Digital Forensics Core Curriculum Design in Higher Education in Ubiquitous Computing Era

Hai-Cheng Chu¹, Whe Dar Lin² and Kuo-Hsiung Chang³*

¹Department of Information Management/International Business, Tunghai University, Taichung, Taiwan 407, R.O.C.
²Department of Accounting & Information Technology, The Overseas Chinese Institute of Technology, Taiwan, R.O.C.
³Department of International Business, Tunghai University, Taichung, Taiwan 407, R.O.C.

Abstract

Due to the unprecedentedly ubiquitous wireless computer networks and mobile devices become prevalent, more unscrupulous technology hacktivists commit illegal conspiracies towards innocent victims via the ever growing Internet technology. Indeed, cybercrimes are relentlessly reported worldwide. The law enforcement agencies have the indispensable responsibility to crack the well-funded crime syndicate in our computer society. Consequently, Digital Forensics (DF) emerges and becomes the critical success factor to prosecute the culprit and prevent the associate cybercrime incidents from occurring. In the meanwhile, the computer society has an urgent demand for competent DF professionals to gather convincing digital evidences to assist indicting heinous perpetrators in order to allay the fears of everlasting computer crimes events in both private and public sectors. The research provides a vivid roadmap and suggested core curriculum design guidelines for higher education institutions to be integrated into their existing similar program or adopting as a groundbreaking reference model. A serial, cross-discipline, and functional approach were combined in order to design the suggested curriculum. Furthermore, the paper is attempting to minimize the theory-practice gap in DF and provide a milestone for higher education institutions to contemplate if necessary.

Key Words: Digital Forensics Core Curriculum, Cybercrime, Internet Technology, Exploited Security Leakage

1. Introduction

As unprecedentedly ubiquitous wireless computer networks and mobile devices become prevalent, more unscrupulous technology hacktivists commit illegal conspiracies towards innocent victims via the ever growing Internet technology. The cybercrime incident has a strong impact toward internal auditors, financial analysts, financial planners, underwriter, and investors in our digital society. DF is an extremely new research field and only a few universities have well organized curricula to provide the crystal guidelines in higher educating worldwide to fill the dramatically vital market demand [1–5]. Digital evidence (DF) is nothing more than information presented in a court of law and it is any information of probative value that is stored or transmitted in a binary form in the digital era [6]. The urgent need for computer forensics specialists is dramatically increasing especially in the private sector. Many corporations are spending substantial amounts of money on computer crimes, cyber vandalism, and digital intellectual property security and investigation. From law enforcement’s point of view, in-
formation concerning malicious acts must be discovered and recovered. Due to voluminous literatures on the problem of cybercrimes, the community need to strengthen the global economy by preparing a growing pool of DF professionals with the skills required to detect computer frauds before significant losses occur worldwide.

For instance, in the past several years, Internet shopping has been a fledging business model accompanied with the emergence of e-Commerce in the past decade. The US Internet Crime Complaint Center (IC3) was founded in May 2000 as a partnership between the National White Collar Crime Center and FBI. The IC3 deals with complaints such as on-line fraud, intellectual property rights, hacking, industrial espionage, child pornography, identity theft and money laundering [7]. Figure 1 indicates complaints received via the IC3 website of the United States between year 2002 and 2008 [8]. Figure 2 represents the dollar loss (in millions) with respect to Figure 1. From the statistical numbers, we deeply consider that computer crimes will hinder the growth of economic growth because the public will lose confidence regarding Information Technology (IT) applications. We have to fortify the economy by preparing a substantive workforce of DF professionals with the state-of-the-art skills to detect those computer cyber frauds.

Unfortunately, the DF is still in its early infant stage and possesses an urgent need for directions in terms of information security. Certifications or curriculum developments are becoming popular in this new arena. The DF involves obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative cases [9]. The DF is an investigation of situations where there is computer-based digital or electronic evidence of a crime or a suspicious computer usage violation, but the crime or behavior may be of any type [10]. This research paper is attempting to close the theory-practice gap in DF core curriculum design and provide a vivid roadmap for higher education institutions to consider integrating their existing degree offering programs into DF arena with a functional, cross-disciplines approach in terms of core curricula course design.

