## Open Access License Notice

# Advanced Forensics Labs to Meet Computer Forensics Challenges Due to Technological Advancements

***Abstract – Computer forensics is a continually evolving field, filled with challenges when existing hardware and software technologies progress and new devices and technologies are added to the mix. It is important for forensics investigators responsible for acquiring, preserving and analyzing digital evidence, to be aware of the challenges facing the forensics field and to apply latest technologies in forensics investigation.***

***This paper discusses the challenges to the traditional forensics procedures and technologies due to evolving hardware and software. The authors present the latest forensics technologies and procedures as well as research ideas to address the challenges, especially in mobile device forensics, Solid State Drive (SSD) evidence recovery and analysis, and Windows memory forensics. Corresponding labs are designed and presented to assist computer forensic students and practitioners in getting acquainted with and practicing the new knowledge and tools.***

***Index terms – Windows Memory Forensics, Mobile Device Forensics, Solid State Drive, Forensics Lab Design, Forensics challenges***

## I. Introduction

With the proliferation of computer and networking technologies, computer crimes such as child pornography, cyber terrorism, espionage, network intrusion, fraud, and theft of intellectual property have been steadily increasing in recent years. Digital forensics, since its inception in 1998, has been evolving fast and gradually maturing in forensics standards, processes and technologies. Digital forensics technologies such as *EnCase* [1], *Forensics Toolkit* (FTK) [2] and *ProDiscover Forensics* [3] were developed, thus allowing analysts to acquire, preserve, and analyze digital evidence locally and remotely. These technologies are widely used in both civil and criminal investigation by forensics examiners and analysts within law enforcement, military, government, and private corporations, seeking to uncover evidence of illegal activity. However, evolving hardware and software technologies such as mobile devices, solid-state drives, cloud computing, memory-only malware, etc. present new challenges to the traditional forensics procedure and technologies of finding digital evidence of a crime [4].

**Memory forensics:** Traditionally, computer forensics has focused on evidences that reside in hard drives after a suspected crime has been committed. Over the past few years, due to the migration of malware into memory, and the increasing use of encryption by adversaries, forensics investigators realized that it is no longer sufficient to pull the plug and take the suspect machine back to the lab for gathering nonvolatile digital evidence [5, 6, 7]. Instead, they also have to include analyzing the computer RAM for examining passwords, running processes, memory and network connections, since this process may be the only way to start an investigation.

**Mobile devices:** Mobile device forensics has expanded significantly over the last decade due to the increasing storage capacity and processing power of these devices, a wide range of advanced applications, various wireless connectivity options, and their portability. Besides storing, processing, and communicating both personal and corporate information, mobile devices have also been widely used in online transactions such as stock trading, flight reservations and check-in, and mobile banking, to name a

few [8]. The great potential for incriminating data to be stored on mobile devices has created a need for mobile device forensics to allow forensics investigators to capture evidence in a criminal investigation. Mobile device forensics is the process of recovering digital evidence from a mobile device under forensically sound conditions and utilizing acceptable methods. It is important for forensics investigators to develop an understanding of the working components of a mobile device and the appropriate tasks to perform when they deal with them for a forensic assessment [8].

**Solid-State Drives:** When presenting admissible evidence to the court, forensics investigators have to ensure its integrity and authenticity. Integrity is ensuring that the act of seizing and acquiring digital media does not modify the evidence (either the original or the copy). Authenticity refers to the ability to confirm the integrity of information. Storage media technology was based on magnetic devices over the past two decades, allowing digital forensics to play a vital role in legal prosecution by providing invaluable and authentic allocated and unallocated data as admissible evidence. This landscape is changing when flash-based solid-state drives are rapidly becoming a popular replacement option for traditional magnetic hard drives. Due to the SSD technologies such as wear-leveling and automatic garbage collection, recovering deleted and unallocated data as well as providing authentic data becomes challenging, even impossible in some cases [9, 10, 11]. This is the first call to challenge traditional forensic practices and procedure [10].

XXXX University is one of the leading institutions that offer courses specifically developed for the digital forensics curriculum and information security degree program. Since our first forensics course was developed in 2003 [12, 13], the digital forensics field has been evolving continuously. The forensics experts in academia, industry and government continue to develop innovative tools to overcome the challenges in this field. The faculty at RIT have been diligently updating the forensics labs to prepare our students with latest forensics technologies, in order to face the new challenges in the digital forensics filed. In this paper, the authors share their latest lab development in memory forensics, mobile device forensics, and SSD data recovery and analysis, with educators and researchers.

