Sensors and Materials, Vol. 36, No. 6 (2024) 2315–2324
MYU Tokyo

S & M 3670

Digital Forensics According to International Organization for Standardization/International Organization for Standardization 27050 and Digital Evidence Forensics Standard Operating Procedure: Use of Sensor Technology

Chao-Meng Lin and I-Long Lin*

Department of Computer Science and Engineering Tatung University, Zhongshan N. Rd., Taipei City 104, Taiwan

(Received January 3, 2024; accepted May 27, 2024)

Keywords: digital evidence forensics, ISO/IEC 27050, DEFSOP, cybercrime, crime investigation

As technology advances and cybercrime rates increase, cyberattacks, cyber fraud, and theft of property are becoming serious. Accordingly, digital evidence is inevitable for investigating related crimes. To obtain digital evidence, digital forensics with advanced sensor technology is required following international standards. For digital evidence preservation and processing, the control measures and norms for effective management are critical. Therefore, we analyzed and compared the international standards of digital evidence identification including the International Organization for Standardization/International Organization for Standardization (ISO/IEC 27050) and Digital Evidence Forensics Standard Operating Procedure (DEFSOP). We also studied how to use sensor technology for the standard and operating procedures of digital evidence forensics in real cybercrime. The results provide a basis for constructing effective evidence preservation by identifying principles of digital evidence identification.

1. Introduction

Forensics is a highly human-labor-intensive task and needs professional background knowledge. Therefore, intensive training is required to cultivate professionals. Owing to the increase in the incidence of cybercrime nowadays, the importance of digital forensics is increasing continuously. The purpose of digital forensics is to find valid, admissible, and reliable evidence to prove cybercrimes and play a decisive role in related legal cases. The challenges faced by digital forensics are related to the rapid development of technology. Therefore, it is vital to develop and use appropriate technology, especially sensor technology, in digital forensics.

Sensor technology plays a crucial role in digital forensics as it can assist investigators in collecting and analyzing evidence using various sensor devices. As IoT devices such as sensors, actuators, and radio-frequency identification tags are widely used, sensor data from such devices can be used as critical evidence. For example, sensor data on temperature, motion, and light can be used to reveal anomalies in a situation or unauthorized access. Vehicle black boxes can

*Corresponding author: e-mail: cyberpaul@gm.ttu.edu.tw
https://doi.org/10.18494/SAM4871

ISSN 0914-4935

capture information on speed, braking, and airbag deployment during accidents, which can be used as evidence in analyzing related accidents or crimes. Wearable devices such as fitness trackers and health sensors may also provide relevant data. In traditional digital forensics, humans must identify and examine digital evidence.[1] However, network sensors, mobile phone sensors, and cameras are advancing rapidly, so it is necessary to validate and standardize sensor data to maintain the integrity of evidence.[2] Recently, as cloud technology is also developing fast, sensors for data flow, access control, and resource usage have been required to investigate illegal data exchange.[3] Sensor technology is essential to digital forensics nowadays as it can provide valuable data from diverse sources. As technology evolves, forensic experts must be knowledgeable in using such technologies to effectively investigate digital crimes.

Thus, we reviewed the process of digital forensics according to the international standards of the International Organization for Standardization /International Organization for Standardization (ISO/IEC) 27050 and Digital Evidence Forensics Standard Operating Procedure (DEFSOP)[3] and discussed how to use sensor technology effectively. The results provide a basis for developing forensic technology coinciding with the rapid development of sensor technology.

2. DEFSOP

We reviewed the analysis and comparison of digital evidence forensics on the basis of the ISO/IEC 27050. In a digital forensics process, the ability of investigators in science and technology crimes is demanded to enhance the effectivity of digital forensics.[4]

2.1 Digital forensics and evidence

Digital forensics, also known as security forensics or computer forensics, is used to find evidence in digital data. Digital forensics is conducted for computer systems, mobile devices, storage media, electronic files, packets over the network, and so on. In particular, forensics in information security is defined as investigating digital evidence using scientific verification and restoring the original appearance of the incident through retrieval, analysis, and restoration to provide a basis for court proceedings.[5,6]

Digital evidence, also known as electronic evidence, is electronic information that is stored or transmitted in digital form. Digital evidence can be any electromagnetic record stored and transmitted using a computer or related electronic equipment. Messages, pictures, audio and video, coordinates, symbols, or other data can be digital evidence. Any electromagnetic records that can be read by appropriate equipment can be used as digital evidence. Digital evidence is used to support or disprove crimes or can be used to express key elements such as criminal motives.[7,8]

