# A Small Scale Digital Device Forensics ontology

David Christopher Harrill and Richard P. Mislan

*Abstract*—**Small Scale Digital Device Forensics (SSDDF) is a relatively new and rapidly changing field of study which is in dire need of direction. Specifically, the devices and their corresponding forensic processes and procedures are vague and in a perpetual state of uncertainty. The purpose of this paper was to develop an ontological to provide law enforcement with the appropriate knowledge regarding the devices found in the SSDD domain. Additionally, this ontology can be used as a method to further develop a set of standards and procedures at which to approach SSDD.**

*Index Terms*—**computer and forensics, cyber and forensics, mobile and devices, PDA and forensics, forensics and small scale digital devices.**

## I. Introduction

In today's world, the forensics field heavily relies on knowledge as an important resource. Due to the ongoing changes in digital technology, the power of knowledge enables innovation and assists in establishing proper standards and procedures. As such, it is necessary to establish a relationship between the information derived from knowledge to form new concepts and ideas. An ontology plays an integral role in the formation of newly emerging ideas in the cyber forensics realm.

Ontology is a term which possesses multiple definitions as it pertains to research. Gruber [1] refers to Ontology as a form of conceptualization which can be identified explicitly or implicitly. According to Pretorius [2], an important distinction should be made between an ontology written with a capital "O" as compared to that of a lower case "o". The lower case ontology describes situations at which knowledge is captured for the purposes of organization or classification [3]. In contrast, Ontology is a term borrowed from philosophy where the meaning is predominantly centered on the state of existence [1]. According to Guarino & Poli [4], Ontologies are aimed at answering questions regarding commonalities between various objects. Noy and McGuinness [5] clarify ontology as a formal description contained within a specialized area. The ideas presented in this paper as they pertain to small scale digital forensics will employ a lower case "o" for categorizing the specific digital devices.

As we continue onward into the 21st Century, the development of efficient digital devices is increasingly being seen as an essential aspect in both the personal and business worlds. Technology has undergone massive strides since the development of the computer systems of the 1940s, identified as first generation machines. Each passing generation signified an increase in computing power and a decrease in the physical size of a device. The proliferation of handheld digital devices has captured the market and is primed to become the next frontier in technology. As such, the main objective of this study was to examine the smaller digital devices associated to the field of cyber forensics. Prior research has been conducted in this field, and this section reviewed related research. The purpose of the literature review was to find a variety of sources that focused their efforts on determining what constitutes a small scale digital device. The following section outlines how the sources were selected and what information was derived in order to assist with this research paper.

### A. Small Scale Digital Forensics

The area of SSDD was established to encompass newly developing technological devices. The SSDD category was broken down into three subparts including cellular telephones, Personal Digital Assistants (PDA), and software components. Brinson et al. [3], asserts that the small and versatile nature of the devices make them extremely difficult to identify and investigate. A cellular telephone, also referred to as a mobile phone, is essentially a portable radio-linked device that took the world by storm in the mid-1980s (Cellular Radio Telephone).

The first cell phones were expensive pieces of equipment that were primarily installed in motor vehicles. Additionally, the handheld versions were equivalent to the size of a brick and had a battery life measured in minutes. In 1990, the inception of the microchip reduced not only the cost but also the physical size of the phones. By the year 2000, the cell phone was no longer restricted for communication purposes. Technological breakthroughs provided small liquid crystal displays to indicate incoming and outgoing phone calls as well as an internal database capable of storing contact information. Additional breakthroughs throughout time provided users with the ability to perform such tasks as executing programs, storing images, documents, calendar information, and sending textual based messages.

The Personal Digital Assistant (PDAs) is another technological breakthrough which was designed to perform a variety of tasks. Jansen & Ayers [6] assert that these handheld devices are essentially miniature desktop computers with incredible computing power. These devices were available to the public during the mid 1970s as advanced calculators and electronic organizers. It was not until the mid 1990s that society accepted the PDA as a mainstream product. By the end of the decade, these handheld computer systems had the capability of playing music, taking pictures, sending electronic messages and making phone calls (PDA). As PDAs continue to increase

D. Harrill is a graduate student in Cyber Forensics in the Department of Computers and Information Technology within the College of Technology, Purdue University, West Lafayette, IN, 47906 USA.

