Forensic Investigation Processes for Cyber Crime and Cyber Space

K. K. Sindhu, Rupali Kombade, Reena Gadge and B. B. Meshram

Abstract Computers are an integral part of our life. A significant percentage of today's transactions and processes take place using the computer and Internet. People have readily adopted Internet technology and innocently trust it while using it with the ignorance of the limitations and threats to the system security. With the advance of technology, equally or more advanced form of crimes started emerging. Different types of cyber attacks from various sources may adversely affect computers, software, a network, an agency's operations, an industry, or the Internet itself. Thus companies and their products aim to take assistance of legal and computer forensics. Digital forensics deals with computer-based evidence to determine who, what, where, when, and how crimes are being committed. Computer and network forensics has evolved to assure proper presentation of cyber crime evidentiary data into court. Forensic tools and techniques are an integral part of criminal investigations used to investigate suspect systems, gathering and preserving evidence, reconstructing or simulating the event, and assessing the current state of an event. In this paper we deliberate on two aspects; first, various types of crimes in the cyber space and various sources of cyber attacks, and second, investigation processes for various cyber attacks with the help of digital forensic tools like WinHex [1].

Keywords Cyber crime · Cyber space · Digital forensic · Network forensic · File system forensic · Email forensic

K. K. Sindhu (✉) · R. Kombade · R. Gadge · B. B. Meshram
Computer Department, Veermata Jijabai Technological Institute, Mumbai, India
e-mail: kksindu@gmail.com

R. Kombade
e-mail: rupalikombade@gmail.com

R. Gadge
e-mail: reena.gadge10@gmail.com

B. B. Meshram
e-mail: bbmeshram@vjti.org.in

S. Sathiakumar et al. (eds.), *Proceedings of International Conference on Internet Computing and Information Communications*, Advances in Intelligent Systems and Computing 216,
DOI: 10.1007/978-81-322-1299-7_19, © Springer India 2014

Introduction

Digital forensics is new in the forensic science and efforts are underway to experiment, explore, discover, enhance, and reconstruct the incidents that work together to make the investigations complete and successful. A digital forensic investigation model is to make the investigation perfect and error free. Each footstep in investigation is decisive and evidence of scrutiny has to surface the facts. Overlooking one step or interchanging any of the steps may lead to incomplete or inconclusive results and erroneous interpretations. A computer crime culprit may escape from light of justice or an innocent suspect may suffer negative consequences. Ultimately, evidence left is in zeros and ones, so forensics investigation can be mislaid by criminal thoughts. Higher levels of concerns are to be on account of a forensics investigation to avoid any misleading and thereby any loop holes to the accused. In this paper we explain the investigation processes of crime committed in cyber space [2].

Cyber space is the electronic space of computer communication or networks. Cyber space was imagined and actually implemented as a borderless new space, transcending physical borders and formal legal rules. Within the past few years a new class of crime scenes has become more prevalent, that is, crimes committed within electronic or digital domains, particularly within cyber space.

Cyber Forensic is the discovery, analysis, and reconstruction of Evidence extracted from and/or contained in a computer, computer system, computer network, computer media, or computer peripheral. A digital forensic investigation is an inquiry into the unfamiliar or questionable activities in a cyber space or digital world. According to the Oxford Dictionary digital forensic science is the systematic gathering of information about electronic devices that can be used in a court of law. Digital forensic science is more popularly called digital forensics and sometimes also called computer forensics as digital forensics is the science of identifying, extracting, analyzing, and presenting the digital evidence that has been stored in the digital electronic storage devices to be used in a court of law.

A cyber crime can be defined as crime committed in the cyber space or crime committed with the assistance of the Internet. In cyber crime externally or internally the computer takes part in the attack. Cyber crime investigations are always difficult because the evidence are very critical, i.e., the life of data are sometimes within fractions of a second. Evidences in the running memory registers are available only in some seconds. Digital evidence [3] at present, the analysis of digital evidence, must depend on forensic tools such as Forensic Toolkit (FTK) of Encase, or WinHex. Most of them are commercial software and are too expensive for the small enterprises or individual. Digital evidence stored in a computer can play a major role in a wide range of crimes, including murder, rape, computer intrusions, espionage, and child pornography as proof of a fact of what did or did not happen. Digital information is fragile in that it can be easily modified, duplicated, restored, or destroyed, etc. In the course of the investigation, the

