FORENSIC INVESTIGATION PROCESS MODEL FOR WINDOWS MOBILE DEVICES

Anup Ramabhadran
Security Group - Tata Elxsi

Abstract

Windows mobile device forensics is relatively a new field of interest among scientific and law enforcement communities. This paper describes the various processes involved in the forensic investigation of Windows mobile devices in the form of a twelve-stage model. The rapid technological advancements and increasing popularity of Windows mobile devices pose great challenges for investigators and law enforcement officials all over the world. These gadgets are compact hybrid devices integrating the capabilities of Personal Digital Assistant (PDA), mobile phone, camera, music player, FM radio, Global Positioning System (GPS) and so on. They have standard computing facilities and advanced communication features including Wireless and Bluetooth. Technology has often proved to be a double-edged sword that breeds crime. Naturally windows mobile devices are of no exception and will play a major role in electronic crimes in future. The methodology and approach are extremely critical in the forensic investigation of such crimes. The Windows mobile forensic process model has been developed with the aim of helping forensic practitioners and organizations for setting up appropriate polices and procedures.

1. Introduction

Portable electronic device forensics is a relatively new and emerging field of interest within digital forensics. In the modern era, Personal Digital Assistants (PDAs) are getting immensely popular. They are prone to get involved in electronic crimes in future, mainly because of their compact size and integrated features. The Federal Bureau of Investigation has highlighted the issue of growing crimes involving handheld devices in their computer crime survey. The PDA family mainly includes Palm devices, Windows mobile devices (Pocket PCs) and Linux based devices. Among these, Windows mobile devices are gaining more popularity of late, as they are based on the popular Microsoft Windows operating system and offer a familiar look and feel. In addition to make and receive phone calls, it allows to browse the Internet, chat, send and receive text/multimedia messages as well as view and edit Word, Excel and PowerPoint files. Discrepancies between computer forensics and portable electronic device forensics exist due to various factors including:

- Wide range of hardware models and accessories.
- Variety of different embedded operating systems.
- Short product cycle with new models emerging very frequently.
- Extreme orientation towards mobility.
- File system residing in volatile memory on certain devices while in non-volatile on some others.
- Hybrid devices with advanced networking and communication features.

- Suspending processes when off or idle, while the device being active in the background.

2. Challenges in Windows Mobile Forensics

Windows mobile devices turn out to be quite challenging for forensic investigations, primarily because of their compact size, integrated features and the availability of a wide range of models and accessories.

- **Volatile data:** Unlike computers, Windows mobile devices do not have hard disks. They generally store data in volatile memory, which will be lost if there is no adequate power. Recovering volatile evidence and analyzing it could turn out to be a tedious task.
- **Generic state of the device:** Even if a device appears to be in off state, it may not be entirely inactive, as background processes may be running. A sudden transition from one state to another may result in loss of data. Care should be taken to identify the current state of the device and the state it should be kept.
- **Dynamic nature of evidence:** Digital evidence may be easily altered either knowingly or accidentally. The data residing in a Windows mobile memory may change dynamically even when the device is left idle. Hence extreme care should be taken in the preservation of evidence and hashing and various cryptographic techniques should be applied whenever needed.
- **Hardware and OS version differences:** The forensic investigator may come across different types of hardware during an investigation. The models may be different in their size, technical specifications and features. The version of the operating system may also differ. Tools applicable to a particular version and model may not work well with another.
- **Accidental reset:** Resetting the device accidentally while examining may result in the loss of data. A hard reset will wipe out everything from RAM. A soft reset reinitializes the dynamic memory and records marked for deletion are removed. Loss of battery life causes a hard reset and hence the battery level needs to be continuously monitored.
- **External memory devices:** Most Windows mobile devices support additional memory devices like MMC, SD and CF cards. It is essential to search and seize such associated memory devices also.
- **Synchronization with other devices:** Potential evidence on Windows mobile devices may include address book, documents, text messages, voice messages, passwords, emails and appointment calendars. This information can be synchronized easily with a personal computer or laptop. Hence they should also be seized and examined.
- **Device alteration:** Possibilities of device alteration may range from removing logos and manufacturer labels to modifying the operating system. The expertise of the suspect should be taken into account. It is possible to remap a hardware key to perform a function other than the default one. Common utilities can be replaced with malicious programs to alter the data in the device.
- **Password recovery:** If the device is password protected, the forensic investigator needs to gain access to the device without damaging the device or the data. The

possible techniques include exploiting system vulnerabilities, authentication weaknesses and gaining access through backdoor.

- **Encryption mechanisms:** Encryption and other techniques might be used to alter the data, if the suspect has a certain level of computer expertise. The investigator should have the tools and expertise to overcome such circumstances.
- **Communication shielding:** Communication mechanisms like wireless could be on and any further possibility of communication should be eliminated.
- **Lack of availability of tools:** There are only few specialized forensic tools for Windows mobile devices. A single tool may not perform all the necessary functions. So in many cases, a combination of tools needs to be used.
- **Malicious programs:** The device may contain malicious software like a virus or a Trojan. Such malicious programs may attempt to spread over other devices either over a wired or wireless interface.
- **Understanding circumstances:** In some investigations, an incident might have occurred but the identity of the offender might be unknown whereas in some cases the offender and the incident are both known. The forensic examiner should have adequate knowledge of the circumstances and then search for evidence accordingly.
- **Legal issues:** Since these devices are extremely compact, there is every possibility of them being involved in crimes, which can easily cross geographical boundaries. In order to tackle these multi-jurisdictional issues, the forensic investigator should be well aware of the nature of the crime and the regional laws.

