IR and Digital Forensics Tools

Table of Contents

Tools 2

The Right Tools for the Job 3

Common Software 7

Common Hardware 11

Notices 16

Tools

**007 So here are some of the tools that are used during the incident response, and in particular the digital forensics piece.

The Right Tools for the Job

The Right Tools for the Job

Knowing the system to be collected is important in the response planning phase.

- Is it Windows, Linux, or Mac?
- Is it a server? If so, can it be removed from the network?
- Do you have physical access or is it a remote collection?

Physical characteristics of the system often dictate collection tools.

- How much RAM does the system have?
- How large are the hard drives? How many are there?
- Are there peripheral devices attached to the system?

CERT | Software Engineering Institute | Carnegie Mellon University 8

**008 In general, you want to get the tool that can get you the best effects for the least amount of work or cost to you, right? So that's the right tool for the job. And part of this, beforehand anyway, you need to-- during your planning, you need to make sure that you have an understanding of is it Windows, is it Linux, is it Mac? Now more and more Macs are showing up in the workplace. Why is that important? Why do you need to know what machines are out there?

Student: Because the machine will determine what tools you're going to use. Not everything that works on a

Mac is not necessarily going to work on Windows, and you have to know what tools you're going to use based on the system that you're going to be collecting from.

Instructor: That's correct.

Student: Also file structures and understanding how the operating system works, and where files are collected.

Instructor: Right, that's also true. For those of you that didn't hear that, he mentioned the file systems, right? Linux has the EXT4 or 3 depending on the thing. You have NTFS for Windows. So this is just the way data is stored in each of the sectors on a hard drive. So if the pattern is this piece first, this piece second, this piece third in a Mac, let's say, it may be in a different order. So you would not be able to read that information if you were to try to open it in, say, an NTFS file structure.

So you definitely want to understand-- have a good understanding of what kind of devices you're talking about, and the different tools don't tend to cross over into other operating systems, unfortunately. Some of them have been ported to another, but you can't use the same-- I'll bring up DD here in a second, but DD is something that was created for the Linux file system to create an image of a hard drive, but there is now a Windows DD, but it's been ported. You can't just take one and bring it

onto Windows and run it as if it's natively run on Windows.

Some of the thoughts with if it is a server. Can it be removed from the network? Do you have physical access or remote access to collection? Right? Each one of those, sometimes-- or I should say most times-- with the remote collection piece you're looking at different piece of software than when you have physical access and you're doing a local pulling. If you're doing smaller data sets, some of the tools that are open source and are free are fine, but I had mentioned before they don't necessarily scale well. They aren't designed to go and get data from 10 thousand machines. So when you're doing remote collection of hundreds, thousands of machines, you're going to be looking at a different toolset for that as well.

Physical characteristics of the system. Sometimes that dictates what kind of tools you're going to be using. How much RAM does that particular device have? How large are their hard drives and how many are there? If you're talking about-- if you're familiar with RAIDing-- that is the Redundant Array of Independent Disks-- is anybody, everybody familiar with RAID, RAIDing? Pretty familiar? Right?

There's multiple ways to use RAID. So Level 0 or RAID 0 is a straight mirroring, so you basically get redundancy. RAID 1 is when you do striping, is there is where you take

some information and you put it in one drive and you take another swath, if you will, of information and you put it on another drive. So you have two different drives with one disk's worth of information. This is strictly for performance. So you can go get information here and here at the same time essentially and two different drives are doing the work for you. So if you have two different processes-- say different threads, multithreaded things that are doing two separate things-- you're going to get better performance.

Now, there's obviously an issue with that. If you go and you do a forensic image of one of the disks and you go and get the other one, there's going to be-- you have to understand how those stripes work, where they start, where they end, and how they're separated and what takes care-- or who keeps track of, if you will-- I don't want to say who-- what keeps track of what's placed where. So there's some instances where that implementation of the hard drives and how many there are will affect how you deal with your forensics.

And then are there peripheral devices attached to the system? Right? We could be talking printer-- I don't know, is there such a thing as a real fax anymore, or a real modem? But I mean, there are some systems actually that do have modems because some remote sites, maybe the military, that have relatively old devices that need communication and they still use modems at times. So

those kind of characteristics. And if you're pulling-- if you're talking about a storage area network and then also the NAS, the Network Attached Storage, some of those have different connectors, right? One's connected using a CAT5 cable or a CAT6 cable the other ones may be the other USB or FireWire or any of those other ones.

