Computer Forensic
Evidence Collection and Management

Chapter 13

Mobile Phone and PDA Investigations

Chapter Objectives

- Become familiar with wireless networks, mobile phones and personal digital assistants (PDAs)
- Identify the various wireless providers and communication devices currently in the wireless network
- Learn the definitions of terms associated with the wireless environment and infrastructure
- Look at the various forensic tools that can be utilized to obtain evidence
- Identify techniques and processes for identifying, retrieving, and managing wireless forensic evidence

Introduction

- Mobile phones have come a long way since their inception.
- The types and amount of data stored on the modern cellular phone increase every year, with cell phones possessing the capability and capacity of sending text messages, e-mail messages, and even sound files.
- Unfortunately, there are times when either a catastrophic even has caused data loss, or the phone is used in a malicious manner and contains critical evidence.
- Mobile phone data storage is proprietary, based on the manufacturer, model, and system.
- Mobile phone forensics includes retrieval and examination of data found on the subscriber identity module or universal subscriber identity module (SIM/USIM), the phone body, and the optional memory cards.
- Security mechanism in mobile phones prevent a direct image of the data being taken.
- The arduous task of data retrieval and examination from a mobile phone or PDA is not an easy one.

Wireless Protocols and Components

- The examiner must have understanding of the protocols used in the wireless network.
- Network components and electronic devices include the SIM, handset, and mobile telephone switching office (MTSO).
- The figure below depicts the connectivity between the mobile device, local telco central office, and the MTSO.

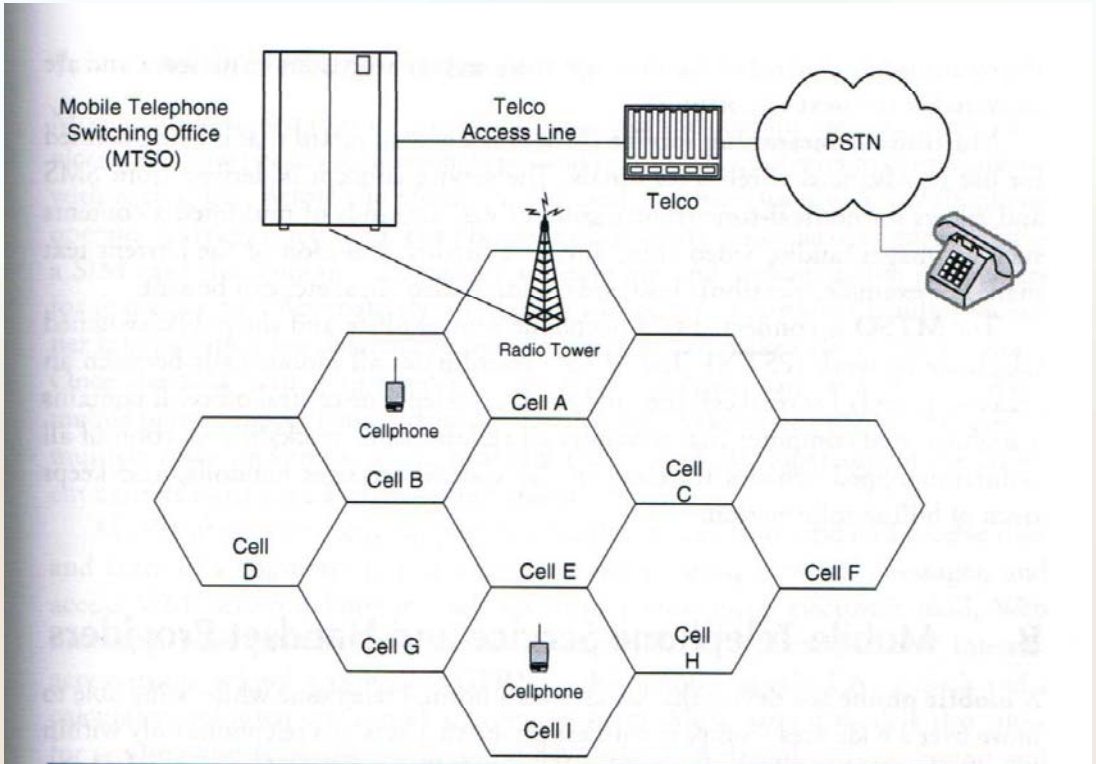

Figure 13.1 Cellular telephone system.

