CYBER SECURITY (PS02EMCA37)

Unit-4 : Computer Forensics & Forensics of Hand-Held Devices

- The Need for Computer Forensics
- Digital Forensics Life Cycle
- Forensics and Social Networking Sites: The Security/Privacy
- Threats
- Technical Challenges in Computer Forensics
- Hand-Held Devices and Digital Forensics
- Forensic Tools

The Need for Computer Forensics

- **What is Forensics?**

  It is the application of scientific methods and techniques to the investigation of crime.

- **What is digital forensics?**

  It is a branch of forensic science covering the recovery and investigation of material found in digital devices.

- **What is computer forensics?**

  It is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.

The Need for Computer Forensics

Need for computer forensics

- Union of ICT advances and the general use of computers worldwide
- High technical capacity of modern computers/computing devices
- New risks for computer users

Widespread use of computer forensics is the result of:

- Increasing dependence of law enforcement on digital evidence
- Everywhere use of computers after microcomputer revolution

Evidence

- Everything that is used to determine or demonstrate the truth of an claim.
- Can be used in court to prisoner people who are believed to have committed crimes.
- Handle carefully.

The Need for Computer Forensics

Cyber Security

Hidden and miniaturized storage media.

The Need for Computer Forensics

- The police officer or detective will take charge of a piece of evidence, document its collection and hand it over to an evidence clerk for storage in a secure place.
- All such transactions as well as every succeeding transaction between evidence, collection and its appearance in court need to be completely documented chronologically to fight legal challenges to the authenticity of the evidence.
- **Documentation must include**
  - Conditions under which the evidence is collected
  - The identity of all those who handled the evidence
  - Duration of evidence custody
  - Security conditions while handling or storing the evidence and
  - The manner in which evidence is transferred to subsequent custodians each time such a transfer occurs.

Digital Forensics Life Cycle

- As per **FBI's (Federal Bureau of Investigation)** view, digital evidence is present in nearly every crime scene.

- Law enforcement must know how to recognize, seize, transport and store original digital evidence to preserve it for forensics examination.

Digital Forensics Life Cycle

Phases in Computer Forensics/Digital Forensics

1. Preparation and identification
2. Collection and Recording
3. Storing and Transporting
4. Examination/Investigation
5. Analysis, Interpretation and Attribution
6. Reporting
7. Testifying

Digital Forensics Life Cycle

1. **Preparation and identification**

- Detect and identify the incident and make risk assessment of vulnerabilities and threats
- Obtain written and signed permissions from the concerned authorities to proceed.
- Prepare the paperwork to document the search
- Identifies potential sources of relevant evidence/information (devices) as well as key custodians and location of data.
- Determine kind of software and hardware for investigation according to suspect operating system.
- Specify tools that are accepted by courts.