R. Mislan is an Assistant Professor for Cyber Forensics in the Department of Computers and Information Technology within the College of Technology, Purdue University, West Lafayette, IN, 47906 USA.

in capability, manufacturers will continue to increase the functionality of PDAs, which have led to the creation of the smart phone.

A clear understanding of the software installed on each SSDD is necessary in order to adequately preserve, identify, and extract useful information [3]. A parallel can be made between the software installed on a SSDD and the operating system installed on a personal computer system. Currently Palm, Windows CD/Pocket PC, and Symbian are the primary operating systems involved within the current market.

It is important to point out that the remaining categories include devices which could potentially fall within the realm of small scale digital devices. As an example, laptops and tablets were classified as components in the computers category. Likewise, thumb drives and digital music players were assigned into the storage devices category. Finally, the Play Station Portable (PSP) is a gaming device that was included into the obscure devices category. The placement of these devices is noteworthy due to their physical size and functionality.

Mislan [7], of Purdue University, developed a course in an attempt to identify and investigate small scale digital devices. The course not only defined key terminology but also established what devices comprise the SSDD field. Mislan [7] describes a SSDD as a small form factor device which utilizes permanent or temporary memory in conjunction with embedded chips to perform a variety of tasks. The field of SSDD was split up into the following categories to account for the various types of small scale devices:

- Embedded Chip Devices
- Personal Digital Assitants
- Cellular Telephones
- Audio / Video Devices
- Gaming Devices

As such, a relationship can be made between Brinson's [3] ontology and Mislan's [7] coursework. Both of the studies include similarities but differ in the categorical placement of the digital devices.

Jansen et al. [6] describes what characterizes a handheld device and the risks that are associated with their usage. As the name suggests, small scale devices are characterized by their physical size. As time has progressed, the miniaturized devices have extended their functionality to store massive amounts of information without the consumption of much battery power [6]. Additionally, the user interface has provided an individual with the means of synchronizing their information to a notebook or desktop computer. Advancements in technology have also allowed these devices to utilize wireless network communications, such as WiFi and Bluetooth, to perform such tasks as sending and receiving electronic mail.

Unfortunately, a small scale digital device also presents several major risks which can impact society on a variety of levels. Most importantly, Jansen et al. [6] identifies that the small size of the devices may cause them to be misplaced or stolen. Likewise, it may be extremely difficult to identify these devices in a crime scene. It is also noteworthy to state that when a mobile device is found to be involved with a crime or other incident, proper techniques from seizure to final report should be established to ensure consistent results [6]. Furthermore, the weak authentication currently in place provides security flaws for users who posses the device.

Reith, Carr & Gunsch [8] performed a study to examine the processes and procedures which encompass the field of computer and digital forensics. The science of Computer Forensics examines the who, what, when, where, and how a specific crime occurred on a computer system. He identified PDAs, peripheral devices, and cell phones as devices which fall outside the realm of computer forensics. Reith et al.[8] specified that the term digital forensics should be modeled to cover current and future digital technologies. As such, it was determined that current digital forensic methodologies fail to address the procedures necessary in responding to SSDD incidents. Useful evidentiary information can be extracted and analyzed from both permanent digital storage as well as non-volatile storage.

The very nature of a digital device may require a forensic investigator to establish unique procedures at which to preserve, identify, and extract useful information. As an example, the field of cyber forensics has established recommended policies, procedures, and tools in order to examine large-scale digital devices, otherwise known as the personal computer system. Ciardhuain [9] proposed a model which focused on the general processing of digital evidence during an investigation. The model was developed as a reference framework to discuss different scenarios supporting tools, techniques, training and certification for investigators. Additionally, this model served as an extension to previous work derived from the DFRWS model [8].The steps of the model are as follows:

- Awareness
- Authorization
- Planning
- Notification
- Search for and identify evidence
- Collection of evidence
- Transport of evidence
- Storage of evidence
- Examination of evidence
- Hypothesis
- Presentation of hypothesis
- Proof/Defense of hypothesis
- Dissemination of information

The steps in the process are primarily concentrated on the crime scene, the analysis stage, and the presentation of data. This approach closely resembles work performed by Mislan [7] in regards to the deconstruction of a small scale digital crime scene.