2. Preliminaries

DF is a relatively new forensic science and is becoming much more important due to the fact that IT-savvy hacktivists are using computers and networks to commit illegal activities. The forensic science community has become aware of the importance of DF and it must be addressed as a professional and a science, which will be closely related to many court cases [11–13]. In addition, the DF is multidisciplinary by nature, which encompasses computing and law and this makes the development of the DF specialists must contain several domain knowledge across academic fields.

2.1 Cybercrime

The cybercrime has been a mushrooming issue concerning the information security in the past two decades because computers and networks become unparalleled ubiquitous. For most computer crackers, they might accidentally leave some kind of digital trails, which contain digital evidences that can be used to prosecute the criminals in a court of law in order to suspend this ever growing high-tech crime, which resulted in tremendous financial losses worldwide [14].

Computer crimes and computer-related crimes have

![Figure 1](image1.png) **Figure 1.** Complaints received via the IC3 website of the United States between year 2002 and 2008.

![Figure 2](image2.png) **Figure 2.** Dollar loss with respect to Figure 1 (in millions).
occurred in all industries. Generally speaking, the computer crime means the computers become the target of cyber attacks, such as Denial of Service (DOS) attacks or virus hit. The computer-related crime stands for the use of computers storage devices and communication tools to commit cybercrimes, such as corporate frauds [10]. The menace from the heinous culprits in the dark side of the cyber net perpetuating digital property through crime syndicate is expanding. Furthermore, the complexity of DF is growing due to the forensic targets with terabytes of storage becomes common and sophisticated IT savvies exist worldwide as well as the well-financed and skilled adversaries.

According to the related researches, well-funded groups in China launched breaking into U.S. government networks for sensitive information via Internet technology through system vulnerabilities. For experienced intruders, they take advantage of the lack of forensic readiness [14]. Cyber criminals are focusing on the vandalism, computer frauds or embezzlements of digital data by unauthorized access on the networks. The compromised information security breaches provided the channels for crackers to turn digits into cash and prizes [15,16]. Law enforcement agencies were desperately cracking the well-organized computer savvy groups and indicting those cyber criminals to justices. Consequently, there is an urgent necessity of DF specialists both in public sectors and private sectors.

2.2 Applications of Internet Technology

More and more enterprises deploy new information systems to be integrated with the legacy systems or replace the existing ones. Internet, intranet and extranet are widely interrelated and dispersed within an organization with different application programs, which are running on different operating systems or platforms. Many enterprises have installed the related information systems in order to achieve more profitability or even to survive in this competitive epoch. Web-based application programs are obviously the main theme in today’s enterprise software architecture. In other words, the communication of massive amount of data through the networks has become the fundamental methodology for data transferring between applications to applications (AP2AP). Therefore, paperless transaction has become the main stream of the routine operations and replaced the manual paper work procedures in the past. One of the greatest advantages is that all the data has been digitalized and stored in heterogeneous databases that are dispersed across the networks. The retrieval of the associated information for some certain task becomes much more efficient. On the contrary, one of the worse drawbacks is that information predators exist somewhere in the network desperately hunting for innocent victims in order to pursue their criminal purposes.

3. A Serial and Cross-Disciplines Approach

Based on existing researches, generally speaking, the DF is an investigation of information security threat where there is a digital evidence for the suspicious behavior regarding computer manipulation. It encompasses the processes of planning, identification, collection, classification, preservation, analysis, reconstruction, documentation, and presentation of electronic evidences in a legitimate manner to investigate the suspect to be inculpatory or exculpatory in a court of law as Figure 3 illustrates [17–19]. In this paper, we will design the core curricula of DF in higher education based on the serial and cross-disciplines basis for law enforcement agency staff, academia, and business organizations respecting the education/training for DF specialists.