3. Windows Mobile Device Architecture

The Windows mobile device platform built on Windows CE architecture consists of four major layers.

- **Hardware Layer:** This consists of microprocessor, RAM, ROM, digital signal processors, various input/output etc.
- **Original Equipment Manufacturer (OEM) Layer:** This includes boot-loader, configuration files, drivers and the OEM Adaptation Layer (OAL). The OAL allows an OEM to adapt to a specific platform and consists of functions related to system start-up, interrupt management, profiling, power management, timer and clock.
- **Operating System Layer:** This includes kernel, core DLL, object store, multimedia technologies, device manager, communication services, networking and Graphic Windowing and Events Subsystem (GWES). The GWES provides an interface between the application, user and the operating system. The object store includes three types of persistent storage, which are the file system, registry and property databases. The registry stores information about system configuration, applications, settings user preferences etc. Property database is a storehouse of data that can be searched and retrieved by associated applications.
- **Application Layer:** This consists of applications like Office mobile, Outlook mobile, Windows media player, Pocket Internet Explorer, Pocket MSN Messenger, Picture and Video Viewer etc., user interface, and various custom applications.

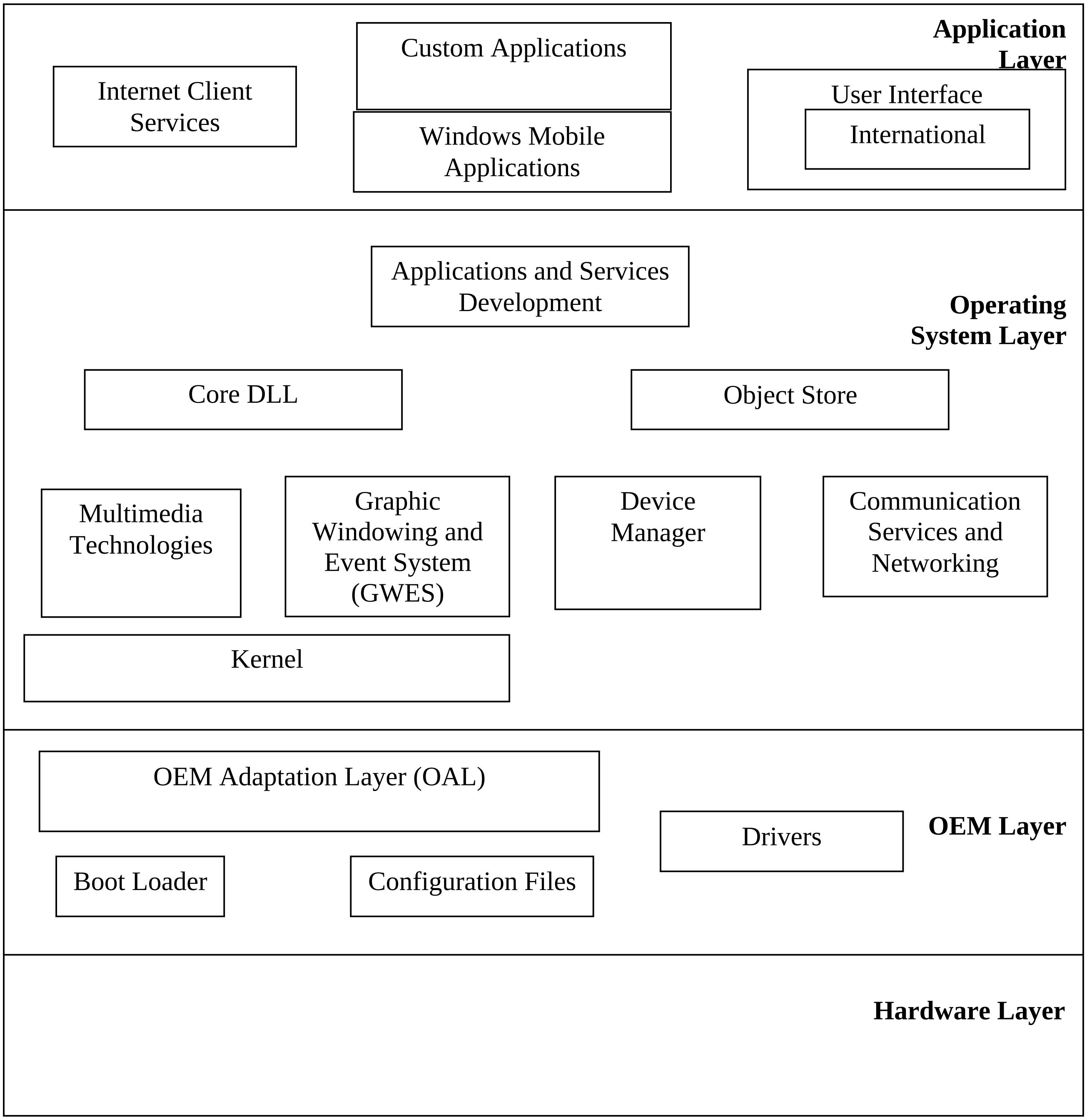

Figure 2: Windows Mobile Simplified Architecture

The different types of memory supported by the operating system are:

- **RAM:** This consists of two areas, the object store in which the data is stored and program memory where programs execute. The object store is similar to a virtual RAM disk and data present will be retained even when the system is suspended. The partition line between object store and program memory can be changed.