Wireless Protocols and Components (Cont.)

- The protocol standards and systems that operate in the wireless environment include:
  - GSM is the most widely used digital mobile phone system and the de facto wireless telephone standard in Europe.
  - TDMA is a digital air interface technology used in cellular, personal communications service (PCS), and enhanced specialized mobile radio (ESMR) networks.
  - CDMA is spread spectrum air interface technology used in some digital cellular, PCS, and other wireless networks.
  - GPRS is a packet-switched technology that allows Internet and other data communications over GSM network.
  - WAP is secured specification that allows users to access information instantly via handheld wireless devices.
  - SMS is available on digital GSM networks allowing text messages of up to 160 characters to be sent and received.
  - Multimedia messaging service (MMS) is a new standard that is being defined for use in advanced wireless terminals.
  - MTSO is connected to a telephone central office and the public switched telephone network (PSTN)

Mobile Telephone Service and Handset Providers

- Mobile phones allow connections to be made to the telephone network, through the MTSO, normally by directly dialing the other part's number on a keypad.
- The mobile phone consists of a handset, software, and memory.
- Many different companies provide a variety of mobile communications devices and services. A short list of providers includes:
  - Verizon
  - Cingular
  - Sprint
  - Nextel
  - BellSouth
  - AT&T
  - T-Mobile
- Handsets with varies features and options are available form a number of vendors.
- This is an issue with forensic examiners, as the number of different models, software, memory devices, and cables are almost infinite.
  - Nokia
  - Motorola
  - Siemens
  - Ericsson
  - Sony
  - Samsung
  - LG
  - PalmOne

Mobile Telephone Service and Handset Providers (Cont.)

Mobile Phone Features

- Mobiles are designed to work on cellular networks and contain a standard set of services that allow pones of different types and in different countries to communication with each other.
- Many mobile phones support auto-roaming, which permits the same phone to be used in multiple zones and countries.
- Mobile phones not only support voice calls, but can also send and received data and faxes, send short messages or test messages, and access WAP services.
- Sound and video recording is often also possible. This features is generally referred to as MMS.
- This give rise to some concern about privacy.
- There are also many additional features, such as user-defined and downloadable ring tones, phonebook, data book, encryption, walkie-talkie, and logos.
- A number of these features can provide the forensic examiner with possible source of evidence.
- A smart phone is generally considered any handheld device that integrates personal information management and mobile phone capabilities in the same device.

Subscriber Identity Module (SIM)

- The SIM is a smart card containing the telephone number of the subscriber, encoded network identification details, the personal identification number (PIN), and many other used data, such as the phone book.
- The terms SIM, smart card, and universal integrated circuit card (UICC) have an unfortunate tendency to be used interchangeably.
- A typical SIM contains several categories of information.
  - Actual identity of the card itself.
  - The actual operation of the device
  - Personalized information.
- A SIM has three main purposes.
  - Uniquely identify the subscriber
  - Determines phone number
  - Contains algorithms for network authentication

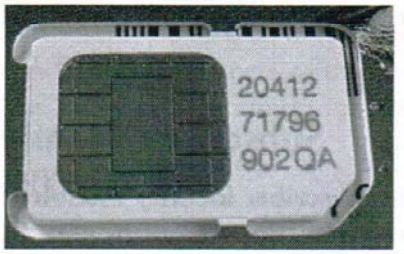

Figure 13.2 Sample SIM.

- The UICC is the chip card used in mobile terminals in 3G telecom networks and system.
- It ensures the integrity and security of all kinds of personal data.
- The UMTS is the upcoming globally standardized system for mobile telephone and data communications.

Subscriber Identity Module (SIM) (Cont.)

SIM Implementation

- SIM Cards can be used in any kind of device or situation where there is a need to authenticate the identity of a user.
- The primary use of SIM cards in the United States is in cell phones.
- Europe has seen a wider use of these cards.
- The cared companies in the Unites States have evidently not seen enough fraud to have a business justification to switch to this technology.
- The SIM uses a hierarchically organized file system that stores names, phone numbers, and received and sent text messages.
- One downside to the user of SIM cards is the amount of thefts that occur.