2.2 DEFSOP

DEFSOP consists of prior process, in-process, and after process. In the prior process, forensic experts develop an investigation plan and collect and safeguard data to ensure the integrity and

confidentiality of the evidence. The in-process involves in-depth analysis and reconstruction of data to extract useful information and evidence. In the after process, forensic experts need to present their analysis results to the court or other relevant parties. Sometimes, they conduct internal training to improve future investigations. The following stages are included in the processes of DEFSOP: principle concept, preparation, operation, and reporting (Fig. 1).[9]

1) Principle concept stage

To acquire digital evidence, the principles of legality and authenticity must be followed. Computer information systems must be investigated legally with consent. Evidence must be collected as early as possible to ensure that it has not been damaged in any way. In processing, the data on the computer or other storage media is assumed to be in its original state, and the content must not be modified. The continuity of evidence must be ensured. When the evidence is formally submitted to the court, any changes between the state of the original acquisition and the state of the evidence in the court must be explained. For the processing of any data and analysis of digital evidence, processing methods, records, and retention results must be stored. Even if the same processing procedures are performed by a third party, the results must be the same. If it is necessary to access original digital evidence, the accessing must be performed by an expert, and such action must be explained. The collection, analysis, and identification process must be recorded and photographed. Strong magnetic fields, water, fire, and virus infections must be avoided.

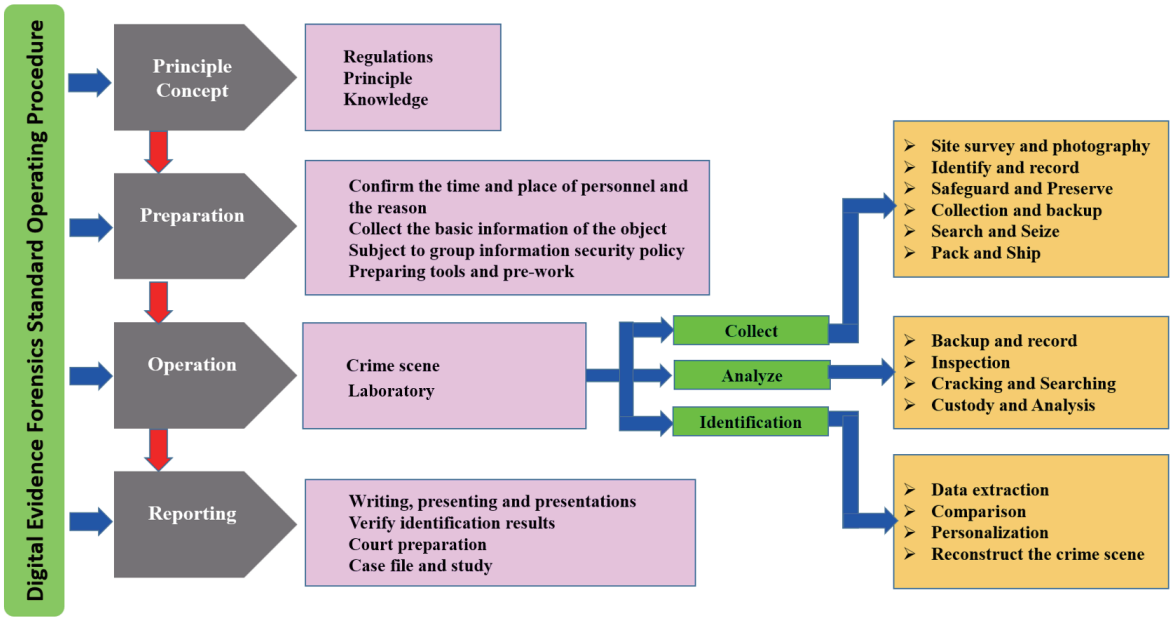


Fig. 1. (Color online) Structure of DEFSOP.[7]

2) Preparation stage

Before forensics and collection of relevant information, basic information on criminal targets, including possible perpetrators, type of crime, and available information, must be collected. Relevant personnel can be interviewed to plan a forensic execution strategy. Then, search location, objects, and time are determined on the basis of the type of crime. It is necessary to prepare a reference and a manual for computer software and hardware specifications, criminal tools, and a cracked computer. Forensic personnel must be professional in using forensic tools with relevant licenses or approvals, and must not miss and destroy valuable data and evidence during the process and destroy digital evidence with prior instructions on the tasks and projects. Software, hardware, and tools must be prepared to avoid unexpected situations.

