2nd INTERNATIONAL DIGITAL FORENSICS CHALLENGE

(IDFC 2025)

JUL 16 - 17 2025
HONG KONG SAR, CHINA

REGULATION

Introduction

With the rapid development of information technology, ranging from continual developments in traditional computing to emerging innovations such as the Internet of Things (IoT) and blockchain, law enforcement agencies are facing increasing challenges in the realms of digital investigation and forensic analysis.

The International Digital Forensics Challenge (IDFC) aims to foster innovation, enhance participants' proficiency with the latest tools and methodologies in digital forensics, address emerging forensic challenges, and facilitate the growth of professional networks. Ultimately, the Challenge seeks to advance the Law Enforcement Agencies of digital forensics on a global scale.

The challenge, designed by forensic experts from the Hong Kong Police Force, requires participants to analyze simulated real cases under strict time constraints. Using specialized forensic tools, participants are tasked with extracting, examining, and interpreting digital evidence from smartphones, computers, and other electronic devices to reconstruct events and uncover critical information. This hands-on approach not only enhances technical proficiency but also promotes international collaboration in combating modern cybercrime.

The first IDFC, held on 19 and 20 November 2024 in Hong Kong, set a high benchmark for excellence. 10 teams from South Korea, Cambodia, Malaysia, Thailand, Uzbekistan, Indonesia, Vietnam, and three Hong Kong agencies participated in a competitive and intense event. Top honours were awarded to Hong Kong's *ICAC*, South Korea's *10VER3*, and Cambodia's *Cyber Task Force,* in recognition of their outstanding analytical capabilities, technical proficiency and teamwork.

Building on the success of last year's inaugural event, we are excited to announce the return of the IDFC in 2025. This year, IDFC 2025 will be held in conjunction with the 10th INTERPOL Digital Forensics Expert Group (DFEG) Meeting, bringing together global digital forensic experts in a dynamic and collaborative environment. We warmly welcome DFEG participants and forensic professionals worldwide to join us in this thrilling exploration of digital forensics, fostering innovation, professional growth, and international collaboration.

IDFC 2025 Organization

- **Organized by:**
  - IDFC Organizing Committee

- **Co-organized by:**
  - School of Computing and Data Science, The University of Hong Kong (HKU)
  - Cyber Security and Technology Crime Bureau (CSTCB) of Hong Kong Police Force
  - Information Security and Forensics Society (ISFS)
  - Dataport Technology Limited

- **Supported by:**
  - INTERPOL

- **Steering Committee Members:**
  - Prof. K.P. Chow, The University of Hong Kong (Chairman)
  - Prof. S.M. Yiu, The University of Hong Kong
  - Chief Superintendent Raymond Lam, Hong Kong Police Force
  - Prof. K.Y. Lam, Nanyang Technological University
  - Prof. R.S. Xu, Chinese Academy of Sciences
  - Prof. Y.H. Qin, China National Police Criminal Investigation University
  - Prof. Y. Guan, Iowa State University
  - Prof. P. Wong, University of Liverpool
  - Prof. Raymond Chan, Singapore Institute of Technology
  - Dr. S.Z. Qin, Dataport Technology Limited (Secretary)

Details of the Event

- **Date:** 16th July 2025 – 17th July 2025
- **Venue:**
  - IDFC Briefing (16th July): Wang Gungwu Lecture Hall, Graduate House, The University of Hong Kong, Pokfulam Road, Hong Kong
  - Challenge (17th July): Centenary Room I&II, G/F, Marco Polo Hongkong Hotel, Harbour City, 3 Canton Road, Tsim Sha Tsui, Kowloon, Hong Kong
- **Participants:**
  - Law enforcement officers with digital forensics expertise
- **Rundown**:
  - 16th July: Introductory briefing of the Challenge
  - 17th July: IDFC 2025

  Please refer to the official website for the detailed rundown.

- **Awards:**

- ➢ Certificates and prizes will be presented to the top-performing teams
- ➢ Certificates of attendance will be awarded to all participants who complete the Challenge

Challenge Format

IDFC 2025 is a team-based digital forensics competition, with each team comprising **1 or 2 member(s)**. Forensic image files and challenge questions will be provided to the teams. Each team is required to **bring their own digital forensic equipment and computers**, with no restrictions on the types of tools to be used.

Registration and Fee

All interested participants are invited to register for the International Digital Forensics Challenge 2025 (IDFC 2025) at: https://www.airmeet.com/e/732dc5a0-232f-11f0-9b54-afc94fa1e19b

- **Registration Fee:**
  - ➢ Participation in the event is free of charge. No registration fee is required.

- **Catering Arrangements:**
  - ➢ A buffet lunch and a formal dinner will be provided to all registered participants on the day of the challenge at no additional cost.

Participants are kindly reminded that travel and accommodation arrangements are to be made at their own expense.

Dress Code

Smart casual attire is considered appropriate for the Challenge.

The Challenge

Participants in the International Digital Forensics Challenge will conduct digital forensics investigations based on simulated real cases, providing a comprehensive assessment of their investigation and technical skills. The Challenge offers an opportunity to acquire the latest digital forensics techniques and best practices in digital forensics, while also fostering collaboration with digital forensics practitioners in other law enforcement agencies. To facilitate a clearer understanding of the Challenge, we are pleased to enclose highlights from IDFC 2024 at **Annex A**. These include the event storyboard and a selection of sample questions for your reference.

