# Storage Media Collection

## Table of Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forensic Imaging</td>
<td>2</td>
</tr>
<tr>
<td>Physical vs Logical Imaging</td>
<td>3</td>
</tr>
<tr>
<td>Encrypted Data</td>
<td>4</td>
</tr>
<tr>
<td>Types of Physical Devices</td>
<td>7</td>
</tr>
<tr>
<td>Hard Drives and Removable Media</td>
<td>10</td>
</tr>
<tr>
<td>How a Write-Blocker Works</td>
<td>11</td>
</tr>
<tr>
<td>Special Imaging Considerations</td>
<td>12</td>
</tr>
<tr>
<td>Notices</td>
<td>14</td>
</tr>
</tbody>
</table>
Forensic Imaging

A forensic image records a given dataset in its entirety.
• This allows examiners to work on an exact replica of the data instead of the original data or evidence.

Forensic images can be collected from many different types of data.
• Individual files
• Folders or Directories
• Volumes/Partitions
• Hard drives

Data must be collected in a forensically sound manner to prevent contamination or modification of the evidence.

**015 Okay, forensic imaging. Right? It records a given data set in its entirety. Allows the examiner to see exact replica of the data, instead of the original data, or yeah, it’s the forensic image of it, so it’s not the original. So you’re not going to mess anything up on the original as part of the evidence. Right.

And then you can go anywhere from individual files, folders or entire directories to volumes and partitions to the entire drive itself, right? We had talked about what level you can actually access the information at. So this allows you to do it pretty much at all levels.
And you’re shooting for forensically sound images, as always, so if you need to present it, as evidence, you’re able to do so.

Physical vs Logical Imaging

Physical vs Logical Imaging

There is a significant difference between physical and logical images.

A physical image collects all bits of data on the storage medium, regardless of whether it is allocated or unallocated to a file system.

A logical image collects only the data that is visible to the file system.

**016 There's a physical versus a logical imaging. The logical image is what the operating system knows to exist, and what it accesses. And then the physical is the actual every single byte that's capable of being written on on that drive.

Very important. It seems like a simple distinction, but if you go and grab one instead of the other, when you really meant to get the other, it could be different for you.
Well, certainly if you meant to get the bit by bit of the entire drive, and you just go get the logical, then you're going to be missing the unallocated space, the slack space, and possibly some of the paging information from RAM. So make sure you know which one you want.

There are times where you want just the logical and that’s fine, but just know the difference and make sure you get the pieces you want.

**Encrypted Data**

**Encrypted Data**

Must be decrypted before being accessed by the system or users

Types that could be collected this way
  - Individual files
  - Encrypted volumes
  - Full-disk encryption

If the temporarily decrypted data is not collected during the response, there may be no way to access the information later.

If an encrypted volume is mounted and active, collect a logical image of the volume.
system has that built in to where once you boot it up and you logon successfully, it starts to decrypt the information there.

And some things, although I understand not be very common, it actually decrypts as it goes. So I don't know how efficient that is, or how slow that is. I've not personally seen.

Has anybody seen anything that does the encrypting/decrypting kind of on the fly, versus all of it at once, and then as you shut down, have you seen?

Student: I think McAfee's drive encryption does it just as far as whatever data's added, it'll encrypt it as it's added to it. So yeah.

Instructor: Oh, oaky.

Student: So yeah. It used to be full disk when it was Version 6. I think Version 7 is when it went to--

Instructor: Just whatever piece--

Student: Whatever data's being used.

Instructor: Oh, okay. Very good. I guess that is good from a forensic standpoint, so you're not messing with it every time you turn it on, or every time you--

Student: Well, it was good from a speed standpoint as well, because it would take hours to decrypt the-- or to encrypt the entire drive, or decrypt it.
Instructor: Or decrypt it. So if you have--

Student: So users--

Instructor: Shut it down.

Student: Yeah.

Instructor: Ah, that definitely would make a difference, for sure. All right.

So you can have encrypted volumes in addition to the full disk encryption. If you've ever used TrueCrypt or VeraCrypt, you can make yourself a small just an encrypted file that you can use and like throw all your personal information on it, and encrypt it and decrypt it as you need it. I recommend it.

. It’s V-E-R-A-Crypt is the name of it. And you can create individual small, you know, whether you make it one gig or 500 meg depending on if you only need documents and such. You can make it smaller and larger. And you can access it as you need it. So, it's a very nice way to kind of protect your stuff.

And if you make it a nice long password, it's my understanding, having talked to some folks that do the other side of the decryption piece of it, that it's a very solid encryption. Would take a very, very long time to break it. That hopefully, being our personal information, it would be kind of moot at that point.
Okay, temporary decrypted data. If it's not collected during the response, there may be no way to access the information later, so this is one of those times where, yes, volatile data is important, but if you know you're going to lose access to something that is currently decrypted, but for whatever reason whoever owns it, whoever's using it said, "I'm shutting down and I'm leaving in an hour," or whatever it is, go ahead and grab this stuff as best you can, if you know you're going to need it.