3) Operation stage

Five tasks are included in collecting and backing up digital evidence: identification and recording, preservation, collection and backup, search and seizure, and packaging and transportation. In analyzing key data, backup and recording, inspection, cracking and searching, and storage and analysis are required. Digital evidence can be identified, processed, captured, compared, and used to restore the crime scene. In this procedure, data are extracted, compared, personalized, and reconstructed for the crime scene.

4) Reporting stage

The forensic operation process, tools, and classification methods must be reported with easy-to-read images. Evidence inspection and presentation must be correct as personnel and physical evidence before appearing in court.

3. ISO/IEC 27050

ISO/IEC 27050 is the standard procedure for the discovery of electronically stored information. Electronic discovery (eDiscovery) involves the following seven major steps.[6]

(1) Identification: Electronically stored information (ESI) is information relevant to the case, location, custodian, and size/quantity.
(2) Preservation: Identified ESI is placed under legal protection and a formal forensic process begins to ensure it is protected from loss/theft, accidental damage, and intentional interference/threats such as manipulation, and substitution. When destroyed, discredited, and devalued, ESI becomes unacceptable or unusable.
(3) Collection: ESI is collected from the original custodian, usually by physically removing the original digital storage media (hard drives, memory sticks and cards, CDs, DVDs, etc.) and possibly related physical evidence (e.g., equipment, media storage boxes, envelopes), which may have fingerprints or DNA evidence linking the suspect to the crime.
(4) Processing: Forensic evidence must be copied and stored using appropriate forensic tools and platforms to search or analyze information relevant to the case.
(5) Review: Forensic evidence and its copies can be retrieved or analyzed.

(6) Analysis: Forensic evidence is analyzed and evaluated for the relevance, applicability, weight, significance, implication, etc. of the information.
(7) Production: The relevant information obtained by the analysis needs to be formally submitted to the court as evidence.

ISO/IEC 27050 was amended four times from 2018 to 2021.[10] In ISO/IEC 27050-1 (2019), the overview and concept of the standard were formulated to guide responsible technical and nontechnical personnel in compliance with statutory and regulatory requirements. Industry standards were added for ESI identification and governance.[9] In ESI identification, the definition of ESI was introduced for identifying electronic evidence, technical means, file attributes, and metadata. In governance, a set of principles was added to guide risk management, compliance requirements, and resource allocation. Governance structure, supervision and control, regulatory compliance, and resource management were defined for the effective management and allocation of ESI, including human, financial, technical, and other resources.[11]

In ISO/IEC 27050-2 (2018), guidance for the governance and management of eDiscovery was included. Terms for identifying, collecting, retaining, searching, and providing relevant information during the legal investigation, litigation, or regulatory review were added. The concepts of eDiscovery, data, reproduction of data, legal requirements, and compliance were added. In processes, the definitions of the following terms were revised: identification, collection, retention, search, analysis, production, review, and monitoring of the eDiscovery process to ensure legal requirements, organizational policies, and best practices.[12]

The code of practice for eDiscovery was strengthened in ISO/IEC 27050-3 (2020) to provide requirements and recommendations for eDiscovery activities. Such activities were redefined for the identification, preservation, collection, processing, review, analysis, and production of ESI. In addition, relevant measures covering the entire life cycle of ESI from initial creation to final disposal were specified.[13]

In ISO/IEC 27050-4 (2021), technical readiness was emphasized to guide organizations to plan, prepare, and implement its proactive measures from a technical and process perspective. The proactive measures were defined for effective and appropriate e-Discovery and processes using forensic tools, preparedness, and the effective use of the standards for improvement, training, and awareness.[14]

In summary, ISO/IEC 27050 has been revised to improve the standard of digital forensics in each stage of DEFSOP. Important revisions of ISO/IEC 27050 in each stage of DEFSOP are summarized in Table 1.

Table 1
Revision status of ISO/IEC 27050 in each stage of DEFSOP.

DEFSOP stage	Standard			
	ISO/IEC 27050-1	ISO/IEC 27050-2	ISO/IEC 27050-3	ISO/IEC 27050-4
Principle concept	✓	✓		
Preparation		✓	✓	✓
Operation			✓	✓
Reporting			✓	

4. Comparison of DEFSOP and ISO/IEC 27050

ISO/IEC 27050 includes seven stages, namely, identification, preservation, processing, collection, review, analysis, and production, whereas DEFSOP has four stages, namely, principal concept, preparation, operation, and reporting. The compatibility of the two groups of stages is compared in Table 2. In the principle concept stage of DEFSOP, the identification stage of ISO/IEC 27050 is included. In the preparation stage of DEFSOP, the identification, preservation, and processing stages of ISO/IEC 27050 are included. In the operation and reporting stages of DEFSOP, all stages of ISO/IEC 27050 are included except for identification and production.

