Cell Phone Forensics

 Bryan S. Goda John Bair Charles Costarella

 godab@uw.edu jbair007@uw.edu costarec@uw.edu

University of Washington, Tacoma
Institute of Technology
Tacoma, Washington, USA 98405

**ABSTRACT**

Cell Phone Forensics is a relatively new field when compared to computer forensics. The need to recover data from mobile devices often overwhelms the processing capabilities of most law enforcement agencies. This paper outlines a three course sequence in mobile digital forensics that has been developed in partnership with law enforcement and forensic tool manufacturers. During the three course sequence, students learn forensic tools, procedures, and how get information from chips removed from cell phone boards. This dynamic partnership has been beneficial to all parties and potential employers are seeking graduates with these new forensic skills.

**Categories and Subject Descriptors**

K.m [Miscellaneous]: Security

**General Terms**

Design, Security, Standardization, Legal Aspects

**Keywords**Mobile Phone Forensics, Digital Evidence, Education, Small Scale Digital Devices, Personal Digital Technologies

# INTRODUCTION

The University of Washington Tacoma (UWT) was founded in 1990 to meet regional needs for community college transfer students. UWT is set in downtown Tacoma’s Union Station neighborhood, a district of historic warehouses. The vision of the University is to provide access to an exceptional university education; provide an interdisciplinary approach to knowledge

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.
*SIGITE'15,* September 30-October 03, 2015, Chicago, IL, USA
©2015 ACM. ISBN 978-1-4503-3835-6/15/09…$15.00
DOI: <http://dx.doi.org/10.1145/2808006.2808022>

and discovery in the 21st century; and develop a strong and mutually supportive relationship between the campus and its surrounding communities. The downtown area has been revitalized by the University’s development and this growth has spread throughout the South Puget Sound Region.

In 2001, the Institute of Technology was launched on the campus with an initial cohort of 30 Computer Science students and a desire to grow into a polytechnic that would support multiple degree programs providing an educated technical work force for the South Puget Sound and the state. In 2008, the Institute started the Information Technology program with an initial cohort of 18 students. The entering class in 2015 will be 70 students.

Marshall University offers a BS in Digital Forensics & Information Assurance [1]. They have a working relationship with the West Virginia State Police where real world problems can be brought into the classroom. Detective John Bair of Tacoma Police department is a recognized leader in the area of cell phone forensics. Two years ago, he was looking for a partner in the local area to create a Marshall-like program. He found that partner in the University of Washington, Tacoma.

# Combining solutions

Detective John Bair approached the University of Washington, Tacoma by addressing the evolving technology needs within his own department, and by targeting the goals of the Institute of Technology. He proposed answers to several questions: 1) How does law enforcement properly prepare individuals tasked with mobile data extraction? 2) How does the City of Tacoma and the University benefit from a combined digital mobile forensics lab and curriculum? 3) What type of service will a combined lab offer – and how will it be different from what is currently available?

# Initial Startup

Starting a series of courses in mobile digital forensics can be a daunting task [2]. There must be: 1) a demonstrated need for these courses, 2) hiring of qualified instructors, 3) procurement of the correct highly specialized equipment, and 4) a level of student interest in taking the courses that is high enough to maintain steady enrollment. A test course was advertised to the Information Technology majors regarding a course in mobile digital forensics. At the time, there was no lab facility with either hardware or software in existence outside of Tacoma Police Department and some students were skeptical about taking a college level course from a police detective.

Probably the biggest obstacle in creating a sequence of courses in
mobile digital forensics is the creation of a lab to support the courses. The lab requires specialized hardware and software and in order to be useful it has to be able to handle the extremely wide variety of mobile phones commonly in use. Today’s smart phones process and store a variety of data streams generated by a variety of use cases, such Multi-Media Messaging Service (MMS), Short Message Service (SMS), Instant Messaging (IM), video capture, photos, electronic mail, ringtones, abbreviated call lists, internet browsing history, and deleted items [3,4]. Device hardware and software can vary widely depending on the carrier, manufacturer, operating system, and the hardware and software versions, including updates [5].