Digital Forensics Life Cycle

2. Collecting and Recording Digital Evidence

✓ Computers , Cell phones

✓ Digital cameras

✓ Hard drives

✓ CD-ROM

✓ USB memory devices

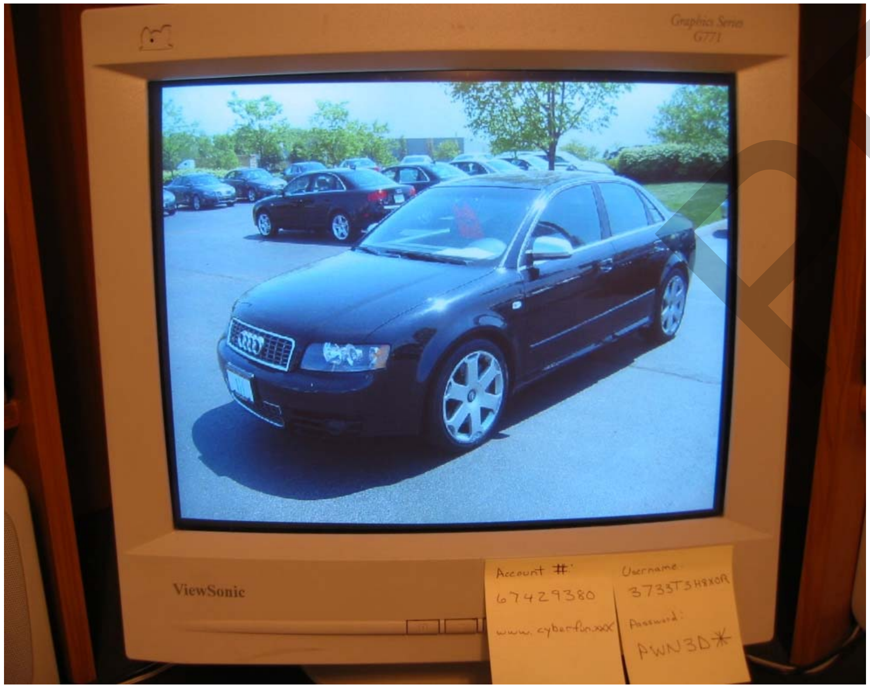
✓ Digital thermometers

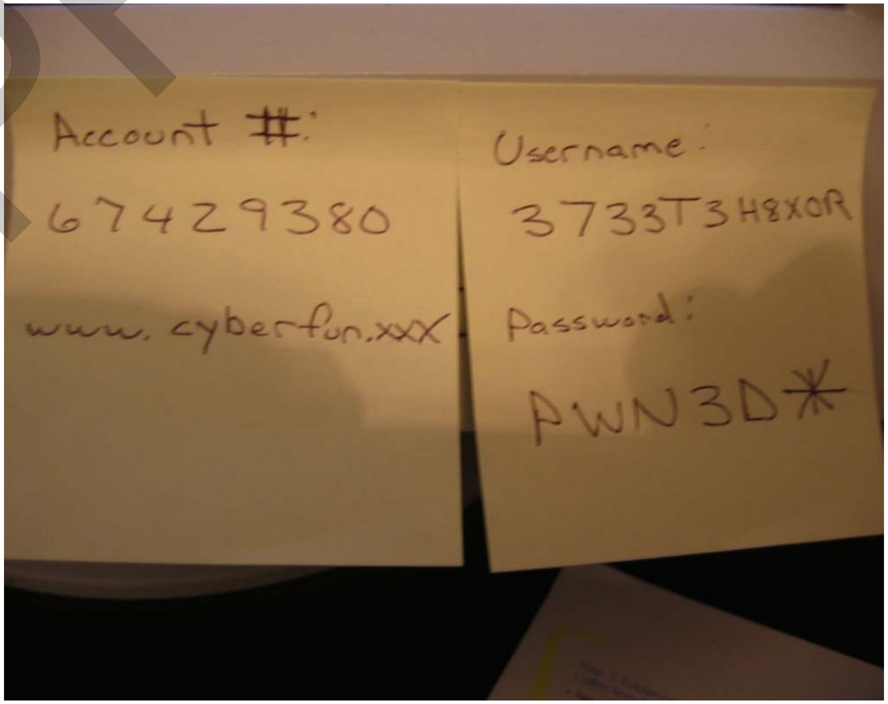
✓ Black boxes inside automobiles

✓ RFID tags and webpages

Collection

- Take detailed photos and notes of the computer / monitor
  - If the computer is "on", take photos of what is displayed on the monitor – DO NOT ALTER THE SCENE





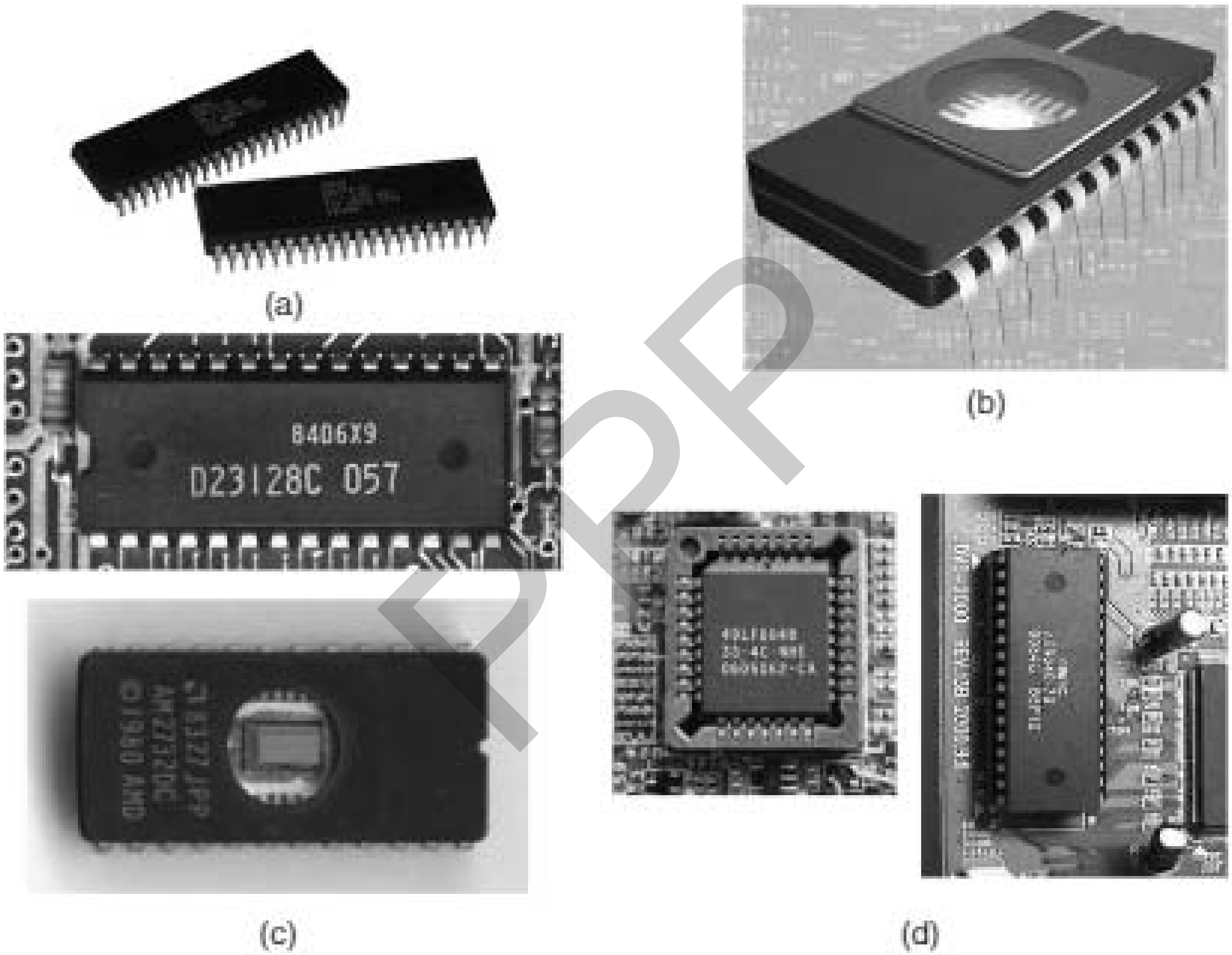
Digital Forensics Life Cycle

5 | Media that can hold digital evidences.

Digital Forensics Life Cycle

.7 | Some more media that can hold digital evidences.

Digital Forensics Life Cycle



Embedded memories inside computer. (a) Read-only memory (ROM) chips; (b) erasable programmable read-only memory (EPROM) chip; (c) programmable read-only memory (PROM) chips; (d) electrify erasable programmable read-only memory (EEPROM) chips.

Digital Forensics Life Cycle

3. Storing and Transporting Digital Evidence

- ✓ Image computer media using a **write-blocking tool** to ensure that no data is added to the suspect device.
- ✓ Establish and maintain the chain of custody
- ✓ Document everything that has been done
- ✓ Only use tools and methods that have been tested and evaluated to validate their accuracy and reliability.
- ✓ Care must be taken in transportation to prevent spoliation (in a hot car, digital media tends to lose bits).
- ✓ Care must be taken to preserve chain of custody and assure that a witness can testify accurately about what took place.