In each amendment of ISO/IEC 27050, the detailed processes of DEFSOP were considered. Table 3 shows which processes of DEFSOP were included in the amended ISO/IEC 27050-1 to ISO/IEC 27050-4.

The operation process of ISO/IEC 27050 is presented in Fig. 2. The prevention, analysis, identification, reporting, and filing of digital evidence comply with the four stages of DEFSOP.

5. Case Study

We reviewed a case to understand how ISO/IEC 27050 was applied to a real crime investigation. The crime occurred from September 2021 to March 2022 in Taoyuan, Taichung, and Tainan in Taiwan. There was a report of investment fraud and property losses. Through the LINE community software, URLs or APPs of fake investment platforms such as “MCK” and “AXA Trading” were randomly sent to text recipients. Fake information including stock prices, foreign exchange rates, and virtual currency was disseminated. The Criminal Police Bureau of Taiwan conducted 165 big data analyses and arrested 42 suspects. Preliminary investigation results showed that the illicit financial flows (IFFs) exceeded USD 3.1 million. To hide personal information, the group used communication software developed overseas or names and images of well-known people. This case was investigated using DEFSOP and ISO/IEC 27050 procedures as shown in Fig. 3. The main operating procedure followed DEFSOP, and each process was conducted according to the procedure of ISO/IEC 27050. It was found that DEFSOP and ISO/IEC 27050 procedures were used to define the procedure of digital forensics and electronic evidence discovery management. In the investigation, the team used the data from network sensors and cloud technology to trace data flows, accesses, and resource usage.

Table 2
Comparison of stages of ISO/IEC 27050 and DEFSOP.

ISO/IEC 27050	DEFSOP			
	Principle concept	Preparation	Operation	Reporting
Identification	✓	✓		
Preservation		✓	✓	✓
Collection		✓	✓	✓
Processing			✓	✓
Review			✓	✓
Analysis			✓	✓
Production			✓	

Table 3
Comparison of DEFSOP and ISO/IEC 27050-1 to ISO/IEC 27050-4.

Detailed process	Standard				
	DEFSOP	ISO/IEC 27050-1	ISO/IEC 27050-2	ISO/IEC 27050-3	ISO/IEC 27050-4
Principle concept stage					
Legality	✓	✓	✓		
Complete record	✓	✓	✓		
Best evidence principle	✓	✓	✓		
Principle of least harm	✓	✓	✓		
Evidence integrity	✓	✓	✓		
Pre-principle	✓	✓	✓		
Principle in the matter	✓	✓	✓		
Expost-pPrinciple	✓	✓	✓		
Preparation stage					
Preparation tools and pre-service education	✓		✓	✓	✓
Determining the time and place of personnel	✓		✓	✓	✓
Collecting basic information of the object	✓		✓	✓	✓
Authorization and security policy	✓		✓	✓	✓
Operation stage					
Site survey and photography	✓			✓	✓
Identification and recording	✓			✓	✓
Preservation and security	✓			✓	✓
Collection and backup	✓			✓	✓
Search and seizure	✓			✓	✓
Backup and recording	✓			✓	✓
Check and search	✓			✓	✓
Analysis and custody	✓			✓	✓
Data extraction	✓			✓	✓
Comparison	✓			✓	✓
Personalization	✓			✓	✓
Crime scene reconstruction	✓			✓	✓
Reporting stage					
Writing, presenting, and presentations	✓			✓	
Verifying identification results	✓			✓	
Court preparation	✓			✓	
Case file and study	✓			✓	

