Journal of Computer Engineering & Information Technology

Research Article

a SciTechnol journal

Modern Technologies for Electronic Forensics

Junjie Xu*

Abstract

With the rapid development of cyberspace technology, electronic forensics technology has become one of the important research directions in the field of cyberspace security defense. This article focuses on the application technology of electronic forensics, and the forensics technology is divided into three categories according to the technology and method of forensics: computer forensics, mobile forensics, and network forensics. The introduction of computer forensics technology in this article is mainly based on Windows and Mac systems, including browser forensics, mail forensics and memory forensics in Windows, as well as log files, diagnostic reports, crash logs, and plist files in Mac. Mobile forensics is mainly divided into manual extraction, logical forensics, physical forensics, chip disassembly, and microcode reading, based on Android and iOS. Finally, this article briefly explains two methods of network forensics: server forensics and router forensics.

Keywords

Electronic Forensics; Computer Forensics; Mobile Forensics; Network Forensics; Cyberspace Security.

Introduction

In 1991, the first International Conference of Computer Investigation Experts was held in the United States, and the concept of “computer evidence” was first put forward [1]. Since then, electronic forensics technology has developed rapidly, forming an interdisciplinary subject of computer science, law science and investigation practice. The following will conduct an in-depth analysis of computer forensics, mobile phone forensics, and network forensics technologies and methods.

Computer Forensics

Electronic data is mainly stored in computers. The two most widely used operating systems are Windows and Mac.

Windows

First, introduce the main forensics technologies of Windows. There are three main types of forensic methods and technologies for Windows: browser forensics, e-mail forensics, and memory forensics.

At present, the mainstream browsers in the world are Chrome, Firefox, Safari, Opera, IE and so on. However, after each user uses a browser to access resources on the Internet, they will leave traces on the computer’s hard drive, such as URL access control lists, caches, and cookies. The new version of the Microsoft’s Edge uses a brand new WebCacheV01.dat database file instead of the traditional index.dat used by IE5-IE9. WebCacheV01.dat is an Extensible Storage Engine (ESE) database, which contains web browsing artifacts for Microsoft Edge. It can be found in <UserName>\AppData\Local\Microsoft\Windows\WebCache. ESE Extensible Storage Engine is a highly flexible database type. When a record is removed from the database, its occupied space will be marked as deleted but the database does not perform the overwrite operation, so the original record may still exist in the unallocated area, which provides the possibility for data recovery. The analysis tools for the WebCacheV01.dat file include ESEDatabaseViews, WebCacheV01.dat Viewer, etc.

In addition to using the normal mode of the browser to surf the Internet, there is also a special mode, that is, private browsing. Private browsing means that the browser does not save any browsing history, search history, download history, form history, cookies, or temporary files during the process of surfing the Internet. The main forensic method for private browsing is data recovery. Even if the cache files and log files are deleted, if the disk management system has not redistributed the disk space and the written data has not overwritten the original data, the deleted file data still exists on the disk, and these data may exist on the disk. On the unallocated storage space, data can be recovered or extracted by reading the physical image of the unallocated disk area. The more important point is that the record of private browsing is still stored in the database file WebCacheV01.dat. Although the information is not complete and comprehensive, this part of the information still has a certain forensic value.

E-mail is one of the most widely used applications besides the browser. The client uses POP3/IMAP, SMTP protocol to send and receive emails, and HTTP protocol can also be used. The forensics of e-mails based on the HTTP protocol is more difficult than other methods, because not all data is stored locally. Kaplan summarizes email forensics into four steps [2]: firstly, find the storage location of the email; secondly, check the email header; thirdly, analyze the email header, and finally, check the email content. Most emails are encoded using the MIME encoding standard, therefore, a decoder, such as Encase, must be used for decoding and viewing.