Types of Physical Devices

There are many types of physical devices that can contain evidence of a security incident or intrusion.

Internal Hard drives
- Solid State Drives (SSD)
- Hard Disk Drives (HDD)
- SCSI drives

Removable Storage
- Flash drives
- USB hard drives
- Memory cards

Mobile Devices
- Smart phones
- Tablets
- Audio players

*018 The types of physical devices. Right? That can show up. You got your
solid state drives, you've got your hard drives, and the SCSI drives are actually pretty much hard drives anyway. They're just able to be attached and connected, daisy-chained, as it's called, in multiple ways.

The hard drives, generally, with the serial ATA has one per strand, or one per cable. IDE drives used to-- they're not very common anymore-- used to be able to really put two of them on one cable, ribbon cable. But sometimes you'll deal with SCSI drives that have multiple. I forget what the maximum. Is it like in a dozen? I mean, in the teens?

Student: Thirty-six.

Instructor: Oh, is it more than that now?

Student: It was up there. It's like thirty-something.

Instructor: Okay, okay. So you could conceivably chain, you know, daisy-chain, up to thirty-something drives. So that's a consideration when you're dealing with-- dealing-- pulling information off of SCSI drives.

Removable storage, right, the flash drives, the thumb drives, USB hard drives, and then now, of course the memory cards that you can put in your cameras, the mini-ones that you put in your phone. Those are all removable storage that you may have to deal with, and may have to make forensic copies of.
So those are the type of things that if you don't deal with them on an everyday basis, right, it's one thing to stick a drive in a USB port and pull it off of a hard drive. But if you're not familiar with how to pull it off of a SD card, or some other formatted card, that's the sort of thing that people should be looking into ahead of time, and practicing and training on.

And many, many people now have smartphones. Lots of people have tablets. And I'm guessing, lots of people have audio players that store information in flash memory as well.

So those mobile devices, you may be dealing with in a collection.
The primary collection method for hard drives and removable media is through forensic imaging.

A full physical image nets more information than just a logical image (slack and unallocated space).

Imaging a hard drive is usually done with the use of a write-blocker, which prevents modification of the data on the device.

**019 Okay, when dealing with hard drives and removable media, I’ve kind of alluded to this earlier, that’s actually a write blocker. Picture of one from Digital Intelligence there.

You want to do forensic imaging, so you pull a complete copy of it off of there, and that’s the one that you can work on, and that way you don’t mess up the original. Right? And you’re also pulling what they call slack space, an unallocated space.

And then we do want to use the write blocker when you’re doing that imaging, so you do not accidentally write, or add anything to that hard drive.
How a Write-Blocker Works

Read signals are relayed through the write-block to the collection system.

Write signals are stopped at the write-blocker before they reach the evidence.

Write-blockers should be periodically tested to ensure proper functionality and retired if found to be defective.

**020 And as I said, you put it in line, your cables connect from the responder's computer. And connect to whatever evidence piece you're trying to get access to, or in this case, it should be a drive that you're trying to make a copy of; but it could be other things.

And that thing, you know, physically, does not allow write commands to go through, or it has a list that it refers to, and it says, "Am I allowed to use this particular command?" And if you are trying to use it as a write blocker, you, of course, would remove any write commands on that list.
And that's important, this bottom paragraph here. Write blockers should be tested periodically. You don't want to assume that's always functioning properly. And then you end up messing up some of your evidence.

So that's another thing that could be checked on a regular basis, as part of a checklist of things to maintain when you're talking about your incident response package.

Special Imaging Considerations

Special Imaging Considerations

Storage devices that use flash memory add a unique factor to the imaging process.

- Solid State Drives
- USB Flash drives
- Mobile phones

Flash memory uses wear leveling, which moves data to other parts of the drive.

The hash value of the drive will likely change during subsequent imaging.

**021 So this is where the SSD items that I was looking for, actually come up. You have multiple different storage
devices that use flash memory, right? Solid state drives, USB flash drives and mobile phones use flash memory.

It's called wear leveling. I think I call it use leveling. But the wear leveling, the flash memory is such that you get a finite number of usages. And therefore, you know, the system knows to go and try to use all of them, and maintain the wear level as much as possible, so you use up the good ones all the way till the very end, so you get the longest amount of durability in that product.

So hash value of the drive can change depending on what you do with it, as Sean mentioned. If you just leave it alone, it is not going to change from when you grabbed it.

If you power it up and do anything on it, and then you go and try to make a forensic copy of a file that's on it, and then you take another hash of it, now that you've turned it on, and you've done some other stuff, an operating system may have interacted with it, now other bits have been tampered with, but changed-- and so your hash will be different.

So you have to be cognizant of that as you work with devices that have flash mem-- yeah, flash memory.