer sheet which is provided together with each sample to submit the data investigation results.
- (2) The Answer sheet includes the findings (digital evidence acquired) and brief analysis of the evidence. Where possible, the information of forensic tools/methods for data investigation should be feedback on

the Answer sheet to help all participants get more information about the effectiveness and comparability of tools/methods.

The Answer Sheet should be returned by Jun. 15, 2022.

10. Evaluation of Performance

- (1) Each participant's performance is evaluated by means of expert judgment on the basis of the pre-established criteria from a multinational expert consensus group.
- (2) The criteria for participants' performance evaluation will be mainly based on the facts whether the findings of digital evidence acquired is consistent with the objective results. Other aspects of the assessment (e.g. whether the analysis of the evidence is comprehensive, and whether the basis of the investigation results is proper and adequate) form part of the criteria. The performance assessment process used will be detailed in the final report.
- (3) The evaluation result is categorized into three grades:
 - A (Satisfied): participants whose performance has been considered satisfactory;
 - B (Questioned): participants are recommended that they review their performance;
 - and C (Unsatisfied): participants will need to investigate their performance.

11. Schedule for Program

By Apr. 28, 2022	Participants application;
By May. 15, 2022	Dispatch PT items through the internet;
By Jun. 15, 2022	Participants' results feedback;
By Aug. 30, 2022	Draft final report.

12. Contact

Ms JIA Rujing (CNAS)

Address: No.8 Nanhuashi Dajie, Dongcheng District, Beijing 100062, P.R.China

Tel: +86-10-6710 5376

Fax (Auto): +86-10-8792 8651

Email: jiarj@cnas.org.cn

Mr. WU Songyang (SDFC)

Address: No.339, Bisheng Road, Zhangjiang Hi-Tech Park, Shanghai, 201204, P.R.China

Tel: +86-21-68571260

Fax (Auto): +86-21-3393 2578

Email: sdfc@stars.org.cn