Physical memory forensic analysis is an important technique in the field of criminal evidence investigation [3]. Since this field was born in the early days of digital forensics, memory here refers to RAM, ROM, non-separable memory, flash memory devices, etc [4,5]. The computer system memory (RAM) is the only place where the computer system runs programs, which contains various behaviors and data that the computer runs. The simplest method for memory forensic analysis is string search technology. Its basic principle is to search for strings with specific semantics from the memory image to provide corresponding evidence for forensic analysis. For example, Encase has this function. However, the information obtained by this forensic method is relatively single and insufficient.

Mac OS

The forensic technologies in Mac OS are like Windows, but some special features that come with Mac OS can make it easier to find electronic evidence, such as log files, diagnostic reports, crash logs, and plist files.

***Corresponding author:** Junjie Xu, Department of Computer Science, Jiangsu University of Technology, China, E-mail: sherlockjjobs@163.com

Received: May 18, 2021 **Accepted:** June 03, 2021 **Published:** June 10, 2021

The audit log of Mac OS is generally stored in the /var/audit directory. As shown in Figure 1. The log file is named start_time. stop_time. Start_time represents the start time and stop_time represents the stop time. The audit log is generated continuously, so the start_time of the next log is the stop_time of the previous log, and the stop_time of the last log file is not_terminated. Use the "ls -ld /var/audit" command to view the log directory. "sudo ls -l /var/audit" command can view the specific log file list. Many log files in Mac OS are stored in the /private/var/log and /Library/Logs paths. In addition, application logs are stored in <username>/Library/Logs.

The diagnostic report is mainly a record of the occurrence of a crash report, which records the accidental exit of the user's application program, the user's choice to force the program to exit, and the system error requesting the user to restart the computer.

Mobile Forensics

One of the key differences between traditional computer forensics and mobile phone forensics is the reproducibility of evidence in the case of dead forensic analysis. This is due to the nature of mobile phone devices being constantly active and updating information on their memory [6]. According to Sam Brothers' proposal, mobile forensics technologies can be divided into five types: manual extraction, logical forensics, physical forensics, chip disassembly, and microcode reading [7]. There are mainly two types of smart phone systems: Android and IOS. This part introduces the application of these 5 forensics technologies based on these two systems.

Manual extraction is the easiest way to extract information through direct viewing. This method does not require special tools and advanced techniques, on the contrary, some information can even be viewed directly. Most users leave traces after using their mobile phones, such as address books, short messages, and Internet records. During manual extraction, investigators access the information stored on the device by using standard interfaces such as keyboards, touch controls, and display consoles, and capture data directly from the screen [8]. For example, in iOS, Safari browser evidence from the backup on a synced computer can be found in

/private/var/mobile/Library/Safari/Bookmarks.plist,

/private/var/mobile/Library/Safari/History.plist,

/private/var/mobile/Library/Safari/SuspendState.plist,

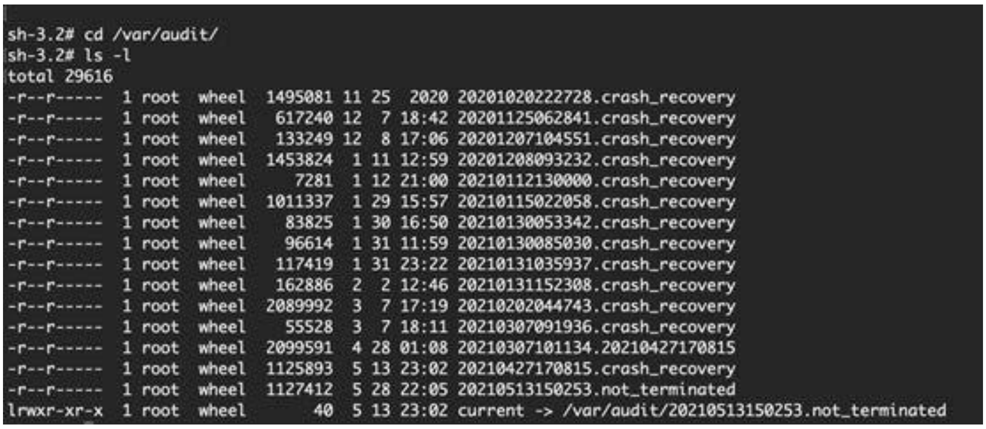
/private/var/mobile/Library/Safari/SMS/sms.db,