The remainder of this paper is organized as follows. Section II describes three emerging forensics areas along with the background knowledge and challenges for each area. The detailed design and activities for the three correspondent labs are presented in Section III. Section IV briefly covers the authors' experiences in using these labs, followed by Conclusion and References in sections V and VI respectively.

## II. Emerging Forensics Areas and Challenges

Digital forensics is a relatively young, but a rapidly evolving field. The years from 1999 to 2007 were considered to be the "Golden Age" for digital forensics, since techniques and processes allowing forensics investigators to recover deleted data from unallocated spaces, email, instant messages and web browsers, and retrieval of deliberately hidden data from storage were developed. However, since 2008, hardware and software changes such as drive encryption, memory-only malware, solid-state drives, mobile devices, and cloud computing, present new challenges to the traditional forensics procedures and analysis. In this section, the authors focus on explaining the three emerging forensics areas: Windows memory analysis, solid-state drive analysis and mobile device analysis.

### *A. Windows Memory Acquisition and Analysis*

Since 2008, the use of drive encryption, data in the cloud, and memory-based malware has increased. Many of digital forensics evidences are only stored in memory, and therefore are not possible to be captured using disk forensics analysis alone. On the other hand, Random Access Memory (RAM) stores volatile information such as running process/threads, network connections, open files and open registry keys for processes, user names and passwords, unpacked/decrypted versions of a program, including memory resident malware [6]. RAM forensics can capture the current state of a machine. As a result,

there has been substantial interest in RAM-based forensics in an effort to help address many of the challenges facing the digital forensics community, including defeating drive encryption and identifying malware that is not written to persistent storage. In 2008, the first Open Memory Forensics Workshop (OMFM), focusing on open source volatile memory analysis [14], was organized to bring together digital investigation researchers and practitioners to discuss the latest advancements in volatile memory analysis. As the authors stated in [15], "Live Digital Forensics is a critical capability for digital forensics practitioners today and will only become more critical as time marches on."

*B. Mobile Device Forensics*

The use of mobile phones in crime has been increasing recent years, but the forensic study of mobile devices is a relatively new field. The proliferation of mobile devices in the consumer market demands a new framework and forensic tools to acquire and analyze information such as e-mail, word processing files, spreadsheets and personal information, including user's Global Positioning System (GPS) tracking information, call history, SMS, MMS and social networking messages, photos, web surfing information etc. [8]

The process of recovering and analyzing digital evidence from a mobile device must follow forensically sound conditions and must utilize acceptable methods. In other words, the evidence has to be handled in a tamper-proof manner and by a justifiable technology or methodology, avoiding unnecessary and undocumented evidence changes, so that the evidence will be admissible according to law in a trial. Even though many mobile forensics tools are being developed for logical and physical mobile device evidence acquisition and analysis, law enforcement and forensics investigators have struggled to effectively manage digital evidence obtained from mobile devices [8].

Some of the challenges faced by a forensics investigator in obtaining information from mobile devices include the following:

1. Data representing evidence on mobile devices can be volatile, because these devices are constantly exchanging information via Wi-Fi, 3G/4G cellular or Bluetooth connections. Therefore new data may be overwritten over original evidence. The most important step for a first responder is to determine the best way to preserve the mobile device and its data, when arriving at the scene of crime. The common process is as follows:

a) Power the mobile device off to preserve data and battery power. In this case, there is a chance of losing critical evidence resided in the flash memory, such as open processes, applications, and deleted information.

b) Place the device in *Airplane Mode*, if the device supports this function, to suspend the device's signal transmitting functions, therefore preserving data.

c) Isolate devices from cellular, Wi-Fi, Bluetooth and other radio signals using appropriate measures such as Black Hole Faraday bags [16] or Ramsey RF Shield Test Enclosure [17] to prevent a potential remote wipe or alternative techniques directed to alter or destroy evidence in the device.

2. File systems that are present in mobile devices operate from volatile memory that requires power to maintain stored information.

3. A large variety of operating systems are embedded in mobile devices, thus making a standardized forensic process development challenging.