Subscriber Identity Module (SIM) (Cont.)

SIM Security

- The personal identification number (PIN) and the card holder verification (CHV) help secure the information located on the SIM.
- Unblocking CHV1 and CHV2 is a secret code made up of 8 to 10 digits that is used to reactivate a SIM card that has been blocked, an to define a new PIN.
- When PIN protection is enabled, every time the phone is turned on, the PIN must be entered.
- If the PIN is incorrectly entered three times in a row, the phone is locked.
- If the PIN is entered 10 ties incorrectly, the SIM is permanently disabled and the SIM must be exchanged.

Memory Cards

- Removable media extends the storage capability of the mobile phone, which allows for the storage of additional information beyond the device's built-in capacity.
- The primary type of removable media for a wireless phone is a memory card, which is similar to a SIM in size, but has different set of specification sand characteristics.
- A wide variety of memory cards exits on the market of mobile phones and other mobile devices.
- This media is normally formatted with conventional file system and can be treated as a disk drive.
- This allows for the cards to be imaged and analyzed using a conventional forensic tool with a compatible media adapter.
- Several types of memory cards currently available include the following devices:
  - Multi-media cards (MMC)
  - Secure digital (SD) cards
  - Memory sticks
  - MicroSD (TransFlash)
  - Compact Flash (CF) card

Mobile Phone Investigation

- Forensic examination of wireless communication and computing devices is a growing subject area in computer forensics.
- Forensic examination tools translate data to a format and structure that is understandable by the examiner and can be effectively used to identify and recover evidence for civil and criminal litigation.
- It is possible that some forensic tools may contain a degree of inaccuracies.
- A suspect may tamper with device information to foil the workings of a tool or apply a wiping tool to remove or eliminate data.

SIM Forensics

- The data that a SIM card can provide the forensics examiner can be invaluable to an investigation.
- Some of this data can help an investigator determine:
  - Phone numbers of call made/received
  - Contacts
  - SMS details (time/date, recipient, etc)
  - SMS text (the message itself)

Mobile Phone Investigation (Cont.)

SIM Data Acquisition

- Data that can be extracted from the SIM card includes:
  - International mobile Subscriber identity (IMSI)
  - Mobile country code (MCC)
  - Mobile network code (MNC)
  - Mobile subscriber identification number (MSIN)
  - Mobile subscriber international ISDN number (MSISDN)
  - Abbreviated dialing number (ADN)
  - Last dialed numbers (LDN)
  - Short message services (SMS)
  - Public land mobile network (PLMN) selector
  - Location information (LOCI)
  - Etc
- Some additional information the service provide might store include:
  - A customer database
  - Call detail records (CDRs)
  - Home location register (HLR)

Mobile Phone Investigation (Cont.)

SIM Card Test Encoding

- Originally the middle-European GSM network used only a 7-bit code derived from the basic ASCII code.
- There was a movement toward a 16-bit code, known as UCS-2, which is now the standard in GSM text encoding.
- This encoding is used to compress the hexadecimal size of certain elements of the SIMs data, particularly in SMS and ADNs

Wireless Device Forensics

- When a cell phone is found, proper forensic protocol says to leave it in the current state.
- The phone should be placed in a Faraday bag, or Faraday cage.
- Differences between mobile device forensics and computer forensics exist due to the following factors:
  - Devices are compact in size, portable, battery powered
  - Device require specialized interfaces, media and hardware
  - Files system can reside in volatile memory versus nonvolatile memory
  - Device can remain active, but in hibernation state, when powered off or idle
  - Devices contain a dives variety of embedded operating systems
  - Mobile devices have a short product cycle
  - Most mobile phones offer a set of basic capabilities that are comparable.
- Most mobile phones provide users with some ability to load additional applications, and store and process personal and sensitive information independently of a desktop or notebook computer.

Wireless Device Forensics (Cont.)