Today several vendors target law enforcement as a client, to use their product(s) in recovering stored user data on mobile devices. The creation of a forensic lab would require that the student understands how some of these products work, and more importantly what changes occur and how to validate their findings [6].

#  Mobile Digital Forensics I

The courses utilize three customized student manuals authored by Detective Bair that include labs in nearly every class. Students begin by first understanding the legal process. This covers the elements of *consent to search*, *exigent circumstances*, and the *search warrant*. The dynamic search warrant language origins are described in detail. This includes the Mobile Network Operator (MNO) and Mobile Virtual Network Operator (MVNO) and how they play an important role in the search warrant execution – and later validation. The law enforcement point of view is focused on legal attribution, which is the overall and final metric of success.

Evidence contamination and prevention exposes students to various Faraday methods to include internal device settings, mesh, foil, and specially designed signal blocking boxes. The device seizure process is examined in detail in order that students understand that moving the seized device translates to changes in the data as network communication continues.

The class stresses how phones communicate through various protocols and the importance of protocol filtering The foundation of this is *Attention Terminal* (AT) labs. This illustrates that forensically processing phones, unlike the traditional desktop forensic process of static imaging, require communication to take place between the devices (evidence) and the forensic tool or utility [7]. This foundation carries into trouble shooting. Students must utilize an understanding of various Windows software/hardware interface settings to help rectify common problems encountered in mobile forensic exams.

Students are exposed to the Subscriber Identity Module (SIM) and shown the various locations within the SIM file system where potential stored artifacts can be logically located. Using SIM Card Seizure, Bitpim, Secure View For Forensics 3, Mobile Phone Examiner Plus (MPE+), and the Cellebrite Universal Extraction Device (UFED) Touch, the class experiences numerous logical extractions utilizing actual phones, SIM cards, and file systems with replicated artifacts from past cases or scenarios. Students experience the various nuances of each tool, including which artifacts the tool may miss, and the core features and strengths of each tool [8].

Students are introduced to manual carving of (logically) missed artifacts utilizing AccessData’s Forensic Tool Kit (FTK) Imager, and open source date and time stamp interpreters. Mobile Digital Forensics I conclude with validation and case reporting. Table 1 outlines the $20k startup costs and $12k annual costs to support the first course in the sequence.

**Table 1: Software and Hardware Costs for Level 1**

|  |  |
| --- | --- |
| **TINFO 444 Digital Mobile Forensics Level I** |  |
| **Forensic Tool** | **Vendor** | **Initial Cost**  | **Annual Renewal** |
| SIM Card Seizure (21 licenses) | Paraben | **$900** | **$240** |
| Secure View 3 (25 licenses) | Susteen | **$5,000** | **$5,000** |
| Mobile Phone Examiner+ (25 licenses) | AccessData | **$4,367** | **$4,367** |
| Universal Forensics Extraction Device Touch (2 units) | Cellebrite | **$10,500** | **$3,080** |

#

# Mobile Digital Forensics II

Level II moves from logical into the physical file system. The course begins with a brief description of the various types of flash memory commonly found on mobile devices. Students learn the history of Toshiba, and how Dr. Fuiho Masuoka invented both NOR and NAND memory [9]. Embedded Multimedia Card (eMMC) and Universal Flash Storage (UFS) are also introduced. Students learn half/full duplexing, command queuing and improving system performance [10]. Students must understand where physical memory resides and how the operating system, wear leveling and garbage collection affect deleted data. Students study how commercially available products function similarly to flasher (repair) boxes in how they acquire physical data.

