Forensics Overview

Table of Contents

Introduction to Mobile Device Forensics and Investigations ............................................................... 2
Objectives........................................................................................................................................ 3
Overview -1 ..................................................................................................................................... 5
Overview -2 ..................................................................................................................................... 7
Overview -3 ................................................................................................................................... 11
Notices .......................................................................................................................................... 12
**001 Shawn Fleury: In this module I'm going to introduce you, at a medium level, to Mobile Device Forensics and Investigations.

I'm not going to go as deep as this is the Hex sector on this type of phone where you'll find information.

We are going to get into the tools that are used in mobile forensics; what is the process that investigators should be using during investigations; and what type of information you may find during an investigation.
Objectives

At the completion of this module, students will be able to:

Describe

- The roles and responsibilities of the Digital Forensics Incident Response team members collecting evidence from mobile devices
- How to identify and preserve evidence from mobile devices
- How to acquire digital evidence from mobile devices
- The features of the major mobile forensics programs and toolkits
- How to analyze digital evidence from mobile devices
- How to report findings of digital evidence from mobile devices

Discuss

- The mobile forensics process framework

Understand

- How the data obtained from the cell smartphone subscriber can aid in a mobile forensics investigation

**003 So at the beginning-- or the end of this block I should say-- students will be able to: Describe the different roles and responsibilities of the digital forensic investigative response team members. There are the people that are on scene. Whether the scene is incident to an arrest where during the arrest I get somebody's cell phone as part of the arrest; or a murder investigation where there's a dead body with a cell phone on the ground. The roles are still the same. And we'll go over what those roles are and what they're responsible for.

How to identify and preserve evidence from mobile devices.
Mobile devices are electronic devices.
The data is stored in 1s and 0s. If they're not handled correctly, you may destroy data on the device.

How to acquire digital evidence from mobile devices. There's special tools that we use in the forensic community to actually get information from the phones.

The features of the major forensic programs and toolkits. I believe we go over five or six different tools that are available for use.

How to analyze the evidence you get using those tools.

How to report your findings- the findings of digital evidence from mobile devices.

We're going to discuss the mobile forensic process framework. First we do this; then we do this; and then we do this. In forensics, we need to have a repeatable process. That's one of the things that makes forensics forensics.

We don't say, "Okay, this time I'm going to do this, and then I'm going to step- skip to Step 5; and then I'll do the chain of custody form, and then I'll do this. Because if that evidence were to go to court, it's very likely in that case that the court would throw that evidence out. And that's not what we want as forensic investigators.

And we're going to also understand how the data obtained from the subscriber can aid in an investigation.
The stuff you find on a phone itself is great. But we can't forget that the carrier might also have a lot of information that either corroborates what we found on the device, or fills in gaps for stuff we didn't find on the phone. Maybe they do have it at the provider level.

Overview -1

As the use of mobile devices become more prevalent, digital forensics is transforming from stationary computer systems to mobile devices.

Some users have transferred the business, communications, and data storage to their mobile device. Others use the computer synchronize the computer system with the mobile device.

**004 So Overview. As the use of mobile devices become more prevalent, there’s billions of mobile devices worldwide. In the U.S. alone, there’s probably somewhere between 500-million and a billion mobile devices; between people having personal devices and work devices, and children having devices, they’re pervasive; they’re everywhere.
Digital forensics is transforming from stationary computer systems to mobile devices.

Even when I got into the forensic field eight years ago-- no, nine years ago now-- the primary focus was on the hard drive from the computer system; because that is more than likely where you would find the digital evidence that supported your case.

Yes, there were smartphones. But due to the limited capabilities of them, the low- the slow processors, the limited amount of RAM, the limited amount of storage, they were not the primary focus of most investigations.

As we've gotten- as the years have progressed, we've seen a change from the computers being the primary focus to the digital devices being as important, or more important, than the computer devices.

On a day-to-day basis, maybe half of the email I send is from my mobile device, while half is from the computer. When I'm on the road, probably 75% of my email is from my mobile device, and only 25% is from the computer.

Which location would an investigator be more likely to find information? Probably on the device I'm sending the most messages from. That's why they've become so important in the field of digital investigations. Some users have transferred the
business, communication and data storage to their mobile devices. Why should I use my laptop-- excuse me-- when I have a tablet and a mobile phone? Those two devices can meet all my needs for most days. Why even use the laptop?

Overview -2

Overview -2

It is imperative that law enforcement and computer incident response team (CIRT) members have the skills and tools to properly collect and analyze mobile devices as they would stationary computer systems.

Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods.

**005 It's imperative that law enforcement and computer incident response team, or CIRT-- we'll see that a couple of times through here-- have the skills and tools to properly collect and analyze the data.

A lot of places we go, the people that are using the forensic tools have not been trained on the use of the forensic tools.
The common thing I hear, when I'm teaching a forensic class is: "Oh we've had this tool for about two years. We read the Instruction Manual when we got it, and we've just figured things out as we've gone along."

What features are you missing? What don’t you know about; what kind of gotchas don’t you understand?

By going to formalized training, the courts look at that formalized training and go: "Okay, you have been trained on the use of this machine. We will allow you to talk about this machine to the court; whether as an expert witness or in some other manner."

If you don’t have the training, the courts are more likely to say: "You're not an expert in this field. We're not going to allow anything you've collected potentially to be used."

Depends on the court; depends on the jurisdiction you’re in, what kind of formalized training you have to have. It's very important to be formally trained with these tools, if possible.

Mobile phone forensics is the science of recovering digital evidence from a mobile phone, or other mobile device, under forensically sound conditions using accepted methods.

So there's a couple of things in that sentence that are very important. It's a science; it's not an art form. It
has to be repeatable: We do this; then this and this. And if we were to do the same process again, we would get the same results.

So the tools that are used in the forensic community have to be repeatable. That's one of the things that make it a forensic tool.

If I, as the police officer, use a tool and get a result, when I-- if I have to give that evidence to the defense expert to do the same investigation, using the tools available, he should get the same results that I get.

Now maybe the results are open to interpretation. Maybe I think it means one thing and the defense thinks it means something else. And that happens all the time in court. All that's open for interpretation.

There should not be a question though of: Well you found this; but I didn't find it using the same tools.

No, the tools should be repeatable. There should be no difference between the first time, the second time and the 100th time of doing a phone.

Primarily the tools are used to collect evidence; either to be used at a later date in court, either civil or criminal.

I know a lot of organizations that have these forensic tools. They have civil cases where their employees are on litigation hold. So they've been-- the organization's been notified
they're going to be sued. You need to collect all information that's relevant to this investigation.

So as part of the lit-hold process, the legal team, or whoever the team is, at the organization goes: "Okay, who might have information pertinent to this case, to this matter? Okay, Person 1, 2 and 3 have information. Where might they have stored that information? Well they have a desktop, they have a laptop, they have access to these shares; oh, and they have a corporate phone."

So as part of the lit-hold process, these tools can be used to create an image of the device-- depending on the device-- that can be used at a later date and time for civil evidence also.

"Forensically sound." Repeatable; again, that comes back to the ability to repeat the process. We're talking- and we'll get into it in this block-- we're talking about things such as hashing. We're going to hash the files to make sure that they have a digital fingerprint; and if they're hashed at a later data and time, the hashes should be identical.

That's how we prove that here's the hashes from when I collected the file. You can see the hashes are the exact same. So the files haven't changed. It's how we digital fingerprint or digital DNA for a file is a hash.
And "accepted methods." So the forensic community, the mobile phone forensic community says: "This is the way the phones need to be processed. This is what you can get off the phones."

Some phones, there are some gotchas with. Well is it an accepted practice to use this kind of tool to get the information if none of the forensic tools are available? That all falls under accepted methods.

Overview

While mobile device forensics is still considered a new science, several vendors offer certifications in cell smartphone and mobile device forensics:

- Cellebrite – Cellebrite Cell smartphone Forensics Certification
- BKForensics – Mobile smartphone Seizure Certification (MPSC)
- PATCtech (Public Agency Training Council) – Cell smartphone Technology and Forensic Data Recovery Certification
- Paraben – Certified Cell smartphone Forensic Examiner (PCME)

**006 While mobile device forensics is still considered a new science, several vendors offer certifications in cell smartphone and mobile device forensics.**
A lot of vendors do. So Cellebrite offers their own certification on the Cellebrite UFED machine that it sells. They developed it. They keep it up to date. They offer a certification that says: "Yes, you Officer Smith are certified to use our device. You've passed-- you've attended the course, you've passed the test, and you showed knowledge of how to use the tool."

And there's some other ones out there.

**Notices**

Copyright 2013 Carnegie Mellon University

This material has been approved for public release and unlimited distribution except as restricted below. This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

NO WARRANTY. THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark of Carnegie Mellon University.