Discussion on the Talents Cultivation of Digital Forensics

Guangxuan Chen[1, a], Di Wu[2, b], Guangxiao Chen[3, c], Bo Hu[1, d] and Anan Huang[1, e *]

[1] Zhejiang Police College, Hangzhou, China

[2] The People's Procuratorate of Hangzhou, Hangzhou, China

[3] Wenzhou Public Security Bureau, Wenzhou, China

[a] chenguangxuan@zjjcxy.cn, [b] erik_wudi@qq.com, [c] relachen@163.com, [d] hubo@zjjcxy.cn,

[* e] huanganan@zjjcxy.cn

*corresponding author

Keywords: Digital Forensics; Talents Cultivation; Curriculum Design

Abstract: Digital forensics is an interdisciplinary major that involves a wide range of fields. Its professional knowledge composition includes computer science, law, and investigation and so on. With the rapid growth of the demand for digital forensics, the current public security, prosecution, courts, enterprises, etc. increasingly need a large number of professional forensics talents. This article discusses how to train professionals in digital forensics, as well as related majors and curriculum construction. Through reasonable curriculum settings and professional experimental practice design, professional students and trainers can systematically master the basic theory and technology of digital forensics, and related cybercrime investigation knowledge, so as to be competent for professional digital forensics and cybercrime investigation work.

1. Introduction

According to the 44th "Statistical Report on Internet Development in China" released by CNNIC, by the time of June 2019, the number of Internet users in China reached to 854 million, an increase of 25.98 million from the end of 2018, and the Internet penetration rate reached to 61.2%, an increase of 1.6 percentage points from the end of 2018 ; The number of mobile Internet users in China reached to 847 million, an increase of 29.84 million from the end of 2018, and the proportion of Internet users using mobile phones to access the Internet reached to 99.1%, an increase of 0.5 percentage points from the end of 2018.

With the advancement of technologies such as mobile Internet, cloud computing, artificial intelligence, VR/AR, Internet of Things, and big data, the crimes in the real world is shifting to cyberspace, and more cyberspaces is giving birth to a large number of unique crimes, such as cyber attacks, online gambling, online fraud, etc. According to statistics, China's cybercrime accounts for 1/3 of the total crimes, and is growing at a rate of over 30% per year. In the face of the continuing high incidence of cybercrime and the complex and ever-changing crime situation, it is required that we have a comprehensive and in-depth knowledge of cybercrime and a strong level of expertise in order to respond to the transformative demands of combating cybercrime.

Digital Forensics plays a key role in combating cybercrime. Its purpose is to provide the "traces" of perpetrators left in computers and related electronic equipment as valid evidence of litigation to the court in order to bring the criminals to justice. With the rapid growth of the demand for digital forensics, the current public security organs, prosecution, courts, enterprises, etc. increasingly need a large number of professional forensics talents. As the forensics scientist Dr. Henry Chang-Yu Lee admits, there is currently a shortage of talents for digital forensics [1]. For example, in the United States, IT practitioners and young university graduates are organized by the law-enforcing departments and receive training so as to become qualified for the digital forensics work. We should

also grasp the new situation in a timely manner, combine with reality, and cultivate forensic talents who are in line with the new era.

2. Digital Forensics

Digital forensics is a special branch of forensic science that handles digital data evidence in various cases. In recent years, electronic devices have been increasingly used in criminal activities, including theft, fraud, hacking, software forgery, computer viruses, child pornography, and so on. When the suspect's electronic equipment is seized, the digital forensics expert is usually required to carry out relevant forensics work. In the field of forensic science, as digital data evidence plays an increasingly important role in cases, law enforcement agencies around the world have become increasingly aware of the importance of digital forensics and how it affects investigation results [2, 3].

Digital forensics is a comprehensive discipline that involves computer science, law and investigative disciplines. Professional digital forensics personnel must not only master excellent computer technology, but also have certain legal knowledge, as well as certain investigative thinking.