- **Expansion RAM:** This is supported to provide additional storage for the users. This is mapped into virtual memory and appears identical to the system RAM in the virtual memory map to the operating system.
- **ROM:** It consists of the operating system, applications, data files, support for uncompressed executables and DLL files. Uncompressed programs are executed there itself whereas if the module is compressed, it is decompressed and loaded into the RAM. When a program is executed directly from ROM, the time required to start an application is less, as it need not have to be loaded into RAM.
- **Persistent Storage:** The persistent storage options are mainly in the form of removable memory cards like Compact Flash (CF), Secure Digital (SD), MultiMedia Cards (MMC) etc. Data stored in such removable storage cards are mapped into the system RAM when required.

4. Hardware Characteristics

Having designed for mobility, Windows mobile devices are very compact in size, battery powered and light weight. There are many hardware manufactures making devices using the Windows mobile platform. All of them have a basic set of comparable features and capabilities. Physical characteristics like size, shape, weight etc. and technical specifications like processor speed, memory capacity, expansion capabilities etc. may vary for each model. The Windows mobile platform gives the flexibility to hardware manufacturer, system integrator or developer to incorporate their choice of services in their device version. A Windows mobile device in general consists of RAM, ROM, microprocessor, touch screen liquid crystal display, communication modules like GSM/GPRS, WLAN, Bluetooth and IrDA, slots for external memory cards and peripherals, optional modules like FM radio, GPS etc., digital signal processor, camera, speaker, microphone and a few hardware keys and interfaces. Figure 2 shows the generic hardware diagram of a modern Windows mobile device.

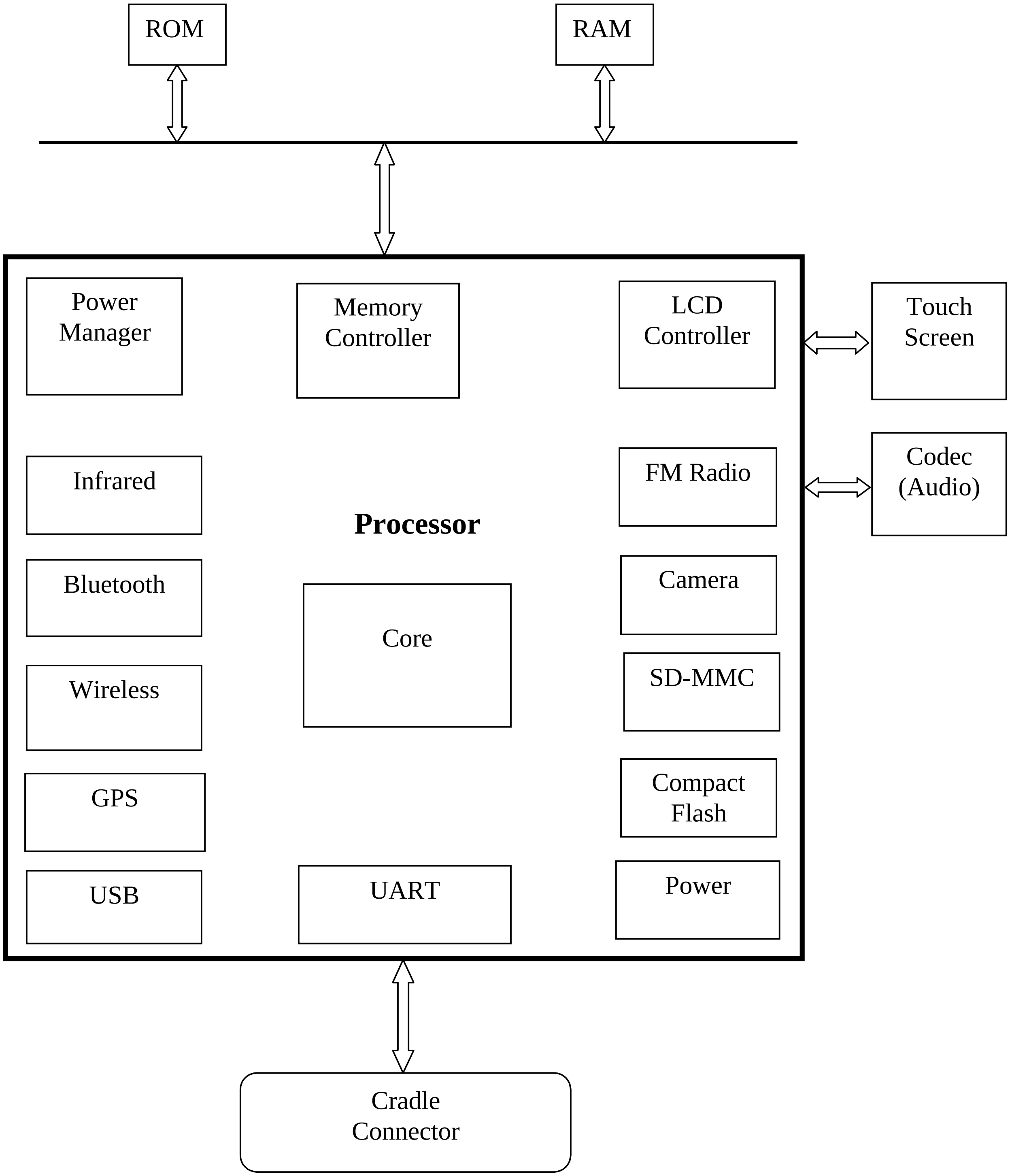

Figure 3: Windows Mobile Device Generic Hardware Diagram

5. Generic States

Unlike most digital devices that could be either in on state or off state, Windows mobile devices or rather PDAs in general, can be in any one of a variety of states at a given point of time.

