Experimental teaching of a digital forensics course based on a cloud computing platform

Xiuli Song†, Hongyao Deng‡, Long Chen† & Zhenlin Wang†

Chongqing University of Posts and Telecommunications, Chongqing, People's Republic of China†
Yangtze Normal University, Chongqing, People's Republic of China‡

ABSTRACT: A novel experimental teaching method for a digital forensics course is presented in this article. The method divides the experimental teaching into two parts. One is 16 experiment lesson times on the ordinary forensics platform, and the other is eight experiment lesson times on the cloud forensics platform. Undergraduate students participating in the forensics experiments include information security, law and computer science majors. The students of different majors have differing theoretical foundation knowledge, but the forensics experimental teaching improves most students' class attendance and greatly increases their interest in learning. It was found that the experimental teaching, especially on a cloud forensics platform, broadens all students' horizons and knowledge of cloud forensics technology.

INTRODUCTION

At present, the digital forensics course at Chongqing University of Posts and Telecommunications has broken from the knowledge framework of a single subject to become a cross-subject curriculum, and the content of it involves many different disciplines including law, investigation science and computer science. The digital forensics course is tightly integrated with other computer security courses. Before taking this course, students should have learned such subjects as computer networks, modern cryptography, information security conspectus, information security regulations, and so on. This means the students should have mastered solid theoretical foundation knowledge and have learnt basic professional skills.

In spring 2005, Chongqing University of Posts and Telecommunications first offered the course, *Computer Crime and Criminal Psychology* for the students of law major. In spring 2007, the course was renamed *Computer Forensics Technology* for undergraduate students studying information security or computer science as majors. The course is compulsory for law and information security majors and is an elective for computer science majors. It helps undergraduate students to learn to solve digital forensics problems. Since the autumn of 2010, it has been structured for undergraduates as an elaborate set of curricula leading to an information security major.

The authors in this article use the term *Digital Forensics Course* as adopted by the Laboratory of Digital Forensics and Preservation (LDFP). The Laboratory was jointly begun by the central and local governments in 2011, and its experimental equipment and training facilities are displayed at Chongqing University of Posts and Telecommunications. The reason why the course was renamed is because digital forensics technology not only collects digital evidence from computer systems and computer networks, but it also collects digital evidence from all digital devices, such as mobile phone, GPS, PDA, iPhone, MP3 and MP4 [1].

BACKGROUND

Over the past 20 years, foreign countries have paid more attention to the research and teaching of digital forensics. For example, in the last century, the mid-90's, the Royal College of Military Science at Shrivenham in the UK initially set up a series of short courses on computer forensics for law enforcement, military and security services, and later began to offer a regular forensics curriculum. Mississippi State University was also early in setting up the Computer Security Research Center [2]. In the centre's laboratory, there was some computer forensics software and tools for teaching and research on crime forensics. The centre offered a computer forensics course as *computer crime and forensics technology*.

However, the digital forensics course was set up differently in China by the gradual addition of forensics content to other relevant courses. The digital forensics course is finally being offered in some universities. In 2001, the China Criminal Police College added digital forensics technology to the criminal investigation course. In autumn 2002, the first undergraduate students to study a major in information security were enrolled to learn electronic forensics. At present, more than 20 institutions, including Wuhan University, East China University of Political Science and Law, and Hunan University of Science and Technology, have offered some courses related to digital forensics.

Chongqing University of Posts and Telecommunications is one of the first institutions in China to open a digital forensics course. When the University offered the digital forensics course in 2005, the textbook used for the course was *Computer Forensics: Incident Response Essentials*, by Warren G. Kruse and Jay G. Heiser [3]. Since 2007, the textbook used by the University teaching staff is Chen Long's *Computer Forensics Technology* [4], supplemented with Chad Steel's *Windows Forensics: The Field Guide for Corporate Computer Investigations* [5], and Chris Prosise's *Incident Response and Computer Forensics* [6]. In teaching, all of the textbook content is divided into six theory topic areas: the ethics and the law; basic forensic technology; Windows/Linux forensics; network forensics; digital device forensics; and case analysis. Table 1 shows the theory topics and lesson hours of the six topic areas.

Table 1: The theory topics and lesson hours of the digital forensics course.