Digital Forensics Life Cycle

4. Examining/Investigating Digital Evidence

- ✓ Special care must be taken to ensure that the forensics specialist has the legal authority to seize, copy and examine the data.
- ✓ Sometimes authority rejects from a search warrant.
- ✓ As a general rule, one should not examine digital information unless one has the legal authority to do so.
- ✓ Unprofessional forensics examiners should keep this in mind before starting any unauthorized investigation.

Digital Forensics Life Cycle

5. Analysis, Interpretation and Attribution

- ✓ Digital evidence is extracted from the device, data is analyzed, and events are reconstructed.
- ✓ Before the analysis of the digital evidence, the digital forensics analyst must be informed of the objectives of the search, and provided with some background knowledge of the case and any other information that was obtained during the investigation that can assist the forensics analyst in this phase (e.g., IP address or MAC addresses).
- ✓ Attribution means meta data and other logs can be used to attribute actions to an individual. For example, personal documents on a computer drive might identify its owner.
- ✓ Open-source tools are available to conduct analysis of open ports, mapped drives on the live computer system.

6. Reporting

Digital Forensics Life Cycle

- ✓ A report is generated.
- ✓ The report may be in a written form or an oral testimony (or combination of the two).
- ✓ Evidence, analysis, interpretation and attribution to be presented in the form of expert reports, statements and testimony.
- ✓ Presentation of the report (a complex and tricky process)

Broad-Level Elements of the Report

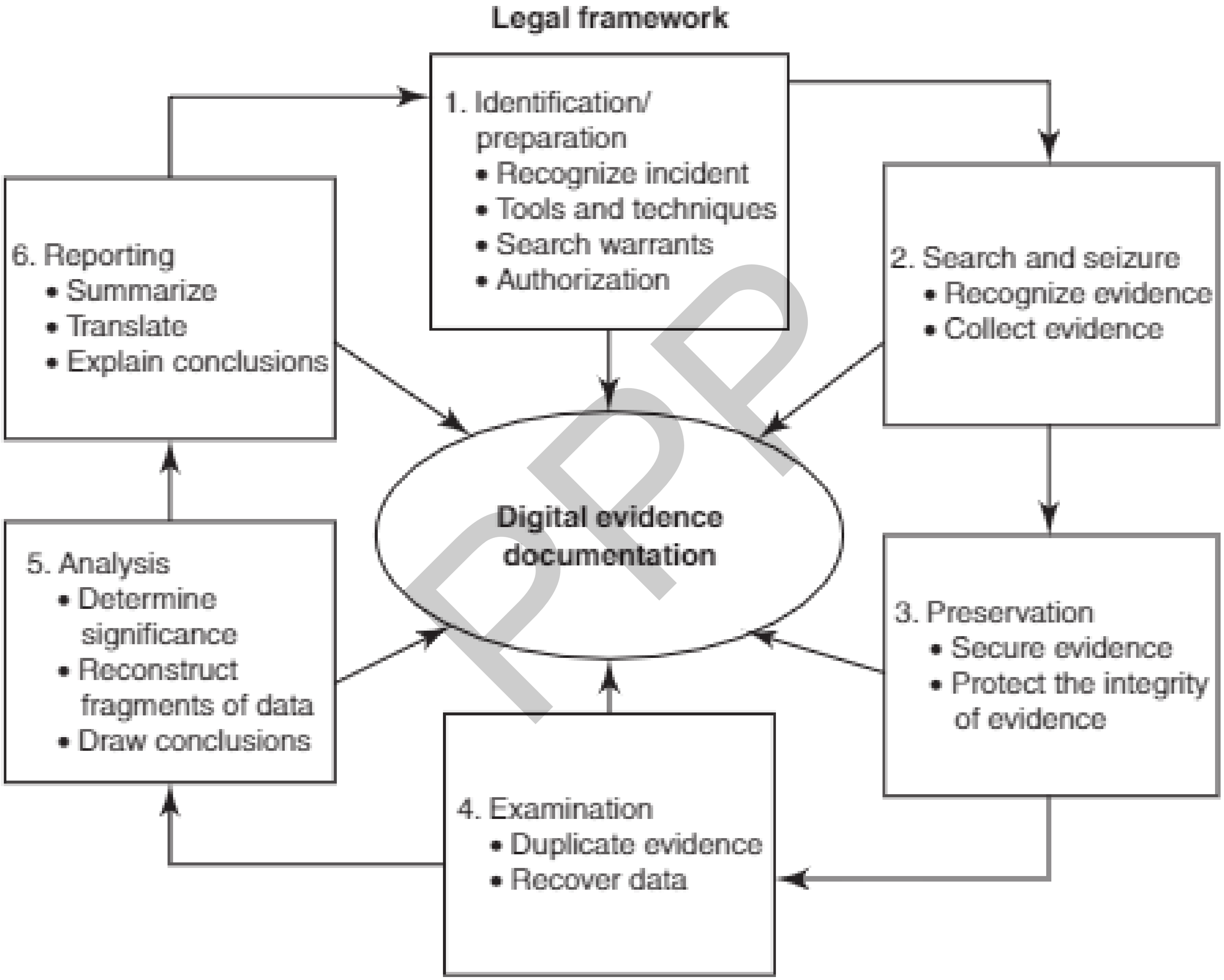
1. Identity of the reporting agency
2. Case identifier or submission number
3. Case investigator
4. Identity of the submitter
5. Date of receipt & Date of report
6. Serial number, make and model
7. Identity and signature of the examiner
8. Steps taken during examination
9. Results/conclusions

Digital Forensics Life Cycle

7. Testifying

- ✓ It involves presentation and cross-examination of expert witnesses.
- ✓ The forensic investigators should approach the expert witness to affirm the accuracy of evidence.
- ✓ An expert witness is a professional who investigates the crime to retrieve evidence.

Digital Forensics Life Cycle



Legal framework

1. Identification/ preparation
- Recognize incident
- Tools and techniques
- Search warrants
- Authorization

2. Search and seizure
- Recognize evidence
- Collect evidence

3. Preservation
- Secure evidence
- Protect the integrity of evidence

4. Examination
- Duplicate evidence
- Recover data

5. Analysis
- Determine significance
- Reconstruct fragments of data
- Draw conclusions

6. Reporting
- Summarize
- Translate
- Explain conclusions

Digital evidence documentation

.5 | Process model for understanding a seizure and handling of forensics evidence legal framework.

