Transforming Digital Forensics Training: A Competition Insight

Tao Leng

{ hjmark2020@gmail.com }

Intelligent Policing Key Laboratory of Sichuan provance, SiChuan Police College ,Sichuan, China

Abstract. With the high incidence of cybercrime cases, there is an urgent need for elite talents in digital forensics. The core of forensics talent training is to build a knowledge system. Through a comprehensive analysis of the inspection background, mirror image, topic assessment knowledge of the world's major digital forensics competitions, we summarized the content of the competition knowledge modules; combined with the public security electronic data forensics workflow, proposed a knowledge map of forensics elite talents; finally the train of thought of talents.

Keywords: cybercrime; digital forensics; knowledge graph; talent training.

1 Introduction

Digital forensics plays a vital role in public law enforcement and combating online crimes in the information age[1]. With an increasing volume of digital evidence in cybercrime cases, the challenges of evidence acquisition have raised the bar for forensic investigators. However, previous research has primarily focused on specific forensic technologies or experiment platforms, overlooking the analysis of knowledge modules in forensic education. This article aims to fill this research gap by analyzing test materials and competition questions from domestic and foreign forensic competitions. It examines knowledge modules, important concepts, and challenging areas in the assessment of forensic talent. Furthermore, it builds a knowledge graph to facilitate the cultivation of forensic expertise and proposes development trends for forensic competitions, along with innovative ideas for talent training.

2 Relatedwork

Liu[2] developed a comprehensive training platform utilizing virtual simulation technology to enhance students' interest in learning and improve their scientific research abilities. Their approach integrated basic experiments from the digital forensics course using virtual machines, which facilitated hands-on practice and reduced hardware costs. Xu[3] proposed the creation of a network-centric digital forensics target area using the OpenStack cloud platform. This method is particularly effective in a single, unified setting. Li [4] proposed the development of a scalable digital forensics training system capable of accommodating the training and learning needs of a large user base. The system was built using node.js, vue, and MongoDB, with the server hosted on the Ali cloud platform. The primary focus of the paper was on platform development, with

NMDME 2023, October 13-15, Xi'an, People's Republic of China

DOI 10.4108/eai.13-10-2023.2341280

the goal of meeting the criteria for digital forensic analysis capacity. Zhang[5] proposed the creation of a cloud-based digital forensics course, which included discussions on cases related to gang crimes, cloud servers, gambling websites, and the establishment of a case library. Xu[6] conducted a survey of digital forensics education in North American iSchools, examining training strategies, curriculum design, course materials, and delivery techniques. Naqvi[7] presented a research-led and practice-driven digital forensics curriculum designed to meet the demands of professional practice. The curriculum has been implemented and practiced at Birmingham City University. Gupta [8] created and open-sourced a digital forensics laboratory that offers case studies and enables case reconstruction. In contrast to the aforementioned works, this paper focuses on analyzing the content of forensic competition examination materials and assessments. Additionally, we proposes ideas for the construction and development of a knowledge system for elite forensic professionals.

3 Approach

Cybercrime is a serious criminal offense, and police officers need to improve their electronic data forensics capabilities. What are the skills modules for electronic data forensics? How to improve it? This article is designed using the method shown in **Fig.1**. By analyzing domestic and foreign electronic data forensics competitions, the knowledge modules of forensics talents are analyzed and summarized, and corresponding training methods and suggestions are proposed. Enhancing the Police's Ability to Combat Cybercrime.