Common Software

Common Software

Forensic imaging software

- FTK Imager
- EnCase Imager
- DD

Hashing utilities for integrity verification

- FTK Imager
- md5deep/sha1deep (other variants available)

Incident Response/Forensic Software for collection and analysis

- Guidance Software's EnCase
- AccessData's FTK (Forensic ToolKit)
- Autopsy/The SleuthKit
- SIFT (SANS Investigative Forensics Toolkit)
- Less obvious built-in software

CERT | Software Engineering Institute | Carnegie Mellon University 9

**009 None of these are-- here's my public service message-- we do not advocate, or we are vendor-agnostic- but here are some of the more common tools used for digital forensics and for incident response.

FTK Imager actually is a free imager. The FTK is the Forensics Tool Kit, and that's actually created by AccessData, is the company, and the FTK-- and actual FTK itself is a much larger software package that does much more, but is not the free piece.

EnCase Imager also helps you do that. EnCase, however, as I understand it, does cost for that imager, and DD is also an imaging piece of software that was originally put together in the Linux operating system.

For hashing utilities, for integrity verification, FTK Imager actually has that built in. There's an actual little icon button that says Verify-- Verify Integrity or Verify Image?-- and it actually does take an MD5 and I do believe a SHA-1 hash of the particular device or image that you connect to it.

And there it says variants available, because SHA-256 is now becoming a little bit more used. Again, the fact that the key would be 256 bits versus some of these use the shorter keys, with as much combinations as can be created. Because hashing can be done not only for a single file, right? It can actually be done for a partition or an entire hard drive and they can take all that data and run it through the hash algorithm and get that 140-bit or however many bit hash message digest, the output of your hash. So as you can imagine, with terabyte drives, multi-terabyte drives, now the results of that many ones and zeros, there could be so many

different combinations that that key size had to get bigger to prevent the collisions that could come about because of how many different options there are-- right?-- permutations of it.

Did that make sense? Did I lose anybody on that? Okay, I just wanted to make sure. So that's kind of the reason that we mention the other variants. They're tending to go up in size now to try to minimize that collision issue.

So the incident response forensics software. So Guidant's software, EnCase, is another entire package. These are like the big enterprise level, or if you do the actual work-- your company actually does investigations, so you have case management-- you have so many cases that just one set of things or even just a couple of copies of things isn't enough. EnCase is the thing that's used when there's quite a few cases to work with. The FTK, as I mentioned, is a pay-for forensic toolkit. Autopsy and the Sleuth toolkit. SIFT is actually just an acronym for the SANS Investigative Forensics Toolkit, and this is one of those that's put together-- kind of best in breed, the item that I mentioned-- or not the item, but the packages or toolkits that I mentioned for-- what they do is they take the best in breed of the time that they're developing it and they put it into a toolkit. So if you're doing data carving, "Here's the best free thing we have right now," or "open source

free thing we have right now." And if you're doing imaging, if you're doing this sort of thing, and they put it into a toolkit, it's not necessarily all-encompassing-- sometimes there's pieces that could be better or there's gaps, where like the EnCase or the FTK tends to be a more comprehensive and robust package that you can get, but you're also paying for it, because it's a good chunk of money. We're talking tens of thousands, if not, I think-- depending on the size of the enterprise or whatever-- you could be in the hundreds of thousands for EnCase. Has anybody used or have used EnCase?

Student: We use EnCase.

Instructor: What pieces?

Student: We use EnCase Forensics and we have an EnCase Command Center for e-discovery jobs, for legal holds.

Instructor: And then I also put in here less obvious built-in software, right? Again, the collection of information, a lot of these things make things very easy to collect them and to place them into files and such, but actually there's stuff built right onto the net series of commands, right? Netuser-- right? Netuse to see what connections you have. Net session-- what sessions are connected to your Windows machine, right? Net stat both in Windows and Linux. Net stat will tell you which connections-- what you have listening, what you have

connected, and what just recently disconnected. So you can just type in netstat -an and it'll show you those connections. It's not fancy. It's built in, so it's real easy and it's stuff that many administrators use anyway on a daily basis. So those are the tools that can be repurposed in incident response and digital forensics pieces. If you need those questions asked, sometimes you don't have to worry about, "Hey, where's that in the EnCase package?" You don't have to go look for it if you know how to get that. Use the most expedient way possible.

Common Hardware

Common Hardware

Physical write blockers to collect images from digital media

- SATA/IDE
- USB
- Firewire

Cables of different technologies and lengths

- Power
- Networking
- Peripheral (USB, IEEE1394, etc.)

