SHS Web of Conferences **25**, 02014 (2016) DOI: 10.1051/shsconf/20162502014
ICITCE 2015

The work about the cybercrime and computer forensics course

Ling Tang*
Department of Information Science and Technology, East China University of Political Science and Law, Shanghai, China

ABSTRACT: Currently, along with the maturity and widespread of computer technology and Internet, cybercrime are worsening. Therefore, it not only brings harm to the society, but also brings problems to traditional forensics. So it is very important for the university to develop a related course and train students to deal with information crime and computer forensics. East China University of Politics and Law has set up a college course named cybercrime and computer forensics for undergraduate students for six years and done some researches. Both of them get great achievements.

Keywords: computer forensics; cybercrime; teaching; research

1 INTRODUCTION

Nowadays, we are living in an information era. That is to say, computer technology and Internet service have become one part of outlives. However, information security and crime problems are increasingly serious. For example, in U.S.A, the economic damage caused by hackers' attack is about 10 billion dollar every year. In China, the amount of IP address which is controlled by hackers is about 1 million, and there are 42 thousand websites which are hacked. Every month, 1.8 million computers are infected by computer virus, which accounts for 30% of the global total.

All in all, information security and internet crime have interrupted our lives seriously, and have threatened national security and society fortune. So it is very important to maintain computer system and internet security. That leads to a new research point: cybercrime and computer forensics.

Many universities have studied the aforementioned problem for years. But usually they divide the problem in two different parts, one is set as complementarity or research point for information security; and the other is forensics and law for law school. It goes without saying to set a course for college students.

Actually, cybercrime and computer forensics is a problem combined with computer science and forensics including law issue. It is better to regard the problem as an intersecting subject rather than two different parts. And it is necessary to set up a course named cybercrime and computer forensics for college students either major in computer science or in other specialties.

East China University of Politics and Law (ECUPL for short) has researched the problem for eight years, and a university course called cybercrime and computer forensics has been taught for six years. The author joined and accomplished several research projects including national project in succession. The author is the core teacher of the course and is also one of the authors of the teaching material. The author has taught the class for five years, 703 students whom major in computer science, law, business and other departments are included. Based on these education and research experience, the author stared her own postdoctoral work in 2011.

2 BACKGROUND OF IN FORMATION SECURITY AND COMPUTER FORENSICS

2.1 *Definition of computer forensics*

Initially, Judd Robbins (senior computer forensic experts) brought out the point that computer forensics is based on the investigation and the analysis techniques which applies to the potential, legal effect evidence. SANS Company believes that computer forensics is

*Corresponding author: ausflug163@163.com

the kind of software and tools, which extract and protect the evidence of computer crime according to some pre-defined procedures, comprehensive examination of computers and related systems [1].

In China, the computer forensics is defined as: computer forensics refers to the court accepted, sufficiently reliable and persuasive electronic evidence which exists in computers and related peripherals device. Other experts consider that computer forensics is a process can confirm, protect, extract and file electronic evidence which exists in computer and related peripherals, and can make it acceptable and reliable by court. [2]

2.2 *Characters*

Computer forensics technology, compared with the traditional ones, has its own characteristics:

1) Digital: the material carriers of computer evidence are electronic components, magnetic materials, etc. IF the perpetrator deliberately operates, changes data or programs from the physical representation. The results are only positive and negative electronic integrated circuits or magnetic magnets. To identify this operation, the methods require special tools, and are entirely different from the traditional ones.
2) Technical: the generation, transmission and storage and collection, analysis and judgments of computer evidence are by means of computer science technology, storage technology and network communication technology.
3) Vulnerability: As the computer information and electronic evidence can easily be modified and be real changed (irreversible changes) without leaving any traces, so that there is a fragile and unreliable side in computer information. It is very common to know that manipulation of data and the destruction of the program are very universal. And because the computer's processing speed becomes faster and faster, the data changes are instantaneous, the computer evidence is sometimes unreliable [3].
4) Easily transmitted: With the popularity of Internet technology, a lot of electronic documents such as Email, E-file, etc. can be quickly transferred around the world, which have caused lots of difficulty for the evidence collection either in time or in space.
5) Human factors: As the computer and network related equipment operation are maintained by operators and system administrators, which need to consider the impact of human factors on the device. The process of computer forensics and equipment should be analyzed in two ways, one is human, and the other is equipment.