Forensics and Social Networking Sites: The Security/Privacy Threats

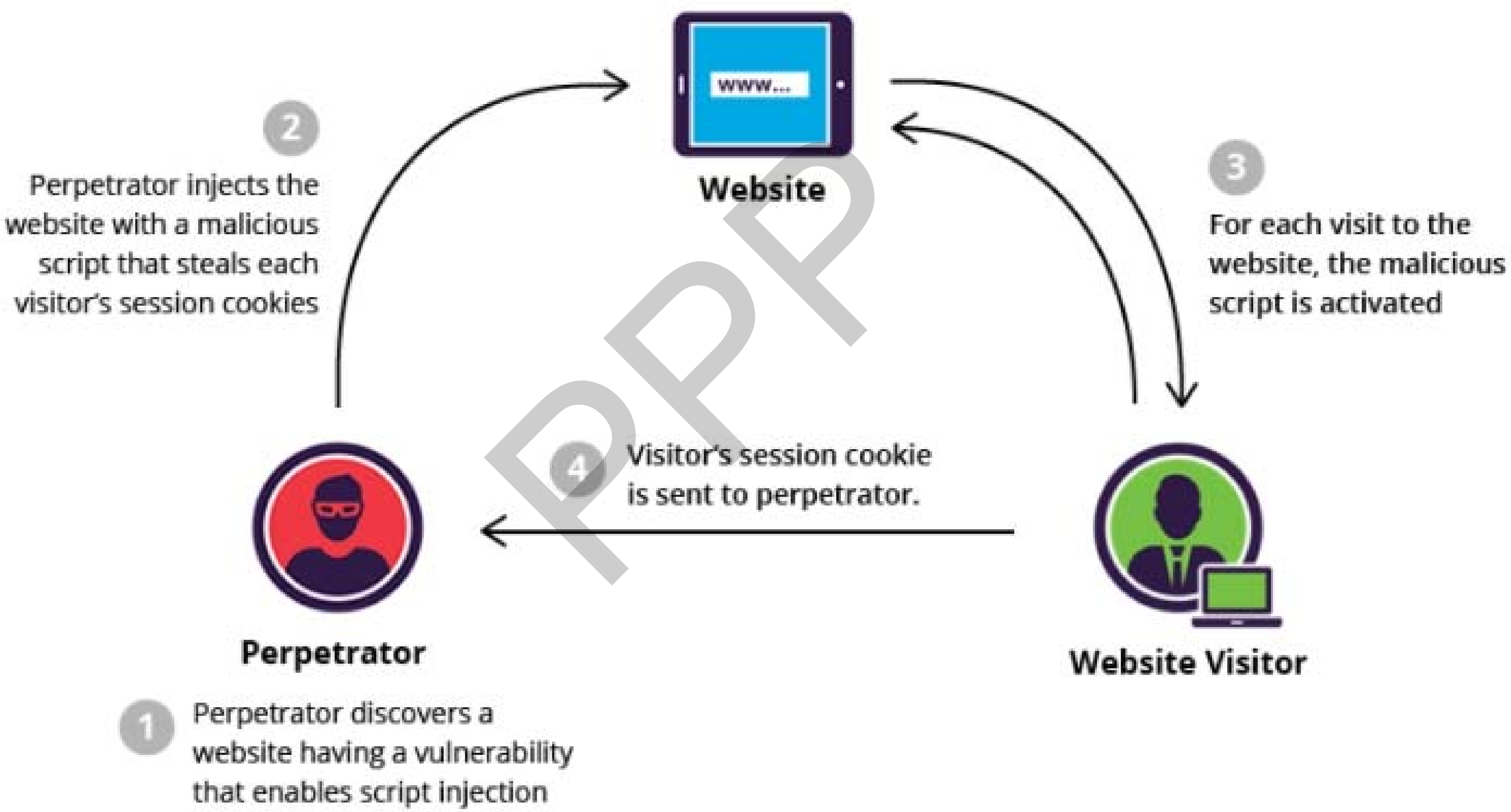
- Social networking Sites / Apps:
  - Orkut, Facebook, MySpace, Bebo, Twitter, LinkedIn, Instagram, WhatsApp etc.
- It enables people to reach out to their old/long lost friends and classmates, relatives, etc.
- Social networking sites help
  - Connect like-minded people,
  - People with the same professions or collaboration and
  - Discussion of ideas.
- Social networking, makes people part of a worldwide community and so the sites are getting popular.
- Maximum use of social networking sites by Kids and Teenagers
- Careless use of social networking sites allow the cyber attacks.

Forensics and Social Networking Sites: The Security/Privacy Threats

Security issues that are associated with social networking sites:

- Corporate espionage
- Cross-site scripting
- Viruses and worms
- Social networking site aggregators
- Spear Phishing and social networking specific Phishing
- Access of networks leading to data leakage
- ID theft
- Bullying
- Difficulty of complete account deletion.
- Spam
- Stalking

Cross Site Scripting



1 Perpetrator discovers a website having a vulnerability that enables script injection

2 Perpetrator injects the website with a malicious script that steals each visitor's session cookies

3 For each visit to the website, the malicious script is activated

4 Visitor's session cookie is sent to perpetrator.

Forensics and Social Networking Sites: The Security/Privacy Threats

Forensics skill is required to analyze and quantify the preserved data to answer the following questions.