### B. Small Scale Digital Device Breakdown

Practitioners working in the area of Small Scale Digital Forensics have different perspectives on what constitutes a device within the SSDD realm. As shown in Figure 1, to be effective, the field of SSDD Forensics must be broken up into the internal fundamental components for each device. The breakdown for each device can be illustrated by the ability to store information magnetically, optically, using solid-state

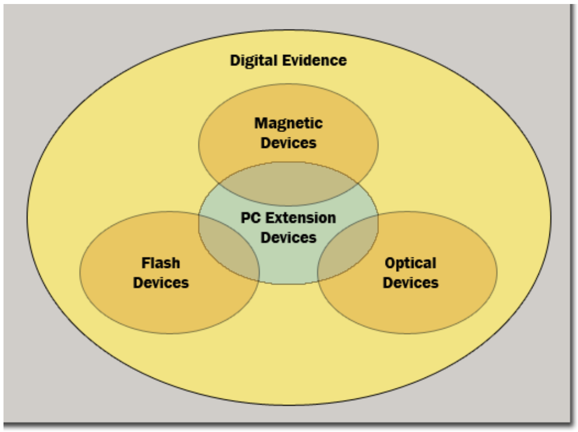


Fig. 1. SSDD Framework

flash memory, and by devices which extend the usage of computer systems.

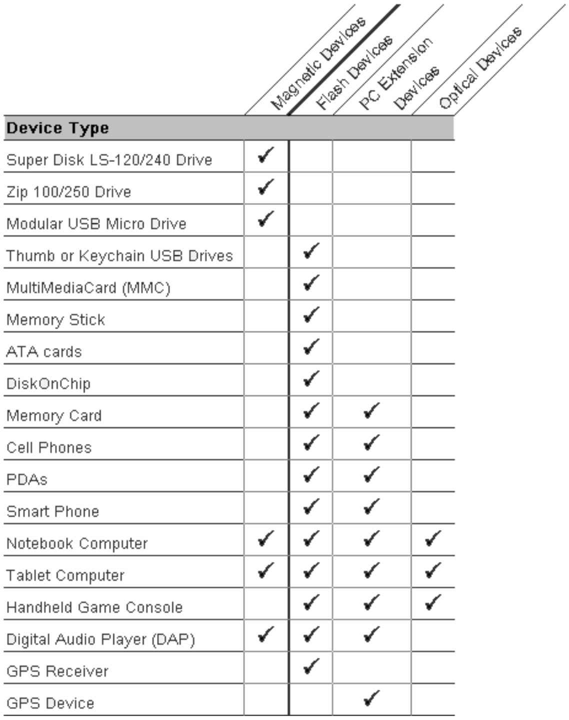
An electronic crime scene has the potential to hold massive amounts of data obtained from media devices. The primary goal of a cyber forensics investigator is to transform raw evidential data into useful data sets. Depending on the particular illegal activity, it is likely that a media device (i.e., Laptops, digital cameras, phones or hard drives) will vary in the size and amount of evidence. As an example, one criminal case may contain a small fraction of information or devices, another criminal case may contain a substantially larger amount of data and multiple devices.

Unfortunately, it may no longer be possible to group all forms of digital devices and their corresponding pieces of evidence to a specific forensic process. Ultimately, the inner components which comprise each device will define both the device category and may determine the forensic implemented to identify and extract evidence. However, it is also very likely that a specific device from within one category will be inspected by a forensic process from another device category.

Regardless of the type of cyber crime an individual commits, the principle of exchange always plays a factor in an investigation. Specifically, Locard's principle of exchange states that a perpetrator of a crime will leave something at the scene that was not present prior to the crime [10]. Locard added that the inability to properly understand the evidence will diminish the overall value of the clues left behind. In this case, the clues left behind have the capability of being any miniature piece of technology. Figure 2 illustrates the pieces of evidence that may be left at a crime scene.