- **Challenge Details**
  - ➢ Date and Time: 17th July, 2025, 10:00 - 13:00 (3 hours)
  - ➢ Question Format: Multiple choice and fill-in-the-blank questions

- **Challenge Materials**
  - ➢ The organizing committee will provide disk images based on simulated real cases which will be distributed between 14th to 16th July, 2025.
  - ➢ **Participants are required to bring their forensic computer or a portable hard drive with at least 450 GB of free space to receive the images**.
  - ➢ At the beginning of the Challenge, teams will receive a password to decrypt the encrypted forensic image files.
  - ➢ The question set will be shown in the scoring system once the Challenge starts.
  - ➢ The scoring system will grade responses in real-time and generate final team rankings upon conclusion.

- **Rules and Regulations**
  - ➢ Rankings will be determined based on total points earned by the team. In the event of a tie, the team that submits earlier will be ranked higher.
  - ➢ Internet access is allowed during the Challenge. However, any attacks on or interference with the Challenge platform/scoring system are strictly prohibited.
  - ➢ If participants encounter system problems or have questions regarding the Challenge, they should immediately contact the on-site support team.
  - ➢ Smoking is strictly prohibited within the venue, including restrooms and all common areas.

Highlights of IDFC 2024 Annex A

IDFC 2024 Event Review

IDFC 2024 Storyboard

On a day in August 2024, the police received a report from a woman named Emma, stating that her sister Clara had been missing for several days. It was reported as a missing person incident. During the police officer's preliminary investigation, which found Emma telling the incident with reservation, you were assigned to conduct a digital forensics examination on Emma's mobile phone to gather more clues with her consent.

On a day in September 2024, while investigating a suspected homicide case in Wan Chai, Hong Kong, the police arrested David, who was suspected of murdering his wife due to a financial dispute. This case was found to be related to Clara's disappearance, as she was confirmed deceased. You conducted a forensic examination of David's electronic devices and suspected that he was part of a fraud ring involving three other individuals: Alice, Ben, and John. It is believed that they are connected to the case. The police subsequently seized the mobile phones and computers of the relevant parties for further investigation. Please analyze the following data to reconstruct the sequence of events.

Images or folders to be analyzed

1. Emma's iOS mobile phone image file (Emma_Mobile_Image.zip)
2. Clara's Android mobile phone image file (Clara_Smartphone.bin)
3. David's Windows laptop image file (David_Laptop_64GB.e01)
4. David's Windows laptop memory file (RAM_Capture_David_Laptop.raw)
5. Alice's MacOS laptop image file (Alice_Macbook.e01)
6. Alice's Android mobile phone image file (Alice_Mobile.bin)
7. Ben's Windows laptop image file (Ben_Laptop.zip)
8. Ben's iOS mobile system file (BeniPhone.zip)
9. Ben's jump station image file (Ben_Jumpstation.zip)
10. John's Windows desktop image file (John_desktop.e01)
11. John's iOS mobile backup file (John_Smartphone_itunebackup.zip)
12. John's NAS drive image file 1 (John_NAS_1.E01)
13. John's NAS drive image file 2 (John_NAS_2.E01)
14. John's VR device image file (John_VR.zip)

Challenge Scope and Recommended Tools

1. Mobile Device Forensics (e.g. Autopsy, Mobile Master)

2. Computer Forensics (e.g. Encase, Forensic Master)
3. Database Analysis (e.g. DB Browser for SQLite, Plist Editor Pro)
4. Storage Device Examination (e.g. USB, NAS)
5. Cryptocurrency Tracing (e.g. BNB Smart Chain Blockchain Explorer)
6. Memory Forensics (e.g. Volatility)
7. APK Analysis (e.g. Android Studio, APKTool)
8. Network Packet Analysis (e.g. Wireshark)
9. Recovery Seed Analysis (e.g. Mnemonic Code Converter)
10. Virtual Machine Analysis
11. IoT Forensics

Sample Questions of IDFC 2024

1. With reference to David_Laptop_64GB.e01, how many devices was David's laptop connected to?
   A: 1;
   B: 2;
   C: 3;
   D: 4;

2. During the search at John's residence, investigators seized a pair of VR glasses for forensic examination. With reference to Quest_3_2G0YC5ZFB307D7.zip file, how many users do the VR glasses have?
   A: 1;
   B: 2;
   C: 3;
   D: 4;

3. With reference to Joshe Investment.apk in Ben_Laptop.zip, in the b.smali file located in the ahmyth/mine/king/ahmyth/ folder, what series of operations does the byte array perform before being sent to the server, and what is the final image format?
   A: The byte array is decoded, encrypted, converted into PNG format, and sent to the server;
   B: The byte array is decoded, compressed into JPEG format, and encapsulated in a JSONObject before being sent to the server;
   C: The byte array is encoded as a String, compressed into BMP format, converted back into a byte array, and sent;

D: The byte array is encoded as a String, compressed into JPEG format, converted back into a byte array, and sent;

4. In September 2024, Tom Victor brought his secretary Amy to the police station to report that his secretary was defrauded of 10,000,000 IDFC by a scammer using an AI video on the morning of August 29, 2024. Please find the transaction hash of the transaction? [FILL_IN_THE_BLANK]

5. Following up on the previous question and referencing Joshe Investment.apk in Ben_Laptop.zip, what is the IP address and port number of the C2 server?
   A: IP:192.168.1.1:8080;
   B: IP:10.0.0.1:80;
   C: IP:172.16.0.1:443;
   D: IP:59.152.211.11:4444;

6. With reference to Alice_Macbook.e01, what is the TeamViewer ID that Alice used to connect to another computer for obtaining the file? (Answer format: please respond only in Arabic numerals) [FILL_IN_THE_BLANK]