The core of level II is the various encodings that can be found within the physical file system. Students must demonstrate that they can locate and decode values in Unicode, ASCII, Reverse Nibble, Hexadecimal, 7Bit PDU, 7Bit reversed, and Big and Little Endian. Using numerous mobile file systems, phone Epoch dates are located and decoded. These dates and times include AOL, GPS, Unix, ISO 8601, PDU, and many others. Students are instructed on how to use the known (parsed) values to then locate deleted artifacts missed by the forensic tool. Labs are streamlined in Level II for focus on analysis as the actual (pulled) file system with the known artifacts to decode supplied to the students. This saves on acquisition times as physical pulls can take hours to complete on the larger and more complex smart phone systems that the students are now examining, commensurate with their growing skills level.

Students next learn to utilize a robust forensic program called Cellebrite Physical Analyzer which works with the previously mentioned UFED Touch to decode and search for mobile artifacts. Cellebrite Mobile Synchronization Ltd. was established in April 1999 and is a subsidiary of Sun Corporation [11]. Cellebrite UFED initially began as a device to transfer contacts and other media from one phone to another and was used primarily by wireless vendors selling mobile phones. The company soon made a forensic version of the same product which is targeted to law enforcement agencies world-wide. There are more than 30,000 UFED units deployed to law enforcement, police and security agencies in 100 countries [12].

Students in Level II conduct physical and advanced logical extractions on iPhones. They understand the limitations of each of these exams based on the version of the iPhone being examined and how user enabled security also effects the extraction. Basic manual carving of user installed application databases (SQlite) are discussed, which stresses how forensic tools do not always carve the schema and vendors who do support application parsing can miss newer applications. Table 2 shows the Cellebrite Physical Analyzer that is the main forensic product used in Level II.

Students conclude Level II by conducting an advanced validation technique using Ultra Compare Professional. They learn how to locate precisely, within the binary and file system, where changes have taken place, even between two different forensic tools that extract the same stored artifacts.

**Table 2: Hardware Costs for Level 2**

|  |
| --- |
| **TINFO 445 Digital Mobile Forensics Level II** |
| **Forensic Tool** | **Vendor** | **Initial Cost**  | **Annual Renewal** |
| Physical Analyzer (20 Licenses) | Cellebrite | **$25,000** | **$5,000** |

# Mobile Digital Forensics III

Students who attend Level III have achieved both the fundamental requirements and core elements of decoding the physical file system and advanced validation. Level III requires more hands on experience with the device and more typical “real-world” user enabled security. Students learn how various programming tools, use of Joint Test Action Group (JTAG) processing, and the chip off extraction process, can be utilized to obtain the physical file system.

Students are required to disassemble phones and research potential areas on the main board or chip number. Students will develop a strategy on both non-destructive and destructive methods that will be employed on their particular test phone. Specialized hardware, re-work stations, solder and de-soldering techniques are expected of each student. The course outlines that encountering a severely damaged device does not necessarily mean the phone’s stored user data cannot be recovered. For law enforcement, this scenario is often the case and skills that students gain in this area will distinguish the graduates of a forensics program.

Specialized chip programming tools, socket readers, JTAG jigs, Molex connectors, and other fabricated tools and techniques are utilized (Table 3). The $10k in hardware costs permits students to extract data from a variety of cell phones when it would not be possible otherwise. This capability exceeds most law enforcement agencies’ capabilities and is another distinguishing feature of UW Tacoma’s mobile digital forensics program. Level III concludes with students taking their binary pulls from these advanced techniques, and utilizes their training from Level II to rebuild the file system. They can then use these results to locate valuable stored user data that would have normally been missed by commercially available tools or due to user enabled security.