(1) Forensics personnel need to master excellent computer technology

Digital evidence in electronic devices is very extensive. Taking a basic computer system as an example, possible investigation subjects include external hard drives, memory sticks, modems, deleted files, network information, cookies, printer spool files, temporary files, swap files, residual space, cache, logs and any other related media files, etc. The object data also have many forms. Among them, activity data is clearly visible information, including various applications and operating system files. In theory, these data are easy to access. The archived data is the data that has been backed up and stored, including data on tapes, CDs, and other hard drives. Generally speaking, for seized storage media, ordinary access usually does not cause problems. However, some data may have been deleted, overwritten or even encrypted, and usually require special tools to access it. In addition, electronic devices are in various forms, and any electronic device that can store digital data is the subject of investigation by forensics personnel. In particular, the popularity of smart phones makes mobile phone forensics a professional discipline in the field of digital forensics. In the process of searching for electronic evidence, the forensics personnel are required to master solid techniques.

(2) Forensics personnel need a solid legal foundation

Digital forensics is a rigorous process because it needs to meet the requirements of legal proceedings. Making digital data information effective legal evidence is also an urgently needed requirement in many fields. At the basic legal level, the state has made clear provisions on the standards of digital forensics and identifications. It requires that forensics personnel and appraisal agencies should observe professional ethics and professional discipline, respect science, and abide by technical operation standards in the whole process of digital forensics and identification. In addition, the Ministry of Justice and the Ministry of Public Security have also made clear provisions on the qualifications, norms and legal analysis of forensics personnel. Therefore, forensics personnel must have a solid legal basis before conducting digital forensics.

(3) Forensics personnel need to have investigative thinking

At present, more and more cases require a special digital forensics department to lead or cooperate with the investigation. In particular, the continuous emergence of anti-forensic technology, many criminals often use various means to destroy evidence, which brings great challenges to investigators. Therefore, the forensic personnel also need to have a certain investigative thinking, and have the ability to analyze and search for possible digital data evidence from both technical and non-technical factors.

3. Curriculum Design of Digital Forensics

Compared with western developed countries, the development of China's digital forensics started late, and it is still in its infancy. It is facing severe challenges, i.e., inadequate related laws and

regulations, insufficient number of digital data identification agencies and professional personnel. Therefore, in addition to establishing and improving relevant laws and regulations, it is urgent to cultivate forensic talents with excellent professional quality.

As for the professional law enforcement agencies, it is necessary to strengthen the team construction, and require the digital forensics personnel to have professional qualifications and corresponding abilities. They also need to have basic knowledge of computer science, law, and investigation, and the ability to learn the latest knowledge and technology in time.

In colleges and universities, especially public security, political and law schools, it is necessary to establish a feasible training system for digital forensics talents, develop a complete set of digital forensics knowledge systems including basic theory, experiments, and practical training, which can reflect the corresponding forensic ability that meets actual combat needs for the students.

Goals of the Curriculum. Curriculum must first meet the needs of talent training. In some colleges and universities, many investigation related majors, network security and law enforcement majors have increased the digital forensics courses to meet the needs of the rapid development of cyber crimes combating. Professional technical personnel for electronic data forensics not only need to have relevant educational backgrounds in computer, network security, law, etc., but also have professional skills in electronic data forensics, including the identification, preservation and collection of digital evidence in crime scenes, locating possible evidence in digital media, obtaining, confirming and restoring forensic images from various digital evidences, and be able to identify, analyze and solve technical and research problems [4]. Therefore, only a scientific and reasonable curriculum can help students improve their professional qualities, solidly and systematically master the principles, technologies, tools, laws and regulations of digital data survey and forensics, and ultimately provide services in practice.