Cyber crimes cover a broad range of criminal activity in a variety of settings. One end of the spectrum involves specific crimes with specific victims. In this instance, a criminal will obtain information with the purpose of committing identify theft to destroying intellectual property. The middle end of the spectrum includes transaction-based crimes including child pornography, digital piracy, money laundering and counterfeiting. The other end of the spectrum involves using spam and/or hacking to disrupt the normal operations of the Internet [11].

The Storage capabilities for computer systems have drastically changed over a period of twenty-five years. Magnetic storage, which fuels the modern computer system, has been in a constant state of evolution since the early 1950s [12]. According to Stevens [12] the evolution of magnetic storage took place over three distinct periods. The first period, ranging from 1953 to 1962 data was typified by the ability to store data on magnetic tape. The UNIVersal Automatic Computer I (UNIVAC), created in 1951 by J. Presper Eckert Jr. and John W. Mauchly, was the first computer with the capability of storing large amounts of information. Johnson [13] asserts that the purpose of the UNIVAC was to process large statistical tables for the 1950 census. The most common form of magnetic storage was exemplified by audio cassettes. Further advancements in magnetic storage from 1963 to 1966 improved the methods of system storage. The third and final period, ranging from 1967 to 1980, was represented by a reduction in the cost of disk storage and further improvements in storage capacity.



| Device Type | Magnetic Devices | Flash Devices | PC Extension Devices | Optical Devices |
|---|---|---|---|---|
| Super Disk LS-120/240 Drive | ✓ | | | |
| Zip 100/250 Drive | ✓ | | | |
| Modular USB Micro Drive | ✓ | | | |
| Thumb or Keychain USB Drives | | ✓ | | |
| MultiMediaCard (MMC) | | ✓ | | |
| Memory Stick | | ✓ | | |
| ATA cards | | ✓ | | |
| DiskOnChip | | ✓ | | |
| Memory Card | | ✓ | ✓ | |
| Cell Phones | | ✓ | ✓ | |
| PDAs | | ✓ | ✓ | |
| Smart Phone | | ✓ | ✓ | |
| Notebook Computer | ✓ | ✓ | ✓ | ✓ |
| Tablet Computer | ✓ | ✓ | ✓ | ✓ |
| Handheld Game Console | | ✓ | ✓ | ✓ |
| Digital Audio Player (DAP) | ✓ | ✓ | ✓ | |
| GPS Receiver | | ✓ | | |
| GPS Device | | | ✓ | |

Fig. 2. Device Breakdown

It can be implied that a fourth period was produced when tape storage was replaced by an alternative technology referred to as magnetic media drives. Hard drives and removable-media drives have become one of the most important methods at which corporations and individuals store strategic and personal information. The introduction of the computer system into mainstream society provided a tool which could be used by a criminal to commit a wide variety of unlawful and unethical activities. Ultimately, the personal desktop computer is comprised of several core components which provide a basis for defining computer forensics.

A computer system primarily acts as a storage device. A prospective criminal's hard drive has the ability to contain gigabytes of intelligence information which can be used to indict an individual in a court of law. Known as persistent data, the hard drive contains a plethora of information that will be preserved even if the system is shut down. The personal desktop computer system however falls outside the realm of the definition of a small scale digital device.

The introduction of the computer system into mainstream society provided a tool which could be used by a criminal to commit a wide variety of unlawful and unethical activities. Ultimately, the personal computer is comprised of several core components which provide a basis for defining computer forensics. A cyber crime investigator can examine such components as Random Access Memory (RAM), floppy disk, CD-ROM drives, DVD-ROM drives, and the hard drive for the identification of malicious or hidden files.