Planning

Once the DF specialist receives the computer crime incident report, the DF specialist should categorize the

![Figure 3. The serial procedures of a typical DF investigation.](image-url)
incident (hacking, vandalism, spoofing, viruses, worms, DOS attack, spam, identity theft, computer fraud, etc.) and proceed the initial assessments. A well-organized plan (number of staff, special expertise, on site investigation/remote access investigation, etc.) is necessary before the formal investigation begins. Suitable Standard Operating Procedure (SOP) and the related protocols must be enforced during the preliminary execution of the investigation. The checklist should be revised for every individual cybercrime incident due to the versatile characteristics of the computer crime. Moreover, forensics sound toolkits should be comprehensive and flexible.

The DF specialist should have the examination plan ready, which describes the types of information to be gathered/recovered as well as the procedures that will be followed in the later stages. In some cases, the search warrant is necessary for the seizure of the related digital evidences that may reside in other media storages. The examiner should be aware of the local law to prevent the investigating case dropped by the jury due to the illegitimate procedures during the investigation process. Hence, unprepared plans might result in the case to be suspended and the cybercrime culprit is still at large eventually. In other words, this stage encompasses the following knowledge: category of crime, initial assessment, incident response, SOP and protocol, examination, warrant, operation plan, checklist, and tools & staff. After reviewing the current global institutions that provide the DF certificate/training/education, we suggest the following related courses to fulfill the knowledge requirements with respect to the Planning stage:

- **Introduction to Digital Forensics** (basic concepts, incident sketch, and digital evidence handling, etc.)
- **Computer & Network Security** (vulnerability, confidentiality, accountability, reliability, availability, and administration, etc.)
- **Operating System** (caches, services, file management system in Windows, Linux and Mac, and FAT or NTFS file structure, etc.)
- **Criminal and Civil Law** (warrant, discovery order, Privacy Act, and jurisdictions, etc.)
- **Network Programming** (C++, Java, and .NET programming, etc.)

The whole structure of DF in the Planning stage is illustrated in Figure 4. The suggested 5 courses is capable of encompassing the above 9 functions in terms of the scope being explored as well as the current international institutions that are offering the related DF curriculum design [3,20–22].

**Identification**

The DF examiner should use the commercial or open-source forensic sound toolkits to perform the related procedures. In business organizations, some unscrupulous employee might sell company’s priceless information to its competitors like the quotation, product design blueprint, customer databases, or detailed sale volume through company’s Intranet, Extranet or SAN (Storage Area Network). The DF examiner should take a serious attitude since vandalism of corporate digital intellectual property occurs in a silent mode and it is not easy to get exposed unless the DF specialist unveils the cyber crime syndicate. Due to the pervasive applications of IT, some people use the Instant Messaging (IM) tools to reveal company’s confidential data through the organization’s firewall, but, partial digital evidences can be still found in the RAM (Random Access Memory) and those network activities are also stored somewhere in the computer systems. Once the power is off, we lost all those digital evidences. Consequently, collecting live data on the fly is the basic skill for those DF specialists in some cases.

Basically, the DF examiner should proceed a quick crime scene evaluation to decide the nature of the incident. In some cases, the digital evidence is volatile like the data being temporarily saved in RAM or the game console (Sony’s PSP and Microsoft’s XBOX, etc.). As soon as the power is shut down, all precious and decisive digital evidences will be gone forever. This is the reason why we suggest the course computer hardware to be in the position with respect the function special expertise staff.

![Figure 4. The whole structure of DF in the Planning stage.](image-url)
By the virtue of IT, wireless communication is popular in many places and could be deployed for criminal exploitation. Near the e-crime scene, ubiquitous Access Point (AP) may be vanished once the raid took place causing crime syndication to elude the investigation by shutting off the AP, which also causes the logs during the wireless transmission erased. Senior and experienced DF examiner will sketch the crime scene in a very short period of time and decide means of collecting those traces in the best manner. In many computer security incident cases, the suspects are IT savvy and new schemes of committing cybercrimes keep renovating. The DF examiner should keep abreast of new skills that computer criminals exploit of the contemporary state-of-the-art IT. Due to pervasive availability of networks and mobility of computing devices, identify theft is a common crime in which an intruder accesses the victim’s sensitive personal information through digital media. In many cases, phishing is a common cybercrime scenario, which means the perpetrator set up a fake web site and tried to dupe the victim providing key information by sending e-mail solicitation messages, which look exactly identical to legitimate business organizations. On the other hand, pharming will redirect web users to bogus web sites even when the individuals type the correct URL into the browser and the criminal conspiracy will be committed at these fake web sites. In short, understanding, discovering and recovering digital evidences are the heart of DF in our computer society. This is the reason why we suggest the course computer criminology to be in the position with respect the function crime scene evaluation.

