The Study of Computer Forensics Based on the Course Construction and Reform

Ling Tang
Dept. Information Science and Technology, East China University of Political Science and Law
Shanghai, China, 201620
E-mail: ausflug163@163.com

***Abstract*—Computer forensics has been an important part among computer science. . There is a course with the name college course named information crime in East China University of Political Science and Law. It has been set up since 2007. In this eight year ,the course get great achievements and honours. Besides, some research work have been carried out based on the course .**

Keywords-component; computer forensics; reform;research.

I. INTRODUCTION

Nowadays, 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, these 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: information crime 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, information crime 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 information crime 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 information crime 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 six years, 855 students whom major in computer science, law, business and other departments are included.

This work is supported by National Social Science Foundation of China (No.11BFX125)
This work is supported by Science Foundation of ECUPL (BM518549)
This work is supported by China Law Society CLS 2013(2013)D171

II. THE RESEARCH OF COMPUTER FORENSICS

A. International research work

The first information crime case happened in the U.S.A. With the foundation of CART(Computer Analysis and Response Team) [1], this indicates the beginning of the research for information crime . 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[2]. 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 information crime and computer forensics.

B. Research work in China

In 1986, the first information crime was found in China. Since then, the related research work has begun. The earlier research result and paper was published in 2002[3].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 information crime and related theory, and promoted the development of China's electronic forensics technology.

In the year2010 and 2011, there were several papers about computer forensics[4][5] .This indicates the widespread of the research work .

In 2011, the 3rd national computer forensics Seminar was held by ECUPL [6]. 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 information crime and computer forensics course for undergraduate students. In 2014, there will be a conference about new technology in computer forensics in ECUPL.

These academic exchange programs impact the research work in China positively. They introduce information security and computer forensics to university students.

III. THE COURSE OF INFORMATION CRIME AND COMPUTER FORENSICS

A. *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 [7]. 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 information crime.

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 information crime and computer forensics has set up for eight years; it is open to the undergraduate students and gets great teaching effect.

B. *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 set up 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 information crime 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 information crime and computer forensics has started [8]. 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 eight grades students in the Department with the amount of 4103 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 445 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 information crime 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.

IV. THE REFORM OF THE COURSE

A. *The reform for the course*

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, the author found that this is not fit for the need of teaching. Information crime and computer forensics demands 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 the author 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, information crime, 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 information crime 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 2million 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 [10].

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.

B. The reform of teaching method t 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 the 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 information crime 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 author set 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.

C. The editing of teaching book

At first, we used a teaching book 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 information crime. 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 book 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 was put into practice. Up to now, the students from 6 grades have used them, and get satisfactory results.

In this summer of 2014, we decide to publish a new teaching book based on our research .Experimental material, to improve the construction of teaching material.

V. RESEARCH WORK AND HONOURS

As a teacher in university, research is also an important work. It is well known that through research, the teacher can improve their professional quality, widen their knowledge. And put the research results into teaching, to further improve the quality of teaching.

A. The achievement of the course

In 2011, the book was honored as the second prize of excellent teaching book of universities in Shanghai .And the teaching book was honored as the first prize of excellent teaching book of ECUPL.

In 2012, the author was honored as the third prize of excellent teaching achievement of ECUPL. The honor is based on the research of this course and article about the education of the course.

In 2013, the course was honored as Important Class of universities in Shanghai.

B. The achievement of the students

After class, the author organize several research teams voluntarily, they can discover the field of information crime and computer forensics by interest.

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, 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 failed in the test paper section. It was a satisfying record.

In 2011, the author mentored 5students in class. They applied for a project named as the creation plan for students in Shanghai Universities. They get the project and have completed the project very well.

C. The research work

The author takes charge of the course for six years. And have get some results based on the course and research. In 2010, a teaching reform project based on the course has been accomplished by the author .In 2011, a project called key course in ECUPL based on the course has also been accomplished by the author. In 2013, the author took charge of *Un*dergraduate course construction in ECUPL based on the course; the project will be finished in 2014.

In 2011, the author joined the research team of National Social Science Foundation of China. In 2013, the author was in charge of a project from China law Society.

In 2011, the author stared her own postdoctoral work, this year 2014, the author will complete her research work and graduated from post doctor working station.

VI. THE FUTURE WORK AND THE CONCLUSION

In this summer 2014, the teaching book will be upgraded. It is planed that there are two books. One is for teaching in class, and the other is a guidance book for experiments. The books will describe the new problems such as big data, mobile device forensics.

In 2015, a book named some related law issues about computer forensics will be written by the author and be published.

With the development of computer technology, new information crime 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.

Information crime and computer forensics is a key course. It related with computer science, forensics and law. Although it is a young subject, it has been developed very fast. The author hopes that more and more scholars and students join in the teaching and research of this area.

REFERENCES

[1] Wang qingqing, The emergy response and computer forensics（2nd edition）, QingHua University Publishing house,2004,pp3-15.

[2] URL:http://www.first.org

[3] Zhao Xiao Min,Chen Qing Zhang.New Issue in Combating Computer Crime- Computer Forensics.Technology,Information Network Security,Vol09,2002.

[4] Lin Ying,Zhang Yan,Ou Yang Jia,the Log Dection Technology In Computer Forensics.Compuer Technology and Development,vol06,2010

[5] Xu Tai,Zhao Xi Jing,the Research of Computer Forensics,The Value of Engineering,vol12,2011.

[6] Ai Na Yan, The Review of the 3rd the 3rd national computer forensics Seminar. The Research of Crime, vol10(2010)

[7] URL: http://www.canterbury.ac.uk/studyhere/HomeNew.aspx

[8] Dang En Hong, the Analssis of computer forensics.China Water Transport.vol08,2007

[9] Song XiuLi, Chen Long, Deng HongYao.The discovery of computer foensics experiments teahing, vol26(16,2007)

[10] URL:http://gate.cupl.edu.cn/yjsy