4. The short product cycles from the manufacturers to provide new mobile devices and their respective operating systems are making it difficult for law enforcement agencies to remain current with new technologies.

### *C. Solid State Drive analysis*

Traditional computer hard drives use magnetic Hard Drive Disk (HDD) to store data. When the disk is asked to write to an unallocated block, Magnetic HDDs operate by overwriting the old data with the new values, if there is already old discarded data in that location. Forensics investigators have well-established procedures for capturing evidence including deleted (not yet overwritten) data from these types of drives and validating the integrity of the data collection (i.e., the collection process does not change any data). Investigators are able to partially or fully recover the contents of a deleted file from magnetic hard drives due to the fact that most operating systems do not clear the deleted data; instead they simply mark the data block as deleted. As a result, recovering deleted files from a magnetic hard drive is one of the most important steps in digital forensics investigation.

Recently, flash-based Solid State Drives (SSD) built with NAND electronic transistors are rapidly becoming a popular replacement option for traditional magnetic hard drives due to SSD's characteristics of high performance, lightweight and low power consumption. However, SSD brings new challenges to the traditional forensics processes and procedures [9, 10, 11].

Some of these challenges are listed below.

1. The flash technology generally requires blocks to be electronically erased before new data being written, in contrast to magnetic disks' "write-over-old-data" property. One common strategy is known as Garbage Collection or "Self Healing", where the onboard SSD controller identifies areas that are not in use, and resets them as soon as possible. Therefore, SSDs will clean the blocks that are marked as "deletion", and destroy the deleted data.
2. Automatic Garbage Collection process, issued by onboard SSD controller, could occur before, during or after a physical acquisition, forensic analysis or validation process, without explicit write commands from the computer**.** If Garbage Collection were to take place during forensic acquisition of the drive image, it would result in evidence integrity failure since the hash of the evidence before the acquisition would not be the same as the hash afterward the procedure.
3. The third challenge from SSDs is wear-leveling. The flash memory media has individually erasable segments, each of which has a limited number of erase cycles before becoming unreliable. In order to prolong the segment's service life, wear-leveling technique, issued by onboard SSD controller, is used to attempt to work around these limitations by arranging data so that erasures and re-writes are distributed evenly across the medium. In this way, no single erase block prematurely fails due to a high concentration of write cycles. However, this technique may result in data being moved at a random time from physical flash memory locations without OS and users' intervene.

To date, minimal research has been conducted in analyzing SSDs Garbage Collection behavior and addressing the impact of SSDs on existing forensics procedures.

## III. LAB DESIGN AND DEVELOPMENT

Labs provide students with the opportunity to understand and demonstrate the above-mentioned forensics challenges. They also allow students to discover new ideas for their future research. Various labs are designed in an effort to address the forensics challenges presented in section II and to allow students to practice related activities in a safe and controlled environment. The listed technologies are selectively included in each lab. The rationale behind choosing "good" tools is to either choose court accepted commercial tools or community open source tools that are endorsed by SANS, NIST, etc. Also, each lab leaves some open-ended questions that allow students to conduct further research, which may evolve into their graduate thesis/project topic.
Consequently, we introduce three labs - each directly addressing the challenges presented in section II.

### *A. Windows Memory Acquisition and Analysis*

The goal of this lab is to allow students to explore the latest forensics memory acquisition and analysis tools to identify the type of evidences that can be captured only via memory forensics, and to develop their problem-solving and investigation strategies. The detailed memory/lab creation, lab design and activities are as follows.

**1. Prepare the Window memory embedded with malicious hidden information**

When attackers do not leave any traces on disk, memory forensics is able to reveal hidden processes and possibly passwords remaining in the memory.
Here are the steps to create a compromised Windows XP Virtual machine for the memory lab:

- Load a memory-resident malware to the unpatched XP system using *Metasploit* [18] by exploiting a vulnerability such as *RPC buffer overflow* or *MS SQL*, from the unpatched Windows XP. Then utilize *Metasploit's Meterpreter* to migrate the malware process to a Window existing stable process.
- Use Windows netcat, *nc*, to create a backdoor that allows an external system to control the compromised machine. Then hide the "*nc*" process using Windows kernel mode rootkits, *FUTO* [19].
- In addition, encrypt the drive with a drive encryption tool, for example, *truecrypt* [20] (This step is optional since it is very challenging). In this case, forensics investigation of the compromised system is impossible to start without knowing the password to decrypt the drive.