Hence, we suggest the following related courses to fulfill the knowledge requirements with respect to the Identification stage:

- **Computer Criminology** (pharming, zombie, phishing, digital extortion, Trojan horse, hacking, key loggers, vandalism, spoofing, spyware, DOS attack, spam, identity theft, computer fraud, and defacement, etc.)
- **Computer Hardware** (BIOS setting, RAM, internal hard drive, external hard drive, USB thumb drives, flash memory card, cellular phone with the SIM card, PDA with the SD card, and game console, etc.)

The whole structure of DF in the Identification stage is illustrated in Figure 5.

**Collection, Classification and Preservation**

This stage plays a critical role in conducting digital investigation. Since digital evidences could be volatile in nature, seizing digital evidences at the crime scene requires special attentions and depends on the nature of the case as well as the alleged computer crime or policy violation. The purpose of DF examination is to identify any potential evidences located on digital media. In many cases, policy violation happens from time to time within some business organizations. For example, high technology industrial espionages may reside in the organization or government department and never get exposed. Hence, the DF staff might seize peripherals and digital media storages like Small Scale Digital Devices (cell phones, memory sticks, USB thumb drives, card reader, etc.) as well as Large Scale Digital Devices (internal hard drives, external hard drives, disk arrays, CD, and DVD, etc.) [3], which are belonged to the company’s property. In order to expedite the DF processes, organizations should label significant tags to identify the company property from personal belongings at the working place due to the fact that personal belongings should not be seized in the private sector. The DF examiner might have to predict what components are critical to the case under time pressure. In other words, onsite preview must be conducted.

A DF examiner might also have to quickly judge the case by its nature. If the suspect’s computer is running, rebooting the computer without forensic boot CD may alter important time stamps of last accessed files [11]. Accidentally modifying vital information may lead the investigation case drop due to the authenticity of the digital evidences, which eventually may be turned down by a jury of laypersons in a court of law.

In digital evidence collection stage, the data being collected must be bit-stream (sector-by-sector) duplication and should be kept in a safe place without the possibility of those evidences being changed or contaminated. The DF examiner should have the solid background knowledge of computer hardware and software due to the reality that the capacity of certain media storage...
might exceed terabytes and it may take days to complete certain operations. Consequently, constantly upgrade the computer forensics facilities is a must. Therefore, there will be a tradeoff between high performance equipments and the budget concern in DF organizations.

If necessary, the DF examiner might have to use digital camera to photograph the crime scene to avoid the possibility of being detected by the suspect and the culprit may come out with the counter-forensic operations and led the collection process biased. After collecting the digital evidences, the storage of those intangible evidences could be a challenge for the working staffs. Sometimes, the investigators are stalled by some incompatible file formats due to the proprietary software developed by different software vendors. If the digital evidences are not properly and securely stored, this could result in the investigation to be compromised by the jury and makes the criminal exculpatory in the long run.

Hence, the sector-by-sector copy from the crime scene needs to be handled in a proper procedure. Those images could occupy up to several terabytes in some cases. Hence, the SAN being deployed in many DF organizations can be utilized because of its high speed and reliability, which is suitable for the DF experts to store and back up the digital evidences. Furthermore, the examiner should always store digital evidences in more than one place just in case the digital evidences contaminated during the analyzing processes.

Furthermore, web mail has been a fundamental communication mechanism in many organizations. Many web mail providers have event logs indicating the time and IP records. If the employee sets the proxy server to access some certain confidential databases, these digital evidences could be collected once the DF examiner contact with the system administrator. For the purpose of ascertaining the suspect to be inculpatory or exculpatory, making forensic disk image from all possible media storages is necessary and this depends on the examiner’s experience and professional training. In public sector, if the search warrant is obtained, the DF staff should bagged and tagged the suspect’s computers and the associate peripherals preserving the digital evidences in the antistatic evidence bags after the search and seizure because the static electricity could destroy the integrity of digital data.