Table 1 Shows sources of evidence in different types of files in a computer

Sources of evidence in a computer	Description
User created files	Address books, E-mail files. Audio/video files. Image/graphics files. Calendars. Internet bookmarks/favorites. Database files. Spreadsheet files. Documents or text files.
User protected files	Compressed files. Misnamed files. Encrypted files. Password-protected files. Hidden files. Steganography.
Computer–created files	Backup files. Log files. Configuration files. Printer spool files. Cookies. Swap files. Hidden files. System files. History files. Temporary files.
Other data areas	Bad clusters, Computer date, time and password. Deleted files, Free space, Hidden partitions. Lost clusters, Metadata. Other partitions. Reserved areas, Slack space, Software registration information, System areas.

investigator should assure that digital evidence is not modified without proper authorization. The typical goal of an investigation is to collect evidence using generally acceptable methods in order to make the evidence accepted and admitted at court.

The final forensic report must include:

(1) Where the evidence was stored?
(2) Who had obtained the evidence?
(3) What had been done to the evidence?

Any step in the process must be carefully recorded in order to prove that the electronic records were not altered in the investigation procedure (Table 1).

Types of Cyber Crimes

Computers are an integral part of our life. A significant percentage of today's transactions and processes take place using information technology and the future is pregnant with innovations, including nanotechnology, silicon chips, quantum computers, and even biochips. People have readily adopted this technology and have innocently trusted it while performing many tasks, with ignorance about the limitations and threats to their securities. With this advance in technology, an equally advanced form of crimes has emerged. The crimes being committed in cyber space like Internet fraud, business espionage, pornography, sexual assault, online child exploitation, cyber terrorism, and more are on the rise. The following statistical data shows various attacks and their total percentage.

Table 2 Shows the statistical data on different types of attacks reported

Attack	Reported cases (%)
Data theft	33
Email abuse	22
Unauthorized access	19
Data alteration	15
Virus attacks	5
DoS attacks	3
Others	3

Data Theft

Data are precious assets in this modern age of Cyberworld. Data are important raw materials for business organizations, call centers, and I.T. companies. Data have also become an important tool and weapon for companies, to capture larger market shares. Due to the importance of data, in this new age, its security has become a major issue in the I.T. industry. The piracy of data is a threat faced by I.T. players who spend millions to compile or buy data from the market. Their profits depend upon the security of the data. The above statistics reveals that 33 % of cyber crime is data stealing (Table 2).

A case has been reported in Bangalore (9 Crore loss) where some key employees of the company had stolen source code and launched a new product based on stolen source code and mailed to former clients. Social engineering techniques can also be applied for such attacks. For example, a beautiful lady meets the young system admin and collects the username and password.

Email Abuse

Email abuse takes many forms, for example: unsolicited commercial email, unsolicited bulk email, mail bombs, email harassment, and email containing abusive or offensive content. The format for submitting reports to the abuse department regarding abuse of email is always the same whatever the offence.

Unauthorized Access

Unauthorized Access is when a person who does not have permission to connect to or use a system gains entry in a manner unintended by the system owner. The popular term is “hacking”.Hacking is the viewing of private accounts, messages, files, or resources, when one has not been given permission from the owner to do so. Viewing confidential information without permission or qualifications can result in legal action.

Data Alteration

Changing /modifying /deleting data causes major losses in the cyber world. In a crime reported in the USA (Cyber murder), a patient file data altered by a criminal caused overdose of medicine and the patient got killed.

Denial of Service

A denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service, large numbers of compromised systems (sometimes called a bonnet) attack a single target. Dos causes

- Attempts to "flood" a network, thereby preventing legitimate network traffic.
- Attempts to disrupt connections between two machines, thereby preventing access to a service.
- Attempts to prevent a particular individual from accessing a service.
- Attempts to disrupt service to a specific system or person.

Impact of the DoS is Denial-of-service attacks can essentially disable your computer or your network. Depending on the nature of your enterprise, this can effectively disable your organization. Secondly, some denial-of-service attacks can be executed with limited resources against a large, sophisticated site.

Malicious Codes

Viruses, worms, and Trojans are types of malicious codes which enter into the system without permission of the user and delete, modify, and capture the user files and data.

Sources of Attacks

Cyber crimes such as network intrusion, hacking, virus distribution, denial of service attacks, hijacking (a computer or network), defacing web sites, cyber stalking, and cyber terrorism are included in this category.