**2. Lab Activities:**

Step 1. Memory acquisition using *Cold Boot Attack*
Since the compromised machine is encrypted, students will have to first recover the password to decrypt the drive. In this lab, students will explore the "cold boot attack" method.

The *cold boot attack*, introduced by the Princeton research team [21], is a technique for acquiring the contents of a computer and finding cryptographic keys in memory images after rebooting a machine [22]. In the paper [21], the researchers confirmed that simply turning off a computer does not necessarily ensure that all its memory contents are lost. Secondly, they have shown that the rate of decay for computer memory is dependent on two key variables, time and temperature, which means that one can pull power off the machine first, and then immediately reboot it and grab the contents of the RAM.
The cold boot attack includes several tools [22].

- *Scraper.bin* – A bootable image to dump the memory to a usb
- *Usbdump* – Dump the RAM from the USB to your forensics system
- *Aeskeyfind* and *rsakeyfind* – searches for AES keys ad RSA keys

Students will boot the compromised machine from a USB that contains *Scraper.bin*. The memory will be automatically dumped to the USB. Then, students will dump the memory content to a forensics machine using *Usbdump* and run *Aeskeyfind* or *rsakeyfind* to attempt to recover the encryption key, in our case, the TrueCrypt key.

The *cold boot attack* obviously is a powerful tool in the computer forensic investigator's bag of tools. However, this method relies on many variables in order to make it actually work. Also, the digital forensics community is still debating whether *cold boot attack* produces a sound forensics memory acquisition. Therefore, this method is only used in extreme circumstances where it may be the only viable option available and may make all the difference between succeeding in finding evidence and leaving empty handed [23].
Students have to justify the circumstances in which they will use the *cold boot attack* method.

Step 2. Memory acquisition using other memory acquisition tools
In a normal scenario when no drive encryption is used and the system is not blocked, students will use uncontroversial (court approved) Windows forensics acquisition tools to dump the memory to an external storage. Many open source and commercial Windows memory acquisition tools are available [24]. Here we have students to choose at least two well-accepted tools from the following list.

- *MoonSols Windows Memory Toolkit* [25] -- an open source memory acquisition tool that is accepted by the forensics community.
- *ManTech's MemoryDD* [26], another open source memory acquisition tool.
- *winen.exe from EnCase* [1]
- *FTK imager* [2].

Step 3. Analysis for identifying malicious processes
When a machine is compromised, it will hide malicious processes/files/registry entries, and network connections. Finding a true running process list is critical for the investigator to identify whether there are any counter-forensic traps in place to hide evidence on the system. A well-known memory analysis tool, *Volatility Framework* [27], is a Python-based toolkit for extracting information from Windows memory images and provides functions of *psscan, thrdscan, dlllist, modules, sockets, sockscan, connections, connscan*, to show hidden processes, models and network connections. Other similar tools include *Mandiant's Memoryze* and *Mandiant Audit Viewer* [28, 29] and *PTFinder* [24].

In this exercise, students will use *Volatilty Framework*, *Mandiant's Memoryze* and *Mandiat Audit Viewer* to discover the hidden "*nc*" network connection. Note that discovering the migrated malware is a challenging activity. Once the malicious processes are identified, students will dump them out (using *Volatility's procdump*, or other tools), finally, use a disassembler such as *debugger IDA Pro* [29] or *ollydbg* [30] to analyze the executable.

At this point, students are comfortable with the Windows memory acquisition and analysis tools. Now the question is whether there are technologies that can defeat Windows memory forensics. In December of 2012, researchers created an anti-forensics tool called *Dementia* [31] that exploits memory acquisition tools and prevent these tools from finding hidden objects and processes. Students will validate whether they still can find hidden processes using *Volatility Framework* after running *Dementia*.

Step 4. Generating the forensics report
Students will follow the forensics procedure and provide a detailed documentation describing the actions, the rationale behind taking the actions, ramification of taking such actions, and the final findings.

