Extraction, Preservation and Analysis of Data from Computer and Server Proficiency Testing Program for Digital Forensics

INTRUDCTION

1. General Information

Currently, the global incidence of reported network viruses is escalating, paralleled by the relentless advancement of cybercrime techniques. Digital forensics has become crucial in addressing these crimes. To improve the quality and comparability of digital forensics across nations/regions, the China National Accreditation Service for Conformity Assessment (CNAS), sponsored by a Research Project, initiates this Proficiency Testing (PT) program.

The PT items/materials which are designed and validated by Shanghai Stars Digital Data Forensics Center (SDFC), whose digital forensics capabilities are accredited in accordance with both ISO/IEC 17025 and ISO/IEC 17043.

CNAS will oversee the PT program, collaborating with multinational experts to plan, set evaluation criteria, and provide performance feedback to participants. The program will furnish all participants the final PT report containing comprehensive evaluations and individualized technical recommendations tailored to each participant's outcomes.

lt is free and open to all laboratories/units engaged in digital forensics, particularly those affiliated with the member countries of the Asia Pacific Accreditation Cooperation (APAC), International Laboratory Accreditation Cooperation (ILAC) and the International Criminal Police Organization (INTERPOL).

2. Objective

This PT program is designed to emulate the ransomware scenarios, reflecting real digital forensic challenges. It aims to facilitate participants in demonstrating their professional capacity in data extraction, preservation and analysis from PCs and servers. Furthermore, it enhances understanding of inter-laboratory differences, guiding participants to identify improvement areas and explore potential opportunities.

3. Organizations of the PT Program

As the organizer of this PT program, CNAS serves as China's national accreditation body, a full member of APAC, ILAC and International Accreditation Forum (IAF) and a signatory of the Mutual 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 PT samples, results analysis and evaluation of the participants' performance, preparation of PT report.

4. Fee for participation
Free of charge.

5. Call for participation
All the labs/units engaged in digital forensics, regardless of ISO/IEC 17025 accreditation status, are invited to this PT program, including labs/units from law enforcement agencies（e.g. police department）,forensic laboratories from social agencies, universities, institutes, and others.
Participants should complete the *APPLICATION FORM* and submit it to the contact person via email no later than **Oct. 19, 2024.**

6. Confidentiality
All participant-provided information within this PT program will be treated in strict confidence. The final PT report will not disclose individual participant identities. A unique identification code assigned during PT process will be used in the report to ensure the confidentiality of each participant's performance.

7. Proficiency Testing Item (PT Sample)
(1) Each participant in this PT program will receive a package of digital files as the PT sample, containing: 1) Guidance: Scenario information; 2) Two image files representing a computer and a server respectively.
(2) All the samples will be distributed through internet. Upon application confirmation, the PT provider will email participants with download links for the samples and a link to submit their results.
(3) Participants who encounter any difficulties in downloading the samples or receive damaged samples are kindly requested to immediately contact the PT provider. Upon request, damaged or unsuccessfully downloaded samples will be promptly replaced.

8. Examination Request
(1) Participants are required to thoroughly examine the provided image files: extracting and preserving relevant data; and analyzing and identifying the evidence for virus form the data.
(2) The examination comprises responses to ten questions, all questions must be answered individually via an online platform according to the results feedback form. The answers include the findings (digital evidence acquired) of examination and brief analysis of the findings.
(3) Participants are expected to handle and analyze the PT sample within their standard workflow, adhering to routine methods/standards.

9. Result Feedback
(1) Participants are kindly requested to submit their results and feedback their answers via the dedicated online platform, whose website link is provided together with each sample.
(2) Kindly ensure that all answers are submitted by **Nov. 30, 2024** and avoid any delays or discrepancies.

10. **Evaluation of Performance**

(1) Each participant's performance is evaluated by expert consensus against the pre-established criteria derived from a multinational expert group.

(2) The criteria for participants' performance evaluation will be mainly based on the consistency of the acquired digital evidence findings with the objective results of samples. Additional factors, including the comprehensiveness of evidence analysis and the appropriateness of investigation methodology, also contribute to the evaluation. Details of the evaluation process will be outlined in the final report.

(3) The performance evaluation outcomes will be categorized into three grades:

- A (Satisfied): participants whose performance has been considered satisfactory；
- B (Questioned):participants are recommended to review their performance；
- and C (Unsatisfied): participants will need to investigate and improve their performance.

11. **Program Schedule**

Event	Period
Preparation of PT samples	June – Aug., 2024
Invitation and Acceptance of Participants	Aug. – Oct., 2024
Sample Dispatch via Online Platform;	Oct., 2024
Examination and Submission of Results	Oct. – Nov., 2024
Result Submission Deadline	Nov. 30, 2024
Results Analysis and Performance Evaluation	Dec., 2024 – Jan.2025
Disclosure of PT Report	Feb., 2025

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: +86-21-6857 1260
Fax (Auto): +86-21-3393 2578
Email: pt@stars.org.cn