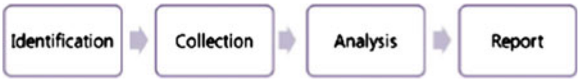


Fig. 1 Shows investigation processes

Basically, the computer itself becomes the "target" as well as "Source" of the crime. This is "unauthorized access" to the targeted system. The transmission of a program, information, code, or command, and as a result of intentionally causes damage without authorization, to a protected computer.

- Program/program source code.
- Disgruntled employees.
- Teenagers.
- Political Hacker.
- Professional Hackers.
- Business Rival.
- Desperados.
- Terrorists.

The Cyber Investigation Process of a Compromised System

Investigation Processes

The entire investigation process can be divided into four phases (Fig. 1).

1. Identification: In this phase it collects the information about the compromised system. System Configuration, software loaded, user profiles, etc [4].
2. Collection Phase: Collects the evidence from the following.
3. Evidence is most commonly found in files that are stored on hard drives and storage devices and media.
4. If file is deleted, recovering data from the deleted files and also collects evidence file deleted files.
5. Analysis phase: Analyze the collecting data/files and find out the actual evidence.
6. Report phase: The audience will be able to understand the evidence data acquired from the evidence collection and analysis phases. The report generation phase records the evidence data found out by each analysis component. Additionally, it records the time and provides hash values of the collected evidence for the chain-of-custody.

Investigating Tools

The goal of the investigator is to find every digital evidence stored in devices, or at least sufficient information for building and supporting a crime logic. Investigating tools are used to collect evidence from the crime scene. Throughout our paper mainly WinHex is using for image creation of compromised disk or folder and image analysis. WinHex [1] can recover deleted files.

Cyber Crime Investigation Steps

1. Assesses the crime scene
2. Evidence collection

   2.1 Select a tool, e.g.: WinHex [1].
   2.2 Create image of the compromised system disk.

      2.2.1 Open WinHex.
      2.2.2 Open particular drive (Tools → open disk).
      2.2.3 Calculate Hash value of the drive/disk (Tools → compute hash) Store hash value in a text file.
      2.2.4 Save disk content as image file extension.img file (Fig. 2).

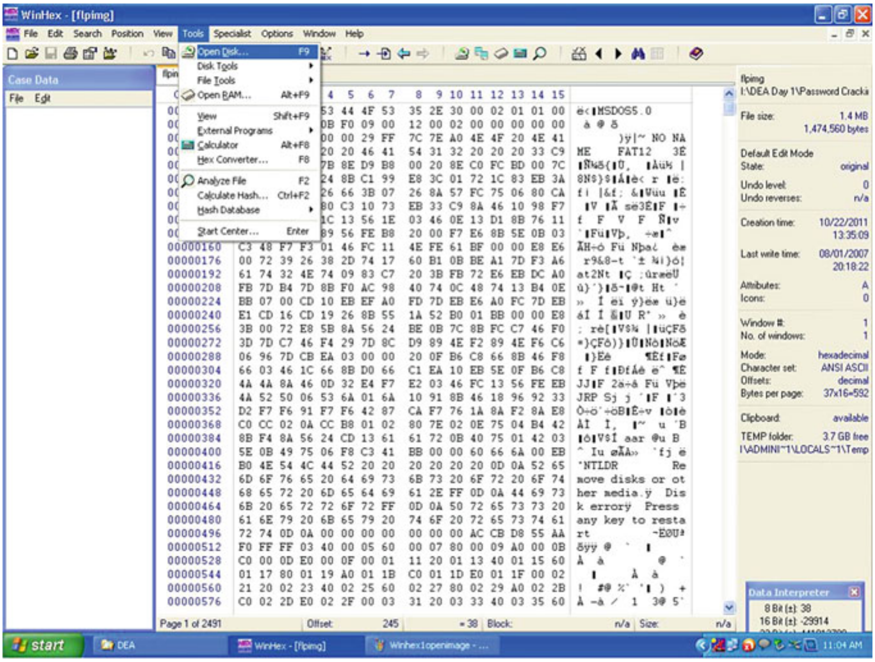
3. Analyze the Disk image

   3.1 Calculate Hash value of image (Tools → compute hash).
   3.2 Compare the Hash value of original with image. If equal start analysis else acquired data altered.
   3.3 Recover the necessary files and deleted files from the disk image. (Specialist → Interpret as image).
   3.4 Copied into a folder.
   3.5 Start analysis of the content recovered files of files.
   3.6 Image analysis, i.e., hidden data inside an image can be analyzed using steganography tools (Stools).
   3.7 Check header and footer of application file. Copy header and footer and paste into text pad. Sometimes evidence should be present in header and footers.