Digital media for storage of collected evidence and information

Live boot CD/DVDs

CERT | Software Engineering Institute | Carnegie Mellon University 10

**010 So some common hardware.

They have what they call write blockers. Anybody have a guess as to what a write blocker is?

Student: The little things on the slides on the actual disk that can block from writing?

Instructor: Well, okay, that is a way to write-block a disk. That is correct. This is more for the forensic piece of it. Anybody? You probably have a pretty good guess, I'm guessing.

Student: It's like hardware where allow only to read from that hard disk but there is no write allowed to that hard disk. So you will keep your evidence out of change, so no one can--

Instructor: Change or cause damage, right? Right. Yep, absolutely. That's correct. These are devices that you put them in line between whatever you're copying them to and the actual piece of evidence. You put a piece, this write blocker in, and the cables go through but the write blocker is designed to stop any command that has to do with writing and/or changing anything to do with the hard drive. So all you can do is actually access for reading only. So it just physically pretty much prevents it from happening.

There's two different implementations, from what I understand. There's one where there's a list, so it allows anything except the stuff on the list. So you

want to put obviously all the right stuff in the list, but if there's a reason to change that at all, you can actually change the list. And then there's other ones that absolutely do not do anything to do with writing and they only allow the reading. So there's one that's slightly more adjustable if you need that kind of flexibility.

So they do have the serial ATA, which is the more common connection for hard drives now. The older ones used to be IDE, and the USBs now, they're starting to get to, what is that, USB 3, 3.1? And USBC, which is supposed to be the common one that-- you can flip it over either way and you can plug it in, so it's not as annoying when you're trying to figure out which way your USB key is trying to go in.

FireWire isn't as common anymore. It used to be-- I believe Sony-- but it used to be a much more common connector, and so they had write blockers built for it.

I did a little research, actually, to see if there were any Thunderbolt connector write blockers on the market, and I did not see any. Has anybody seen anything dealing with Thunderbolt? You would think-- it's been around for a little while now-- that they would have that, but currently they don't. Maybe they're just able to get through it using USB. I'm not positive. It doesn't have to be the super-fast acquiring.

So other hardware that you'll need, of course, are the cables, right? Everybody loves it when you pick the wrong USB cable out of your cable packet and it's get the wrong end. It's not the mini, or it is the mini. So you need to be looking at the different kinds of power cords. They do have that generic power supply cord that you can use. The networking cables. Sometimes places-- and it's not very common-- but if you're looking at fiber optic cable, then you need to have the ability to user fiber optic cable in addition to your CAT5 or CAT6 that you would like to use. Right? And then they have the peripheral cables that we just talked about for like printers and such. The USB for a printer is different than the regular USB that you have for, say, charging your phone, etcetera.

IEEE 1394-- just a trivia question-- what is that? Anybody?

Student: Is it FireWire?

Instructor: It is actually FireWire. That's correct. Yeah. I'm not sure why they put it like that. They should have put-- I would think-- they should have put FireWire in there because it'd be a little easier to understand. But for any peripherals that you need, that should be something that you have in a kit and that is good, right? Because we've all probably had the situation where you pulled your CAT5 cable that you don't know how old it is and you plug it in and for some reason you still have no

connectivity. So those items should be tested on a somewhat semi-regular basis, right?

And the digital media for storage. That's something that you got to have, and you got to have plenty of it, because you are talking about terabytes of data on up.

And then having a live boot CD or DVD. This is where the software will run directly out of the CDROM device and then you can-- the operating system itself will sit-- and maybe you've seen it already-- in some Linux distribution as they come on CDs, and you can just run them right from there, and then they treat the hardware-- in this case, like the hard drive-- as just another hard drive that's just sitting there. So it can go view it without actually cranking up the operating system that you would need on the hard drive. You can run it.

And they also have live USB, if you've not heard of that before, where you can do the same thing, where you can put on a copy of-- some of the other tools that I had mentioned come on a USB drive and you can actually just plug them in and they'll run right off the USB drive, and that way you're not tainting or-- I don't want to say tainting-- but you're minimizing the effect that you might have by having to load that tool onto the actual hard drive just to go grab it off of-- if you're only grabbing some folders or just some files themselves, you don't have to worry

about taking the entire disk. You can actually load software on that disk if you would like. But in order to minimize the contact and the possibility of changing that evidence, you would want either a live CD or perhaps a live USB drive to do that collection or the analysis.

Notices

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.

CERT | Software Engineering Institute | Carnegie Mellon University