Acquisitions and Device Seizures

- There a number of issues that must be addressed when acquiring evidence from electronic devices such as mobile phones and PDAs. These include:
  - Reporting acquired data
  - Review of seizure techniques
  - Faraday technology
  - Power issues
  - Order of acquisition
  - Protection of device
  - SIM processing
  - Device processing without SIM
  - Network tracing and systems
- Interpreting provider data
  - How to get it?
  - What do to with it?
  - How do you write protect a phone?
  - Registry modifications
  - USB write protection
  - Software drivers
  - Other techniques for phones
- Project a phone: Hardware and software tools.

Wireless Device Forensics (Cont.)

To Prevent a Phone from Becoming PIN-Locked.

- A radio screened foil bag is used to protect an active exhibit from the ingress of new data, such as phone calls or text messages.
- The process is as follows:
- Place the phone into the Faraday bag.
- Tightly fold the open edge of the bag. Make at least five folds, smoothing between folds.
- Fold over the excess bag and place inside the tamper-proof container.
- Exhibit must be placed inside an evidence bag and then sealed.
- Be aware of the phones' limited battery life.

Figure below depicts a Paraben tool bag, stronghold bag, and a first-responder kit.

Figure 13.3 Paraben first-responder tools.

Wireless Device Forensics (Cont.)

Figure below depicts the basic cellular device seizure procedures.

