Research on the Course System of Electronic Data Forensics

Min Tu
Department of Security Management Technology
Jiangxi Police College
Nanchang, China
14371789@qq.com

Jianying Xiong*
Department of Security Management Technology
Jiangxi Police College
Nanchang, China
special8212@sohu.com

***Abstract*—With the increasing of computer crimes, the value of computer data evidence is becoming more and more obvious. Electronic forensics has also become a new frontier discipline. Because this is a comprehensive discipline and needs to be compatible with many majors in police colleges, lots of factors that need to be considered in the construction of the course structure. The research will discuss the construction method of the curriculum system from the content of the subject and the goal of the discipline construction. It includes the reform of the knowledge system of electronic data forensics, the design of interdisciplinary comprehensive courses and the design of forensics courses for the multi professional background. According to the background and demand of the subject, we design the content of the knowledge and make a fixed position of curriculum. A teaching model based on the process of ability level and ability promotion is put forward to promote the construction of the new curriculum system of electronic forensics.**

Keywords—electronic data forensics; course system; teaching method; forensics training; teaching process

I. INTRODUCTION

With the development of information technology, electronic data forensics and identification have become an important research content in the field of network security science, forensic science and other fields. Electronic data forensics and identification, is also refer to "Computer Forensics". It is the activity of proof by providing the data forensics of professionals based on the principles and techniques of computer science. The professionals should to find, fix, extract, analyze, inspect, record and display electronic settings in accordance with the procedures stipulated in the law [1]. Electronic data forensics and identification involve a wide range of technical fields, which require a comprehensive use of a variety of technical knowledge to solve practical problems [2]. In every aspect of our daily life, we are increasingly dependent on digital devices; these devices are also increasingly involved in various legal investigations. Electronic data forensics is a science that related to the collection, preservation, record, inspection, analysis, and the evidence extraction from the computer, the network and other electronic devices [3]. Electronic data forensics is now an important part in criminal and civil investigations, law enforcement agencies, private investigators; data recovery and diagnosis often use its various techniques. Although electronic data forensics plays an important role in our society, it is still an emerging and rapidly developing research area [4].

The new criminal procedure law, the revision of the administrative procedure law and the Supreme Court on the interpretation of the application of the civil procedure law already set electronic data as one of the eight major evidence of the law. It is not only an effective application of Computer Science in forensic technology, but also a powerful complement to the existing information security system. However, in our country current judicial practice, our judicial officials lack the professional knowledge of electronic data forensics. It’s a top priority to carry out a timely and effective electronic data forensics professional knowledge training for all officers [5].

II. GOALS OF COURSE SYSTEM

Electronic data forensics is a new edge discipline, becasue it is a complex of of jurisprudence, criminology, investigative science, psychology, sociology, electronic science, computer science and related disciplines. We can reconstruct our course through studying these different kinds of course system that we mentioned above. Then strengthen the cross and integration between different disciplines, strengthen the content of legal knowledge and management skills in psychology, social engineering, electronic data forensics technology, network forensics, mobile device forensics, malicious software and jurisprudence. It should be to promote the reform of teaching content and teaching methods, and strive to form an adaptive course system to meet the requirements of the new era of talent training mode [6].

Our main goals of the course system can be summarized as follows: Students should be familiar with the terms, technology, and digital forensics research process, which includes electronic data forensics, network forensics, mobile device forensics sub disciplines [7]. Students should learn how to use scientific methods to carry out digital forensic investigation and the importance of doing this Students should be familiar with the different types of digital forensic evidence, and to understand the limitations of the existing technology. Students should understand the basic laws of the judicial system and the operation of the court. Students should know the relevant laws of digital evidence collection, and how they affect the practice of digital forensics. Students should understand the importance of related fields [8], such as information security, data recovery, network crime, etc..

We can achieve the goal of the course through the following methods:

A. The reforming of teach electronic data forensics theoretical knowledge.

Students should know some basic theory before practice, not just know how to do it. College graduates are not more than a professional talent to meet the needs of the market, not because they know how to perform better than those trained by professional technology, but because they have a better understanding of the technical principles and theoretical basis, so that they can better adapt and innovate in the face of new problems.

In order to achieve this purpose, in the curriculum design should focus on in-depth understanding of knowledge, rather than rote procedures and standards.For example, we can focus on the evidence of file system, reduce the size of electronic data forensics module until it can be managed, because these systems are students will be the most familiar and most likely encountered in practice.

