## Purpose of Computer and Network Forensics

### Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose of Computer and Network Forensics</td>
<td>2</td>
</tr>
<tr>
<td>What Is Digital Forensics?</td>
<td>3</td>
</tr>
<tr>
<td>Need for Digital Forensics -1</td>
<td>4</td>
</tr>
<tr>
<td>Need for Digital Forensics -2</td>
<td>6</td>
</tr>
<tr>
<td>Purpose of Digital Forensics</td>
<td>8</td>
</tr>
<tr>
<td>Notices</td>
<td>12</td>
</tr>
</tbody>
</table>
Okay. So we'll start out with the purpose of computer and network forensics.
What Is Digital Forensics?

As defined in NIST Guide to Integrating Forensic Techniques into Incident Response:

“Application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data”

Also known as or called computer forensics and network forensics, and includes mobile device forensics

All better called one term: Digital Forensics

**005 Okay. So we have our NIST definition, right? So it's the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. Right. So that makes sense. If you're going after folks, you got to make sure everything is done properly, is done right.

And hear it called multiple things. Sometimes it's computer, if you're talking about host. Sometimes it's called network, if you're looking at the network data piece of it. And, of course, more recent times the mobile
device forensics is getting bigger and bigger now. Everybody has a phone. Many people have tablets. So it's heading in that direction. In general, if you use the term digital forensics, right, the 1's and 0's is what we're really talking about, no matter what it's sitting on or what it's flowing through. It tends to become a little easier. People understand what you're talking about if you use the term digital forensics.

Need for Digital Forensics -1

No major organization can afford to be without a digital forensics capability due to the amount of data in play and of the importance of that data to the organization.

• If that data is damaged, stolen, or otherwise compromised, the organization needs the capability to reconstruct what occurred.

**006 You’ve heard about the OPM breach. You’ve heard of a while back, Target, Nieman Marcus. You’ve heard of lot of different
companies. So basically it's coming down to the point where all organizations, say no major, but actually, all organizations should be looking at getting a forensic capability.

Now, there's a spectrum of this capability, right? I'm not saying every organization needs a team of three or five people that go out and actually do digital forensics and incident response so much as sometimes it's enough if it's a small enough organization to have a phone number that you can call and a reliable organization that you can reach out to. So that's the sort of thing we're talking about here. Right? If the data is damaged, stolen, otherwise compromised, the organization should have the capability, as some of you are all part of this kind of a team, should have the capability to reconstruct what happened.
Cybersecurity market expansion

- Global cybersecurity market was $63.7 billion in 2011\(^1\)
- Expected to grow to $120.1 billion in 2017\(^1\)

Growing threat of cybercrime

- Costs of global cybercrime was $110 billion in 2011\(^2\)
- Costs of global cybercrime was $445 billion in 2014\(^2\)
- 2014 study shows a 22% increase of successful attacks per company\(^3\)
  - 1.3 successful attacks each week per company; 2012\(^3\)
  - 1.7 successful attacks each week per company; 2014\(^3\)

In summary: You WILL be exploited.

\(^1\) http://www.darkreading.com/study-cybersecurity-market-to-double-in-next-five-years/id/d-id/1137973
\(^2\) http://www.zdnet.com/article/norton-cybercrime-cost-110-billion-last-year/

**007 So the need for digital forensics from a numbers standpoint. Looking back in 2011, it was almost 64 billion dollars for global cybersecurity. The market was spending that much, and between now and 2017 it is looking to almost double. That’s a significant amount of money, right, 120 billion dollars going to be spent. And as I just also mentioned, the cybercrime seems to be climbing very rapidly. Keep hearing about it pretty much every week or so. You’ll hear about somebody getting hacked or some data being compromised.
The costs for global cybercrime in 2011 was 110,000. And you can see in 2014, just last year, that quadruple to 445 billion dollars. And that is way, way fast for what’s happening, right? That’s going to end up being a lot, a lot worse, before it gets better, I believe. And the 2014 study shoes 22 percent increase in successful attacks, right. You know that there’s always things hitting your firewall. Always these things that are trying to get at the users through phishing e-mails. But when there’s a 22 percent increase in successful things happening, are they getting better, are we not paying attention? So there’s a little bit of possibly both of that, right? One point three successful attacks each week per company, and then--back in 2012, and then 1.7 now, in increase. Or I shouldn’t say now. In 2014.