Theory topics	Lesson hours
Ethics and the law	4
Basic forensic technology	8
Windows/Linux forensics	8
Network forensics	8
Digital device forensics	8
Case analysis	4

In recent years, cloud forensics has become *hot* new research in the forensics field. Cloud forensics is a cross-discipline of cloud computing and digital forensics. Cloud computing is a shared collection of configurable networked resources (e.g. networks, servers, storage, applications and services) that can be reconfigured quickly with minimal effort [7]. Digital forensics is the application of computer science principles to acquire digital evidence for presentation in a court of law.

Cloud forensic investigations are likely to involve evidence acquisition, and preservation and analysis in a cloud. From the investigators' perspective, storing digital evidence remotely in a cloud has appealing benefits: a relieving of the burden for storage management, and avoiding capital expenditure on hardware, software and maintenance personnel [8].

In teaching digital forensics, it is important that theory is combined with practice. Through experimental teaching of this course, students can not only become familiar with the principles and methodologies of digital forensics, but they also can master forensics processes, techniques and tools relevant to the six topic areas listed above. At last, this course will develop students' manipulative ability and experimental skills, as well as cultivating good team spirit and science literacy. To help students improve their practical capability and advanced knowledge of digital forensics, this course provides hands-on experiment exercises on an ordinary forensic platform and cloud platform.

THE EXPERIMENTS ON AN ORDINARY FORENSICS PLATFORM

Since 2005, forensic experiments have been considered necessary, along with in-class teaching, for practical learning. But then, there was no special forensics laboratory and no ready-made forensic software, hardware and tools to carry out experiments. In the absence of a funding subsidisation, the authors downloaded some free forensic software and tools from the Internet to carry out experiments with the aid of the Fundamental Laboratory of Computer Science Department (FLCSD). The FLCSD owned 30 computers, and each computer was connected to the network of Chongqing University of Posts and Telecommunications. The forensics course enrolment only had about 20 students and experimental lesson hours were designed to be eight hours each semester, these computers could just satisfy the requirements for forensic experiments by the students.

In spring of 2011, the LDFP was set up at the University. The Laboratory introduced a new batch of digital forensics equipment and software resources from home and abroad. For example, the commercial software of the professional version of WinHex, Encase and FTK (Forensic Toolkit) provide an advanced comprehensive forensics capability. Xiamen Meiya Pico company's Forensics Magic Cube and Forensics Tower can quickly image and analyse evidence. An Ethernet technology company's On-line Network Forensics and Analysis System can fully collect and analyse real-time network evidence. The experimental platform based on the hardware equipment and software resources is called an *ordinary forensics platform* and gives the forensics course strong experimental support.

Once these new forensic equipment and tools became available, the experiments section of the digital forensics course was reformed. The reform was in three stages: First, some experimental topics using old forensic software were removed, e.g. *imaging* the drive using the *ghost* tool. Also some new experimental topics were added, based on the new forensic equipment, such as *imaging* and analysing the evidence using a forensics Magic Cube. Second, the teaching content of new forensic experiments was added to broaden students' insights and knowledge. The lesson hours for teaching experiments were increased, from eight to 16 hours. The experiment topics and lesson hours on the ordinary forensics platform are shown in Table 2, covering the range of theory topics in Table 1.

Table 2: The experiment topics and lesson hours on the ordinary forensics platform.

Week	Experiment topics	Lesson hours
1	Collecting volatile data	2
2	Imaging a drive	2
3	Deleted data recovery	2
4	Password cracking	2
5	Local system forensic	2
6	Digital device forensics	2
7	Network tacking	2
8	Analysing evidence	2

Third, more targeted action has been taken in the choice of the experimental teaching content. The digital forensics course is offered to law, information security and computer science majors and the experimental teaching content shown in Table 2 is compulsory for the three majors. The students of the three different majors have different professional background knowledge. So, a different elective experimental teaching content is provided for the students studying the three majors. As an example, the law major students may choose the experiment on analysing and preserving the evidence of a special criminal case. Students studying an information security major may choose the experiment on detecting and preventing network attacks.

THE EXPERIMENTS ON A CLOUD FORENSICS PLATFORM

In autumn 2011, the authors' Department received an additional budget for building a cloud computing platform in the Computer Science Laboratory. The platform can be used for teaching experiments, as well as for scientific research and information services. A range of system software is available based on a cloud platform, such as a cloud platform management system, a cloud access system, a cloud security management system, an intelligent parallel computation system, a data analysis system and a cloud environment-related software system. The platform provides a shared resource for research and practice, data processing, intelligent analysis, software development, information security, system simulation, etc.