**Table 3: Hardware Costs for Level 3**

|  |
| --- |
| **TINFO 446 Digital Mobile Forensics Level III** |
| **Forensic Tool** | **Vendor** | **Cost**  |
| UP 828 Programmer w/adapters | Forensic Store | **$4,100** |
| RIFF Box (5) | IP Mart | **$475** |
| Rework Station w/smoke absorber (2) | The LA Shop | **$340** |
| T-862 IR Rework | wholesale2worldwide - ebay | **$178** |
| Sireda Adapters (1 set) | Teel Technologies | **$2,438** |
| Jtag jigs with w/Adapters (5) | FoneFunShop | **$461** |
| BST Dongle (5) | FoneFunShop | **$615** |
| Power Supply (5) | The LA Shop | **$325** |

# Real Cases – New Ideas

During the courses, the instructor is also working full time examining mobile devices from criminal cases from the City of Tacoma and surrounding Puget Sound area. This unique relationship allows the opportunity for students to be part of the investigative process at a technical level. Since the first beta class on this series, Detective Bair has allocated students extra credit to develop concepts, methods, or validated exploits to assist with problems encountered with criminal case work. The concept of this integration with the course is outlined as follows:

1) The (new) case problem is introduced to the class. It typically involves a security enabled device, file system anomaly, or some other tough, real world issue pertaining to a case.
2) Students conduct their own research and potential solution. They are allowed to test the concept on non-evidential mobile devices that match the actual evidence. Through reverse engineering or other means, a solution may be reached. This opportunity allows for students to immediately apply what they have learned, and in some cases knowledge they may already have achieved through academia or other means.
3) The concept is validated and applied to the actual case by Detective Bair.

Cases thus far that have arisen (during the normal class quarters) have involved an unsolved homicide, malware anomaly, and a child exploitation incident. Having real cases as part of the classroom environment has peaked student interest and students can readily see what they are learning is important, useful, and timely.

# Conclusions

The IT majors who attend these courses may or may not choose to enter into law enforcement or the private sector dealing with mobile forensic extractions. As an elective series, the curriculum is designed to complement the programs already in place at UWT. The student ratings are very high for these series of electives. Our first graduates who have taken these electives are sending us interesting notes:

*Hello Director of the Institute,*

*My name is \_\_\_\_\_\_. I just graduated from UWT with a BA of Science in Information Technology and Systems. Thankfully, I have been offered an ITCFP position with Boeing, in Charleston, SC in the Mobile Application and Support department. During the spring quarter 2014, I took Mobile Digital Forensics class with Mr. Bair. To be honest, I wasn't a big fan, because I kept asking myself.."Why do I need this class?"*

*Well it looks like I did need this class, but I just didn't know it yet!! In order to start working with Boeing, they have to find a position for you that best suits your needs and Boeing needs. During my interview with the Mobile App's team with Boeing, I was asked questions about support roles, handling customers, etc. Unfortunately, on my resume, I had not mentioned anything about the mobile forensics tools or class that I had just completed. When I had mentioned this to the interviewer, he immediately asked why this wasn't in my resume. I had told him that I had just graduated and didn't know I could add things to my resume since Boeing had already accepted me. He then continued to ask, what was the class about? I talked to him about my knowledge in hand-carving deleted messages, all the different tools that I had used (Cellebrite, UFED Analyzer, SIMcon; just to name a few), and all the different techniques that there are to get information out of a cell phone. The manager was so impressed, that he offered me the job on the spot.*

*That same day, I gave John Bair a phone call, and told him about my success story because of his class. He was extremely happy and sounded like he wanted to cry. :)  And now, I am emailing you, Institute Director, just to let you know that this class was a very good class to attend and that even though I didn't understand why, it turned out to be very critical to the success of IT students from UWT.*

*Thank you.*

The three course sequence is a great opportunity for students at the University of Washington Tacoma and law enforcement. The courses are designed to be updated as technology changes and new technology problems face law enforcement. Students in the future will face even more issues centered on mobile forensics, user enabled security, encryption and cloud forensics.