In other words, this stage encompasses the following knowledge: file recovery, file system, Large Scale Digital Device, Small Scale Digital Device, foot printing, packet sniffing, encryption, steganography, forensic boot CD, imaging digital evidences, write blocking devices, chain of custody, bagged and tagged, photograph crime scene, wireless network AP, game console, and onsite preview. After reviewing the current global institutions that provide the DF certificate/training/education, we suggest the following related courses to fulfill the knowledge requirements with respect to the Collection, Classification and Preservation stage:

- **Wireless Network Security** (foot printing, packet sniffing, and vulnerability, etc.)
- **Virtual Private Network** (switch, router, proxy server, and firewall, etc.)
- **Digital Evidence Handling** (forensic boot CD, imaging of digital evidences, write blocking devices, forensic disk image, chain of custody, bagged and tagged using evidence bag, photographing crime scene, hidden files in logs, caches, swap files, deleted files, or unwritten segments, etc.)
- **Data Encryption** (encryption and decryption algorithms, steganography, etc.)
- **Security Auditing** (intrusion detection, file recovery, file system, Registry in Windows, and remote procedure call, etc.)

The suggested 5 courses is capable of encompassing the above 17 functions in terms of the scope being explored as well as the current international institutions that are offering the related curriculum design. The whole structure of DF in this stage is illustrated in Figure 6.
Analysis and Reconstruction

After seizing the digital evidences, the examiner is going to analyze the collected data in order to infer the possible causes for the computer frauds or misconducts. Based on the digital evidences, criminology should be also involved. Personal background checking is necessary as long as the suspect’s authority reaches within an organization. Profile of suspect should be obtained as a basic reference.

Several DF workstations should be set up in a secure lab hosting diverse operating systems or proprietary software. The examiner must always only utilize DF workstations to analyze the digital evidences and preserve the result on that workstation, which resides the bit-stream copy of the original digital evidences. The reason behind this is that DF staff can’t afford to crash the original digital evidences.

The bit-stream copy should create associate digital fingerprint of files to authenticate or ensure data integrity. This procedure is called hashing. Currently, the DF staff performs Secure Hash Algorithm version 1 (SHA-1) or Message Digest 5 (MD 5), which was the first algorithm for DF examiners to verify data integrity. The DF specialist must have the capability to create a forensically sound copy of the media and validate it as well as preview the storage media without altering its original content.

The system logs can be collected in many applications or peripherals. For example, some organizations use EIP (Enterprise Information Portal) as the entry point for other applications. Web-based e-mail system will keep recording user’s IP, logon time as event logs and save in the system. Logs are always a useful reference to be used in terms of computer crime incident investigation. The DF examiner can systematically check the event logs within the systems and try to run the cross examination to come out with the data mining concerning a specific user about his/her operational profile. The examiner might have to analyze the time stamp of each transaction and the IP of the computer that the employee was using. In the meanwhile, MAC (Media Access Control) address on the NIC (Network Interface Card) is globally unique. For the end users, they might not have the clues as we stated above, but for the professional DF staffs, they have to be alert and sensitive to those data.

Looking for hidden, deleted or encrypted files is also essential during this stage. There are some DF toolkits can recover deleted files, the formatted disk or drive and deleted e-mails whether using SMTP or POP3. Some of the DF toolkits are commercially available, others are open source sharewares. Updating of those DF tools is critical and the examiners should keep several versions of the toolsets simultaneously to deal with the high pace of changing in operating systems or enterprise applications.

Disaster recovery is another key issue in this stage. The DF examiner needs to plan for unforeseen disaster like the hard disk failure, typhoon, power outage or earthquake that hinders the normal operation of the DF lab. A well planned disaster recovery plan can help the DF examiner restore the workstation back to the state before the catastrophic failure and this situation should be common due to the complexity of the DF by its nature. On site/off site backup should be performed from time to time in the DF lab in order to prepare for the unexpected factors occurring during the analyzing stage. The purpose of managing the DF lab is to ensure data confidentiality, integrity, availability and authenticity of the digital evidences that were collected. The DF experts are capable of making inferences and interpretations regarding the recovered or discovered evidences.