A computer system primarily acts as a storage device. A prospective criminal's hard drive has the ability to contain gigabytes of intelligence information which can be used to indict an individual in a court of law. Known as persistent data, the hard drive contains a plethora of information that will be preserved even if the system is shut down. In the case a computer system is still active, it may be possible to retrieve pertinent information from the temporary storage location, referred to as RAM. Unfortunately, if the computer is turned off, the RAM, otherwise referred to as volatile data, will be completely lost. This information, stored in memory, is located in such areas as the registry and cache. Examination of the registry could provide a great deal of information on previously installed hardware and/or software. For example, the registry may indicate if a suspect had previously installed any anti-forensic applications on the computer system. As such, an investigator must be aware of the various ways to capture pertinent information from either persistent or volatile data.

From a small scale digital device standpoint, it is imperative for forensic investigators to be aware of removable magnetic storage devices. A removable magnetic media device is similar to a floppy but possess a much higher storage capacity than the standard floppy disk. This form of media, popularized during the late 1990s, has recently decreased in overall market value. Al-Refaee [14] asserts that magnetic based storage devices are available in a variety of flavors. Specifically, some examples of removable storage devices include LS-120/240 SuperDisk, Zip 100/250 drives, and modular USB micro drives. Mueller [15] identified that a potential drawback from using this form of media is the lack and discontinued device support. Additionally, Mueller [15] provided an overview of the current magnetic removable media devices, depicted in Table 1. It is essential that law enforcement have the proper knowledge in regards to this storage media as it is very possible criminals will use the lack of support to their own advantage.

There are several key characteristics which distinguish the small scale magnetic devices from each other. Unlike the SuperDisks, the Zip drive does not have the cross functional capability of running the standard 3  inch floppy disks. As illustrated in Table 1, the devices have the capability of storing 100 megabytes (MB) to 750 MB of information. In contrast, the SuperDisks use Floppy OPTICAL technology to increase storage capacity while lowering production costs. According to Williams & Adkisson [16], FLOPTICAL disk drives employ the usage of optical alignment in combination with magnetic recording techniques to enable a higher storage capacity. Finally, the Orb and Peerless removable media drives essentially act as miniaturized hard drives. However, a major drawback is the drive's reliance on proprietary manufacturer support.

TABLE I
CURRENT AND RECENT HIGH-CAPACITY MAGNETIC REMOVABLE-MEDIA DRIVES [15]

| Removable Media Drive | Status |
|---|---|
| PocketZip | Discontinued |
| Zip 100 | Current |
| LS-120 SuperDisk | Discontinued |
| Zip 250 | Current |
| Zip 750 | Current |
| SparQ | Discontinued |
| Jaz | Discontinued |
| Orb 2.2 GB | Discontinued |
| Orb 5.7 GB | Discontinued |
| Peerless | Discontinued |

The modular micro drive is a miniature mobile magnetic storage device which can be transported very easily. Similar to a thumb drive, the modular drive connects to computer systems using the standard USB port or hub. Although the drive is smaller than a quarter, it is capable of storing massive amounts of digital data up to 4 GB.

The solid-state flash section of the model can be broken down into nearly a dozen formats. Flash media is extremely attractive due to its fast, inexpensive, and massive storage capacity. These devices are referred to as solid-state and are unique due to their lack of internalized moving parts. Unlike magnetic media, flash memory devices are referred to as a transistor based technology. Thus, flash memory is a very mature form of technology which operates different on the internal level as compared to other forms of media.

Specifically, the basic flash memory cell consists of two transistors. One transistor is referred to as a floating gate and separated from the other transistor by a thin gate oxide layer. The ability of the electrons to flow freely from the floating gate to the control gate depends on the amount of data on the flash storage device. Additionally, by applying low voltages to the floating gate and stimulating the electrons, a value of 0 will be created thus allowing information to be stored on the device. Essentially, the electrons move through the thin oxide layer and are trapped on the side containing the control gate. To restore the cell to a value of 1, an electric field can be applied to the cell and electrons.

Once restricted to the use of personal computer systems, the inception of the digital camera and MP3 players have transformed this technology into an essential day-to-day storage device. Similar to that of hard drives, flash media is considered a type of non-volatile memory. However, unlike a hard drive, the memory is split up into blocks as opposed to bytes. Flash memory can be separated into two types of technologies: NOR and NAND. NOR flash is capable of retrieving information on the byte level. Furthermore, NOR is most commonly found in cellular telephones and PDAs. In contrast, NAND is a form of flash memory which uses blocks to handle data [17]. NAND flash memory can be found in digital cameras, audio devices, video devices, cell phones and solid-state hard drives.