3 THE RESEARCH WORK OFCYBERCRIME AND COMPUTER FORENSICS

3.1 *International research work*

The first cybercrime case happened in the U.S.A. With the foundation of CART (Computer Analysis and Response Team) [4], this indicates the beginning of the research for cybercrime. As the appearance of Internet, more and more experts and professors started this research.

The FIRST (Forum of Incident Response and Security Teams) was formed in 1990 in response to this problem [5]. Since that time, it has continued to grow and evolve in response to the changing needs of the incident response and security teams and their constituencies. FIRST brings together a wide variety of security and incident response teams including especially product security teams from the government, commercial, and academic sectors. By the year of 2012, FIRST has organized 24 conferences on Computer Security Incident Handling.These annual conferences are a 4-5 day global event that focuses on the issues of incident response and security teams and brings together incident response and security professionals from around the world who share their experiences and expertise. Security professionals in all areas will find the interaction with incident response teams educational. It promotes the development of cybercrime and computer forensics.

3.2 *Research work in China*

In 1986, the first cybercrime was found in China. Since then, the related research work has begun. The earlier research result and paper was published in 2002 [6]. Some national research projects has completed, such as electronic data forensics technology (from 2001-2005), National Social Science Foundation of China 2002: computer forensics and relevant legal issues. It reflects the academic standards of China in the earlier time.

In 2004-2010, there was several conferences focus on computer forensics in China. They put a positive impact on cybercrime and related theory, and promoted the development of China's electronic forensics technology.

In the year 2010 and 2011, there were several papers about computer forensics [7][8]. This indicates the widespread of the research work.

In 2011, the 3rd National Computer Forensics Seminar was held by ECUPL [9]. In the conference, several experts and professors conducted their academic reports and exchanged their ideas. Some research work was very excellent, such as the lab development for computer forensics, the practices of computer forensics and the law issue of computer forensics. The author took the speech of the introduction of cybercrime and computer forensics course for undergradu-

ate students .These academic exchange programs impact the research work in China positively.

4 LAYOUT OF TEXT EDUCATION OF INFORMATION SECURITY AND COMPUTER FORENSICS FOR UNIVERSITY STUDENTS

This part introduces the course itself. The achievement will be brought forth. The reason of its success will be discussed. The future will be designed. And even more, the status of the course all over the word will also be expounded.

4.1 *The status of the course*

This course is a new subject. At first, it was called computer forensics, which was a complementarity to information security specialty. In the recent years, several universities all over the word began to set up special computer forensics subject and some teaching work has started. At the same time, some research institutions also joined in this field. For example, Canterbury Christ Church University sets up the Master Degree of Science in Forensic Computing [10]. It brings together every important aspect of digital forensic examination to support criminal investigation involving digital evidence. The subject areas covered in this outline achieves a balance between the practice and their underpinning theory. As such it is ideally suited for those who are already engaged, or are aiming to develop a career in law enforcement or associated areas both in the UK and elsewhere. In U.S.A., the center of security information system provides some related courses for the Master. California University established the lab for computer security and has begun some technical research.

We can see that these institutions treat the course as a master course or a research point. None of them set up the course in undergraduate education period. This is regret for the college students. And also it is not fit for the situation of cybercrime.

In China, computer forensics course are only set up for professional police school or set up as a supplement for traditional forensics school. None of the colleges or universities has set up a related course for undergraduate students.

However, in ECUPL, a course called cybercrime and computer forensics has set up for six years; it is open to the undergraduate students and gets great teaching effect.

4.2 *The course in ECUPL*

ECUPL is a University famous of law school for sixty years. It is one of the first legal universities in China. So undoubtedly, it owns abundant legal background.

The course is setup by the Department of information science and technology, Criminalistics School. The Criminalistics School has stated forensic education and research for more than twenty years. So based on these academic background, we set up the course named cybercrime and computer forensics as a character subject. It combines computer science and forensics technology even legal knowledge together, and interdisciplinary among each disciplines. We set the course as a professional characteristics class.