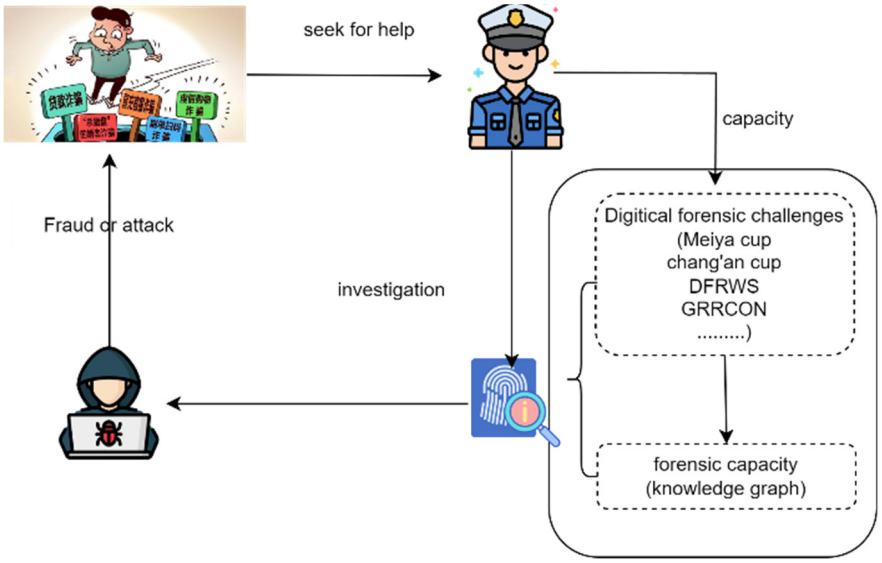

Fig. 1. Approach

This paper needs to answer the questions:

RQ1:Investigate the basic situation of digital forensics competition?

RQ2:What are the main content and knowledge modules of the digital forensics competition?

RQ3:What should be the knowledge graph of digital forensics talents?

RQ4:Knowledge mapping-based teaching suggestions?

Through the investigation of digital forensics competition all over the world, we analyze the knowledge graph to assist cultivate digital forensics talents.

3.1 Chinese Digital challenges

The primary forensic challenges in China include the Meiya Cup[9], the Chang'an Cup[10], and digital forensic competitions organized by industrial units. The research discussed in the following sections primarily focuses on the Meiya Cup and the Chang'an Cup. Case Background is a crucial factor in facilitating in-depth forensic analysis of cases. **Table 1** presents the keywords associated with the case backgrounds in the Meiya Cup competition. Analysis of the competition in recent years reveals a notable trend in criminal cases, with a predominant focus on cyber attacks. Starting from 2020, Meiya Cup started providing comprehensive case background investigation materials and reports on the investigation process. These materials serve the dual purpose of explaining the cases and guiding students in conducting on-site investigations.

TABLE 1. MEIYA CASE KEYWORD

Year	Key word of Case
2015	Child pornography, nude chat extortion; bomb making; counterfeit money making, theft of sensitive user information; online auction platform fraud
2016	Intrusion, writing and distributing viruses, Internet fraud
2017	Want to make money quickily, ransomware attack
2018	Information leakage, email extortion, hacking cloud servers to obtain personal information, bitcoin extortion
2019	Selling customer data, hacking, darknet
2020	Credit card fraud, hacking online stores
2021	Computer hacking, mining attack
2022	mediaserver hacking, credit card fraud,cyber phishing

The Chang'an Cup, held since 2019, featured different material designs each year with a focus on various knowledge points. The 2019 competition focused on a fraud case related to personal information leakage. the inspection materials covered topics such as website reconstruction, docker forensics, financial website database server forensics, VPN server forensics, laptop and mobile phone backups, and virtual machine forensics. In 2020, the case involved illegal trading, the difficluties shifted the focus to website reverse proxy, real website code analysis, and real website database server forensics. and in 2021, it revolved around live broadcast naked chat extortion. the emphasis was on APP forensics and pagoda panel forensics. In 2022, A case involving virtual currency investment fraud. Detailed design information can be found in **Table 2**, providing investigation ideas based on the background of the inspection materials.

TABLE 2. CHANG'AN CUP CASE GROUND

Year	Case Ground
2019	Victim: (The financial management system of a P2P website has been attacked-> leaked user information) ->victim received fake public security information-> filled in her

2020	own information and bound bank card on the designated website-> bank card was used by others Police investigation routine: retrieve the mirror of the p2p financial website server (materia1) -> wealth management website database server (materia2) -> VPN server (materia3) -> the suspect's laptop (materia4, notebook Including mobile backup and virtual machine) Police investigation: Illegal website mirror (material1, reverse proxy) -> real website (material 3) -> real website database server (material 4) -> suspect's PC (material 2)
2021	Victim's mobile phone (APP, materia 1) -> background server (app connection, load balancing, materia 2) -> destination server (materia 3) -> suspect's PC and mobile phone (materia 4)
2022	According to the victim provided the domain name and ip of the website, the police retrieved the server image server. (materia 1) -> Landed on an ip address, captured the techie, seized the PC.(materia 2) -> According to the technician's computer, the back-end server of the website was found, and the server image was retrieved. (materia 3) -> Capture users and use Android emulators for forensics(materia 4)