1. Who posted the offending content?

2. Is there a 'real live' person to whom the offending content can be attributed even when evidence exists?

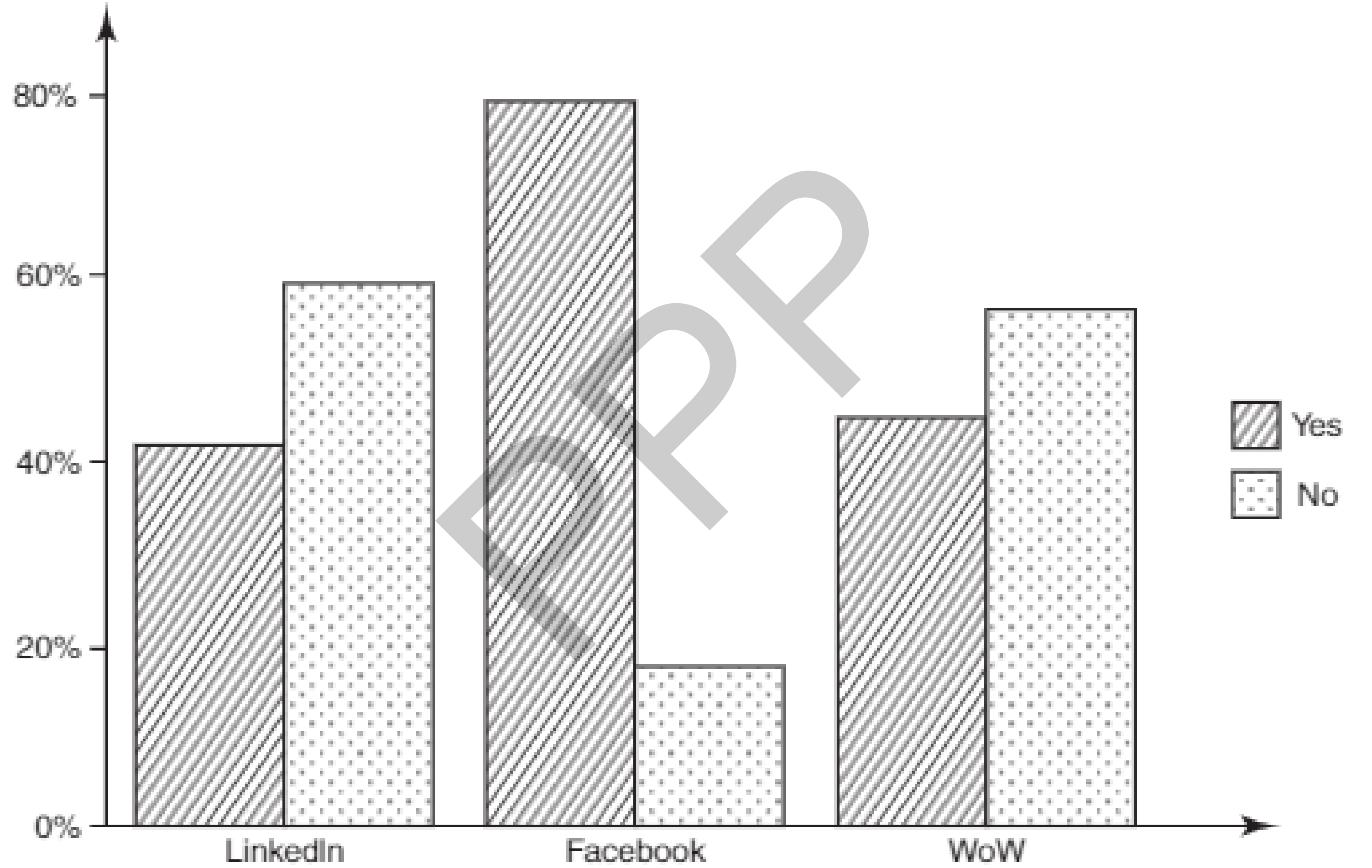
3. Can we identify the time frame associated with the posting of the offending content?

4. How much of the offending content exists across the entire social networking platform?

5. Is there other evidence that supports interpretation of the relevant content?

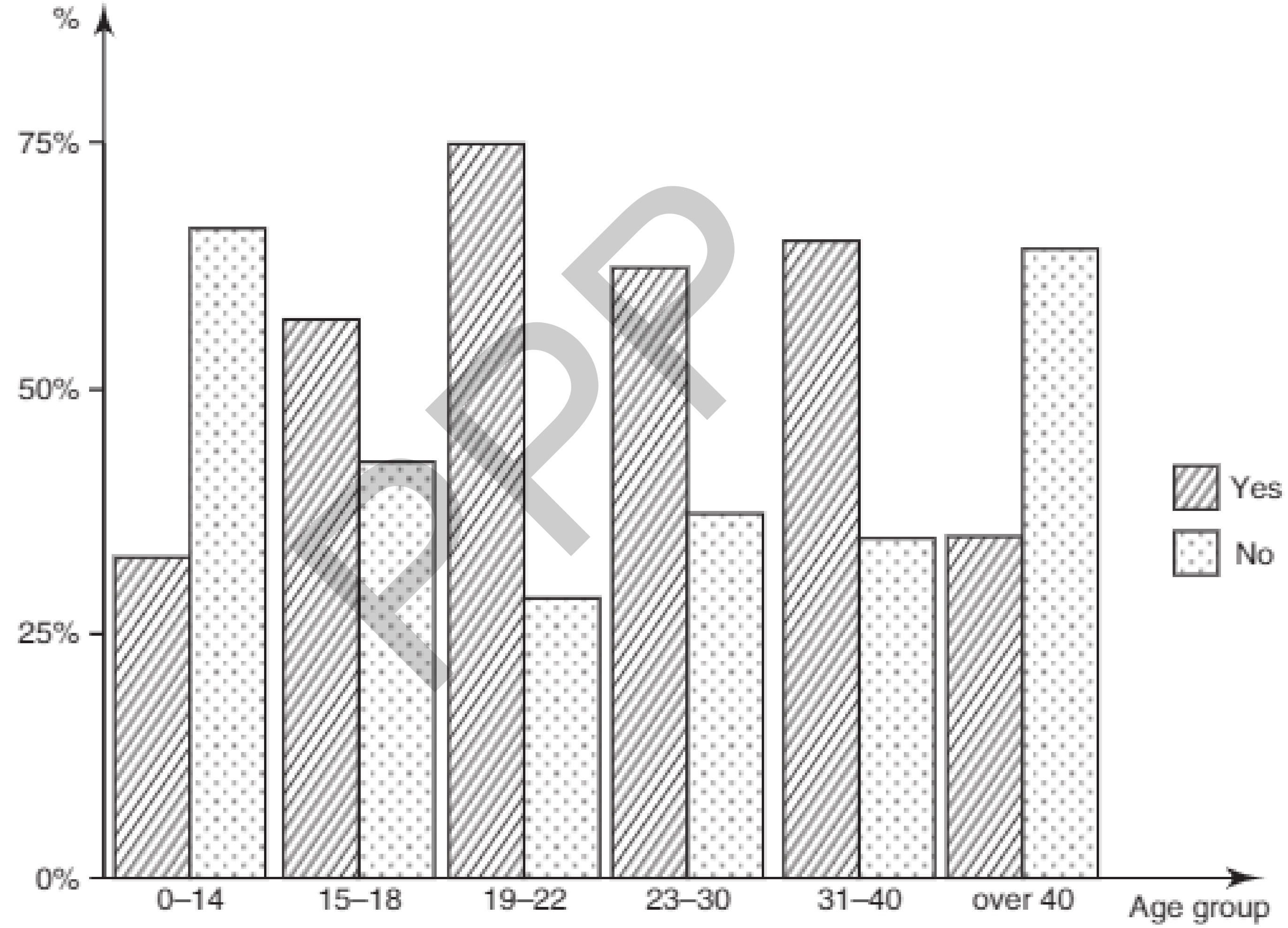
6. How accurate is the reported physical location?