4. Conclude the investigation and generate report.

Recover Deleted File Using WinHex

1 Open Drive image [1].
2 Make as file view mode.



```
          4  5  6  7   8  9 10 11 12 13 14 15
00       53 44 4F 53  35 2E 30 00 02 01 01 00  ë<▮MSDOS5.0
00       0B F0 09 00  12 00 02 00 00 00 00 00   à @ ð
00       00 00 29 FF  7C 7E A0 4E 4F 20 4E 41          )ÿ|~ NO NA
00       20 20 46 41  54 31 32 20 20 20 33 C9  ME     FAT12   3É
00       7B 8E D9 B8  00 20 8E C0 FC BD 00 7C  ▮Ñ¼ð{▮Ù,  ▮Àü½ |
00       24 8B C1 99  E8 3C 01 72 1C 83 EB 3A  8N$}$▮Á▮è< r ▮ë:
00       26 66 3B 07  26 8A 57 FC 75 06 80 CA  f| |&f; &▮Wüu ▮Ê
00       80 C3 10 73  EB 33 C9 8A 46 10 98 F7   ▮V ▮Ã së3É▮F ▮÷
00       1C 13 56 1E  03 46 0E 13 D1 8B 76 11  f  F  V  F  Ñ▮v
00       89 56 FE B8  20 00 F7 E6 8B 5E 0B 03  `▮Fü▮Vþ,  ÷æ▮^
00000160 C3 48 F7 F3 01 46 FC 11  4E FE 61 BF 00 00 E8 E6  ÃH÷ó Fü Nþa¿  èæ
00000176 00 72 39 26 38 2D 74 17  60 B1 0B BE A1 7D F3 A6   r9&8-t `± ¾¡}ó¦
00000192 61 74 32 4E 74 09 83 C7  20 3B FB 72 E6 EB DC A0  at2Nt ▮Ç ;ûræëÜ
00000208 FB 7D B4 7D 8B F0 AC 98  40 74 0C 48 74 13 B4 0E  û}´}▮ð¬▮@t Ht ´
00000224 BB 07 00 CD 10 EB EF A0  FD 7D EB E6 A0 FC 7D EB  »  Í ëï ý}ëæ ü}ë
00000240 E1 CD 16 CD 19 26 8B 55  1A 52 B0 01 BB 00 00 E8  áÍ Í &▮U R° »  è
00000256 3B 00 72 E8 5B 8A 56 24  BE 0B 7C 8B FC C7 46 F0  ; rè[▮V$¾ |▮üÇFð
00000272 3D 7D C7 46 F4 29 7D 8C  D9 89 4E F2 89 4E F6 C6  =}ÇFô)}▮Ù▮Nò▮NöÆ
00000288 06 96 7D CB EA 03 00 00  20 0F B6 C8 66 8B 46 F8   ▮}Ëê     ¶Èf▮Fø
00000304 66 03 46 1C 66 8B D0 66  C1 EA 10 EB 5E 0F B6 C8  f F f▮ÐfÁê ë^ ¶È
00000320 4A 4A 8A 46 0D 32 E4 F7  E2 03 46 FC 13 56 FE EB  JJ▮F 2ä÷â Fü Vþë
00000336 4A 52 50 06 53 6A 01 6A  10 91 8B 46 18 96 92 33  JRP Sj j ▮▮F ▮▮3
00000352 D2 F7 F6 91 F7 F6 42 87  CA F7 76 1A 8A F2 8A E8  Ò÷ö▮÷öB▮Ê÷v ▮ò▮è
00000368 C0 CC 02 0A CC B8 01 02  80 7E 02 0E 75 04 B4 42  ÀÌ  Ì,  ▮~  u ´B
00000384 8B F4 8A 56 24 CD 13 61  61 72 0B 40 75 01 42 03  ▮ô▮V$Í aar @u B
00000400 5E 0B 49 75 06 F8 C3 41  BB 00 00 60 66 6A 00 EB  ^ Iu øÃA»  `fj ë
00000416 B0 4E 54 4C 44 52 20 20  20 20 20 20 0D 0A 52 65  °NTLDR        Re
00000432 6D 6F 76 65 20 64 69 73  6B 73 20 6F 72 20 6F 74  move disks or ot
00000448 68 65 72 20 6D 65 64 69  61 2E FF 0D 0A 44 69 73  her media.ÿ  Dis
00000464 6B 20 65 72 72 6F 72 FF  0D 0A 50 72 65 73 73 20  k errorÿ  Press
00000480 61 6E 79 20 6B 65 79 20  74 6F 20 72 65 73 74 61  any key to resta
00000496 72 74 0D 0A 00 00 00 00  00 00 00 AC CB D8 55 AA  rt         ¬ËØUª
00000512 F0 FF FF 03 40 00 05 60  00 07 80 00 09 A0 00 0B  ðÿÿ @  `  ▮
00000528 C0 00 0D E0 00 0F 00 01  11 20 01 13 40 01 15 60  À  à        @  `
00000544 01 17 80 01 19 A0 01 1B  C0 01 1D E0 01 1F 00 02   ▮     À  à
00000560 21 20 02 23 40 02 25 60  02 27 80 02 29 A0 02 2B  !  #@ %` '▮ )  +
00000576 C0 02 2D E0 02 2F 00 03  31 20 03 33 40 03 35 60  À -à /  1  3@ 5`
Page 1 of 2491    Offset:    245    = 38  Block:    n/a  Size:    n/a
```