3.2 Other famous Digital challenges

DFRWS[11] has been organizing digital forensics challenges since 2005, covering various topics such as Windows memory forensics, data carving, Linux memory forensics, mobile device forensics, and more. These challenges aim to advance research in digital forensics and explore emerging areas of investigation. The Honeynet[12] forensics Challenge is based on real attacks and covers various topics, including log forensics, network traffic forensics, malicious code analysis, and more. The challenge aims to investigate and reconstruct the attack process. Grrcon has been organizing DFIR challenges during its conference since 2012, focusing on memory forensics as the main area of analysis. magnet has also been organizing Forensics challenges since 2018, similar to the Chinese e-data forensics competitions, but with fewer examinations and participants. Additionally, there are other forensics challenges published by companies or research enthusiasts, such as the digital forensics challenge mirror designed by Dr. Ali Hadi[13]. These competitions are well-designed and contribute to the development of forensic talent and the improvement of individuals' skills. The topic design of these competitions primarily revolves around attacks, requiring participants to analyze given materials and reconstruct the attack process.

3.3 Design of knowledge modules in challenges

By analyzing the questions in the competition, we summarize the knowledge modules involved in the competition, as shown in **Table 3.**

Table 3. Knowledge modules.

Forensic Subject	Module	Contents
Windows Forensic	Disk analysis	Disk partions, MBR, master boot record,sectors,clusters,physical offset,LBA
	System and application basic information	System, Software, Sam, Ntuser.dat,Usrclass.dat, Prefetch file analysis,Application Analysis; timeline analysis
	File engraving and keyword search	combined with data recovery, bitlocker key acquisition, File Information and Search
	Browser forensics	Download and access history, cache, bookmarks,tor browser forensic
	Email Forensics	Mail client forensics,mail content forensic, mail attachment analysis
	Shortcuts and Recycle Bin Forensics	Metadata of shortcuts and Recycle Bin
	Malicious Code Forensic	Software Reversing ,malicious documents analysis
	Memory Forensic in windows	Process,dll,registry,sockets,cmdline info of memory images
Linux Forensic	Log forensics	Web logs, FTP server, system logs, router logs, database logs
	Basic System Information	System information,network information,log information, Encrypted containers
	RAID Reconstruction	Raid arrays，volume group info，
	Docker Forensics	Docker images，containers basic information，docker web services reconstruction
	WebSite and Database forensics	WebSite reconstruction,Web Analysis,Database Analysis
	Mining Server Forensics	Mining servers, mining programs, log analysis
	Vpn Server Forensics	Vpn software information,Vpn log
	Memory forensic in linux	Malicious activity in linux
Mac Forensic	Basic Information	Mac system forensic, mac app analysis
Mobile Forensic	Basic Information	Mobile system information, app database analysis
	Malicious App Forensic	APP Basic Information, Network info, Code Function Analysis
Network Forensic	Packet Analysis	Packet Analysis
New Smart Device Forensic	Smart Router forensic	Log analysis,network information
	Drone Forensics	Drone flight records, specified time location, APK database analysis, video analysis
	Raspberry Pi	File system info
investigate thinking	Cyber Attack Thinking	the entry point of the attack,attack path, attack timeline anaysis
	Open Source Intelligence	Google, metadata forensic
	Case ideas	Technical ideas for cybercrime cases

4. Results and Measures

4.1 Knowledge graph

Forensic competitions are based on real cases and involve constructing examination materials and designing questions around forensic technology knowledge points. The competitions follow a format similar to Capture the Flag (CTF) contests. The knowledge graph in **Figure2** summarizes the forensic talent areas, including electronic data scene inspection and remote inspection. These areas cover a wide range of topics such as Windows, Linux, macOS, mobile forensics, network equipment forensics, IoT, and UAV forensics. Remote inspection includes web page solidification, remote server image forensics, and cloud forensics. The forensic process should adhere to national standards, industry standards, and technical specifications, ensuring authenticity, legality, and relevance. Investigative thinking and understanding attacker methods are crucial, and evidence collection should focus on court support based on the specific case.