### *B. Mobile Device Forensics*

Mobile device forensics is particularly challenging due to the volatile nature of evidence and the rapidly changing proprietary technologies in software, OS and hardware for mobile devices. Evidence that can be potentially recovered from a mobile device comes from several different sources, including mobile device memory, SIM card, and externally attached memory cards. We designed an iPhone forensics lab by following the forensic process of seizure, acquisition, and examination/analysis, to address some of the challenges described in section II. Students will use different seizure methods described in section II, acquire the available evidence in each scenario, then analyze and compare the differences in the evidence. Finally, students will be required to document the seizure actions, and justify whether each action will potentially modify the original evidence or fail to capture pertinent evidence.

**Lab Activities:**

Step 1. Seizure

Mobiles devices are often seized live. As the aim of seizure is to preserve mobile evidence when transporting the device to a safe location for acquisition, the first responders may use a seizure method listed below.

a. Turn off the iPhone
b. Place the iPhone in *Airplane Mode* to suspend the device's signal transmitting functions therefore preserving data.
c. Isolate the iPhone from cellular, Wi-Fi, Bluetooth and other radio signals using appropriate techniques such as *Black Hole Faraday* or *Ramsey RF Shield Test Enclosure*, to prevent data exchange/changes.

Step 2. Acquisition and Analysis

The next step is to acquire evidence from the iPhone. There are two types of acquisition – logical acquisition and physical acquisition. Logical acquisition implies a bit-by-bit copy of logical storage objects that reside on a logical store (e.g., a file system partition) such as call logs, voicemail, calendar, SMS/text, photos, videos, email, app data/files, address book, etc. Physical acquisition implies a bit-for-bit copy of an entire physical store. It will acquire information from the device by directly accessing the flash memory. Therefore, a physical acquisition has the advantage of allowing open applications and deleted files/data remnants such as location history, screen shot cache, web history, map history, username/password to be examined. Following each method used in seizure, students will performance acquisition and analysis accordingly.

When the iPhone is turned off, the examiner could choose to remove the SIM card and removable flash cards from the seized iPhone for acquisition or turn the iPhone back on for acquisition and analysis. However, one must be aware that turning off/on a mobile phone is prone to modification of evidence. Therefore, it is not a forensically sound approach for mobile forensics.

SIM card stores information of the make and model of the mobile handset, the subscriber (international Mobile Subscriber Identity), a list of the numbers the subscriber called or received, the SMS messages sent or received by the subscriber, calendar entries; photographs/video stored in the handset, subscriber's location, the provider information, etc. SIM card acquisition only extracts evidence resided in the card. Various SIM card acquisition and analysis tools exist for mobile devices, for example, *Paraben SIM Card Seizure* [32], *SIMiFOR* [33], *SIM Explorer* [34], *BOBILedit!* [35], and *SimCon* [36].

When the iPhone is on when it is seized, data can be retrieved directly from the phone by using forensic software through a cable or usb connection. Examples of the physical acquisition forensics tools are *iXAM* [37], *FTK imager, EnCase, Zdziarski technique* [38], *Cellebrite's UFED* [39], *Lantern* [40], *Oxygen* [41] and *AccessData Mobile Phone Examiner Plus (MPE+)* [42].

After the mobile data is acquired, mobile forensics analysis tools are utilized to analyze and identify critical information from the mobile Operating System (OS), the system partition, data partition which includes all user data, the cellular carrier, serial number of the iPhone, and mobile device's model. In the case of iPhone, students also utilize *PlistEditPro* to analyze property lists (.plist) and *SQLite databases* that store user and application settings.

Many mobile forensics acquisition tools listed above are also capable of mobile forensics analysis. For example, *EnCase, AccessData FTK, Cellebrite's UFED, Lantern, Oxygen* and *MPE+* are among the popular analysis tools that are accepted by the court of law.

Step 3. Documentation and Report

Students are required to document the seizure actions. After trying different types of seizure and acquisition methods, students will document the analysis results including pertinent evidence. Based on the analysis result, student will justify whether some actions will potentially modify the original evidence or fail to capture pertinent evidence. They should conclude: If the device is found switched on, DO NOT switch it off and if the device is found switched off, DO NOT switch it on.

### *C. Solid State Drives Data Analysis*

As mention in Section II, SSD challenges the traditional forensic practices due to wear-leveling and the automatic Garbage Collection. In this section, the authors attempt to introduce lab exercises and research questions to the forensic class to make students aware of the risk of tampering or destroying evidence using a normal data acquisition and recovery process when SSDs are involved in forensics investigations. The lab activities are described below.