- **Nascent State:** The device contains no user data and observes factory configuration settings. Usually the device must be charged for a minimum amount of time before entering into this state. Any user action will result in a transition from this state. This state can be achieved any time by doing a hard reset of the device or by allowing the battery to discharge totally.
- **Active State:** The device attains this state whenever it is powered on and the user is performing some tasks and the file system is having data. This state can be achieved by doing a soft reset, which clears the working memory.
- **Quiescent State:** This appears to be an inactive mode, though background functions are being performed and all user data are being maintained while conserving battery life. This state is attained when the power button is pressed while in active or semi-active state. Also when the inactivity timer expires while in semi-active state a transition to this state occurs. Generally the device is said to be ‘off’ if it is in the quiescent state and ‘on’ if it is in any other state.
- **Semi-Active State:** The device in this state is in between active and quiescent states, attained when a timer is triggered after a period of inactivity. This conserves battery life by reducing the backlight and other similar functions. Performing a soft reset, pressing any button or tapping the screen causes transition to this state.

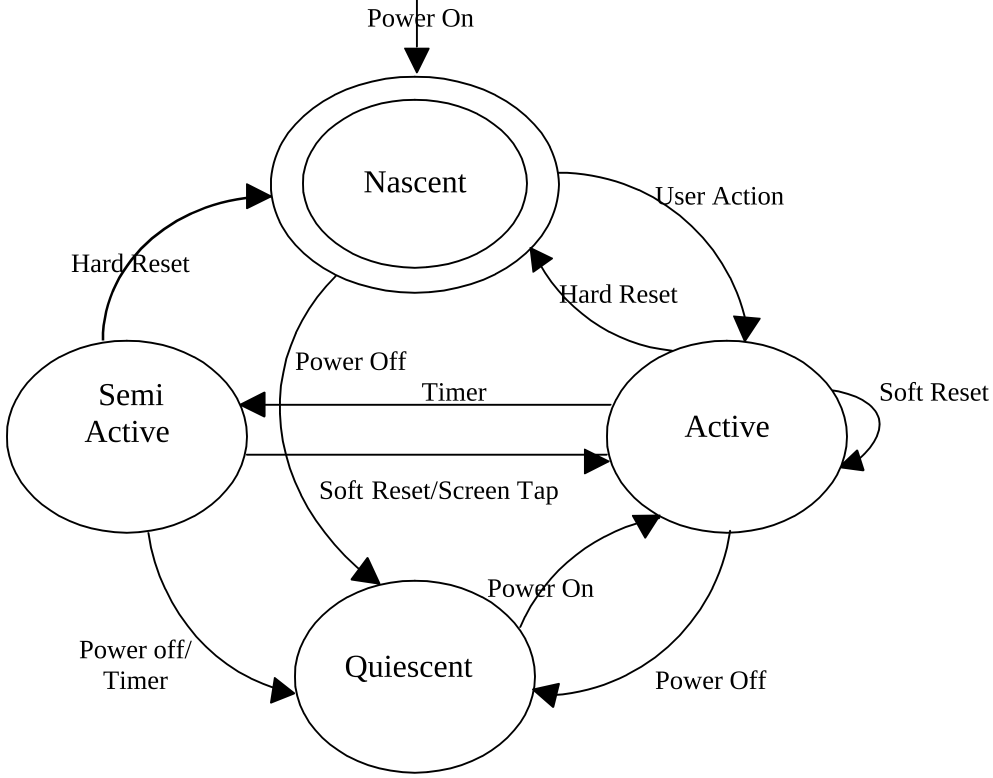

Figure 4: Generic States of a Windows Mobile Device

6. Windows Mobile Forensic Process Model

There are many digital forensic models proposed in different parts of the world. However no conclusion has been reached as which is the most appropriate one. Each framework may work well with a particular type of investigation. None of these models focus on the specific information flow associated with the forensic investigation of Windows mobile devices. The Windows mobile device forensic process model has been developed to help forensic practitioners and law enforcement officials in the investigation of crimes involving such devices. The standard practices and techniques in the physical and digital investigation world are incorporated, wherever appropriate. This model attempts to overcome the major shortcomings of the existing digital forensic models discussed in the earlier chapter and emphasises a systematic and methodical approach for digital forensic investigation. The proposed model consists of twelve stages, which are explained in the subsequent sections.