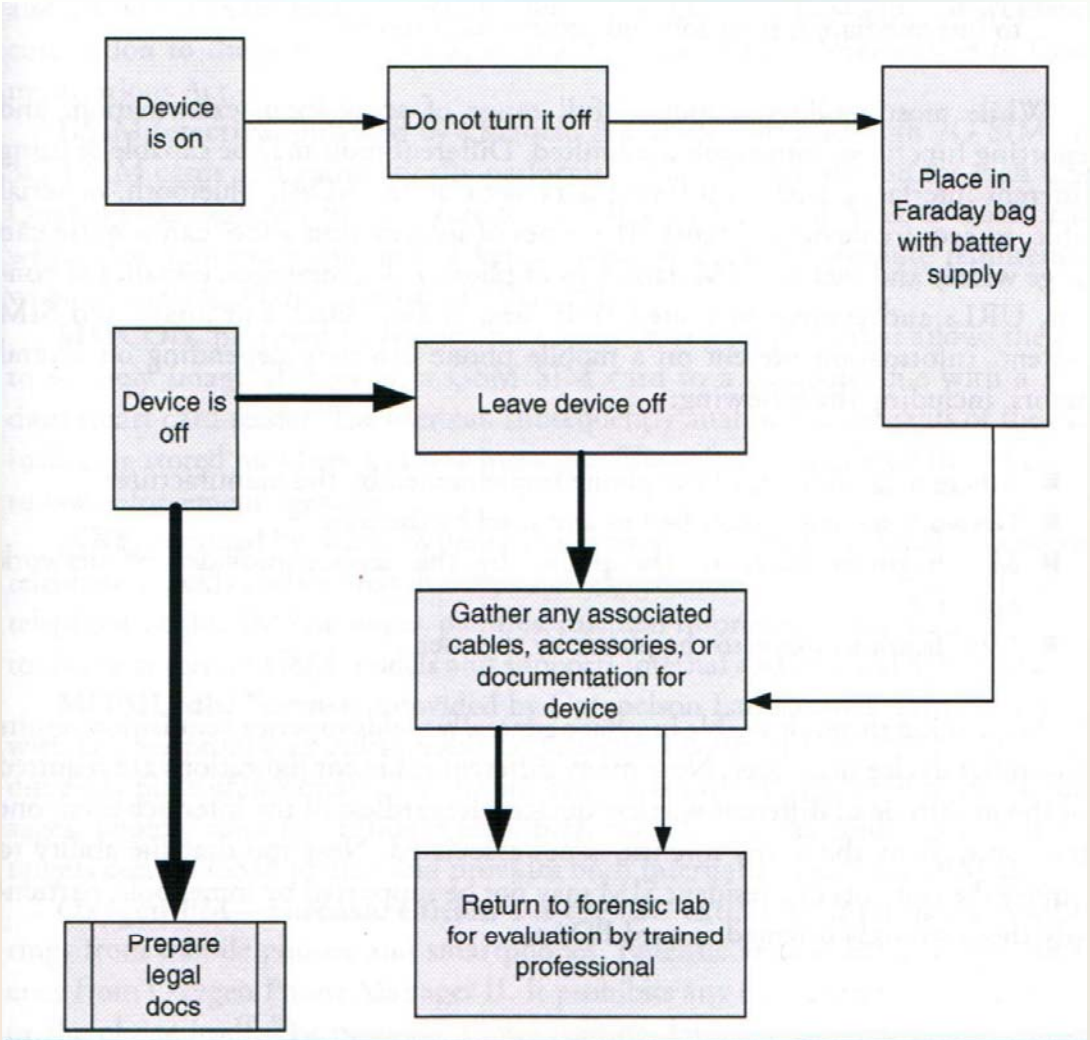

Figure 13.4 Cellular device seizure procedures.

Wireless Device Forensics (Cont.)

Forensic Tools

- The variety of forensic toolkits for mobile phones and other handheld device is considerable.
- The following criteria highlight some items to consider when choosing among available tools:
  - Accuracy
  - Acceptance
  - Affordability
  - Capability
  - Comprehensiveness
  - Determinism
  - Quality
  - Usability
  - Verifiability
- While most toolkits support a full range of acquisition examination and reporting functions, some tools are limited.

Wireless Device Forensics (Cont.)

- Different tools may be capable of using different interfaces, such as infrared data association, Bluetooth, or serial cable to acquire device contents.
- Information present on a mobile phone can vary depending on several factors, including the following:
  - Inherent capabilities of the phone implemented by the manufacturer
  - Network services subscribed to and used by the user
  - Modifications made to the phone by the service provider or network operator
  - Modifications made to the phone by the user
- Acquisition through a cable interface yields superior acquisition results than other device interfaces.

Forensic Software Tools

- There are a number of mobile phone forensic tools available in the commercial market.
- Note that GSM mobile phones are logically and physically partitioned into a handset and SIM, resulting in some forensic tools that deal exclusively with SIM.
- A short overview of some forensic products follows:
  - Device Seizure takes the SIM card acquisition and analysis components and puts it into a specializes SIM card forensic acquisition and analysis tool.
  - ForensicSIM allows trained operators to easily close a SIM card and examine it without any chance of damaging the evidence.
  - USIMdetective can read both 2G SIM and 3G USIM cards.
  - SIMCON is a program that allows the user to securely image all files on a GSM SIM card to a computer file with a standard smart card reader.
  - .XRY retrieves information stored on a mobile telephone quickly and securely.
  - MOBILedit! Forensic provides reports with tamper-proof and indisputable evidence in a court of law.
  - Oxygen PM-Forensic edition lets the user extract all information and settings from mobile phones and smart phones.
  - BitPim is an open source program that allows a user to view and manipulate data on many CDMA phones .
  - TULP2G is a .NET 2.0-based open source forensic software framework for extracting and decoding data stored in electronic devices.

PDA Investigations

- A PDA is a handheld device that combines computing, telephone/fax, and networking features.
- The PDA could be a handheld device .
- The many uses and tasks of a basic PDA include many features.

PDA Devices

- PDA devices are available in many configurations, with various features.
- The list of available devices and models changes frequently as the technology improves:
  - Psion
  - Apple Newton
  - Blackberry
  - Hp iPAQ Pocket PC
  - Hp Jornada Pocket PC
  - Palm Pilot
  - Tungsten
  - LifeDrive
  - Treo
  - Zire
  - Sharp Wizard
  - Zaurus
  - Sony CLIE
  - Tapwave Zodiac
  - AlphaSmart Dana
  - Dell Axim
  - GMate Yopy
  - Fujitsu Siemens Loox
  - PocketMail

PDA Investigations (Cont.)

- Most types of PDAs employ an operating system and application software and posses hardware features and capabilities.
- They house a microprocessor, read-only memory (ROM), random access memory (RAM), a variety of hardware keys and interfaces, and a touch-sensitive, liquid crystal display.
- The latest PDAs include considerable memory capacity and contain slots that support memory cards and peripherals.
- Wireless communications such as infrared, IrDA, Bluetooth, and Wi-Fi may also be built.
- Additionally, ,PDA capabilities are sometimes combined with those of other devices such as cell phones, Global Positioning Systems (GPSs), and cameras to form new types of hybrid devices.
- A wide array of memory cards also exists on the PDA market.
- Unlike the RAM of a PDA, removable media is nonvolatile storage.
- Fortunately, I a PDA forensic tool cannot handle such media, the memory card can be treated similarly to a removable disk drive.