**Lab Activities:**

Step 1. Observing evidence changes caused by Wear-Leveling and Garbage Collection

Both Wear-Leveling and Garbage Collection algorithms may result in data being moved around or removed from physical flash memory locations without any external input by users. Since these operations are managed by the onboard SSD controller, deletions may occur independently of any commands issued by a host device controller of the motherboard or the operating system.

Student will explore and verify that SSDs can present different evidence compared to HDDs, when actions such as creation and deletion of data have occurred for both in precisely the same manner. Various forensics tools such as *EnCase* and *FTK* can be used to analysis the deleted sectors to determine whether the sectors are cleaned/overwritten/intact.

A variety of test scenarios will be designed by students to track the results of minor changes in the contents of a drive. These tests could include the modification of an individual file, the deletion of an individual file using various operating systems, the partial overwriting of a file, and the formatting of the drive with both quick and full formatting.

Step 2. Determining whether a write-blocker will prevent evidence changes on an SSD

Hardware or software write-blockers are commonly used in forensics acquisition as standard mechanisms to prevent modification of drive contents by blocking write commands. Unfortunately, the presence of a write-blocker to a SSD does not prevent irrecoverable data loss from occurring. Students will explore and demonstrate that even a physical hardware write- blocker fails to prevent automated evidence changes on an SSD.

Step 3. Determining the events that trigger evidence change and loss

After observing the changes caused by wear-leveling and Garbage Collection, students will further research and determine which events are more likely to trigger evidence loss. For example, students will study the SSD-specific command TRIM to understand its behavior. The TRIM command is designed to enable the operating system to notify the SSD of the pages of data that are marked to be erased by the user or operating system itself. During a delete operation, the OS will not only mark the sectors as free for new data, but it will also send a TRIM command to the SSD with the associated Logical Block Addressing (LBAs) to be marked as no longer valid. After that point, the SSD knows that those marked LBAs can be cleaned during Garbage Collection.

Step 4. Developing methodology to rebuild evidence for forensics investigation (Bonus Point)

To address these challenges, students will research for technologies that may rebuild evidence utilizing logged information from a journaling OS and existing software tools after data change has occurred. As this is an open-ended question, many students choose to work on it as an independent study or a thesis topic (for graduate students).

Step 5. Generating the forensics report

Students will provide a detailed documentation describing the design, actions, and the final findings for each activity.

## IV. Student Lab Experience

Both the Windows Memory acquisition and analysis (without *Dementia* and *Metasploit*) and the mobile forensics labs were offered twice for forensics students. The labs truly inspired students' curiosity and interests in forensics research and developed their critical thinking capability. The SDD lab was newly designed and was first offered as a graduate-level group research project. Students are especially interested in discovering the hidden SDD controller activities to impact the traditional forensics process and procedure. Many students expended the project and labs activities and worked on these challenging areas as independent studies and even M.S. thesis.

## V. Conclusion

Digital forensics is an ever-evolving field filled with challenges and opportunities. As the technologies, software and hardware are advancing, students have to be aware of the challenges and acquaint the latest technologies to stay on top of forensics field. This paper presents the design and authors' experience in developing three research-oriented forensics labs – Windows memory acquisition and analysis, Mobile forensics analysis and Solid State Drive analysis. These labs introduce the challenges facing the forensics investigators as well as the cutting edge technologies to address the challenges in the digital forensics field. We believe that these forensics labs will help other forensics educators to update their forensics lab activities and encourage them to introduce similar research oriented labs and activities in their forensics courses.

## VI. References

[1] EnCase from Guidance Software, http://www.guidancesoftware.com/encase-forensic.htm
[2] FTK from AccessData, http://www.accessdata.com/products/digital-forensics/ftk
[3] ProDiscover Forensics, http://www.techpathways.com/prodiscoverdft.htm
[4] S. L. Garfinkel, Digital forensics research: The next 10 years, *Digital Investigation 7 (2010),* S65-S73
[5] J. H. Sawyer, Tech Insight: Digital Forensics Incident Response Go Live, http://www.darkreading.com/security/news/211600781, 2008
[6] M. Wade, Memory Forensics: Where to Start, http://www.dfinews.com, 2011
[7] C. Waits, J. Alinyele, R. Nolan, andn L. Rogers, Computer Forensics: Results of Live Response Inquiry vs. Memory Image Analysis, *CMU/SEI-2008-TN-017*, 2008.
[8] D. Bennett, The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations, *Forensics Focus*, 2011.
[9] Y. Gubanov, O. Afonin, Why SSD Drives Destroy Court Evidence, and What Can Be Done About It, http://www.dfinews.com/print/7100, 2012
[10] G. B. Bell and R. Boddington. Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? *Journal of Digital Forensics, Security and Law*. 5(3). pp.1-20, 2010.
[11] L. M. Grupp, et al. Characterizing Flash Memory: Anomalies, Observations, and Applications. *New York: ACM*, 2009.