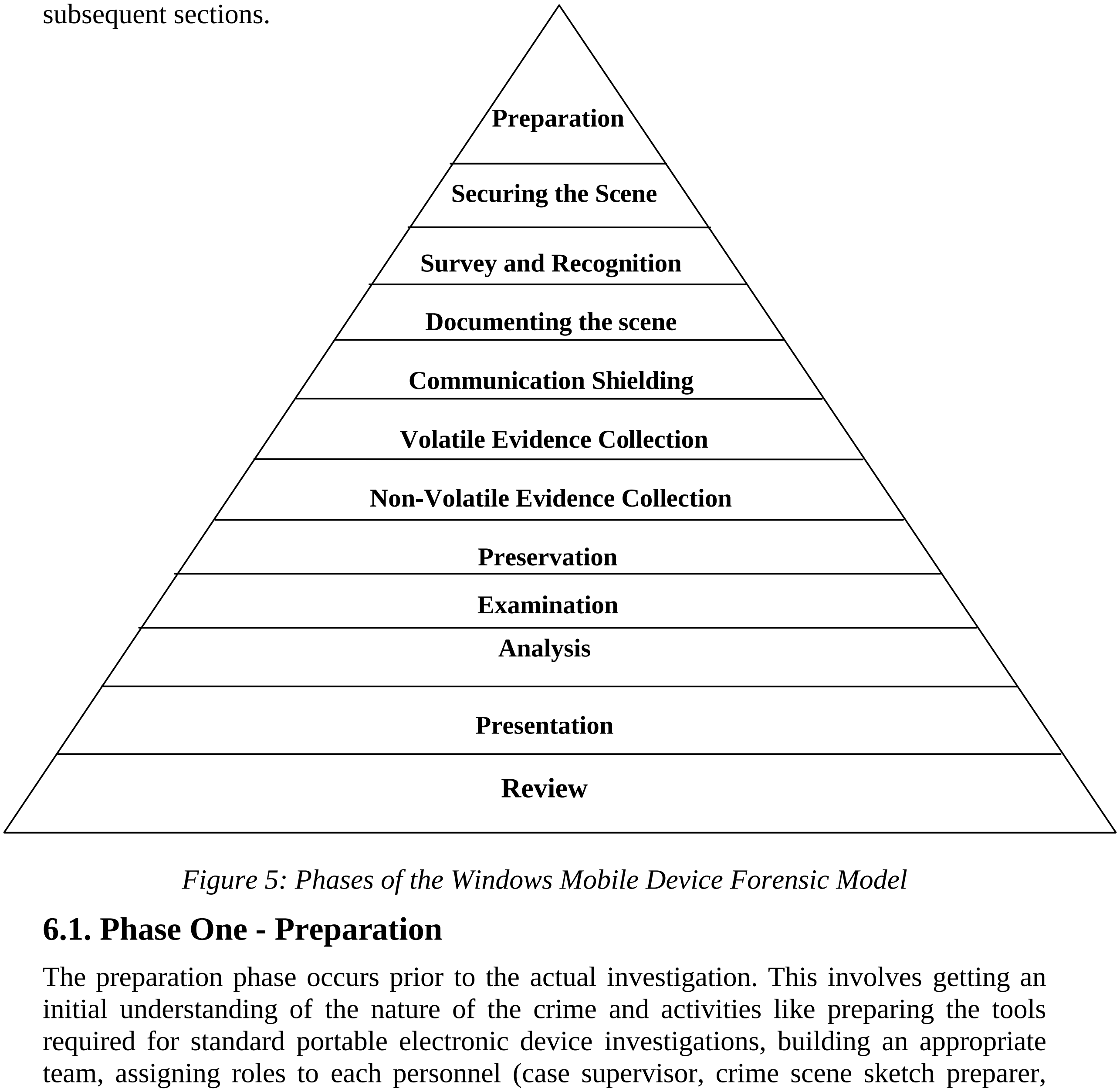

Figure 5: Phases of the Windows Mobile Device Forensic Model

6.1. Phase One - Preparation

The preparation phase occurs prior to the actual investigation. This involves getting an initial understanding of the nature of the crime and activities like preparing the tools required for standard portable electronic device investigations, building an appropriate team, assigning roles to each personnel (case supervisor, crime scene sketch preparer, evidence recorder and so on), accumulating materials for packing evidence sources etc. It is very important to obtain the best possible assessment of the circumstances relating to the crime, prior to proceeding to the crime scene. Knowledge of various mobile devices, accessories, features, specific issues etc. will be beneficial. A critical issue in the investigations involving Windows mobile devices is that the power runs out before evidence collection is over. So it is essential to prepare a toolkit consisting of standard power supplies, cables and cradles. The investigation should follow the various legal constraints and jurisdictional as well as organizational restrictions. This stage also involves obtaining search warrants, support from the management, required authorizations etc. before proceeding to the crime scene. The privacy rights of suspects should be taken into account. Legal notice must be provided to all concerned parties notifying about the forensic investigation. An appropriate strategy for investigation should be developed, having taken into account the nature of the incident and various technical, legal and business factors. Training, education and experience of the investigators will contribute in this phase. Having a thorough preparation phase increases the quality of evidence and minimizes the risks and threats associated with an investigation.

6.2. Phase Two - Securing the Scene

This stage primarily deals with securing the crime scene from unauthorized access and preserving the evidence from being contaminated. There should be a formal protocol for handing over a crime scene in order to ensure that the chain of custody is properly followed. It will be difficult to judge how much at the crime scene is actually the evidence. The investigators should identify the scope of the crime and establish a perimeter. Ensuring the safety of all people at the scene and protecting the integrity of all evidence should also be the targets at this stage. The investigators should have absolute control of the scene and interference from unwanted people should be avoided. As the number of people at the crime scene increases, the possibilities for the contamination and destruction of evidence also increase. However an attempt should not be made to determine what is present in the device and external storage media at this stage. The devices must be left in their existing state until a proper assessment is made. If the device is on, it is better to leave it on. Similarly, if the device is off, never turn it on. Nobody should be allowed to touch any electronic device in the scene. Top priority should be given at this stage in minimising the corruption of evidence. Any item that could be of evidence should not be tampered with. This phase plays a major role in the overall investigative process as it determines the quality of evidence.