PDA OS

- The currently major PDA operating systems include:
  - Palm OS is a compact operating system developed and licensed by PalmSource, Inc. It is designed to be easy to use and similar compared with desktop operating system such as MS Windows.
  - Windows Mobile 5.0 marks the convergence of the phone Edition and Professional Edition operating systems into one system that contains both phone and PDA capabilities. Windows Mobile 5.0 is compatible with Microsoft's Smartphone operating system and is capable of running Smartphone applications.
  - Blackberry: RIM develops its own software for its devices, using C++ and Java technology.
  - Symbian oS is an operating system, designed for mobile devices, with associated libraries, user interface frameworks, and reference implementations of common tools, producec by Symbina Ltd.

PDA Forensics

- As with digital computers in general, both the functionality and information capacity of handheld devices are improving rapidly.
- Though an investigator can browse the contents of the device through its user interface to obtain evidence, the approach is highly impractical and problematic, and should be used only as a last resort.
- A number of specialized tools are available for PDA forensic examinations. These include:
  - Device Seizure: A Paraben product that supports forensic acquisition, examination, and analysis of PDA devices for the PALM, Windows CE, and Blackberry operating systems. It provides for capture and report on data form PDAs by a two step acquisition of PDA device: all files in original structure and full memory. Card acquisition.
  - Palm dd (pdd): A Windows-based tool for memory imaging and forensic acquisition of data form the Palm OS family of PDAs. pdd will preserve the crime scene by obtaining a bit-for-bit image or “snapshot” of the Palm device’s memory contents.
  - Pilot-Link: A suite of tools used to connect a Palm or Palm OS compatible handheld with Unix, Linux, and other POSX-compatible machine. The two programs of interest to forensic specialists are pi-getram and pi-getrom, which respectively retrieve the contends of RAM and ROM form a device.
  - Palm OS Emulator (POSE): The Palm OS Emulator is a software that emulates the hardware of various models of Palm powered handhelds. Since it allows a user to create “virtual” handhelds on Windows, Mac OS, or Unix computers, the Palm OS Emulator is extremely valuable for writing, testing, and debugging applications.

PDA Forensics

- Duplicate Disk (dd): A common UNIX program whose primary purpose is the low-level copying and conversion of files. Unlike the other tools described above, dd executes directly on the PDA.

- A number of forensic examinations are relevant to PDA devices. The activates of the examiner could involve PDA evidence the following categories:
  - Device content acquisition
  - PIM applications
  - Web and e-mail applications
  - Graphics file formats
  - Compressed file archive formats
  - Deleted files
  - Misnamed files
  - Peripheral memory cards
  - Cleared devices
  - Password protected devices.
- Tests conducted on PDA devices using the tools discussed above resulted in mixed.
- It might be necessary and desirable to use several different tools in the forensic examination process.

PDA Forensics (Cont.)

A Caution when Using Forensic Tools

- Unlike the situation with desktop computes and workstations, the number and variety of toolkits for PDAs and other handheld devices are limited.
- Since Palm OS devices have been around the longest, more forensic tools are available for them than for other device families.
- Most tools require the examiner have unobstructed access to acquire contents, which means no authentication technique needs to be satisfied to gain access.
- Forensic tools acquire data from a device in one of two ways:
  - Physical acquisition implies a bit-by-bit copy of an entire physical store.
  - Logical acquisition implies a bit-by-bit copy of logical storage objects.
- Physical acquisition has advantages over logical acquisition , since it allows deleted files and any data remnants present to be examined.
- A logical structure has the advantage that it is a more natural organization to understand and use during examination.
- Tools not designed specifically for forensic purposes are questionable and should be thoroughly evaluated before use.

PDA Forensics (Cont.)