Cloud forensics has become a hot topic of research in digital forensics technology. When storing electronic evidence remotely on a cloud platform, it can relieve the burden of storing mass evidence and save capital expenditure on forensic software and tools. Also, it can simplify the review procedure of evidence in court, and effectively assess the fairness and justice in the administration of the court. But, when attempting to locate evidence in a cloud, the distributed and virtual nature of the cloud are likely to increase the difficulty of evidence collection, preservation and analysis. Also, it may make tracing and reconstruction of evidence more challenging [9].

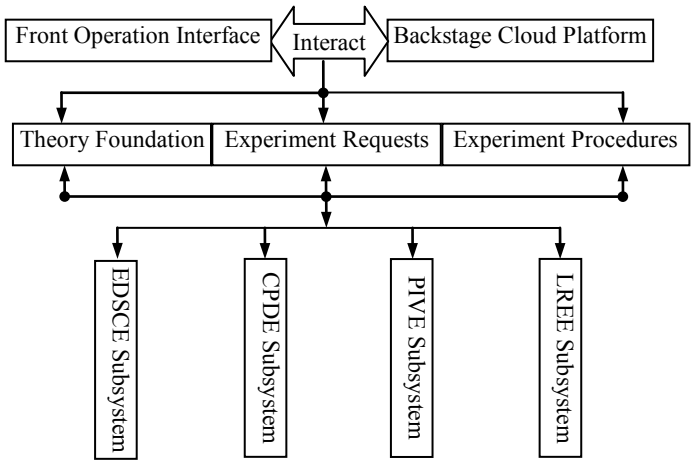

Figure 1: The forensics experiment system on the cloud platform.

In order to let students become familiar with knowledge at the forefront of digital forensics technology, and to understand the obvious advantages and potential risks of cloud forensics, a forensics experimental teaching system was built, based on the cloud platform.

The system consists of four teaching subsystems: Encryption and Decryption of Static Cipher Evidence (EDSCE); Collection and Preservation of Dynamic Evidence (CPDE); the Possession and Integrity Verification of the Evidence (PIVE); and Location and Recovery of Error Evidence (LREE). The forensics experimental teaching system and its four subsystems are shown as Figure 1.

From Figure 1, it can be seen that the forensics experimental teaching system mainly includes a front operation interface and backstage cloud platform. The two parts interact during experimental teaching. When students operate the interfaces of the four teaching subsystems, the server connecting the backstage cloud platform (the authors have called it a cloud server) will respond to the operating requests.

The forensics experiment system on the cloud platform is named a *cloud forensics platform*, and two lesson hours have been arranged about the platform for each teaching subsystem. The topics on the experiment and lesson hours on the cloud forensics platform are shown as Table 3. Before even one experiment actually begins, students should be familiar with the theoretical foundations, as well as the experimental requests and procedures of the teaching subsystem. The teacher and students may refer to the literature for details about the foundations of the theoretical knowledge [10-17].

Table 3: The experiment topics and lesson hours on the cloud forensics platform.

Week	Experiment topics	Lesson hours
1	EDSCE	2
2	CPDE	2
3	PIVE	2
4	LREE	2

The Encryption and Decryption of Static Cipher Evidence (EDSCE) Subsystem

The EDSCE subsystem can gather static cipher evidence from the cloud server and decrypt cipher evidence to the original plain text. In the experimental teaching, the students are divided into two groups. One group represents the client and the other group represents the investigator. The client encrypts their evidence file and sends it to the cloud server. The client has two methods by which to encrypt the file. In one method, the client uses a symmetric encryption algorithm to encrypt the file and the symmetric key is saved by the client. In the other method, the client uses a homomorphic encryption algorithm to encrypt the file. The cipher text allows for some computations, such as addition and multiplication. The client saves his/her private key locally and publishes the public key to the public. The investigator gathers static cipher evidence from the cloud server and uses password-cracking tools to decrypt the cipher evidence.