Law enforcement will in turn have a cutting edge research center lab that is equipped to handle these challenges here in the Pacific Northwest. We are currently starting new partnerships with the Highway Patrol, Secret Service, and FBI. Students with forensics skills will be highly desired in internships and future employment. The explosion of mobile devices will mean that the ability to extract information will be a critical and necessary skill for the foreseeable future.

**REFERENCES**

[1] Marshall University. Retrieved April 30, 2015 from <http://www.marshall.edu/isat/dfia/digital-forensics.asp>

[2] Srinvasan, S., Computer Forensics Curriculum in Security Education. In *InfoSecCD ’09,* Kennesaw Georgia USA, September 25-26, 2009.

[3] Mislan, R., Creating Laboratories for Undergraduate Courses/Building Government-Industry Partnerships. In *SIGITE 2010*. Midland, Michigan USA, October 7-9, 2010, 111-115.

[4] Jansen, W., Delaitre, A., Moenner, L., Overcoming Impediments to Cell Phone Forensics. In *Proceedings of the 41st Hawaii International Conference on System Sciences 2008,*Wailoloa Big Island Hawaii USA, January 7-10, 2008.

[5] Kim, K., Hong, D., Chung, K., Forensics for Korean Cell Phone. In *e-Forensics ’08,* Adelaide Australia, January 21-23, 2008.

[6] Tuttle, J., Walls, R., Miller, E., Levine, B., Reverse Engineering for Mobile Systems, Forensics with Ares. In *Insider Threats ’10,* Chicago Illinois, USA, October 8 2010.

[7] NIST Special Publication 800-101 Revision 1, Guidelines on Mobile Device Forensics, May 2014.

[8] Hill, L., An Inexpensive Method to Shield Wireless Devices During Hardware Forensic Investigation in a Laboratory Setting. In *SIGITE ‘07*, Destin Florida, USA, October 18-20, 2007.

[9] Toshiba. Retrieved May 11, 2015 from

<http://www.flash25.toshiba.com/downloads/toshiba-timeline.pdf>

[10] Toshiba. Retrieved May 11, 2015 from <http://www.toshiba.com/taec/Catalog/Line.do?familyid=7&subfamilyid=900116&lineid=2095185>

[11] Suncorporation. Retrived May 11, 2015 from <http://www.sundenshi.co.jp/eng/company/group/index.shtml#o01>

[12] Cellebrite. Retrieved May 11, 2015 from <http://www.cellebrite.com/About-Cellebrite>

[13] Rocha, A., Scheirer, W., Boult, T., Goldenstein, S., Vision of the Unseen: Current Trends and Challenges in Digital Image and Video Forensics. ACM Comput. Surv. 43, 4, Article 26 (October 2011), 42 pages.

[14] Yates, M., Chi, H., A Framework for Designing Benchmarks of Investigating Digital Forensics Tools for Mobile Device. In *49th ACM Southeast Conference*, Kennesaw Georgia, USA, March 24-26, 2011.

[15] Turnbull, B., The Adaptability of Electronic Evidence Acquisition Guides for New Technologies. In *e-Forensics ’08,* Adelaide Australia, January 21-23, 2008.

[16] Yates, M., Practical Investigations of Digital Forensic Tools for Mobile Devices. In *InfoSecCD ’10,* Kennesaw Georgia, USA, October 1-2, 2010, 156-162.

[17] Egelman, S., Jain, S., Portnoff, R., Liao, K., Consolvo, S., Wagner, D., Are You Ready to Lock? In *CCS ’14*, Scottsdale Arizona USA, November 3-7, 2014, 750-761.

[18] Marturana, F., Me, G., Berte, R., Tacconi, S., A Quantitative Approach to Triaging in Mobile Forensics. In *International Joint Conference of IEEE TrustCom ’11*, Changsha China, November 16-18, 2011, 582-588.

[19] Gutmann, P., Naccache, D., Palmer, C., Crytography, Law Enforcement, and Mobile Communications. In *Security and Privacy,* Volume:4, Issue:6, November 2006, 67-70.