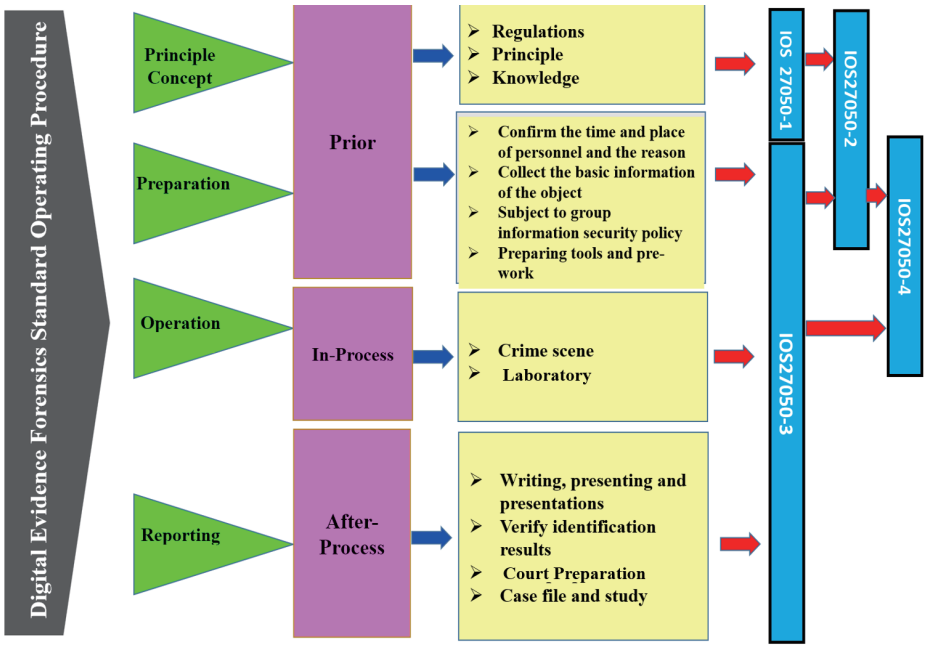


Fig. 2. (Color online) Operation process of ISO/IEC 27050 and its compliance with DEFSOP.

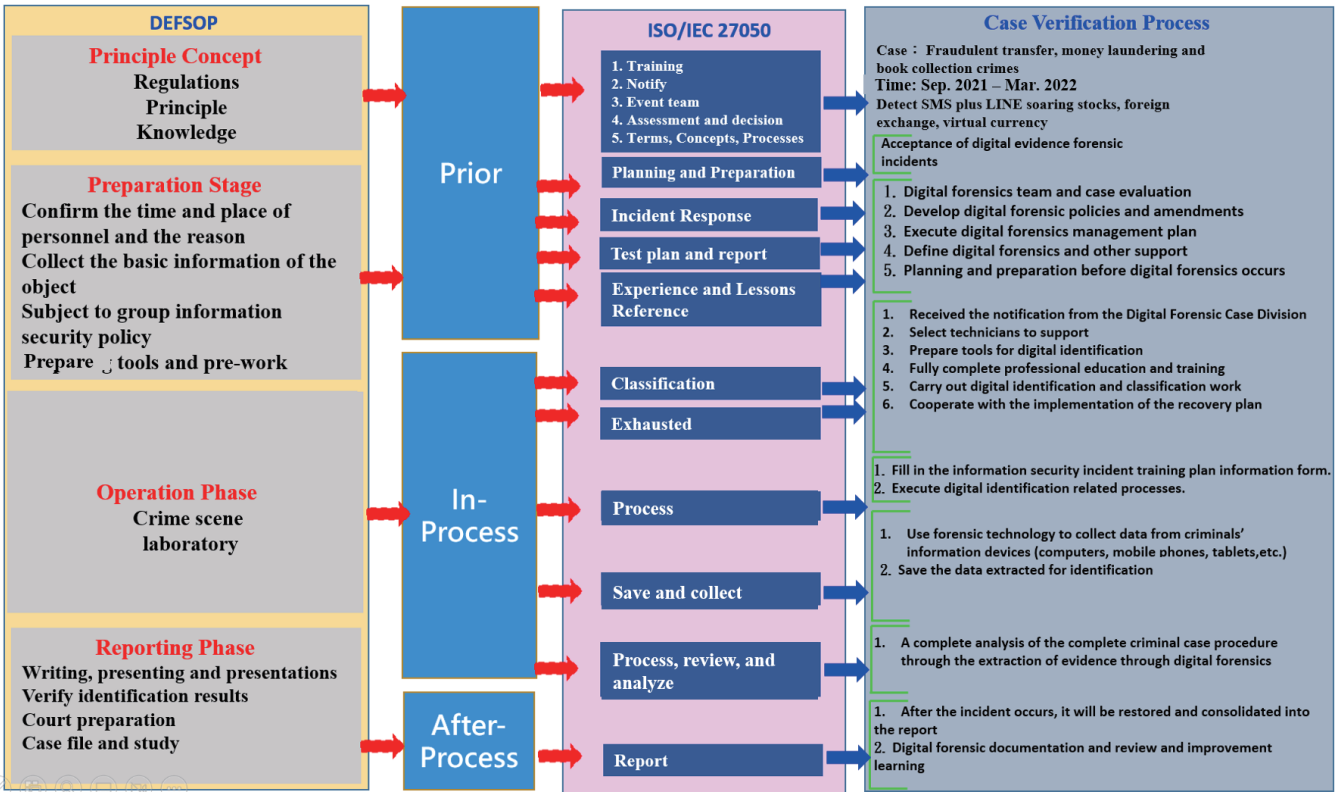


Fig. 3. (Color online) Investigation of cyber fraud following DEFSOP and ISO/IEC 27050.