flpimg
I:\DEA Day 1\Password Cracki

File size: 1.4 MB
1,474,560 bytes

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Creation time: 10/22/2011 13:35:09

Last write time: 08/01/2007 20:18:22

Attributes: A
Icons: 0

Window #: 1
No. of windows: 1

Mode: hexadecimal
Character set: ANSI ASCII
Offsets: decimal
Bytes per page: 37x16=592

Clipboard: available

TEMP folder: 3.7 GB free
I\ADMINI~1\LOCALS~1\Temp

Data Interpreter
8 Bit (±): 38
16 Bit (±): -29914

Fig. 2 Shows screenshot of Winhex [1] for creating an image of DISK

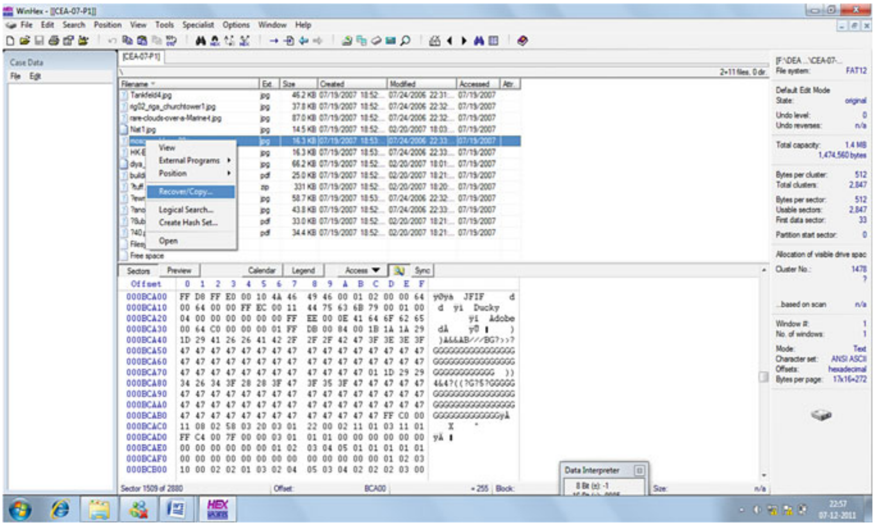
3 Recover the necessary files and deleted files from the disk image. (Specialist → Interpret as image).
4 Copy into a folder.
5 Start analysis of the content recovered files.
6 Open drive image–select file and right click.

Investigation on IPR Crime–Source Code Theft

IP crime is generally known as counterfeiting and piracy. Counterfeiting is intentional trademark infringement, while piracy involves intentional copyright infringement. Now, IPR crimes are becoming a big issue in big businesses. However, it is not a new phenomenon but due to globalization and advances in technology counterfeiting and piracy become big business (Fig. 3).

The investigation procedure of a source code theft

1. Assess the crime scene.
2. Find which source code files are thefts.
3. Calculate hash value of the theft files and save it into text file.
4. Find out who are involved in the project.