In 2005, some research work of cybercrime and computer forensics has started [11]. The investigation and evaluation of setting a curse has lasted for 2 years. Finally, the Department decided to set up the course.

In 2007, the course was started. Up to now, it is accumulated that six grades students in the Department with the amount of nearly 600 have been taught. So the author gets a lot of teaching experience. At first, the course is set as a required class for the students of Department of information science and technology.

At the same time, with our investigation, many students in ECUPL are interested in this filed. Thus, in 2009, an elective public class for all of the students in ECUPL was set up. It is set up for five semesters and about 900 students are taught so far.

It should be noted that the required class and the elective class are different and have their own characters. The former is a professional class, and the students are major in computer science. So it is difficulty of profession and requires seven experiments. The latter is for all of the students in the university. Most of them come from legal school, business school, even from sociology school. So considering their background and their intension are for broadening their knowledge, the difficulty of the class is reduced, the interest of the class is enhanced. Some information security knowledge even some skills to prevent their computers form hackers are taught in class. As to the professional experiments, they are demonstrated by teacher instead of practicing by students.

From the students achievements and their evaluation of the class， we can see that the course is not only competent for a professional characteristics class, but also can improve the knowledge of cybercrime and computer forensics for the students all over the university, and to widen their knowledge. So we can draw the conclusion that the course gets satisfying teaching effects.

5 THE COURSE IN DETAILS

In this section, the details of the course will be introduced. And the achievement of the students will also been shown. The teaching material will be discussed.

5.1 *The required course in detail*

At first, the course was 3 credits, that is to say, there were three continuous classes ever week, including experiment class. But after a period of teaching, we

found that this is not fit for the need of teaching. Cybercrime and computer forensics demand too much knowledge for computer science, forensics technology and law. And three continuous classes were too difficult for the students to study and understand the knowledge. It even increased the fear of hardship among the students.

So we adjusted the teaching plan. First, the course is changed into 4 credits, which means 4 classes are taught every week. The 4 classes are divided into 2 parts. The course is taught for 2 times every week, each time there are only 2 continuous classes. And considering the difficulty of the course, there is at least one -day interval between 2 times of teaching. For example, 2 classes are set on Tuesday, the other are set on Thursday. So on Wednesday, the students can have sufficient time to review and preview the course. According to effect of the students, this adjustment achieves great results.

Nowadays, the course includes information security, cybercrime, the invasion of computer, computer forensics, the collecting of electronic evidence, the recovery of electronic data, the analysis and evaluation of electronic evidence, the tools of computer forensics, and the introduction to some related laws. It covers the knowledge of information security, computer science, and cybercrime and computer forensics. It is the most comprehensive and professional course so far.

This course requires not only theoretical exploration but also practice capacity. So the teacher attaches great importance to the experiment. There are seven experiments in this class, including the recovery of hard disk, the encryption and decryption of electronic data, the forensics of computer log system, and sniffer on Internet. The department invested 2 million RMB to build a professional internet and information lab. And bought some software, hardware and supporting equipment .Now it can support about 50 students to practice at the same time. In order to improve the effect of experiments, the lab is divided into 8 groups; each one is settled by a hexagonal lab table and can form a subnet. Every group is connected by network with each other. The teacher's computer is set as server to connect with Internet. The students in each group can cooperate with each other to complete the experiment. And the teacher also can arrange a simulated computer attack and defense scene. Some groups act as the roles of hackers. Some act as the roles of computer forensics experts. So they can interact with each other and the interest of the class is improved [12].

These experiments not only consolidate the theoretical knowledge, but also improve their practice capacity. It is because of our attention to the experiments; our students can not only get excellent ranking in related competition, but also be popular with employers. At the end of each experiment, the students should finish their experimental reports. In order to be strict with quality of the class, the teacher always checks their results by random .Their score will be part of their final grade.

5.2 *The elective class in detail*

As mentioned above, there is an elective class with the same name but different class ID and difficulty in the university. It is open to all of the students in the university and is set for 2 classes every week. Considering the conflict with their professional classes, the course is arranged in the evening. And due to their knowledge of computer science is not professional, the difficulty is decreased. The assessment method of the class is more flexible, most of the time; the exam is the demand of an article. As to the experiments, owing to their lack of computer science knowledge, the teacher demonstrates the experiments in lab instead of the traditional experiment manners. In this way, not only has the burden of the students been lightened, but also can learn through practice.

