Digital Forensics Guidelines, Policies, and Procedures

Table of Contents

Guidelines, Policies, and Procedures ................................................................. 2
Importance of Policies and Procedures ............................................................. 4
Guidelines, Policies, and Procedures -1 ............................................................. 7
Guidelines, Policies, and Procedures -2 ............................................................. 9
Notices .............................................................................................................. 11
**018 Switch it up a little bit here. Talk about some guidelines, policies and procedures. So before delving into this too deeply, as I mentioned, keep in mind as we go forward the whole thing about answering the questions. Digital forensics should be question or impact or effect based, meaning you’re looking for specific things, right. You’re not necessarily just grabbing a ton of stuff and then have to go weed through. You’re looking for a particular item or you’re looking for a particular path. Your initial time, yes. You’re pretty much gathering a lot of information. But
try to stay on track with answering specific questions throughout.

So just keep in the back of your mind as we go along that the idea behind this is still, right, taking care of it in such a way that it’s going to be good for evidence or if it's not necessarily for evidence, it may be to possibly fire somebody. So as we go through this, keep in mind that if you have the questions, go to a general council. Try to get the information there. Ask for help. This isn’t supposed to be done in a vacuum. Yeah, you're by yourself and you're pulling data off the drives and such. But in the way you handle things, remember to reach out and use your resources as you go through this process.

So part of that, of course, is if you have guidelines, policies and procedures--
Importance of Policies and Procedures

Due to legal circumstances, direct and precise policies are necessary when developing a digital forensics capability.

Policy must be enforced in order for investigations to hold up in court, when concerning criminal activity.

Without proper policy and procedures, your organization runs the risk of expending a large amount of effort to no avail.

Even if criminal activity is not a concern, federal regulations often dictate that certain sectors follow a particular set of guidelines.

**019 These are extremely important to maintaining the integrity of the process and your information, right.

It says due to legal circumstances, but it could be for other reasons, right. Yeah.

Your organization should put together very concise, very accurate, very well-written policies and guidelines for digital forensics. This is in order to keep that integrity alive. It should be a cultural thing within your organization. When you do digital forensics, it should be with the end in mind. In this case, making
sure you’re, to use a term, chain of custody is good. Right. We haven’t gotten quite there yet, but we’re talking about the entire process. And it starts with these, right. The policies and procedures are what’s going to help you. If you don’t quite know, it should be in your policies and your procedures, your checklist should help you do these correctly. You should not mess up an investigation. You should not mess up some sort of collection because you had fuzzy instructions, right.

So this is very, very important that your organization puts together. And I realize most of you will probably be the ones putting them together, actually, because you’ll be the ones probably on the ground, if not specifically the ones that handle the keyboard. Maybe middle management level folks who are setting these policies and these procedures up, so..But just remember that the key is having solid policies and having solid procedures and checklists to go through this.

And along with having the policy, it has to be enforced. Right? You have to make sure. And I think of, since I was in the military, I think of classified information as being a huge thing, right. We had policies, and if you broke them, you could lose your security clearance, right. And that's a big deal. So not quite the same in the civilian sector, I don't think. But you don’t want to sit there and do all this effort, all this work, and then just because one of your procedures was
slightly off and it wasn't actually the correct way of doing things that'll be good for evidentiary proof, if you will, you don't want that to be the reason that you spent all these man hours and all this money to do this investigation and then it just goes for naught because the policy or the--or maybe not the policy. I shouldn't say that--the procedures and the checklists aren't done right.

So going forward, remember that this is the starting point, the baseline of what it is, right? You're going to talk about what you need to do, why you need it, right, and then you're going to go into even more details with your checklists and your procedures. So just keep that in the back of your mind going forward. When you set up a team, make sure you have solid policies, guidelines and procedures. Okay.

Okay. Any questions?
Guidelines, Policies, and Procedures - 1

Guidelines, Policies, and Procedures - 1

Guidelines for tool use should be one of the main components of building a digital forensics capability.

The NIST Guide to Integrating Forensic Techniques into Incident Response provides solid reasoning for tool use guidelines.

“Although the technologies have many benefits, they can also be misused accidentally or intentionally to provide unauthorized access to information, or to alter or destroy information, including evidence of an incident.”

Guidelines on tool use should specify personnel’s authority for specific tools.

• Network admins, help desk personnel, and forensics technicians should not have access to the same level of monitoring tools.

**020 Alrighty. So the guidelines for tool use should be very well written as well. I’m trying to talk about the analogy, okay? So the level of use for the tools should be commensurate to the level of the person doing the work. So this is already the case in regular network, right? You have your basic user, you have kind of maybe a power user or somebody that has more power within their little area. You have your local admins and then you have your domain admins. Not everybody should have the ability to use all the tools that you’re talking about. These tools are very powerful. They’re able to do many, many
things, right, and get access to information that's normally not accessible through the regular user interface.

So just as it says here, right, there's a lot of benefits, but they can also be misused accidentally or intentionally to provide unauthorized access to information or to alter or destroy information, right, in getting evidence. Or, I'm sorry, including evidence of an incident. So you want the right people to do the right things and to have access to the right level of tools. So not everybody should have access to the things that can do all these things, right. So think about those things. Also when you're working on your policies and your procedures, you should have levels commensurate to what it is they need to take care of as they do their duties for digital forensics.

Okay. And just like this says, network admins, help desks personnel and forensics technicians should not have access to the same level of monitoring tools, or any other tools, for that matter. So also take that back with you as part of the policies and procedures.
In order for forensic investigation results to be legitimate the evidence must be reliable and not prejudicial.

All stages of a digital forensic investigation must be at the forefront of the technician’s analysis.

“Information is rapidly migrating to a form in which all the information assets exist in electronic form. In both the public and private sectors, it is increasingly important to demonstrate conclusively the authenticity, credibility, and reliability of electronic records, such as the performance of a specific action or decision, or the existence of a certain item of information.”

– NIST Guide to Integrating Forensic Techniques into Incident Response

**021 Okay. So this information that they're gathering, right, has to be able to go all the way. Maybe not necessarily to court, but if you're going to use it to fire somebody, it has to be done correctly. So during all stages of the forensic piece, the technicians should have in the forefront thinking about making sure that they take care of this stuff in a way that it’s going to be admissible in court if at all possible. So that would be pretty much the highest level that it needs to be taken care of. So why not shoot for that, unless it’s for some reason monetarily or timewise would take so much effort that it’s not worth that? But for the most
part, this is just handling things in the proper way. So if that’s the case, in the policies and procedures, all of the analysts that are involved have to understand and be trained up to probably, if at all possible, the maximum level.

Right. So...And NIST has a nice little definition that everything is switching to electronic form, right. Both in public and the private sectors. And it’s increasingly important to demonstrate conclusively the authenticity, the credibility and the reliability of electronic records. So again, this is dealing with integrity of the materials that are being handled.
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, an 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.