B. Designing a interdisciplinary course system of electronic data forensics

Different disciplines have different important research views, for example, lawyers, computer scientists and psychologists have totally different opinions when they meet the electronic data forensics. Lawyers believe that it can be helpful to solve their cases; computer scientists think it is a way of operating computer; psychologists regard it as a way to understand the psychological. Our curriculum will integrate these teachers' opinions from the relevant disciplines and develop interdisciplinary module, to make students benefiting from it. Not only teaching students how to check the hard drive in the lab, but discussing how to make the electronic data forensic technology applying more widely. When facing the network intrusion cases, the investigation is often not focused on the resort to the law, but rather to assess and reduce the damage it caused, and enhanced defense later. These investigations, are fundamentally different from the criminal investigation, because the evidence is only the custody of the victim, not accepted by the court, the identity of the attacker is secondary. We also introduce students to other application areas to prove the wide of application of electronic data forensics knowledge, Such as network fraud crime investigation, to make students understanding that the survey is often not only in the use of forensic technology, but social engineering, criminal psychology, criminal investigation, resort to legal proceedings, etc.. [9]

C. The curriculum is designed to be suitable for students from all kinds of subjects.

We believe that electronic data forensics courses will become an important supplement to many students' education, even if they do not intend to become a electronic data forensics professional. In the course, there are a lot of topics that are important to everyone, such as the majority of students know less about the legal system and the law related to computer crime. In addition, a lot of students want to know how the evidence from the computer and the network can be better to guide practice activities, such as the legal professional students interested in electronic data forensics, they can better understand and use electronic data forensics knowledge in the case. However, designing a electronic data forensics course for a variety of professional students is very difficult [10].

III. Make Teaching Content

The electronic data forensics course involves many contents, such as computer crime legal countermeasures (Law), computer crime (Criminology), Internet Security and prevent hackers (Psychology, social engineering, computer networks, etc.), network security protection technology (Information Security), information encryption (cryptography), which computer technology is part of the main, but not the only one, the formulation of the teaching content should break through the limitation of subject, the sequence knowledge, the teaching ideas, reflecting the application, comprehensive, scientific and interest.

Electronic data forensics teaching must go through the reconstructing of the different kind of course that we mentioned above, then strengthen the cross and integration between different disciplines, strengthen the content of legal knowledge and management skills in psychology, social engineering, electronic data forensics,network forensics,mobile device forensics, malicious software and jurisprudence.

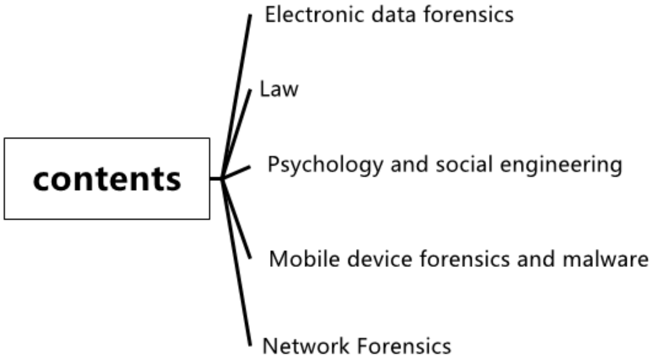
contents
Electronic data forensics
Law
Psychology and social engineering
Mobile device forensics and malware
Network Forensics

Fig. 1. Knowledge involved

The contents of the course include the following five major modules:

1) Psychology and social engineering

Criminal psychology, crime analysis, social engineering, etc..

2) Law

Evidence science, relevant laws of computer crime, the legal process, laws and ethics, etc.

3) *Electronic data forensics*

File system analysis, file recovery, registry, log file, link file analysis, Web browser forensics, e-mail evidence, EXIF, etc..

4) *Network Forensics*

Protocol analysis, data packet analysis, traffic analysis, network intrusion detection and analysis, etc..

5) *Mobile device forensics and malware*

Mobile device technology, mobile device forensics and analysis, network evidence of mobile devices, the classification and detection of malicious software, etc..

IV. Design the teaching process

Education couldn't be a one-way input that student acquire knowledge from the teacher,and the teaching must according to students' aptitude. The course of electronic data forensics course can be designed as an open case teaching process.

In order to develop a digital forensics course that is consistent with the nature of the cross disciplinary nature, the curriculum development team can be formed, This team includes computer technology, computer network security, law, civil and criminal investigation, fraud investigation, psychology and sociology experts, Take modular approach to develop the courses, the leading professional experts to develop their professional field of teaching module, these modules are connected to become a coherent teaching, to make students accessing to the important point of the field of digital forensics.

In order to improve the smoothness of the transition between modules, make the theme more clear, we can design a fictional case throughout the course. Case studies will be carried out along with the progress of the study; new cases and assignments will be tied to the case to keep the students interested.