[12] Troell, L., Pan, Y., and Stackpole, B., "Forensic Course Development," *Proc. of Conference on Information Technology Curriculum 4*. North Carolina, 2003.
[13] Troell, L., Pan, Y., and Stackpole, B., "Forensic Course Development – One Year Later," *Proc. of the SIGITE 2004 conference,* Salt Lake CIty, Utah, 2004.
[14] Open Memory Forensics Workshop (OMFW), https://www.volatilesystems.com/default/omfw, 2008.
[15] M. J. Decker, W. G. Kruse, B. Long, and G. Kelley, Dispelling Common Myths of Live Digital Forensics, www.dfcb.org/docs/LiveDigitalForensics-MythVersusReality.pdf
[16] Black Hole Faraday bags, http://edecdf.com/products?iProdId=1
[17] Ramsey RF Shield Test Enclosure, http://www.ramayes.com/rf_shielded_forensics_enclosure.htm
[18] David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni. Metasploit - The Penetration Tester's Guide. *No Starch Press*, San Francisco, 2011
[19] FUTo Rootkit: http://www.rootkit.com/board_project_fused.php?did=proj31
[20] Truecrypt: http://www.truecrypt.org/
[21] Halderman, J. Alex, Schoen, Seth D., Heninger, Nadia, et al. Lest We Remember: Cold Boot Attacks on Encryption Keys, *Proc. of 2008 USENIX Security Symposium*, http://citp.princeton.edu/pub/coldboot.pdf, Princeton University 2008.
[22] Cold Boot Attacks code, https://citp.princeton.edu/research/memory/code, 2008
[23] R. Carbone, C. Bean, and M. Salois, An in-depth analysis of the cold boot attack: Can it be used for sound forensic memory acquisition? *Defense R&D Canada, TM 2010-296*, 2011
[24] N. Davis, Live Memory Acquisition for Windows Operating System, *Eastern Michigan University, www.cert.org/archive/pdf/08tn017.pdf,* 2008.
[25] MoonSols Windows Memory Toolkit, http://moonsols.com/product
[26] ManTech's MemoryDD, http://www.thefreelibrary.com/ManTech+Memory+DD+Version+1.3+for+Forensic+Analysis+of+Computer...-a0182984027
[27] The Volatility Framework https://www.volatilesystems.com/default/volatility
[28] Memoryze, http://www.mandiant.com/products/free_software/memoryze/
[29] Mandiant Audit Viewer, http://www.mandiant.com/products/free_software/mandiant_audit_viewer/
[29] IDA Pro https://www.hex-rays.com/products/ida/index.shtml
[30] ollydbg, http://www.ollydbg.de/
[31] dementia, http://events.ccc.de/congress/2012/Fahrplan/events/5301.en.html
[32] Paraben SIM Card Seizure, http://www.forensicswiki.org/wiki/Paraben_SIM_Card_Seizure
[33] SIMiFOR, http://www.forensicswiki.org/wiki/SIMiFOR,
[34] SIM Explorer, http://www.forensicswiki.org/wiki/SIM_Explorer
[35] BOBILedit!, http://www.mobiledit.com/
[36] SimCon, http://www.forensicswiki.org/wiki/SIMCon
[37] Physical acquisition tools iXAM, http://ixam-forensics.com,
[38] Zdziarski technique, http://www.iosresearch.org/
[39] Cellebrite's UFED, http://www.cellebrite.com/forensic-products/ufed-support-center/tutorials.html
[40] Lantern, http://katanaforensics.com/
[41] Oxygen, http://www.oxygen-forensic.com/en/download/
[42] AccessData Mobile Phone Examiner Plus (MPE+), http://accessdata.com/products/computer-forensics/mobile-phone-examiner