6.3. Phase Three – Survey and Recognition

This stage involves an initial survey conducted by the investigators for evaluating the scene, identifying potential sources of evidence and formulating an appropriate search plan. In a complex environment, this may not be straightforward. In the case of Windows mobile devices, the major sources of evidence other than the device itself are the power adaptor, cradle, external memory cards, cables and other accessories. Since the information present in these devices can be easily synchronized with computers, any personal computer or laptop at the crime scene may also contain evidence. Evaluate the electronic equipments at the scene to determine whether any expert assistance is required in processing the scene. Identifying people in the scene and conducting preliminary interviews are extremely important. The owners or users of the electronic devices or system administrators can provide valuable information like the purpose of the system, security schemes, various applications present in the devices, user names, passwords, encryption details etc. Without violating the jurisdictional laws and corporate policies, the investigators must try to obtain the maximum information from the various people present in the scene. If it becomes necessary to search for items that are not included in the search warrant, appropriate amendments must be made to the existing warrant or a new warrant must be obtained, which includes the additional items. An initial plan for collecting and analysing evidence must be developed at the end of the survey and recognition phase.

6.4. Phase Four - Documenting the Scene

This stage involves proper documentation of the crime scene along with photographing, sketching and crime-scene mapping. All the electronic devices at the scene must be photographed along with the power adaptors, cables, cradles and other accessories. If the mobile device is in the on state, what is appearing on the screen should also be documented. A record of all visible data must be created, which helps in recreating the scene and reviewing it any time. This is particularly important when the forensic specialist has to do a testimony in a court, which could be several months after the investigation. Circumstances surrounding the incident, including those who reported the incident initially and at what date and time, should be included. It is necessary to keep a log of those who were present on the scene, those who arrived, those who left etc., along with the summary of their activities while they were at the scene. It is necessary to classify the people into separate groups like victims, suspects, bystanders, witnesses, other assisting personnel etc. and record their location at the time of entry. Documentation is a continuous activity, required in all the stages and is quite critical for maintaining proper chain of custody.

6.5. Phase Five – Communication Shielding

This step occurs prior to evidence collection. At this stage, all further possible communication options of the devices should be blocked. Even if the device appears to be in off state, some communication features like wireless or Bluetooth may be enabled. This may result in overwriting the existing information and hence such possibilities should be avoided. In other situations where the device is in the cradle connected to a computer, synchronization mechanisms using ActiveSync might be enabled. This may also lead to the corruption of evidence. The best option after seizing a device is to isolate it by disabling all its communication capabilities. If the device is in the cradle, remove any USB or serial cable, which connects it to a computer.

6.6. Phase Six – Volatile Evidence Collection

Majority of the evidence involving mobile devices will be of volatile nature, being present in ROM. Collecting volatile evidence presents a problem as the device state and memory contents may be changed. The decision whether to collect evidence at the crime scene or later at a secured forensic workshop depends on the nature of the particular situation including the current power state. If the device is running out of battery power, the entire information will be lost soon. In that case, adequate power needs to be maintained if possible by using the power adaptor or replacing batteries. If maintaining the battery power seems doubtful, the contents of the memory should be imaged using appropriate tools as quickly as possible. Paraben PDA Seizure is a major commercial forensic tool, which can be used for memory acquisition, in addition to several open source tools. A combination of tools must be used to obtain better results. If possible, an adequate power supply must be maintained by recharging the device or replacing the battery, whichever is appropriate. If it is not possible to provide sufficient power, the device must be switched off to preserve battery life and the contents of the memory. The presence of any malicious software installed by the user should also be checked at this stage.

6.7. Phase Seven – Non-volatile Evidence Collection

This phase involves collecting evidence from external storage media supported by these devices, like MMC cards, compact flash (CF) cards, memory sticks, secure digital (SD) cards, USB memory sticks etc. Evidence from computers, which are synchronized with these devices, must be collected. If the device has integrated phone features, the acquisition of sim card information takes place at this stage. Appropriate forensic tools must be used for collecting evidence to ensure its admissibility in a court of law. The integrity and authenticity of the evidence collected should be ensured through mechanisms like hashing, write protection etc. All power cables, adaptors, cradle and other accessories should also be collected. Care should be also taken to look for evidence of non-electronic nature, like written passwords, hardware and software manuals and related documents, computer printouts etc.

6.8. Phase Eight – Preservation

This phase includes packaging, transportation and storage. Appropriate procedures should be followed and documented to ensure that the electronic evidence collected is not altered or destroyed. All potential sources of evidence should be identified and labelled properly before packing. Use of ordinary plastic bags may cause static electricity. Hence anti-static packaging of evidence is essential. The device and accessories should be put in an envelope and sealed before placing it in the evidence bag. The evidence bag must be kept in a radio frequency isolation container to avoid further communications with any other device. All the containers holding these evidence bags must also be properly labelled. Adequate precautions are necessary as the sources of evidence could be easily damaged while transportation because of shock, excessive pressure, humidity or temperature. Afterwards the device can be moved to a secure location where a proper chain of custody can be maintained and examination and processing of evidence can be started. The evidence should be stored in a secure area and should be protected from electromagnetic radiations, dust, heat and moisture. Unauthorized people should not have access to the storage area. National Institute of Standards and Technology guideline highlights the need of proper transportation and storage procedures, for maintaining a proper chain of custody.