/private/var/mobile/Library/Cookies/Cookies.plist

In logic forensics, Android phones usually use the Android Debug Bridge (ADB) tool that comes with the Android SDK to obtain information. By default, the ADB function of Android phones is disabled, so forensics personnel need to manually turn on the USB debugging mode and need to obtain root permissions for the phone. Most of the data in the Android is stored in the SQLite database. In addition to using mobile phone forensics tools, it is also necessary to extract the corresponding files from the Android phones and use the corresponding software for analysis, to realize the logical data extraction of the Android phone. The premise of logical forensics is to obtain the root permission of the phone.

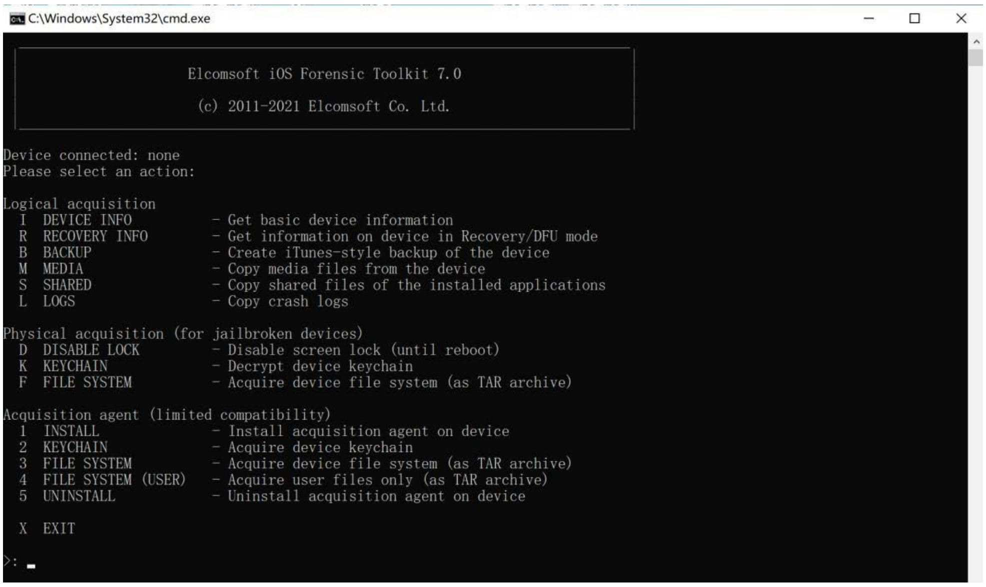
Like the Android system, the logical forensics method for iPhone is to back up the system files and then analyze them. The most used tool for iOS logic forensics is Elcomsoft iOS Forensic Toolkit (EIFT), as shown in the Figure 2, it has six modes: I (Info), R(Recovery), B (Backup), M (Media), S (Shared), L(Logs). Info logical acquisition option returns detailed information about the device including device name, exact model designation, iOS version and build number, total/ free space, serial number, as well as the list of applications installed. Device information is acquired through the lockdownd service, and application information through installation_proxy. Therefore, logical forensics is usually the preferred method for forensics personnel.