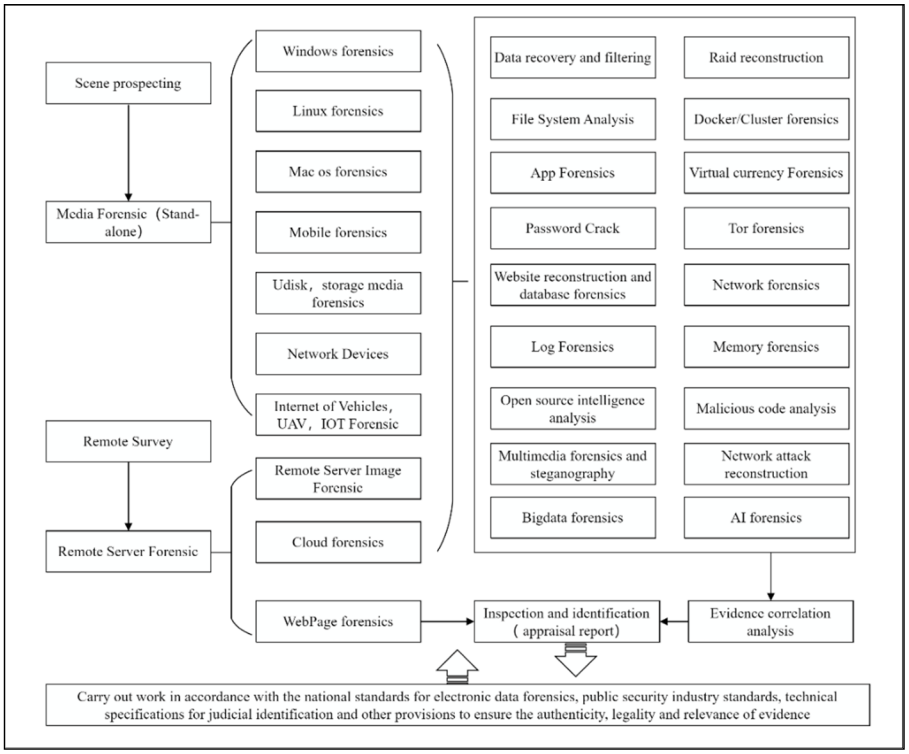

Fig. 2. Knowledge graph

4.2 Case analysis

The local police received a report from a victim claiming that they were defrauded on a cryptocurrency trading website. The website claimed to use "USTD Coin" to purchase so-called "HT Coin". After the victim deposited funds, not only was the "HT Coin" unavailable for

withdrawal or trading, but malicious software also locked the victim's phone for ransom. Based on the cryptocurrency trading website provided by the victim, the police obtained the corresponding server image and launched an investigation into the case. The inspection knowledge modules include computer forensic analysis, server/website forensic analysis, mobile phone forensic analysis, and program function analysis. By analyzing this case(**Figure.3**), the boss behind the scenes hired technical staff to build a virtual currency website that separated the front and back ends of the website, and asked promoters to forge investment data to attract users to invest. Targeted phishing attacks and ransomware virus attacks were also carried out on investment victims. The entire case was designed with installation simulator forensics, malicious apk forensics, docker-based springbot+vue website forensics, ransomware analysis, wsl subsystem forensics under windows system and other knowledge points. It includes the hot spots of virtual currency cases, program analysis and other difficulties, and trains investigative thinking.