Forensics and Social Networking Sites: The Security/Privacy Threats



.23 User concerns about privacy on social networking sites (LinkedIn, Facebook, WoW).
Source: The Paper by Helen Drislane and Kelly Heffner, 14 May 2007, is available at http://www.eecs.harvard.edu/cs199r/fp/HelenKelly.pdf (25 January 2010).

Forensics and Social Networking Sites: The Security/Privacy Threats



24 Privacy concerns about social networking sites vary with age.
Note: This is with regard to openness about sharing personal information.
Source: The paper by Helen Drislane and Kelly Heffner (14 May 2007) is available at http://www.eecs.harvard.edu/cs199r/fp/HelenKelly.pdf (25 January 2010).

Forensics and Social Networking Sites: The Security/Privacy Threats

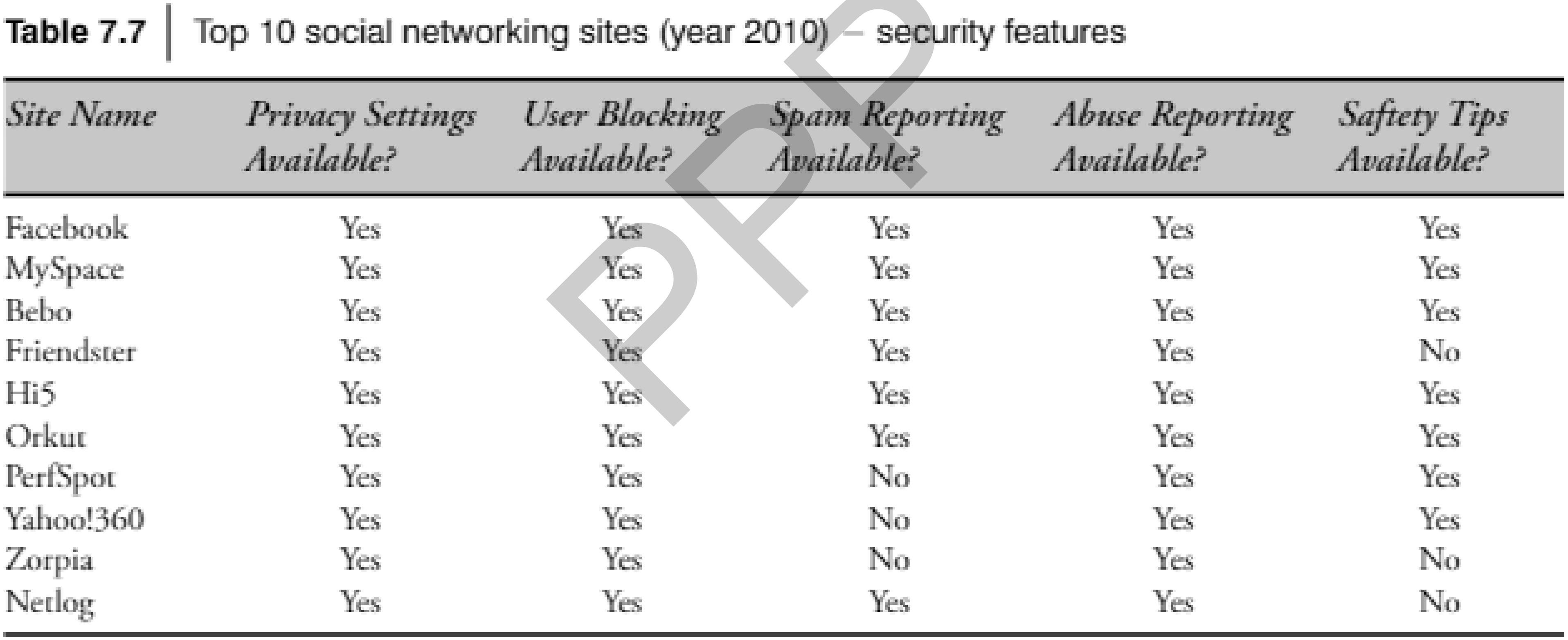
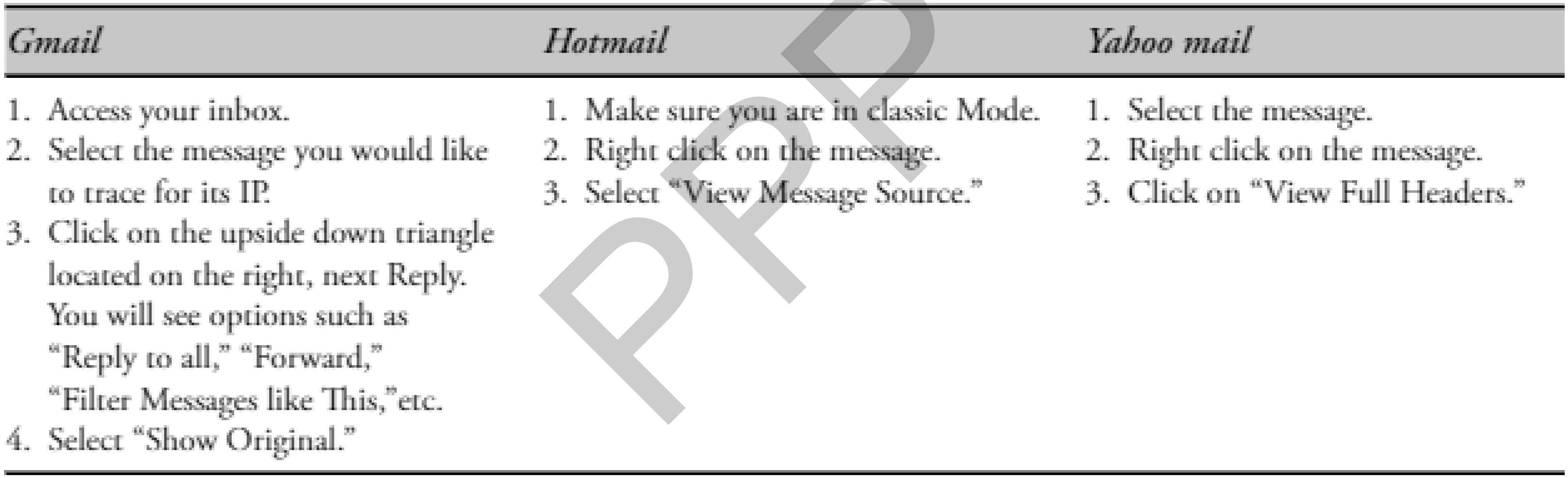