Physical extraction is also referred to as hex dump. Physical forensics technologies can be divided into software physical forensics and hardware physical forensics, as shown in Figure 3. The Android system usually first adopts software physical forensics [9]. There are two main software methods: one is to use a special loader for booting to achieve physical reading, and the other is to run the dd command under the condition of root permissions to obtain the partition image. There are three main hardware physical forensics technologies: chip disassembly, JTAG, and microcode reading. On one hand, the hardware physical extraction for Android mainly uses JTAG. JTAG is a test standard. Android mobile phones generally have a JTAG port, which can be used to read and restore memory. JTAG methods and tools can also be used to enter a locked device to retrieve all data from the phone's memory. This will bypass the locked USB port (disable USB debugging) and probe the test access port between the USB port



```
sh-3.2# cd /var/audit/
sh-3.2# ls -l
total 29616
-r--r-----  1 root  wheel  1495081 11 25  2020 20201020222728.crash_recovery
-r--r-----  1 root  wheel   617240 12  7 18:42 20201125062841.crash_recovery
-r--r-----  1 root  wheel   133249 12  8 17:06 20201207104551.crash_recovery
-r--r-----  1 root  wheel  1453824  1 11 12:59 20201208093232.crash_recovery
-r--r-----  1 root  wheel     7281  1 12 21:00 20210112130000.crash_recovery
-r--r-----  1 root  wheel  1011337  1 29 15:57 20210115022058.crash_recovery
-r--r-----  1 root  wheel    83825  1 30 16:50 20210130053342.crash_recovery
-r--r-----  1 root  wheel    96614  1 31 11:59 20210130085030.crash_recovery
-r--r-----  1 root  wheel   117419  1 31 23:22 20210131035937.crash_recovery
-r--r-----  1 root  wheel   162886  2  2 12:46 20210131152308.crash_recovery
-r--r-----  1 root  wheel  2089992  3  7 17:19 20210202044743.crash_recovery
-r--r-----  1 root  wheel    55528  3  7 18:11 20210307091936.crash_recovery
-r--r-----  1 root  wheel  2099591  4 28 01:08 20210307101134.20210427170815
-r--r-----  1 root  wheel  1125893  5 13 23:02 20210427170815.crash_recovery
-r--r-----  1 root  wheel  1127412  5 28 22:05 20210513150253.not_terminated
lrwxr-xr-x  1 root  wheel       40  5 13 23:02 current -> /var/audit/20210513150253.not_terminated
```

Figure 1: Audit log in /var/audit directory.



```
                    Elcomsoft iOS Forensic Toolkit 7.0

                     (c) 2011-2021 Elcomsoft Co. Ltd.

Device connected: none
Please select an action:

Logical acquisition
  I  DEVICE INFO          - Get basic device information
  R  RECOVERY INFO        - Get information on device in Recovery/DFU mode
  B  BACKUP               - Create iTunes-style backup of the device
  M  MEDIA                - Copy media files from the device
  S  SHARED               - Copy shared files of the installed applications
  L  LOGS                 - Copy crash logs

Physical acquisition (for jailbroken devices)
  D  DISABLE LOCK         - Disable screen lock (until reboot)
  K  KEYCHAIN             - Decrypt device keychain
  F  FILE SYSTEM          - Acquire device file system (as TAR archive)

Acquisition agent (limited compatibility)
  1  INSTALL              - Install acquisition agent on device
  2  KEYCHAIN             - Acquire device keychain
  3  FILE SYSTEM          - Acquire device file system (as TAR archive)
  4  FILE SYSTEM (USER)   - Acquire user files only (as TAR archive)
  5  UNINSTALL            - Uninstall acquisition agent on device

  X  EXIT

>: _
```

Figure 2: Logical acquisition with Elcomsoft iOS Forensic Toolkit.

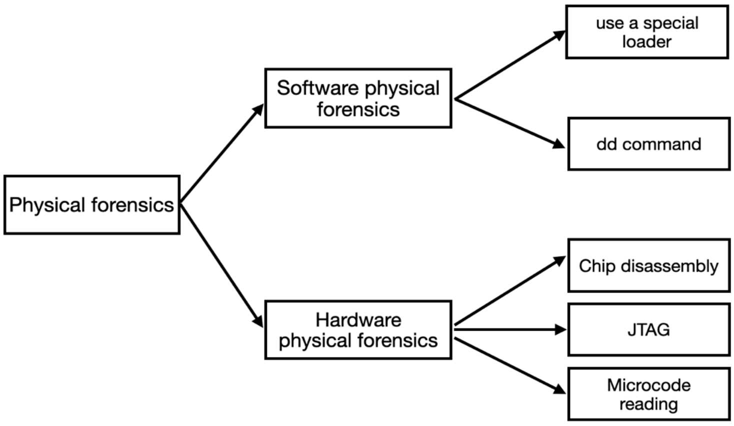


Figure 3: Classification of physical forensics.

and the CPU. JTAG provides communication with NAND memory through the CPU, allowing the memory to be read. On the other hand, due to its closed features, IOS mainly uses chip disassembly and microcode reading for physical reading.