The Collection and Preservation of Dynamic Evidence (CPDE) Subsystem

The CPDE subsystem can collect dynamic evidence from the cloud server and preserve this evidence intact. In the experimental teaching, the students are divided into two groups. One group represents a malicious adversary and the other group represents the investigator. After several attempts, the adversary gets a successful unauthorised access to the cloud server. Then, the adversary steals, alters or deletes the files on the cloud server, and these files include Web files, system files, database files, and so on. The investigator looks for exit traces on systems and networks used by the adversary. The investigator searches Web sites visited, files downloaded and browser cookies to collect potential evidence. Also, the investigator uses snapshot technology to freeze dynamic system states of processed information, allocated data and the virtual machine. Finally, the investigator obtains static images from the snapshot and, moreover, uses a digital digest, digital signature and time stamp technology to preserve them intact.

The Possession and Integrity Verification of the Evidence (PIVE) Subsystem

The PIVE subsystem can provide probabilistic proof that the cloud server stores an evidence file. In the experimental teaching, the students are divided into two groups. One group represents the client and the other group represents the cloud server. The client wants to store an important evidence file to the cloud server. The client firstly splits the evidence file into blocks and generates a tag for each block of the file, then, stores the file blocks and their tags to the cloud server. The client deletes the original evidence file and only stores a small amount of metadata locally. To verify the possession and integrity of the evidence file on the cloud server, the client generates a random challenge to the cloud server. The cloud server uses the queried blocks and their corresponding tags to generate a proof of possession. The client verifies the proof to prove whether the cloud server stores intact the evidence file or not.

The Location and Recovery of Error Evidence (LREE) Subsystem

The LREE subsystem can guarantee the correctness and availability of the evidence files being stored on the cloud server. In the experimental teaching, the students are also divided into two groups. One group represents the client and the other group represents the cloud server. The LREE subsystem is similar to the PIVE subsystem; the evidence file is split into blocks and stored to the cloud server. The difference here, as compared to the other subsystem, is that the cloud server needs to encode the file blocks and their tags using erasure code technology in the LREE subsystem. When the client needs the evidence file, he/she sends a request message to the cloud server. The cloud server sends back to the client all blocks of the evidence file. The client uses piecewise hashing technology to check the integrity of the evidence blocks, to find in which block the error lies. If the client has found error data blocks of the evidence file, he/she will notify the cloud server and the cloud server will fast recover the storage error blocks using erasure code technology.

COURSE FEEDBACK

In spring 2013, the forensics experimental teaching system based on the cloud platform was first used in the digital forensics course at Chongqing University of Posts and Telecommunications. Students who joined the course already had previous forensics experience on an ordinary forensic platform during their last term. A total of 75 undergraduate students participating in the course experiment included three different majors: information security (30 students), law (20 students), and computer science (25 students). A survey questionnaire was administered to these students about several aspects of the course experiments. The feedback of the survey questionnaire is shown in Table 4.

Table 4: The forensics experiments feedback for three majors.

Questions	Information Security Major (Agreed Percentage)	Law Major (Agreed Percentage)	Computer Science Major (Agreed Percentage)
1. These forensics experiments are quite satisfactory and exciting	86.67%	85.00%	84.00%
2. I became interested in the forensics course through these forensics experiments	90.00%	90.00%	88.00%
3. The experiments are well related to the course lectures	83.33%	80.00%	80.00%
4. I will recommend this course to other students	90.00%	90.00%	92.00%
5. I think that cloud forensics is more difficult than ordinary forensics	70.00%	75.00%	68.00%
6. I have learned some new knowledge on cloud forensics, and these contents do not occur in ordinary forensics	93.33%	90.00%	92.00%

From Table 4, it can be seen that most students think the forensics experiments are quite satisfactory and exciting, and they became interested in the forensics course through these forensics experiments. In the experimental teaching, the students of the different majors had differing foundations in theory, and so they do not feel the same about the degree of difficulty of the forensics experiments. For example, students studying for a major in law have a weak background knowledge of computer science, and so 75% of those students think that cloud forensics is more difficult than ordinary forensics. But, most students across the three different majors think they have acquired new knowledge about cloud forensics that does not occur in ordinary forensics. Therefore, the students believe the forensic experiments broaden their horizons and knowledge of advanced technology.

CONCLUSIONS

The authors have carried out some reform to the experiments of the digital forensics course since the LDFP was set up at Chongqing University of Posts and Telecommunications in 2011. The forensics experiments of 16 lesson hours were arranged on an ordinary forensics platform. Later, the University Department built a cloud computing platform in the Computer Science Laboratory.