6.9. Phase Nine – Examination

This phase involves examining the contents of the collected evidence by forensic specialists and extracting information, which is critical for proving the case. Appropriate number of evidence back-ups must be created before proceeding to examination. This phase aims at making the evidence visible, while explaining its originality and significance. Huge volumes of data collected during the volatile and non-volatile collection phases need to be converted into a manageable size and form for future analysis. Data filtering, validation, pattern matching and searching for particular keywords with regard to the nature of the crime or suspicious incident, recovering relevant ASCII as well as non- ASCII data etc. are some of the major steps performed during this phase. Personal organizer information data like address book, appointments, calendar, scheduler etc, text messages, voice messages, documents and emails are some of the common sources of evidence, which are to be examined in detail. Finding evidence for system tampering, data hiding or deleting utilities, unauthorized system modifications etc. should also be performed. Detecting and recovering hidden or obscured information is a major tedious task involved. Data should be searched thoroughly for recovering passwords, finding unusual hidden files or directories, file extension and signature mismatches etc. The capabilities of the forensic tools used by the examiner play an important part in the examination phase. When the evidence is checked-out for examination and checked-in, the date, time, name of investigator and other details must be documented. It is required to prove that the evidence has not been altered after being possessed by the forensic specialist and hence hashing techniques like md5 must be used for mathematical authentication of data.

6.10. Phase Ten – Analysis

This step is more of a technical review conducted by the investigative team on the basis of the results of the examination of the evidence. Identifying relationships between fragments of data, analyzing hidden data, determining the significance of the information obtained from the examination phase, reconstructing the event data, based on the extracted data and arriving at proper conclusions etc. are some of the activities to be performed at this stage. The National Institute of Justice (2004) guidelines recommend timeframe analysis, hidden data analysis, application analysis and file analysis of the extracted data. Results of the analysis phase may indicate the need for additional steps in the extraction and analysis processes. It must be determined whether the chain of evidence and timeline of the events are consistent. Using a combination of tools for analysis will yield better results. The results of analysis should be completely and accurately documented.

6.11. Phase Eleven - Presentation

After extracting and analyzing the evidence collected, the results may need to be presented before a wide variety of audience including law enforcement officials, technical experts, legal experts, corporate management etc. Depending on the nature of the incident or crime, the findings must be presented in a court of law, if it is a police investigation or before appropriate corporate management, if it is an internal company investigation. As a result of this phase, it should be possible to confirm or discard the allegations regarding the particular crime or suspicious incident. The individual results of each of the previous phases may not be sufficient to arrive at a proper conclusion about the crime. The results of examination and analysis must be reviewed in their entirety to get a complete picture. A report consisting of a detailed summary of the various steps in the process of investigation and the conclusions reached must be provided. In many cases, the forensic specialist may have to give an expert testimony in court. The complex terms involved in various stages of investigation process needs to be explained in layman's terminology. The expertise and knowledge of the forensic examiner, the methodology adopted, tools and techniques used etc. are all likely to be challenged before a jury. Along with the report, supporting materials like copies of digital evidence, chain of custody document, printouts of various items of evidence etc. should also be submitted.

6.12. Phase Twelve - Review

The final stage in the model is the review phase. This involves reviewing all the steps in the investigation and identifying areas of improvement. As part of the review phase, the results and their subsequent interpretation can be used for further refining the gathering, examination and analysis of evidence in future investigations. In many cases, much iteration of examination and analysis phases are required to get the total picture of an incident or crime. This information will also help to establish better policies and procedures in place in future.

7. Comparison with Existing Models

Table below gives a comparison of the activities in the proposed model with those in the major existing models described in the previous chapter. Some of the relevant activities in other models are incorporated in the proposed model. However there are many activities like communication shielding and volatile evidence collection, which are unique for this model, as it is clear from the table.

Windows Mobile Forensic Process Model	**NIJ Law Enforcement Model**	**DFRWS Model**	**Abstract Digital Forensic Model**	**IDIP Model**
Preparation			✓	✓
Securing the scene		✓		✓
Survey and Recognition		✓	✓	✓
Documenting the scene				✓
Communication Shielding				
Volatile Evidence Collection				
Non-volatile Evidence Collection	✓	✓	✓	✓
Preservation		✓	✓	✓
Examination	✓	✓	✓	✓

Analysis	✓	✓	✓	
Presentation	✓	✓	✓	✓
Review				✓

Table 1: Comparison of Activities in the Major Forensic Models

There may not always be a one-to-one mapping between the activities in the proposed model and other previous models. In some cases, though the process is similar, the terms used in other existing forensic models may differ. Table 2 gives a comparison of terminology used for different processes in the proposed model and various other models discussed in the previous chapter.