Chip disassembly is also known as chip extraction technology. The RAM chip is separated from the motherboard by physical methods such as a hot air gun and then loaded on a chip reader to read data. After extracting the data from the flash memory, investigators create a binary image of the removed chip. To create a binary image of the chip, reverse engineering is performed on the wear levelling algorithm [10]. Chip disassembly technology is generally used for mobile phones that have been maliciously damaged, mobile phones whose data interface cannot be used, and mobile phones with passwords that cannot be cracked, such as iPhones. However, chip disassembly is highly technical and takes a long time to obtain evidence. There will be many original binary data format conversions during the forensic process, and the risk of chip damage is high. Microcode reading technology mainly refers to the observation of the state of the NAND chip storage under an electron microscope, and the conversion of binary data into ASCII characters by analyzing the physical level threshold on the chip. The above two methods are rarely used in practice due to their high technicality. Instead, Elcomsoft iOS Forensic Toolkit allows limited physical acquisition of Apple's 64-bit devices, mainly obtain the full file system and keychain, as shown in Figure 1.

Network Forensics

Network forensics is a branch of digital forensics, which mainly involves monitoring and analyzing computer network traffic. Network forensics mainly includes web server forensics, router forensics.

Proposed Methodology

The web server will record the data of each visitor in the form of log files on the web server. If there is a problem with the web server, the data log file will be very useful [11]. Web server forensics first analyzes the configuration file of the target client, finds the storage

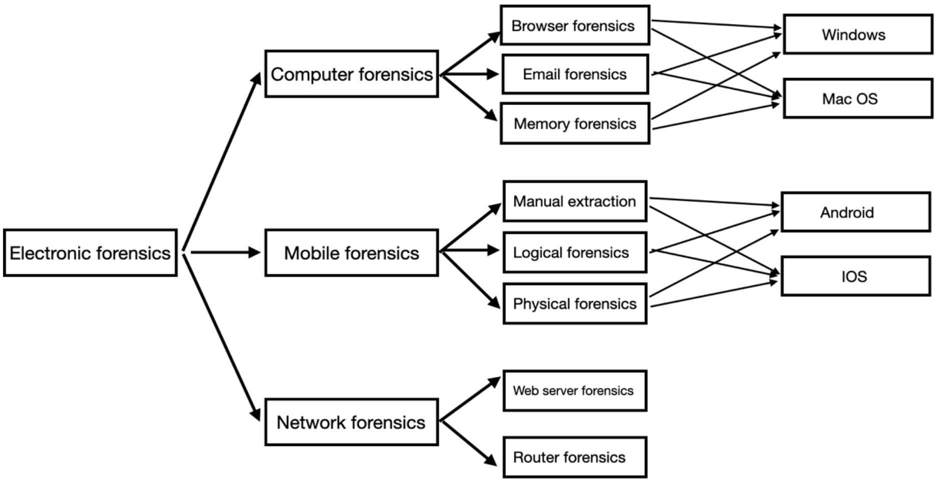


Figure 4: Classification and application of electronic forensics.

directory and all codes of the corresponding website, and exports all code files. Then, analyzes the configuration of the website server file to find out the database type and IP address used by the website server as well as the login name and password to access the database and export all the data in the database. In addition to classic IDS, Snort is a software that detects system commands. It can analyze traffic in real time and record IP addresses, analyze ports and detect various attacks from the outside [12]. Finally, analyze the exported code and data, and simulate building a website based on them and try the corresponding user operations.