Filename	Ext.	Size	Created	Modified	Accessed	Attr.
Tankfeld4.jpg	jpg	46.2 KB	07/19/2007 18:52:...	07/24/2006 22:31:...	07/19/2007	
rig02_riga_churchtower1.jpg	jpg	37.8 KB	07/19/2007 18:52:...	07/24/2006 22:32:...	07/19/2007	
rare-clouds-over-a-Maine4.jpg	jpg	87.0 KB	07/19/2007 18:52:...	07/24/2006 22:32:...	07/19/2007	
Nat1.jpg	jpg	14.5 KB	07/19/2007 18:52:...	02/20/2007 18:03:...	07/19/2007	
mosc	jpg	16.3 KB	07/19/2007 18:53:...	07/24/2006 22:33:...	07/19/2007	
HK-E	jpg	16.3 KB	07/19/2007 18:53:...	07/24/2006 22:33:...	07/19/2007	
dya_	jpg	66.2 KB	07/19/2007 18:52:...	02/20/2007 18:01:...	07/19/2007	
buildi	pdf	25.0 KB	07/19/2007 18:52:...	02/20/2007 18:21:...	07/19/2007	
?uff	zip	331 KB	07/19/2007 18:52:...	02/20/2007 18:20:...	07/19/2007	
?ewr	jpg	58.7 KB	07/19/2007 18:53:...	07/24/2006 22:32:...	07/19/2007	
?ano	jpg	43.8 KB	07/19/2007 18:52:...	07/24/2006 22:33:...	07/19/2007	
?8ub	pdf	33.0 KB	07/19/2007 18:52:...	02/20/2007 18:21:...	07/19/2007	
?40.p	pdf	34.4 KB	07/19/2007 18:52:...	02/20/2007 18:21:...	07/19/2007	
Files						
Free space						