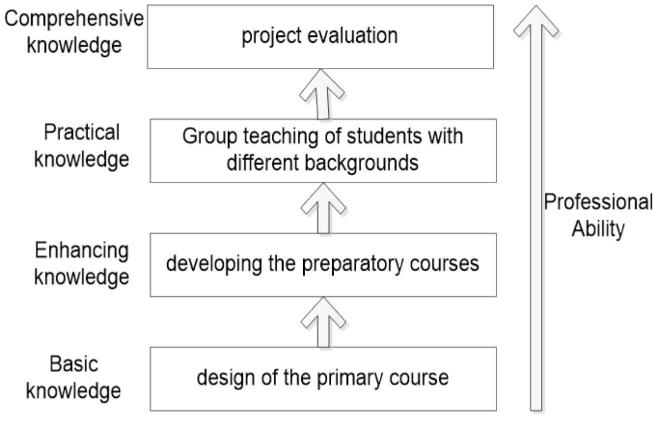
Comprehensive knowledge
project evaluation
Practical knowledge
Group teaching of students with different backgrounds
Enhancing knowledge
developing the preparatory courses
Basic knowledge
design of the primary course
Professional Ability

Fig. 2. Teaching process

In the design of modules sequence, before the technical materials ,we will learn the legal module. Because these modules provide a wider social impact for electronic data forensics, and shows how to use electronic data forensics in court, which will enable students to learn how to use the knowledge of digital evidence, and why should implement digital forensics.

In order to improve the teaching effect, the following methods are implemented in the teaching process as fig 1.

First, the design of the primary course. Mainly from various disciplines to introduce the field of digital forensics, the focus is on the computer forensics, network forensics and mobile device forensics branch disciplines, and to provide the relevant views of other disciplines. It is difficult to introduce digital evidence in one field, and it must cover the main sub discipline, and introduce the views of many other subjects, and increase the breadth of the subject of the introduction course.

Second, developing the preparatory courses. Basic technical knowledge that may be given to the students before the class. It will include some important knowledge into the basic concept of interpretation, to wake up the memory of the students who might have learned the knowledge, and also to have a more profound reading of the students who lack relevant knowledge.

Third, Group teaching of students with different backgrounds. In the latter part of the course, the students can be divided into groups, with different backgrounds, students can look at the problem from different angles, use the knowledge of the course to investigate the problem and analyze the evidence, so that all the students can get a better understanding of the learning problem.

Fourth, the project evaluation. Team project is an important part of the exam, the teacher give assessment results according to the case study analysis, project demonstration and the case of the respondent.

When building team project team, the students of law major must be in partnership with the students majoring in computer science. In the development of team work, the project of the law and computer professional students play different roles, they submitted a virtual case report together. They can learn from each other when the project team practices, so that students can solve the problem by using the knowledge of their professional knowledge better.

V. Conclusion

Electronic data forensics is a very practical subject, so it must be attached great importance to the cultivation of professional practice. Practice should be carried out throughout the learning process, the actual combat skills training must be combined with teaching, and students must be organized to participate in electronic data forensics cases of comprehensive practice training, these will achieve the goals of training.

References

[1] Research on the Standard System of Electronic Data Examination, Chinese Journal of Forensic Sciences, 2011, 1,49-52, In Chinese.

[2] Tang, Ling. "The Education and Study of Electronic Data." Applied Mechanics & Materials 644-650(2014):5655-5658.

[3] Sun, Cui. "Study on Investigation and Forensics by Computer under Cloud Computing Environment." International Conference on Management, Computer and Education Informatization 2015.

[4] Anthony Lang, Masooda Bashir, Roy Campbell, Lizanne DeStefano. Developing a new digital forensics curriculum. Digital Investigation 11 (2014) S76-S84

[5] Fahdi, M. Al, et al. "A suspect-oriented intelligent and automated computer forensic analysis." Digital Investigation 18(2016):65-76.

[6] Tu Min. Computer crime investigation course system research. Information Security, 2009.10, In Chinese.

[7] Zhu, Shijie. "Research of Computer Network Crimes Investigation and Legal Supervision Measures." International Conference on Education, Social Science, Management and Sports 2017.

[8] Na, Li. "Research on Computers Applied to Investigating Criminal Cases on the Crime Scene." Applied Mechanics & Materials 687-691(2014):4666-4669.

[9] ACM/IEEE-CS Joint Task Force on Computing Curricula. Computer Science Curricula 2013 [Tech. rep.]. ACM Press and IEEE Computer Society Press; December 2013.

[10] Chi H, Dix-Richardson F, Evans D. Designing a electronic data forensics con-centration for cross-disciplinary undergraduate students. In: Pro-ceding's of the 2010 Information Security Curriculum Development Conference. New York, NY, USA: ACM; 2010. pp. 52-7.