Table 7.7 | Top 10 social networking sites (year 2010) – security features

Site Name	*Privacy Settings Available?*	*User Blocking Available?*	*Spam Reporting Available?*	*Abuse Reporting Available?*	*Saftety Tips Available?*
Facebook	Yes	Yes	Yes	Yes	Yes
MySpace	Yes	Yes	Yes	Yes	Yes
Bebo	Yes	Yes	Yes	Yes	Yes
Friendster	Yes	Yes	Yes	Yes	No
Hi5	Yes	Yes	Yes	Yes	Yes
Orkut	Yes	Yes	Yes	Yes	Yes
PerfSpot	Yes	Yes	No	Yes	Yes
Yahoo!360	Yes	Yes	No	Yes	Yes
Zorpia	Yes	Yes	No	Yes	No
Netlog	Yes	Yes	Yes	Yes	No

Forensics and Social Networking Sites: The Security/Privacy Threats

Table 7.8 | Retrieving sender's IP address from E-Mail received



Gmail	*Hotmail*	*Yahoo mail*
1. Access your inbox. 2. Select the message you would like to trace for its IP. 3. Click on the upside down triangle located on the right, next Reply. You will see options such as "Reply to all," "Forward," "Filter Messages like This,"etc. 4. Select "Show Original."	1. Make sure you are in classic Mode. 2. Right click on the message. 3. Select "View Message Source."	1. Select the message. 2. Right click on the message. 3. Click on "View Full Headers."

Technical Challenges: Understanding the Raw Data and its Structure

Two aspects of technical challenges:

Complexity Problem

Quantity problem

<u>“Complexity” problem :</u>

Selected data is typically at the lowest and most row format.

- Non-technical person may not be able to understand such format.
- To resolve such problem tools are used to translate data through one or more **“abstraction layer”** until it can be understood.
- The data that represents the files in a directory exist in formats that are too low level to identify without the assistance of tools.
- **The directory is a layer of abstraction in the file system.**

Technical Challenges: Understanding the Raw Data and its Structure

- **Examples of Non-file system layers of abstraction include:**
  1. ASCII
  2. HTML Files
  3. Windows Registry
  4. Network Packets
  5. Source Code.

“Quantity” problem

- it involves the hugeness of digital forensics to analyze.
- It is inefficient to analyze every single piece of it.
- Data reduction techniques need to be used to solve this.
- Data reduction is done by grouping data into one larger event or by removing known data.

Technical Challenges: Understanding the Raw Data and its Structure

Examples of abstraction layers are data reduction techniques

1. Identifying known network packets using IDS (Intrusion Detection System) signature.

2. Identifying unknown entries during log processing.

3. Identifying known files using hash databases.

4. Sorting files by their type.

Technical Challenges: Understanding the Raw Data and its Structure

ASCII is an example of abstraction.

- Every letter of the English alphabet is assigned to a number between 32 and 127.
- When a text file is saved, the letters are translated to their numerical representation and the value is saved on the media as bits (o and 1).
- When the file is viewed in the raw, it shows a series of ones and zeros.
- **When the ASCII layer of abstraction is applied**, the numerical values get mapped to their corresponding characters and the file is displayed as series of letters, numbers and symbols.
- A **text editor is an example of a tool** operating at this layer of abstraction.

Hand-Held Devices and Digital Forensics

Device forensics has many aspects such as

1. Mobile phone forensics
2. PDA forensics
3. Digital music forensics
4. iPod forensics
5. Printer and Scanner forensics

Mobile Phone Forensics

- The science of recovering digital evidence from a mobile phone.
- Mobile phones are not covered in classical computer forensics.
- Cell phones vary in design and are continually evolving in terms of functionality and features as current technologies continue to become obsolete and new technologies are introduced.
- Cell phone forensics includes the analysis of SIM and phone memory.

Hand-Held Devices and Digital Forensics

- The “IMEI number” (International Mobile Equipment Identity) of a cell phone is a very important starting point for the First Information Report (FIR) procedure.

- A cell phone can be traced with its IMEI number.

- Every time a cell phone is switched ON or a call is made, the IMEI number is transmitted out to the network provider where it gets tallied against an information directory called Equipment Identity Register (EIR).