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000BCA00  FF D8 FF E0 00 10 4A 46  49 46 00 01 02 00 00 64  ÿØÿà  JFIF     d
000BCA10  00 64 00 00 FF EC 00 11  44 75 63 6B 79 00 01 00   d  ÿì  Ducky
000BCA20  04 00 00 00 00 00 00 FF  EE 00 0E 41 64 6F 62 65         ÿî  Adobe
000BCA30  00 64 C0 00 00 00 01 FF  DB 00 84 00 1B 1A 1A 29   dÀ     ÿÛ ▮     )
000BCA40  1D 29 41 26 26 41 42 2F  2F 2F 42 47 3F 3E 3E 3F   )A&&AB///BG?>>?
000BCA50  47 47 47 47 47 47 47 47  47 47 47 47 47 47 47 47  GGGGGGGGGGGGGGGG
000BCA60  47 47 47 47 47 47 47 47  47 47 47 47 47 47 47 47  GGGGGGGGGGGGGGGG
000BCA70  47 47 47 47 47 47 47 47  47 47 47 47 01 1D 29 29  GGGGGGGGGGGG  ))
000BCA80  34 26 34 3F 28 28 3F 47  3F 35 3F 47 47 47 47 47  4&4?((?G?5?GGGGG
000BCA90  47 47 47 47 47 47 47 47  47 47 47 47 47 47 47 47  GGGGGGGGGGGGGGGG
000BCAA0  47 47 47 47 47 47 47 47  47 47 47 47 47 47 47 47  GGGGGGGGGGGGGGGG
000BCAB0  47 47 47 47 47 47 47 47  47 47 47 47 47 FF C0 00  GGGGGGGGGGGGGÿÀ
000BCAC0  11 08 02 58 03 20 03 01  22 00 02 11 01 03 11 01     X    "
000BCAD0  FF C4 00 7F 00 00 03 01  01 01 00 00 00 00 00 00  ÿÄ ▮
000BCAE0  00 00 00 00 00 00 01 02  03 04 05 01 01 01 01 01
000BCAF0  00 00 00 00 00 00 00 00  00 00 00 00 00 01 02 03
000BCB00  10 00 02 02 01 03 02 04  05 03 04 02 02 02 03 00
```

Sector 1509 of 2880 Offset: BCA00 = 255 Block: Size: n/a

[F:\DEA ...\CEA-07-...
File system: FAT12

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Total capacity: 1.4 MB
1,474,560 bytes

Bytes per cluster: 512
Total clusters: 2,847

Bytes per sector: 512
Usable sectors: 2,847
First data sector: 33

Partition start sector: 0

Allocation of visible drive spac
Cluster No.: 1478
?

...based on scan n/a

Window #: 1
No. of windows: 1

Mode: Text
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 17x16=272

22:57
07-12-2011

Fig. 3 Screenshot of Winhex tool [1] to recover/copy deleted file

5. Investigate their USBs and PCs–Take an image of all drives using Winhex tool…
6. Investigate their email accounts—take an image of Email folders using Winhex tool.
7. Analyze the drives–Open drive images in Winhex.

   (Tools → open disk).

8. Calculate hash value of the drive/disk.

   (Tools → compute hash).

9. Store hash value in a text file.
10. Find out if source codes are available in drives.
11. If deleted recover all deleted files using winHex (Right click on the files folder and recover).
12. Again calculate the hash value of the recovered files.
13. If the hash value of the recovered source code files are equal, then commit the crime happened by the person who owns the above files.
14. Sometimes source code can hide inside the image.
15. We can find out the hidden data using steganography tools or click the particular image in the winHex and check the content displaying window. If the content contains hidden text data then it will display directly.

Algorithm to Find Evidence in the Storage Media

1. Start.
2. Take the image of the disk drive (using tools like Winhex or Linux dd command) (For integrity, perform hash value calculation).
3. Perform chkdisk of the particular drive.
4. Shows the number of bad sectors.
5. Open the particular drive using Runtime Explorer or Anadisk/BXDR.
6. Copy the content of bad clusters.
7. Analyze using any hexeditors.

Investigating Emails

Email is an essential type of communication in the current fast world. It is the most preferred form of communication. The ease, speed, and relative secrecy of emails have made it a powerful tool for criminals.

The following are the major email-related crimes.

1 Email spoofing.
2 Sending malicious codes through email.
3 Email bombing.
4 Sending threatening emails.
5 Defamatory emails.
6 Email frauds.

Email Investigation Procedure

Email investigation can be done with two methods Email tracking and Email tracing. Email Tracking tells us that tracking down an IP address will give a general idea of what city, state, and other geographical information pertains to the original sender. You can also determine what ISP a computer user is networked with through an IP address lookup tool. www.ReadNotify.com is an online service for email tracking. It tracks an email as to when it was read/reopened/forwarded, and much more. In cases where only an email ID is obtained as clue to track the sender of an email, services like ReadNotify.com can prove helpful. Email Tracing gives other information, such as how many times an email was sent to various servers and is an important method used for determining the original source of an email. By tracing an email you can determine the original sender's IP address, therefore giving you a geographical location of the email sender.

1. Assess the crime scene.
2. Take a copy of compromised email folder.

3. Analyze Email folder.

   3.1.1 Open Email folders–inbox, outbox, spam.
   3.1.2 Open each mail and analyze header of email.
   3.1.3 From header can identify IP address of source.

4. Analyze Body message.

   4.1.1 Copy body message into a notepad (text file).It shows any hidden formatted messages.

5. Download any attachments the particular email has.

If it contains any images, then check with steganography tools. All these analyses give the necessary evidence of the email crime.

Networks Forensic

Network forensics is a subfield of digital forensics where evidence is captured from networks and interpretation is substantially based on the knowledge of cyber attacks. It aims to locate attackers and reconstruct their attacks actions through the analysis of log files and monitoring network traffic.

Log File Analysis