The typical thumb or keychain USB devices are commonly known devices used on a day-to-day basis. The thumb or keychain USB devices are becoming the preferred storage media due to several key characteristics. The following attributes are key advantages for using a USB thumb drive.

- **Capacity.** The USB thumb drives have the ability to virtually store any type of data and range in capacity from 128 MB to 4 GB.
- **Portability.** Similar to mobile magnetic media, USB thumb drives are small, light, and durable allowing for quick and easy transportation. Additionally, these devices can be built into items ranging from pens or pencils to sushi.
- **Ease of use.** USB thumb drives have the ability to directly connect into any USB port. In most cases, older operating systems require a driver to read the device. However, the newer versions of Windows automatically detect the device and assign it a drive letter.
- **Security.** In some instances, USB thumb drives provide protection from threats including data encryption and biometric security.

Although flash drives come in a variety of shapes and sizes, they are used similarly on a day to day basis. As previously stated, flash drives have been utilized to store sensitive digital data including documents, pictures, audio, and video files. Prior to any data being stored on the device, a file management system must be created to identify files. Furthermore, using specialized software, a thumb drive can also be used as a bootable drive to gain access to an operating system.

According to Mueller [15], flash technology has also been used as a memory device employed in such devices as digital cameras, portable music players, cellular telephones, and printers. According to Hu [18], the cards available for each of the mobile devices vary in the storage capacity, physical characteristics and ability to read and write information. Such examples of flash media include Memory Sticks and Media Cards. From a forensics standpoint, it may be necessary to physically examine a device in conjunction with various techniques to match the card to a specific device. However, regardless of the device, the memory stick will communicate with a specific device using a certain number of exposed metallic contacts. Additionally, Hu [18] asserts that the memory stick on a digital camera can store images which possess metadata. The metadata provides investigators with the ability to associate the card to a specific camera.

The solid-state PC extension section of the model is broken up into MP3 Players, notebook PCs, tablet PCs, cellular telephones, smart phones, PDAs, and handheld gaming consoles. The placement of the extension devices primarily depends on its ability to run with or without flash based memory and its reliance on internalized processing power in conjunction with an operating system. Similar to solid-state flash devices, the PC extension devices are unique due to their lack of moving parts. The nature at which a device exists in its original form will determine the placement in the model.

Currently, cellular telephones are being used to store massive amounts of information relating to an individual's actions. Cell phones have the capability of performing a multitude of functions in a variety of settings. Specifically, the communication patterns of a cell phone in conjunction with other media files can link a person to a specific event. Due to differing technical and physical characteristics, a cell phone can be classified into one of three categories: (a) basic, (b) advanced, and (c) smart phones [6]. According to Jansen et al. [6], all cell phones are comprised of a microprocessor, read only memory (ROM), and random access memory (RAM). ROM is considered a type of non-volatile storage and contains the operating system (OS) of the device. In contrast, RAM is a form of temporary storage which typically houses sensitive user data.

Cell phones that are categorized as basic can store a limited amount of data and possess very limited storage. Technological advances have increased the functionality of basic cell phones by incorporating built-in memory slots. The Mini Secure Digital and Multimedia Card Mobile are examples of flash media capable of increasing the storage capacity of cell phones. Due to their independent nature, it is noteworthy to state that these built-in and removable flash memory cards fall solely within the solid-state flash device section of this model.

The GSM (Global System for Mobile communications) is the largest digital system providing both speech and data services [19]. The GSM system is comprised of a mobile Station (MS) consisting of two components: (a) the Mobile Equipment otherwise referred to as the cell phone and (b) the Subscriber Identity Module (SIM). According to Willassen [19], the SIM card is a removable component which contains subscriber information. The SIM card is a form of smart card which is used to authenticate a user on the network and stores personal information. The SIM card differs from other removable memory devices because it contains a processor and non-volatile memory [19]. Similar to flash media, the portability of the SIM cards allow them to be transferred between compatible phones. The next generation of cell phones further substantiated the claim that cell phones have become an indispensable part of daily life. The smart phone combined the functionality of the advanced cell phones with the PDA to extend a user's capabilities.