Consequently, this stage encompasses the following knowledge: logs analysis, incident sketch, exculpatory/inculpatory, crime reconstruction, suspect profiling, and digest. After referring to the modern global institutions that provide the DF certificate/training/education, we suggest the following related courses to fulfill the knowledge requirements with respect to the Analysis and Reconstruction stage:

- **Forensics Lab Practicum** (crime scene reconstruction, honeypots, suspect profiling, spam, virus, worm, Trojan horse, computer fraud, spoliation, logs auditing and analysis of e-mail server, web servers, and EIP server in real case study)
- **Information Assurance (IA)** (obtaining a unique digital hash value – use hash functions like MD 5 or SHA-1, authentication, etc.)
- **Computer Forensics Tools** (EnCASE and Forensic ToolKit (FTK) for Windows, Knoppix for Linux, Intrusion Detection System (IDS), network utilities, packet sniffers, and vulnerability assessment, etc.)
- **Forensics Lab Management** (authorized access, and
disaster recovery, etc.)
- Cryptography (public key cryptography, digital signatures, and password cracking, etc.)

The suggested 5 courses are capable of encompassing the above 6 functions in terms of the scope being explored as well as the current international institutions that are offering the related DF curriculum design. The whole structure of the DF in this stage is illustrated in Figure 7.

Documentation and Presentation
The final stage of DF is to provide the solid digital evidences to a court of law in the public sector to indict the computer criminal suspect or executive management in the private sector to terminate the employment of the suspect. In the private sector, most organizations prefer to handle the investigation internally if they are capable of examining digital evidences themselves instead of going public because that may reveal some confidentiality of the enterprise to avoid the competitor might take advantage of the issue and obtain competitiveness in this scenario. Once the computer security incident was sent to the court, the stock price may plunge due to the fact that obfuscated investors would lose confidence concerning the operation of the company. In the public sector, the DF examiner could be a technical witness or an expert witness to make testimony in a court. For being a technical witness, the DF expert only provides the fact that he/she found during the investigation. In other words, the DF expert does not offer conclusions, only the facts. On the other hand, being an expert witness, the DF specialist is working for the attorney, neither plaintiff nor defendant. The expert witness only has opinions regarding the digital evidences collected and observed.

The greatest challenge for DF is that digital evidence has no natural physical character and it is essentially intangible. The professional DF specialist is able to effectively and accurately testify in a court concerning the interpretation of the cybercrime incident. We suggest the following related courses to fulfill the knowledge requirements with respect to the Documentation and Presentation stage:
- Jurisdiction Legislation (civil law, international law, etc.)
- Litigation (testimony as a technical witness or an expert witness)
- Investigation report (ethics, report writing, etc.)

The above suggested 3 courses are capable of encompassing the above 3 functions in terms of the scope being explored as well as the current international institutions that are offering the related DF curriculum design concerning the Documentation and Presentation stage. The whole structure of the DF in this stage is illustrated in Figure 8.

4. Conclusion

Nowadays, not too many higher education institutions provide the training/education/certificate for DF specialists worldwide. The computer society has an urgent need for the comprehensive curricula in DF in higher education systems in order to alleviate the information security or cybercrime issue in both public and private sectors. Demonstrably, many organizations are desperately hunting for DF specialists to deal with the mushrooming cybercrimes, which resulted in millions of dollar loss globally. Although the law enforcement agencies are indispensable and fighting assiduously respecting the associate cybercrimes, there is still a huge gap between the demand and supply regarding decent DF specialists. Consequently, in this research paper, we provided solid core curricula design in DF arena. The sug-
gested curriculum design was completed after comparing and referencing current institutions that provide similar training/education/certificate worldwide.

References


Manuscript Received: Jan. 8, 2010
Accepted: Mar. 3, 2010