The source of students comes from more than five schools. Most of the students (45%) come from law school. It validates the character of the course: combining computer science with forensics and law issues. 21% of the students are from business school. With the development of electronic business, more and more business disputes or crimes involve electronic data, such as electronic signature, electronic accounting. This leads to the concern of computer forensics. It is a new challenge and requirement for forensic accounting. Nowadays, more and more experts have realized this problem. For example, in 2010, China University of Political Science and Law began to recruit he students major in electronic forensic accounting for Master Degree [13]. In the ECUPL, some graduate students in business school also do some research in electronic forensic accounting. But as the above mentioned content in this paper, due to the students are lack of cybercrime and computer forensics education background in undergraduate period, they have difficulty in understanding this concept. So the elective course is a good introduction or complementarity for them. Thus, this explains the percent of business school in this course.18% of the students are from intellectual property rights school. At present, with the popularity of computers and the Internet, many works, audio and video products are made from electronic form. So their copyrights are easily pirated and are difficult to be tracked. This situation results in the focus of computer forensics whether in cases or in research. Other students are from foreign language school, sociology school, etc. They choose this course because of interest. So they put great enthusiasm in learning this course. In the latter part of this paper, the author will explain why some students are good at their research work and bring out some innovation view in this field.

In conclusion, by the use of scientific teaching methods, the author succeeds in teaching the course as a required one and an elective one against different

students.

5.3 *The interactive between teacher and student in class*

As a teacher, the author thinks that teaching in class does not simply mean imparting what is written in the book. It is also very important to train their capability to gain knowledge by themselves, to inspire their capability to discover new fields.

So the author is keeping on discovering pluralistic teaching mode. Through PPT and other Multimedia courseware, the class becomes more interesting. In class, the teacher not only teaches the knowledge in book, but also combines the actual cases with professional technology. So the students can enhance their understanding of the knowledge. What's more, the teacher usually ask the students to suppose themselves as hackers or a computer forensics experts, and what would they do in the supposed scene and why they do so. As a result, the interactive between the teacher and the students is improved.

In order to train their innovation capability, 3 or 5 students constitute several research teams voluntarily. They are asked to do some research of cybercrime or computer forensics. The subject is chosen by themselves. At the end of the semester, each team should stand on the podium and demonstrate their research results. Their performance will infect their final scores.

The author compares the students' performance of the required class with the elective class. The results is a little unexpectedly but reasonable. Speaking of the passion, the elective class is more passionate than the required class. Although the former's research is not as professional as the latter's, the former's subjects are more innovative. For example, one team from sociology school studied the hacker phenomena, instead of focus on computer technology; they discussed it from the angle of view of culture, even raised to philosophical perspective. And their view is very innovative and reasonable .They won the applause for a long time and got A naturally.

The author thinks that it is because the students whom select the elective class are really interested in this field, their research are more innovative and most of them are based on their professional knowledge, such as law, sociology, business, etc. The students in computer science department treat the class as a professional class. The research is a task to them; some of them learn it just for grades. As a teacher, the author knows the interest is the best guider. So the difference is obvious.

Meanwhile, the teacher sets up the online class through Internet. The students can communicate with the teacher after class; it is a very useful complement to the rational teaching method.

All in all, according to the above method, the atmosphere in class becomes active, the interest and effect of the students are inspired. The achievement is excellent naturally.

5.4 *The build of teaching material*

At first, we used a teaching material named Internet crime and computer forensics. But as time went on, we found that it was not fit for the class. For example, crime on Internet is only a part of cybercrime. There are other forms of crime, such as mobile crime, PDA crime, etc. With our research of the teaching material market, we drew the conclusion that none of the books meet our need. And Based on our teaching experience, in2009, our department and Dr. Qi Man in Canterbury Christ church university decided to wrote a teaching material by ourselves. The book is named as <information crime and computer forensics>, published by Beijing University publishing house. The author wrote chapter five: the discovery and collecting of electronic evidence. The chapter is about 50,000 words. In September, 2010, the book is put into practice. Up to now, students from 4 grades have used them, and get satisfactory results. In 2011, the book is horned as the second prize of excellent teaching material of university in Shanghai 2011.In 2016, the book will be reprinted. What's more, there will be a training course books as companion.