- Using the EIR information, a telecom company can locate a particular cell phone by pinpointing its proximity to the nearest tower.

Hand-Held Devices and Digital Forensics

PDA Forensics

Personal digital assistant (PDA) is also referred to as “palm device” or “hand-held.”

✓The most common operating system (OS) used are the Palm OS (Palm, Sony, Handspring), Windows for Palm (HP), MS Pocket PC (Compaq), Embedix (Sharp).

✓Modern PDAs are hybrid devices integrating wireless, Bluetooth, infrared, Wi-Fi, mobile phone, camera, GPS, basic computing capabilities, Internet, etc.

✓Criminals are increasingly using PDAs in committing electronic crimes

✓Given the compact size and integrated features of PDAs, it becomes convenient for criminals to use them.

Hand-Held Devices and Digital Forensics

Printer Forensics

- Printers are simply installed and, as long as they work, nobody pays any attention to them until it is time to reload the paper or replace the toner cartridge.

- Modern day printers have computer-like characteristics with internal storage, FTP uploading, Simple Network Management Protocol (SNMP), etc.

- Some printers are loaded with vulnerable applications.

- Hackers can access classified information sent to the printer.

- Printers can be turned into remote-controlled Bots and be used as a launching pad for further attacks.

Hand-Held Devices and Digital Forensics

Printer Forensics

Possible attacks through printer exploits are as follows:

1. Modifying IP address of the printer to an unused address on the same subnet.
2. Changing IP address of the target machine to the IP address of the printer.
3. Capturing all traffic sent over Port 9100 to the IP address to which end-users are configured to print. The attacker can keep collecting print jobs until it is found out.
4. Forwarding all print jobs onto the "new" IP address of the printer; when the end-user who submitted the job goes to the printer in question to collect the print job, he/she finds that it has been processed as normal.

Hand-Held Devices and Digital Forensics

Smartphone Forensics

✓ Smartphones are gaining momentum as a device option for people working at the field.

✓ The main reason for rising popularity of Smartphones is their high functionality.

✓ Smartphones are mobile phones based on high-level OS.

Hand-Held Devices and Digital Forensics

Some of the Features in a Smartphone

- It has address book, messenger, photo and video camera.
- It has GPS navigation facility.
- It works as a Web Client to access Web-based applications.
- It is a platform for third-party applications.
- IMEI number, hardware and software version numbers
- **Event log**

  incoming, outgoing,

  missed calls history,

  sent and received messages history,

  GPRS and Wi-Fi sessions, etc.
- SIM card contains the International Mobile Subscriber Identity (IMSI)
- Caller group information and assigned speed dial information.

Hand-Held Devices and Digital Forensics

iPhone Forensics

- The Apple iPhone already has a significant footprint in forensics investigations.

- The iPhone has an active ethical hacking community that is engaged in research and has yielded tools to support forensics investigations.

- Several commercial software packages now offer iPhone support.

Forensics techniques utilized with iPhone

1. Acquire data directly from the iPhone
2. Acquire a backup or logical copy of the iPhone file system using Apple's protocol
3. Physical bit-by-bit copy

Hand-Held Devices and Digital Forensics

Some tools used for iPhone forensics

1. MacLockPick
2. WOLF
3. Cellebrite UFED Forensics System
4. MDBackup Extract
5. Zdziarski’s method

Hand-Held Devices and Digital Forensics

Challenges in Forensics of the Digital Images and Still Camera

✓ Experts may come across a number of digital photographs.

✓ Digital image forensics technique is used to distinguish images captured by a digital camera from computer-generated images.

✓ Digital rights management, locating steganographic images, etc. are some more technical examples.

✓ Forensic institutions and wider law enforcement agencies have concerns regarding security, integrity and continuity of digital images.

Hand-Held Devices and Digital Forensics

<u>Two main interests in image forensics</u>

1.Source identification

2.Forgery detection

<u>Image source identification may include one of the following approaches</u>

1. Verifying and evaluating the image statistics.

2. Detecting, classifying and measuring the qualities of structures

3. Identifying signatures to detect traces of certain types of operations used in image generation.

Forensic Tools

Acquisition of data from a hand-held device is carried out in the following two ways:

1. Physical acquisition : An exact copy bit-by-bit is collected of the entire physical storage which can be either a RAM chip or a disk drive.

2. Logical acquisition : An exact copy bit-by-bit of the logical storage such as file and directories, involved residing on a logical store which could be several disk drives.

Forensic Tools

1. EnCase :

- It is tool for PCs and Palm OS.
- **Support following features:**

  Analytical tools

  Suspect media acquisition

  Data capture

  Documentation

  Bookmarking (Highlight Files, Folders or sections of files)
- Forensics examiner can then look over the device content to trace any evidence without the original data being getting manipulated.

2. Device Seizure and PDA Seizure

- These are two famous tools from Paraben.
- **Device Seizure** used for viewing cell phone data.
- **PDA Seizure** is used to obtain and examine the data on PDAs.
- It can produce a forensics image of Palm OS and Pocket PC devices.
- It also used for bookmark and organize information.
- It provides collection of images according to their file extensions.

Forensic Tools

Tools available for cell phone forensics

3. Forensics Card Reader (FCR)

- It allows to acquire data from SIM cards without modification and a smart card reader with USB connection.
- To select specific data elements like

  Phone Directory

  Abbreviated dialling numbers

  Fixed dialling numbers

  SMS messages

  Deleted messages

  E-mail addresses

- FCR reader allows examiners to use either small or large SIM cards without the need for an adapter.

- FCR also reads SIM cards for GSM mobiles and 3G mobiles.

Forensic Tools

Tools available for cell phone forensics

4. Cell Seizure

- It is software toolkit used for acquiring, searching, examining and reporting data associated with cell phones operating over CDMA, GSM and TDMA.
- Following data can be obtained.

  SMS history : inbox / outbox

  Phonebook : SIM card, speed dialling, fixed dialling

  Call logs : Dialled numbers, received calls, missed calls

  Calandar : Reminder, meeting, memo

  Graphics: Wallpaper, picture camera images

  WAP (Wireless Application Protocol): WAP settings