In many cyber crime cases (especially web defacement cases), analysis of FTP and web server logs gives the most crucial evidence—IP address of the suspect [5]. Log files are key informers of web usage. Log files typically keep logs of the requests they receive. Data that are often logged by web servers for each request include Timestamps; IP address, Web server version, Web browser version, and OS of the host making the request; Type of request (GET/POST) read data or write data; the resource is requested and the status code. The response to each request includes a three-digit status code that indicates the success or failure of the request. Log file investigation procedure.

Step1 Collect server log file from the network administrator.
Step2 Open file notepad.
Step3 Searching key words (Given in the case scenario–or IP or admin username) from this file using searching utility of notepad.
Step 4 Copy and Paste those particular lines into another text file.
Step 5 Analyze all fields of logfile, for e.g.: IP, Access Time, file Path, status codes, methods (GET/POST).

Network Traffic Analysis

Network traffic analysis will help investigators to reconstruct and analyze network-based attacks and inappropriate network usage, as well as to troubleshoot various types of operational problems. Network forensic analysis relies on all of the layers. Analysts begin to examine data, likely an IP address, protocol, and port information. Collecting network traffic can create legal issues. Capture (intentional or incidental) of information breaks privacy or security implications, such as passwords or the contents of e-mails.

Sources of Network Traffic

- Firewalls and routers.
- Packet sniffers and protocol analyzers.
- Intrusion detection system.
- Remote access.
- Network forensic analysis tools.
- Other sources are:
- Dynamic Host Configuration Protocol Servers.
- Network Monitoring Software.
- Internet Service Provider Records.
- Client/Server Applications.
- Hosts. Network Configurations and Connections.

Examination and Analysis of Network Traffic

The examination process extracts and prepares data for analysis. The examination process involves data translation, reduction, recovery, organization, and searching. For example, known files are excluded to reduce the amount of data, and encrypted data are decrypted whenever possible to recover incriminating evidence. A thorough examination results in all relevant data being organized and presented in a manner that facilitates detailed analysis. The analysis process involves critical thinking, assessment, experimentation, fusion, correlation, and validation to gain an understanding of and reach conclusions about the incident based on available evidence (Casey and Palmer, 2004). In general, the aim of the analysis process is to gain insight into what happened, where, when, how, who was involved, and why [6].

The first step in the examination process is the identification of an event of interest. There are two types of identification.

1. Someone within the organization–system administrator, network administrator, user, or employee.
2. Some monitoring system like IDS or Firewall alerts showing an incident happened [6].

Child Pornography Investigation Examination Process Would Include

1. Examining all graphics or video files from network traffic.
2. Examining all web sites accessed.
3. Examining all Internet communications such as IRC, Instant Messaging (IM), and email.
4. A search for specific usernames and keywords to locate additional data that may be relevant.
5. Most of the relevant data to the investigation have been extracted from network traffic.
6. Extracted data made readable.
7. They can be organized in ways that help an individual analyze them.
8. Gain an understanding of the crime.

As the analysis process proceeds, a complete picture of the crime emerges often resulting in leads or questions that require the analyst to return to the original data to locate additional evidence, test hypotheses, and validate specific conclusions (Fig. 4).

Flow Reconstruction [6]

Because most networks use TCP/IP to transmit data between hosts each TCP connection is bi-directional, comprising one flow for receiving data and a second flow for sending data. Because TCP breaks data into packets prior to transmission, tools for examining network traffic require some ability to reconstruct flows [6].

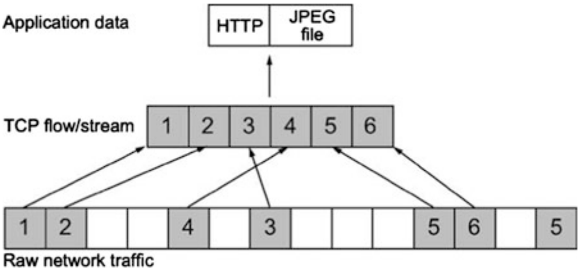


Fig. 4 A conceptual representation of packets in network traffic relating to a single flow being extracted and reconstituted to obtain the data they carry [6]

Conclusion

This paper explains introduction to digital forensics and summarizes different types of attacks and its sources in Sect. “Types of Cyber Crimes”. Section “The Cyber Investigation Process of a Compromised System” explains steps in the investigation process practically with WinHex tool. Section “Networks Forensic” explains the network forensics and investigation procedures in the log files as well as in the Network traffic.

References

1. WinHex (http://www.WinHex.com)
2. Carrier, B.D., Spafford, E.H.: Categories of digital investigation analysis techniques based on the computer history model. J. Digit Invest. Sci. 3S, S121–S130 (2006)
3. Di Pietro, R., Verde, N.V.: Digital forensic techniques and tools chapter 17 of security handbook of electronic security and digital forensics
4. Choi, J., Savoldi, A., Gubian, P., Lee, S., Lee, S.: Live forensic analysis of a compromised Linux system using LECT (Linux Evidence Collection Tool) 2008 IEEE
5. Arasteh, A.R., Debbabi, M., Sakha, A., Saleh, M.: Analyzing multiple logs for forensic evidence. Digit. Invest. J. Sci. 4S, S82–S91 (2007)
6. Casey, E.: Network traffic as a source of evidence: tool strengths, weaknesses, and future needs. Digit. Invest. J. 9–148 (2003)