System of Knowledge. Digital forensics is a cross-discipline that integrates computer science, information security and law. It is one of the core curriculum systems of the undergraduate major in network security & law enforcement and the master of police in network security & law enforcement technology. It uses technical methods to extract data from computer systems and related digital devices, or to retrieve information from files that have been deleted, encrypted, or destroyed, and to collect, protect, extract, and organize complete, effective, objective and convincing evidence in accordance with legal procedures, so as to find the truth of the incidents. The course of digital forensics is multidisciplinary, and it should include basic and practical knowledge in computer and information science, as well as judicial trial courses. In addition, graduates in this field should be proficient in writing skills and familiar with security measures and forensic software applications. In short, the curriculum should cover the knowledge points of the above subjects, thus forming a complete knowledge system.

It is not necessary to set too many basic courses for digital forensics and the key is to grasp the content of courses; at the same time, as digital forensics is a highly practical major, we should set up independent experimental courses to improve students' practical ability. Therefore, we should make some choices in the curriculum setting, focusing on the combination of multiple levels of content, not only to allow students to master the entire knowledge system of network & law enforcement, but also to take into account the special teaching of digital forensics courses, so as to enhance students' practical ability and the potential for further study in various aspects [5].

Setting of Curriculum. General courses are set up in the professional curriculum of digital forensics, and the proportion of forensics courses is also increased in basic courses, professional advanced courses and experimental courses. Students are emphasized on the study of computer and information mathematics and other leading courses. Gradient and selective digital forensics courses are offered. At the same time, referring to the experience of domestic and foreign industry academic institutions in digital forensics training, the course is taught in three gradients. Figure 1 shows the curriculum structure of digital data forensics. In the basic courses, three knowledge systems are summarized, including mathematics and law foundation, computer hardware and software foundation, and information security courses. Table 1 shows a general curriculum design for digital forensics.

Table 1. General curriculum design for digital forensics

Type of Courses	Name of Courses
Foundation Courses	Discrete mathematics, Probability statistics, Procedural law, Principle of microcomputer, Computer Architecture, Principles of Operating System, Database, Programming, Computer Network, Cryptography, Information Security, Network Attack and Defense
Core Courses	Introduction to Computer Forensics, Data Recovery Technology, Computer Crime Investigation, Analysis of File and Operating System, Analysis of Storage Device and Software, Mobile Phone Forensics
Advanced and Elective Courses	Advanced Computer Forensics, Network Forensics, Personal Electronic Device Forensics, Embedded Device Forensics, Incident Response, Reverse Engineering and Countermeasures, Encrypted Data Forensics, Cloud Forensics

Table 2 shows the typical courses suitable for the bachelor degree of digital forensics related majors, and Table 3 shows the advanced courses suitable for the master degree of digital forensics related majors.

Table 2. Typical courses suitable for the bachelor degree of digital forensics

Course Group	Content
Introduction to Computer & Storage Media	Computer Composition Principle, General Storage Media (USB, SCSI, IDE, Firewire, SATA,...), Data Backup And Data Recovery Technology, Special Storage Media
OS & Applications	The General OS (including Windows, Linux, Unix, Macintosh) and Applications
Computer & Network Security	Security Foundation, System Security (Windows & Linux), Hacker Attack and Defense, Malicious Code Analysis, Communication Security, Analysis of Common Application Protocols, Web & Script Attack Technology, Firewall Technology, Intrusion Detection System Technology (IDS), Encryption & VPN Technology, Product Security , Security Management
Foundation of Computer Forensics	Introduction to Computer Crime, Introduction to Computer Forensics, Legal Issues of Computer Forensics, Computer Forensics Technology, Windows Forensics, Linux Forensics, Computer Forensics in a Network Environment, Typical Cases, Practice of Computer Forensics
File System	File System Concept, File System Management, Typical File Systems, Disk Partition, Data Fault Tolerance Mechanism, Network File System, Cloud Storage, Journal File System