5.5 *The achievement of the students*

After class, the author organize several research teams voluntarily, they can discover the field of cybercrime and computer forensics by interest. Two of them are very excellent, and get the support of the university fund for students.

In 2008, the author led two teams of students to join in the 1st information security competition of all universities in Shanghai. One team is honored as the runner-up, and the other team is honored as the prize for excellence. It should be noted that the runner-up won the championship in the experiment section and over time section, only lost in the test paper section. It was a satisfying record.

As to the student employment, due to the course meets the need of the employers. So the students can not only become a normally called software engineer, but also get jobs as the engineer of computer forensics development, or become a forensics expert or a network policeman. It reaches the target of bring up the interdisciplinary and integrated application talents.

6 THE IDEAS FOR THE FUTURE WORK

With the development of computer technology, new cybercrime comes out endlessly. So the computer forensics has to keep on developing. So the author needs improve the teaching work, surmise and optimize the experience of teaching. Enlarge the current

teaching achievement, improve the quality of teaching. The concrete methods are the following:

1) The teachers keep on join in the training class to improve themselves. Pay close attention to the latest development of this discipline, and make it useful in the teaching process. So the students can grasp the latest developments.
2) The teachers should continue to organize the students to join in the related competition, to put their knowledge into practice and resolve the actual problems. It is complementary to the teaching in class.
3) The teachers use more flexible and more multiform way to examine the students. The aim of the exam is not for score but for the students to grasp the knowledge and comprehend the progress of the discipline. And to improve the creativity and research capability.

7 SUM UP

In this article, the author introduces the current situation of cybercrime and computer forensics and the production of the class. Based on this, the author summarizes the development and thinks about the trend of the discipline. Information crime and computer forensics is a cross subject. It combines computer science with forensics and law. Although it is a young subject, it is a super excellence way to resolve the increasingly serious cybercrime situation. Thus, the subject will develop very soon. The author hopes that more and more scholars and professionals can devote to the construction and research of this subject.

ACKNOWLEDGEMENT

This work is financially supported by the National Social Science Foundation of China (No.11BFX125); Science Foundation of ECUPL (BM518549); Building the Course of ECUPL (A-333-13-12754); National Social Important Science Foundation of China (No.C-6501-14-06101).

REFERENCES

[1] Robbins, Judd. An Explanation of Computer Forensics. URL: http://www.computerforensics.net/forensics.htm.
[2] Chen Long, Mai Yonghao & Huang Chuanhe. 2007. *The Technology of Computer Forensics*, Wuhan: Wuhan University Publishing House, pp.1-10.
[3] Peter Sommer: Computer Forensics: An Introduction. URL: http://www.virtualcity.co.uk/vcaforens.htm
[4] Wang Qingqing. 2004. *The Emerging Response and Computer Forensics (2nd edition)*, Beijing: Qinghua University Publishing House, pp.3-15.
[5] URL: http://www.first.org
[6] Zhao Xiaomin & Chen Qingzhang. 2002. New issue in combating computer crime-computer forensics. *Technology, Information Network Security*, 9,
[7] Lin Ying, Zhang Yan & Ou Yang Jia, 2010. The log detection technology in computer forensics. *Computer Technology and Development*, 06,
[8] Xu Tai & Zhao Xijing, 2011. The research of computer forensics, *The Value of Engineering*, 12.
[9] Ai Nayan. 2010. The review of the 3rd National Computer Forensics Seminar. *The Research of Crime*, 10.
[10] URL:http://www.canterbury.ac.uk/studyhere/HomeNew.aspx
[11] Dang Enhong. 2007. The analysis of computer forensics. *China Water Transport*, 08.
[12] Song Xiuli, Chen Long & Deng Hongyao. The discovery of computer forensics experiments teaching, 26(16).
[13] URL: http://gate.cupl.edu.cn/yjsy