Based on the cloud platform, a forensics experimental teaching system was built, which consisted of four teaching subsystems: the EDSCE, CPDE, PIVE and LREE. For each subsystem, two lesson hours were arranged for forensics

experimental teaching. Therefore, undergraduate students of information security, law and computer science majors could carry out forensics experiments both on the ordinary forensics platform and on the cloud forensics platform.

Feedback from the students indicates the forensics experimental teaching improves their class attendance and greatly increases their interest in learning. By using the cloud forensics platform, it was found that experimental teaching broadens the students' horizons and knowledge of cloud forensics technology. However, cloud forensics is a new challenging research field, and four experimental teaching subsystems still do not have the support of mature technology. Also, the students studying different majors have different background theoretical knowledge. Therefore, a few students believe the cloud forensic experiments are more difficult than ordinary forensic experiments. In the future, further improvements will be made to the cloud forensics experimental teaching system, to make it more effective in satisfying the requirements of all students who study different majors.

ACKNOWLEDGEMENTS

This work is partially supported by the Science & Technology Research Foundation of Education Committee of Chongqing of China under Grant No. KJ110505, Found of Educational Reform of Education Committee of Chongqing of China under Grant No.133178 and Fund of Innovation Scheme of Postgraduate Education of Chongqing University of Posts and Telecommunications of China under Grant No. Y201107.

REFERENCES

1. Peterson, G.L., Raines, R.A. and Baldwin, R.O., Graduate digital forensics education at the Air Force Institute of Technology. *Proc. 40th Hawaii Inter. Conf. on System Sciences*, 264c (2007).
2. Center for Computer Security Research, http://www.security.cse.msstate.edu/research.shtml
3. Kruse, W.G. and Heiser, J.G., *Computer Forensics: Incident Response Essentials*. Addison-Wesley (2002).
4. Chen, L., Mai, Y.H., Huang, C.H., Dong, Z.X., Shi, W.M. and Song, X.L., *Computer Forensics Technology*. Wuhan: Wuhan University Press (2007) (in Chinese).
5. Steel, C., *Windows Forensics: The Field Guide for Corporate Computer Investigations*. John Wiley & Sons (2007).
6. Mandia, K. and Prosise, C., *Incident Response and Computer Forensics.* (2nd Ed), McGraw Hill Professional (2003).
7. Mell, P. and Grance, T., The NIST Definition of Cloud Computing. Special Publication 800-45, Gaithersburg, Maryland, USA: National Institute of Standards and Technology (2011).
8. Kent, K., Chevalier, S., Grance, T. and Dang, H., Guide to Integrating Forensic Techniques into Incident Response. Special Publication 800-86, Gaithersburg, Maryland, USA: National Institute of Standards and Technology (2006).
9. Wolthusen, S.D., Overcast: Forensic discovery in cloud environments. *Proc. Fifth Inter. Conf. on IT Security Incident Manage. and IT Forensics*, Stuttgart, Germany, 3-9 (2009).
10. Wikipedia, Homomorphic Encryption, http://en.wikipedia.org/wiki/Homomorphic_encryption
11. Gentry, C., A Fully Homomorphic Encryption Scheme. PhD Thesis, Stanford University (2009).
12. Taylor, M., Haggerty, J., Gresty, D. and Hegarty, R., Digital evidence in cloud computing systems. *Computer Law and Security Review,* 26, 304-308 (2010).
13. Birk, D. and Wegener, C., Technical issues of forensic investigations in cloud computing environments. *Proc. 6th Inter. Workshop on Systematic Approaches to Digital Forensic Engng.*, Oakland, CA, USA, 1-10 (2011).
14. Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z. and Song, D., Provable data possession at untrusted stores. *Proc. 14th ACM Conf. on Computer and Communications Security,* Alexandria, VA, USA, 598–609 (2007).
15. Wang, Q., Wang, C., Ren, K. and Lou, W.J., Enabling public auditability and data dynamics for storage security in cloud computing. *IEEE Transactions on Parallel and Distributed Systems*, 22, 847-859 (2011).
16. Song, X.L. and Deng, H.Y., Lightweight proofs of retrievability for electronic evidence in cloud. *Information*, 4, 262-282 (2013).
17. Juels, A. and Kaliski, B.S., PORs: proofs of retrievability for large files. *Proc.14th ACM Conf. on Computer and Communications Security*, Alexandria, VA, USA, 584-597 (2007).