The PDA acts as a personal organizer which was designed to store multiple types of information. The internalized components of a PDA are very similar to the advanced cell phones. According to Jansen et al. [6], PDAs are equipped with a microprocessor and uses a combination of ROM and RAM to store information. Additionally, these devices have the capability of using built-in flash memory in conjunction with flash memory slots to extend the memory capacity of the device.

Marsico & Rogers [20] specified that the Apple iPod is the most popular digital audio player (DAP). Similar to cell phones and PDAs, iPods have the capability of storing various audio formats and personal documents. Similar to other portable devices, some of the small scale music players have expansion memory slots. Prior to digital audio players, music was stored on storage devices which required moving parts to store and retrieve information. The hard drive players were not advantageous due to their bulky size, insufficient battery life, and inconsistent audio playback. Currently, a digital audio player utilizes solid-state flash memory in conjunction with a microprocessor to store and replay songs. As such, digital audio players can be placed in all three categories.

Portable gaming devices possess the ability to not only store information but also serve as leisurely gaming devices. The rapid growth of gaming on the personal computer has led hardware and software developers to create new forms of technology for the modern mobile era. Gaming devices, which include such hardware as the Sony PSP, will fall within the PC extension and optical device category. The PSP handheld utilize a small but sleek design with powerful processing power. However, the device is unique because it stores information using a high-capacity optical format referred to as Universal Media Disc (UMD). Optical drives use a laser to read information on the disk medium. Additionally, the PSP can use external memory sticks to increase the memory capability of the portable entertainment player.

Both the notebook PC and tablet PC are exact parallels of regular desktop computer system. Emerging technologies have provided the ability for these devices to potentially fall within each of the predefined categories. Both miniaturized computer systems can contain either a solid-state or magnetic drive. Additionally, these systems have the capability of storing files using such external media as flash or optical compact discs.

## II. Conclusion

The ongoing advancements in technology have produced a trend which has reduced the physical size and altered the internalized storage components of digital devices. It is essential for law enforcement to be aware of the potential devices present at a crime scene. The purpose of this paper was to provide a guiding framework at which to place small scale digital devices. Due to the massive scope of digital devices in mainstream society, it is possible that this study failed to address both archaic as well as the most recent of digital devices. However, the established framework should allow for the placement of these devices in one of the aforementioned categories. Further research in the field of small scale digital devices must examine the various forms of evidence and the procedures which are associated with each categorized device.

## References

[1] T. Gruber. "What is an Ontology?," 2004. [Online]. Available: http://www-ksl.stanford.edu/kst/what-is-an-ontology.html. [Accessed November 15, 2006].

[2] A. Pretorius, "Ontologies - Introduction and Overview," 2004. [Online]. Available: http://www.starlab.vub.ac.be/teaching/Ontologies_Intr_Overv.pdf. [Accessed November 16, 2006].

[3] A. Brinson, A. Robinson and M. Rogers, "A cyber forensics ontology: Creating a new approach to studying cyber forensics," 2006. [Online]. Available: http://www.dfrws.org/2006/proceedings/5-Brinson.pdf. [Accessed October 2, 2006].

[4] N. Guarino and R. Poli, "Formal Ontology in Conceptual Analysis and Knowledge Representation.," 1995. [Online]. Available: http://www.loa-cnr.it/Papers/FormOntKR.pdf. [Accessed October 10, 2006].

[5] N. Noy and D. Mcguinness, "Ontology Development 101: A Guide to Creating Your First Ontology," 2001. [Online]. Available: http://www.ip-super.org/res/related/ontology101.pdf. [Accessed November 16, 2006].

[6] W. Jansen and R. Ayers, "Guidelines on Cell Phone Forensics," 2006. [Online]. Available: http://csrc.nist.gov/publications/drafts/Draft-SP800-101.pdf. [Accessed November 28, 2006].