Router forensics is relatively simple. As a key device connecting network nodes, routers will not only record routing information for general data transmission, but also record access information of some key IP addresses or MAC addresses. Most routers have log function, and forensics personnel can extract the log and analyze it to get useful information. Routers usually rely on the established and maintained routing tables to decide how to forward data. The routing table is divided into static routing table and dynamic routing table. The static routing table is a routing table pre-set by the system administrator according to the network situation and will not change with the change of the network structure. Dynamic routing table router automatically learning and memory formation, due to power failure or network address adaptation varies depending on routing protocols [13-15]. Therefore, when obtaining evidence for routers, pay special attention to the dynamic routing table, as shown in figure 4.

Conclusion

At present, computer crimes have become the main means of illegal crimes, which can destroy criminal evidence during crimes. However, with the development of forensic technology, electronic forensics provides sufficient evidence for solving cases. This article divides electronic forensics technology into three categories: computer forensics, mobile phone forensics, and network forensics, focusing on the principles and applications of various forensics technologies.

In addition to the forensic technology involved in this article, there are also new technical directions such as instant messaging (IM) forensic technology and cloud computing forensic technology. For example, in the research direction of WhatsApp forensics, Gudipaty LP et al. decrypted the encrypted WhatsApp database in an unrooted Android mobile phone. With the advancement and development of science and technology, more and more electronic forensics technologies will appear, replacing traditional forensics technologies, which is conducive to the governance of cyberspace security.

References

1. Jahankhani H, Watson DL, Me G (2010). Handbook of electronic security and digital forensics. Singapore: World Scientific Publishing Company,573-583.
2. Kaplan RE (2008). Computer forensics —what is it good for? Journal of Digital Forensic Practice, 2(2): 57-61.
3. Vomel S, Freiling FC (2011). A survey of main memory acquisition and analysis techniques for the windows operating system. Digital Investigation, 8(1), 3-22.
4. Paul Joseph D, Norman J (2019). An Analysis of Digital Forensics in Cyber Security. In: Bapi R., Rao K., Prasad M. (eds) First International Conference on Artificial Intelligence and Cognitive Computing. Advances in Intelligent Systems and Computing, 815. Springer, Singapore.
5. Amit Singh (2006). Mac OS X Internals: A Systems Approach. Addison Wesley.
6. Ahmed R, Rajiv V (2008). “Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective.” 6th international conference on e-governance, iceg, emerging technologies in e-government, m-government.
7. Ayers R, Brothers S, Jansen W, (2014) “Guidelines on Mobile Device Forensics,” NIST Special Publication, 800-101.
8. Chernyshev M, Zeadally S, Baig Z, Woodward A, (2017). “Mobile Forensics: Advances, Challenges, and Research Opportunities,” in IEEE Security & Privacy, 15(6), 42-51.
9. Qing SH (2016) Research progress on Android security. Ruan Jian Xue Bao / Journal of Software, 27(1):45-71.
10. Lohiya R, John P, Shah P (2015) Survey on mobile forensics [J]. International Journal of Computer Applications, 118(16).
11. Cahyanto T, Prayudi Y (2014). “Web Server Logs Forensic Investigation to Find Attack’s Digital Evidence Using Hidden Markov Models Method ,” Snati,15-19.
12. Khadka B, Withana C, Alsadoon A, Elchouemi A (2015) “Distributed Denial of Service attack on Cloud : Detection and Prevention,”.
13. Husain MI, Sridhar R (2010). iForensics: Forensic Analysis of Instant Messaging on Smart Phones. Digital Forensics and Cyber Crime, 9-18.

14. Taylor M, Haggerty J, Gresty D, Lamb D (2011). Forensic investigation of cloud computing systems. Network Security, (3), 4-10.
15. GudipatyLP,JhalaKY(2015)WhatsAppForensics:DecryptionofEncrypted WhatsApp Databases on Non-Rooted Android Devices. J Inform Tech Softw Eng 5:147.

Author Affiliation

Top

Department of Computer Science, Jiangsu University of Technology, China