- Non forensic software tools generally focus on logical acquisition, using an available protocol for device synchronization and management to communicate with the device.
- As with any tool, forensic issues might be associated with the usage of a nonforensic tool.
- On one hand, nonforensic tools might be the only means to retrieve information that could be relevant as evidence.

Data Retrieval

- In forensics, data retrieval is a most sensitive issue. Some of the simplest things can corrupt the data and so the retrieval must be done in a manner that is tamper-proof an indisputable in court.
- Because we are surrounded by mobile network cells, RFID tags, two-way pagers, and EX-passes, interference with mobile phones is difficult to prevent.

To avoid a mobile phone from becoming PIN-Locked, the radio screened Faraday bag can be used to protect active exhibits from the ingress of new data such as phone calls or text message.

Figure 13.5 Paraben first responder kit and Faraday tent.

Forensic Examination Protocol

- There a number of specific steps the investigator must follow to successfully identify, retrieve, and preserve mobile phone and PDA evidence.
- These include those documentation and chain-of-custody actions that must be followed in all forensic investigations. These include:
  - Indentify the specific make and model of the device
  - Preserve the device as much as possible
  - Do not under any circumstances access the device
  - Do not turn the device on/off
  - Tyr to obtain the PIN number for the phone
  - Store the device in a Faraday bag where possible or another suitable storage media
  - Time is an issue. If the battery dies, evidence can be lost
  - Check the device for fingerprints and DNA
  - Check the crime scene for any related items, such as SIM cards, memory cards, batteries, charger, cables, manual, etc.
- Remember the PDA devices require power be maintained in order for the potential evidence to remain intact.

Forensic Examination Protocol (Cont.)

- The evidence recovered will be transported to the forensics lab.
- The chain-of-custody form must be completed, as does the other documentation required in any electronic forensic investigation.
- Figure blew depicts the rule for seizing a PDA device:

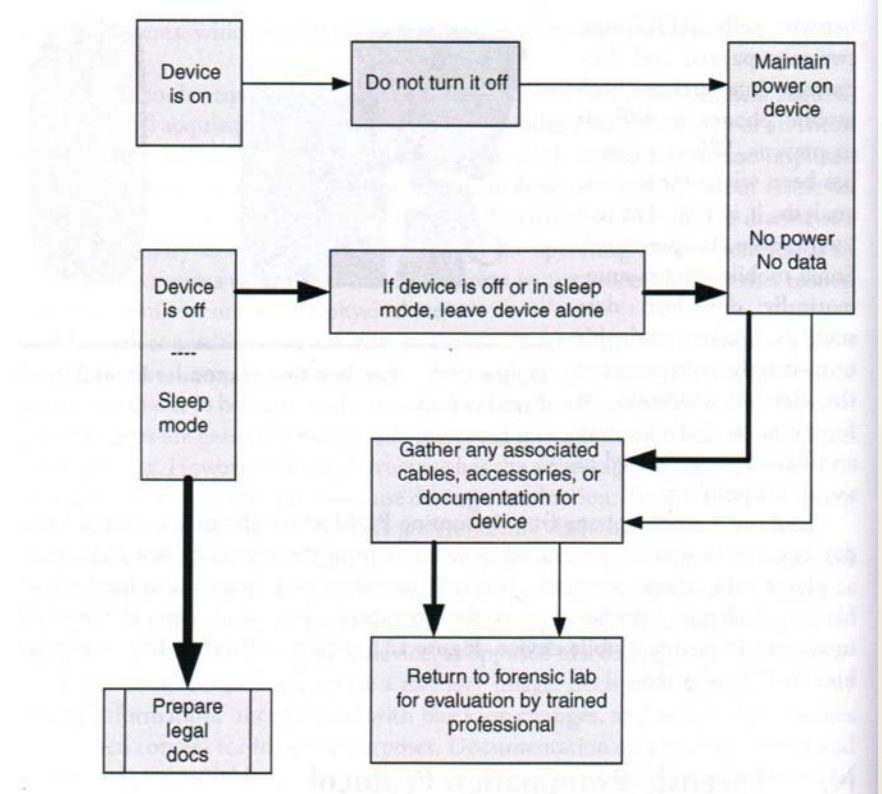

Figure 13.6 PDA device seizure on/off rule.