Windows Mobile Forensic Process Model	**NIJ Law Enforcement Model**	**DFRWS Model**	**Abstract Digital Forensic Model**	**IDIP Model**
Preparation			Preparation	Readiness
Securing the scene		Preservation		Preservation
Survey and Recognition		Identification	Identification	Survey
Documenting the scene				Documentation
Communication Shielding				
Volatile Evidence Collection				
Non-volatile Evidence Collection	Collection	Collection	Collection	Search and Collection
Preservation		Preservation	Preservation	Preservation
Examination	Examination	Examination	Examination	Reconstruction
Analysis	Analysis	Analysis	Analysis	
Presentation	Reporting	Presentation	Presentation	Presentation
Review				Review

Table 2: Mapping of Major Forensic Models to the Proposed Model

8. Advantages of the Model

There are numerous benefits for the proposed model. This model can be used as a standard for the forensic investigation of any Windows mobile device. When compared to the existing digital process models which try to capture as much as possible of the investigative process, the proposed model restricts itself to a subset of portable electronic device forensics, thereby offering further benefits. It separates the primary investigation of crimes involving Windows mobile devices and those involving computers. In addition to standardizing the forensic investigation of Windows mobile devices, it allows organizations for setting up appropriate polices and procedures when crimes involving such devices occur.

The model is applicable to corporate and law enforcement investigations and incident response activities alike. The proven practices in the field of physical investigation are incorporated. An attempt is made to capture the entire scope of an investigation, rather than only evidence processing. The major tasks associated with an investigation including preservation, identification, collection and analysis of evidence are described and proper information flow among the various phases has been ensured. A proper chain of evidence custody has been maintained, which makes it a good model for law enforcement. At the same time care has been taken to take into account the various technical issues associated with the investigation involving Windows mobile devices, which is required for a digital investigation process model. Thereby this model bridges the gap between a law enforcement model and a digital investigation model to a certain extent.

9. Conclusion and Future Work

A new forensic process model has been proposed, focusing exclusively on the issues surrounding Windows mobile device forensic investigation and standardizing the approach. This model is an initial step towards bridging the gap between law enforcement models and digital investigation models. The proposed set of activities in the model is not complete and there is considerable scope of work in the future. Though the model works as a standard for the Windows mobile family, additional procedures are needed to standardize it for the entire PDA family, which includes Palm and Linux devices also. But for such a generic model, when it comes to the volatile evidence collection phase, the procedures of memory acquisition will be different depending on the operating system. Additional work must be done to make sure that the model can be applied to other family of digital electronic devices including portable music players, digital cameras, mobile phones, removable data storage devices and so on. However the addition of new procedures may make this model clumsy.

The model needs to be tested for its practicality. There is not a simple method for testing the model. The application of the model in different contexts should be studied to verify that this is a general reference framework. The model needs to be comprehensively evaluated by forensic specialists and law enforcement officials in different parts of the world for further refinement of the processes. The technology associated with handheld devices is changing dramatically day by day. This model is constrained on the current range of products. As more and more features are incorporated into these devices in future, the challenges for forensic investigators will also increase. Hence the model needs to be consistently reviewed and additional procedures need to be added as and when required.

10. References

Baryamureeba, V. and Tushabe, F. (2004) The Enhanced Digital Investigation Process Model. *Digital Forensic Research Workshop.*

Beebe, N.L. and Clark J.G. (2004) A Hierarchical Objectives-Based Framework for the Digital Investigation Process. *Digital Forensic Research Workshop.*

Brill, A.E. and Pollitt, M. (2006) The Evolution of Computer Forensic Best Practices. *Journal of Digital Forensic Practice*.

Carrier, B. and Spafford, E. (2003) Getting Physical with the Digital Investigation Model. *International Journal of Digital Evidence.*.

Ciardhuáin, S. (2004) An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidenc.*.

Horsewell (2004) *The Practice of Crime Scene Investigation*, New York, CRC.

Heiser, J.G. and Kruse, W.G. (2002) *Computer Forensics - Incident Response Essentials*, Boston, Addison-Wesley.

Johnson, T.A. (2006) *Forensic Computer Crime Investigation*, New York, CRC.

Leong, R. (2006) FORZA – Digital Forensics Investigation Framework That Incorporate Legal Issues. *Elsevier Journal of Digital Investigation.*

Mohay, G., Anderson, A., Collie, B., Vel, O. and McKemmish, R. (2003) *Computer and Intrusion Forensics*, London, Artech House.

National Institute of Justice (2001) *Electronic Crime Scene Investigation – A Guide for First Responders*.

National Institute of Justice (2004) *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*.

National Institute of Standards and Technology (2004a) *Guidelines on PDA Forensics*. (Special Publication 800-72)

National Institute of Standards and Technology (2004b) *PDA Forensic Tools: An Overview and Analysis*. [online]. Available from: http://www.csrc.nist.gov/publications/nistir/nistir-7100-PDAForensics.pdf [accessed May 31, 2007].

Nelson, B., Philips, A., Enfinger, F. and Steuart, C. (2005) *Guide to Computer Forensics and Investigations*, 2nd edition, Canada, Thomson Learning Inc.-Course Technology.

Palmer, G.L. (2001) *A Roadmap for Digital Forensic Research - Report from the First Digital forensics Research Workshop*, New York, The MITRE Corporation.

Reith, M., Carr, C. and Gunsch, G. (2002) An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, **1** (3), pp.1-12.

Schweitzer, D. (2003) *Incident Response Computer Forensics Toolkit*, Indianapolis, Wiley Publishing.

Shinder, D. and Tittel, E. (2002) *Scene of the Cybercrime: Computer Forensics Handbook*, Massachusetts, Syngress Publishing.

Vacca, J. (2005) *Computer Forensics - Computer Crime Scene Investigation*. 2nd edition, Hingham, Charles River Media Inc.