So generally speaking, getting owned, getting hacked, may be a foregone conclusion. It’s not guaranteed, obviously. But in many cases it’s happening. Just a matter of when you either recognize it or when they finish and they leave.
Purpose of Digital Forensics

To answer some basic questions
- Who perpetrated the act? Is there attribution?
- What did they gain from the attack? What did we lose?
- Where did it happen? On a server or a host?
- When did the exploit occur? Over what timespan?
- How did they execute the exploit?

To get the facts, not necessarily guilt or innocence

**008 Okay. So the true purpose of digital forensics is to get answers to questions, right? So this is the who, what, where, when, how part of things? Right. Who actually did the perpetration? I should say who perpetrated the act? Is there attribution?

This piece is very difficult, as you've probably seen in the news. Sometimes they leave very little traces and you have to guess as to who might've done these things. If it's industrial espionage, maybe it's one of your competitors, right. If it's governmental, maybe it's a nation/state. Sometime the
attribution is obvious. They throw it in your face, right? They deface your Facebook page or your Twitter account or whatever it is, and some hacktivists, you know, announce it to the world that, "We took care of these folks," or, "We took care of this organization." So that piece can be answered sometimes. But most times, especially through forensics, it’s quite difficult. You end up with a user account that got used to attack you or an IP address that it came from or a domain that it came from. So that part can be a little bit difficult to actually attribute.

So what did they gain from the attack? That’s a key piece, right? That’s what you really need to know. What did they take? What were they looking for, right? And when you find that out, when you figure that portion of it out, you figure out, "What did we lose?" Was it PII, personally identifiable information for our people? Are we talking about credit card numbers? Are we talking about social security numbers? It could be intellectual property, right? So it could be a pretty big thing.

Where did it happen? These, these are part of the forensics piece that you’ll be dealing with and that you’ll be able to see, depending on where your indications come from. Sometimes they come internally from your alerts. Sometimes the FBI knocks on your door or somebody else calls you up and says, "We happened to have found some of your data, or some of your
information, on our servers," or et cetera. So that portion of it can happen as well. You know, did it happen on a server, on a host? That's the kind of things that you'll be looking for when you're doing the actual digital forensics piece of it.

And then when did the exploit occur? Right? And over what time span? This is something that also, as soon as you find out what's going on, and depending on where in the process, it's quite rare to start, or be able to see things happening at the very beginning of an attack. Most times you find out that you've already been hacked or data was leaving that you discovered through your, if you have a data loss prevention program, or some other way, you'll find out what happened kind of at the end. The information's already gone. And so your timeline starts with now we found out, how long have they been here? How long have they been doing what they've been doing?

And then how did they execute the exploit? That part's also a chain. Usually starting backwards as well. You'll find out that something happened and you go from there. How did they get here? Do they go laterally inside our networks? How did they get in initially? Did they get somebody to click on a phishing e-mail? Did they do a drive-by website where people went to a website thinking it was fine and they downloaded something and they ran it?
So those are the kind of questions that you're answering with digital forensics. So that last line is pretty key. When you hear the term forensics, what do you think? Can I have somebody just to--what sort of things do you think of when you hear forensics?

Student: Evidence.

Student: Deep investigation.

Instructor: Okay.

Student: Evidence.

Instructor: Okay.

Student: After the fact.

Instructor: After the fact. Okay. So a lot of times, as I understand it, and maybe forensics in the traditional sense, right, is a crime scene. And so the idea of guilt and innocence, like, really finding the bad guy, is there. But actually for digital forensics, lot of times it'd be very difficult to actually get to the guilt portion of it. You'll be able to say what happened and from there the analysts, perhaps, and the investigators, perhaps, can get to a whether or not this person did something wrong, actually did something wrong. But you got to get the pieces first. So that's what the digital forensics piece is actually about is to get the answers to those questions.
Notices

© 2016 Carnegie Mellon University

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 was created in the performance of Federal Government Contract Number 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.

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 owned by Carnegie Mellon University.