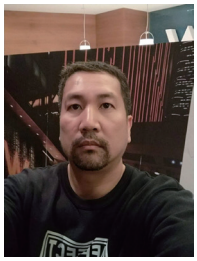
6. Conclusions

We reviewed ISO/IEC 27050 and DEFSOP, which are international standard procedures for the eDiscovery of evidence, and how sensor technology was used for the investigation of a real cybercrime. The concept and significance of digital forensics are integrated in the standard procedures. Electronic tools such as computers, mobile phones, and tablets are used in cybercrimes, which makes forensics more difficult than in traditional crimes. Advanced sensor technology allows the identification, extraction, and analysis of cybercrimes to be performed efficiently and also helps digital forensics experts have professional perspectives and cognition on such crimes. As the importance of digital forensics and electronic evidence discovery is further emphasized, it is necessary to develop sensor technology for more effective digital forensics, complying with international standards such as ISO/IEC 27050 and DEFSOP.

References

1 T. Janarthanan, M. Bagheri, and S. Zargari: IoT Forensics: An Overview of the Current Issues and Challenges (Sspringer Verag, Berlin, 1969) pp. 223–254.
2 Azo Sensors: https://www.azosensors.com/article.aspx?ArticleID=2956 (accessed April 2024).
3 J. Mennel and I. Shaw: Meas. Control. **42** (2009) 314. https://doi.org/10.1177/002029400904201005
4 ISO 27001 Security: https://www.iso27001security.com/html/27050.html (accessed April 2024).
5 American Scientist: https://www.americanscientist.org/article/digital-forensics (accessed April 2024).
6 D. Kim, S. Oh, and T. Shon: Forensic Sci. Int.: Digit. Invest. **46** (2023) 301608. https://doi.org/10.1016/j.fsidi.2023.301608
7 D. Roni, N. S. Gill, and P. Gulla: J. Ind. Inf. Integr. **38** (2024) 100568. https://doi.org/10.1016/j.jii.2024.100568
8 S. M. Pedapudi and N. Vadlamani: Meas.: Sens. **29** (2023) 100860. https://doi.org/10.1016/j.measen.2023.100860
9 I. L. Lin, Y. S. Yen, and F. Y. Leu: Proc. 2014 8th Int. Conf. Innovative Mobile and Internet Services in Ubiquitous Computing (IEEE, 2014) 511–516. https://doi.org/10.1109/IMIS.2014.74
10 INFORSEc Solutions: https://www.solutions-inc.co.uk/iso-iec-27050/ (accessed April 2024).
11 ISO: https://www.iso.org/standard/78647.html (accessed April 2024).
12 ISO: https://www.iso.org/standard/66230.html (accessed April 2024).
13 ISO: https://www.iso.org/standard/78648.html (accessed April 2024).
14 ISO: https://www.iso.org/standard/74034.html (accessed April 2024).

About the Authors



Chao-Meng Lin received his B.S. degree from Lunghwa University, Taiwan in 2012 and his M.S. degree from Ilzm University, Taiwan in 2019. From 2002 to 2018, he was a network engineer at Lccnet, Taiwan, and a senior network engineer at TCCI. Since 2018, he has been a product manager at Mikotek, and since 2021, he has been studying digital forensics, cybersecurity, and network routing and switching in the doctoral program of the Department of Computer Science and Engineering of Tatung University. (po6150@gmail.com)

I-Long Lin received his B.S. degree from Central Police University, Taiwan, in 1983, and his M.S. and Ph.D. degrees from Tamkang University and National Taiwan University of Science and Technology in 1989 and 1998, respectively. From 1983 to 2011, he was a professor at Central Police University, Taiwan. From 2012 to 2021, he was a professor at Yuanpei University of Medical Technology, Taiwan. Since 2021, he has been a professor at Tatung University. His research interests include digital evidence, forensics, and cybersecurity. (cyberpaul@gm.ttu.edu.tw)