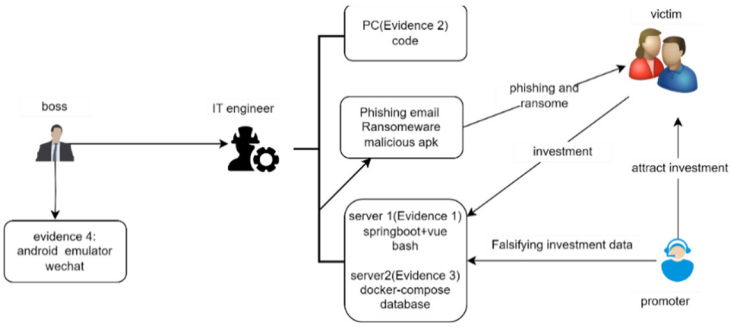

Fig. 3. Case sorting

4.3 Suggestion and Measures

Talent development should concentrate on the following areas in accordance with the demands of the job and the competition: (1) Use knowledge mapping to enhance cultivation, study cases, determine attackers' thought processes, and improve forensic accuracy[14]. (2) In accordance with the trial-centered forensic thinking, national forensic standards and pertinent forensic specifications should be used to direct the forensic process, which includes gathering forensic evidence, investigating crime scenes, conducting forensic analyses, reconstructing crime scenes, and submitting identification reports. (3) Create a framework for forensic cases for online practical training. Although some institutions or government agencies have developed an electronic data forensics training platform, the development of resources still needs to be strengthened. Other open source online platforms, such cyberdefenders and other open source training sites, are available to improve a soldier's skills. (4) Investigate new tools for forensic automation and the frontier of big data forensics[15] and artificial intelligence forensics[16].

5. Conclusions

This paper highlights the urgent need for skilled professionals in the field of digital forensics due to the increasing prevalence of cybercrime. By analyzing major digital forensics competitions worldwide, we have synthesized essential knowledge modules and proposed a

comprehensive knowledge map for training elite digital forensics talents. Our systematic approach aims to bridge the skill gap and equip professionals with the necessary expertise to combat cybercrime effectively.

Acknowledgment. Supported by the Independent Project of Intelligent Policing Key Laboratory of Sichuan Province, No. ZNJW2022ZZQN002, and Sichuan Police College Graduate Education Reform Project,No. CJYJG22B004.

References

[1] Liu Hao Yang, Yang Xiu Lei. "The current situation and challenges of electronic data forensic identification in public security organs". China Forensic Identification,2022(01):54-59.

[2] Liu Chen. "Design and practice of a comprehensive training platform for electronic data forensics". Experimental Technology and Management,2021,38(02):144-148.

[3] Xu G. T. "Construction of a network range training system for forensic capability improvement". Police Technology,2020(03):69-73.

[4] Li Bei. "Design and implementation of an electronic data forensics training system". Computer Knowledge and Technology,2022,18(09):27-29+35.

[5]Zhang P,Peng JX."Construction and practice of e-discovery courses in public security colleges and universities based on cloud platform ". China Information Technology Education,2021(14):101-107.

[6]Xu Xiaotong,Xiao Qiuhui. "Research on the practice of information management and digital forensics composite talent education in North America iSchools". Library Intelligence Knowledge,2022,39(03):83-94.

[7]Naqvi S, Sommer P, Josephs M. "A research-led practice-driven digital forensic curriculum to train next generation of cyber firefighters". 2019 IEEE Global Engineering Education Conference (EDUCON). IEEE, 2019: 1204-1211.

[8]Gupta K, Neyaz A, Shashidhar N, et al. "Digital Forensics Lab Design: A framework". 2022 10th International Symposium on Digital Forensics and Security (ISDFS). IEEE, 2022: 1-6.

[9]meiyacup."https://www.meiyacup.com/".2023

[10]changancup."http://changancup.com/".2023

[11]DFRWS.Forensic challenges. "https://dfrws.org/".(2022-09-19)

[12]honeynet. "https://www.honeynet.org/challenges/"

[13]dfir challenges."https://www.ashemery.com/dfir.html"

[14]Huiji Zhang. "Research on the Application of Artificial Intelligence in Electronic Data Forensics". China Security,2021(07):85-89.

[15]Baig Z, Khan M A, Mohammad N, et al. "Drone Forensics and Machine Learning: Sustaining the Investigation Process". Sustainability, 2022, 14(8): 4861.

[16]Hall S W, Sakzad A, Choo K K R. "Explainable artificial intelligence for digital forensics". Wiley Interdisciplinary Reviews: Forensic Science, 2022, 4(2): e1434.