Table 3. Typical courses suitable for the bachelor degree of digital forensics

Course Group	Content
Advanced computer forensics	Basic Evidence Acquisition Methods, Program Encryption and Anti-Forensics, Evaluation of Forensics Tools and Methods
Network Forensics	Basic Network Protocols, Network Data Recovery Technology, P2P, Wireless, VoIP Related Forensics, Network Tools, Network File System
Storage System	Common Storage Devices, General File Systems (Fat, Ntfs, Ext2/3, Hfs +), Disk Partitioning And Data Analysis Technology
Personal digital device forensics	Architecture and System Principles Of Personal Electronic Devices PED (Such As Mobile Phones, PDAs, Mp3 Players, GPS Devices), Electronic Evidence in Personal Electronic Devices, Forensics and

	Anti-Forensics of Personal Electronic Devices, Mirroring and Detection of Personal Electronic Devices
Embedded device forensics	The Principle and Basic Structure of Common Embedded Equipment Such as Automobile Driving Computer, Industrial Control System PCSS, Electronic Consumer Auxiliary Equipment, Data Recovery Technology of Embedded Equipment
Reverse engineering technology	Assembly Language, Compiler, Decompilation and Debugger Application Using Assembly Language.
Multimedia forensics	Analysis, Identification, Encoding, Decoding, Compression, and Format Conversion of Sound, Video and Image, Etc.

In addition, the practical department and universities can also cooperate with enterprises, third-party institutions and other departments to carry out related scientific research, training cooperation and academic exchanges, so as to promote the improvement of digital forensics technology, research and development of forensics tools, etc.

Summary

As an emerging technology, digital forensics has obvious advantages in cyber crime combating and forensics. However, its development still faces many problems, especially the shortage of professional talents. Talent cultivation is a systematic project and requires a complete scientific management system to regulate it. We should establish a sound management system for the training system, and strive to promote the healthy development of digital forensics, and improve the academic, theoretical and practical levels of digital forensics. This has important practical significance for combating cyber crime.

Acknowledgments

This work was supported by the Basic Public Welfare Research Program of Zhejiang Province under Grant No. LGF19F020006, Demonstration Course Construction Program of Zhejiang Police College under Grant No. 20190306, and the College-Bureau Collaborative Research Program of Zhejiang Police College under Grant No.2018XJY003.

References

[1] L.P. Ding, Thinking on the Training of Digital Forensics Talents, China Information Security, 5(2019), p. 74-75. (In Chinese)

[2] G.X. Chen, Y.H. Du, P.K. Qin and J. Du, Suggestions to digital forensics in Cloud computing ERA, Proc. IEEE International Conference on Network Infrastructure & Digital Content, 2012, p.540-544.

[3] G.X. Chen, Y.H. Du, J. Du and N. Li, Research of Digital Forensics under Cloud Computing Environment, NetInfo Security, 8(2013), p. 93-96. (In Chinese)

[4] J.J. Liu, G.X. Chen, Research on Digital Forensics Technology System, Network Security Technology & Application, 5(2013), pp. 10-12. (In Chinese)

[5] M.C. Cai, Y. Wang, Discussion on Digital Data Curriculum in Public Security Politics and Law Colleges, Computer Education, 24(2012), p. 72-75. (In Chinese)

[6] G.X. Chen, X.H. Liu, Challenges of Mobile Phone Forensics, China Information Security, 5(2019), p. 69-70. (In Chinese)

[7] H.Q. Pu, Y.F. Guo, Survey on Electronic Forensics Research, Computer Systems & Applications, 28(2019), p. 10-16. (In Chinese)

[8] K.T. Seong, G.H. Kim, Implementation of voyage data recording device using a digital forensics-based hash algorithm, International Journal of Electrical and Computer Engineering, (9)2019, p. 5412

[9] Z.G. Qiang, Research on Forensic Methods in Computer Intrusion, Network Security Technology & Application, 4(2020), p. 152-153. (In Chinese)

[10] Y. Li, Computer forensics technology and its development trend, Computer products and distribution, 12(2019), p. 6. (In Chinese)