[7] R. Mislan, "Small Scale Digital Device Forensics," 2006. [Online]. Available: http://courses.tech.purdue.edu/cit/CPT499D/. [Accessed October 3, 2006].

[8] M. Reith, C. Carr and G. Gunsch, "An examination of Digital Forensics Models," *International Journal of Digital Evidence*, vol. 1, issue3, Fall 2002.

[9] S. Ciardhuain, "An Extended Model of Cybercrime Investigations," 2004. [Online]. Available: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf. [Accessed August 20, 2006].

[10] M. Rogers and K. Siegfried, "DCSA: A Practical Approach to Digital Crime Scene Analysis," 2004. [Online]. Available: http://courses.tech.purdue.edu/cit/CPT499F/Readings/DigitalCSA6Rogers.pdf. [Accessed November 3, 2006].

[11] R.D. Cliford, *CyberCrime The Investigation, Prosecution and Defense of a Computer-Related Crime*. Carolina: Academic Press, 2001.

[12] L.D. Stevens, "The Evolution of Magnetic Storage," 1981. [Online]. Available: http://www.research.ibm.com/journal/rd/255/ibmrd2505ZB.pdf. [Accessed November 20, 2006].

[13] L.R. Johnson, "Coming to grips with Univac," 2006. [Online]. Available: http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/85/34215/01631912.pdf. [Accessed November 5, 2006].

[14] F. Al-refaee, "Counterpoint: Magnetic storage solutions vs. flash in portables," 2004. [Online]. Available: http://pd.pennnet.com/Articles/Article_Display.cfm?Section=Articles&Subsection=Display&ARTICLE_ID=209999. [Accessed November 25, 2006].

[15] S. Mueller, *Upgrading and Repairing PCs*, 14th ed., Que, 2002.

[16] R. Williams and J. Adkisson, "Increasing Diskette Capacity With Floptical Technology," 1989. [Online]. Available: http://ieeexplore.ieee.org/iel2/231/7454/00301918.pdf?isnumber=&arnumber=301918. [Accessed December 1, 2006].

[17] Kingston Technology, "Flash Memory Guide," 2006. [Online]. Available: http://www.kingston.com/products/DMTechGuide.pdf. [Accessed November 27, 2006].

[18] C. Hu, "A Preliminary Examination of Tool Markings on Flash Memory Cards," 2004. [Online]. Available: http://scissec.scis.ecu.edu.au/publications/forensics04/Hu.pdf. [Accessed November 20, 2006].

[19] S. Willassen, "Forensics and the GSM mobile telephone system," 2003. [Online]. Available: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0658858-BFF6-C537-7CF86A78D6DE746D.pdf. [Accessed November 3, 2006].

[20] C. Marsico and M. Rogers, "iPod Forensics," 2005. [Online]. Available: https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2005-13.pdf. [Accessed November 3, 2006].

**David Christopher Harrill** David currently serves as a Systems Engineer with Lockheed Martin. His research interest includes computer forensics and data mining. He received his Masters of Science in Technology from Purdue University. Contact him at harrill@purdue.edu

**Richard P. Mislan** Rick currently teaches graduate and undergraduate courses in Small Scale Digital Device Forensics and Special Topics in Cyber Forensics. Rick has also served as a Communications Electronic Warfare Officer for the U.S. Army and a Technology Director and Educator for various school districts.

Rick's areas of research include Small Scale Digital Device Forensics, Unusual Sources of Digital Evidence, and the Application of Artificial Intelligence Techniques for Improving Efficiency in Cyber Forensics.

Rick has authored several articles in the area of Small Scale Digital Device Forensics, served as a reviewing editor for the National Institute of Standards on Cell Phone Forensic Guidelines and Tools as well as PDA Forensic Guidelines and Tools, and is in the process of completing his doctoral dissertation as well as acts as the Co-Editor of the Small Scale Digital Device Forensics Journal.

Through his consulting practice, SmartPhoneForensics, Richard also works with federal, state, and local law enforcement agencies in PDA, Cell Phone, and SmartPhone Forensics.