Digital forensics is the art, the science of collecting, storing, and quantifying digital evidence to be used as the result of some action that takes place. Now in our world, most forensics are going to take place from one of two reasons.

Number one there's going to be some incident that takes place in-house.
Somebody has broken an important policy and we need to be able to document that they've done this and we have to go through a process of forensics.

The other place this can happen is from a legal hold. Legal holds are documents that are sent to an organization from another organization to let them know that they are going to be doing some exploratory information and that we have to provide that information for them in such a way that they can do whatever legal discovery they need to do to take care of that.

Now before I get into a lot of detail here, for the exam digital forensics is pretty basic and the whole concept of digital forensics is huge. You can get a doctorate in digital forensics these days.
But as far as the exam is concerned if you really think in terms of one computer where one person has done something naughty you'll usually be in better shape.

So probably the first thing I want to talk about is the idea of chain of custody.
The whole idea behind chain of custody is the fact that you or someone underneath your purview is going to be gathering evidence against somebody or something and that somebody or something has a chance of losing their job or losing money or losing freedom or even losing honor or whatever it might be. If we are going to be presenting evidence we have to show that the data that we've collected is of high integrity. We don't want somebody going: Oh well he changed that name, or Oh that didn't come from here, or no that was gathered days later. So the whole idea of chain of custody is to show good integrity of the evidence itself.

So the best way to do this is let's march through the chain of custody process.
The cornerstone of chain of custody is a chain of custody form. And here's an example form that I got from the NIST to give you an idea of how this looks. Basically we're looking for very specific types of information.

- Number one we define the evidence. What are we actually collecting here, and what does it look like. Well how does it form? That could be an image of a hard drive. It could be an image from a thumb drive. It could be a video. Whatever it might be, but we define it.
- Number two we document the collection method. One of the big things that we have to worry about is that people will challenge us that we may have changed data. So there's a number of collection methods that allow us to grab data from mass storage without affecting it.
- Number three. Date and time collected. It can be very important that we determine exactly when this particular evidence was collected.
- Number four the people handling the evidence. We need to know the names that includes contact information email that type of information. Exactly telling who's handled the evidence and we're not just talking about the people who collected it. Anybody down the chain as well.
- Number five the function of the person handling the evidence. That actually means is this person an in-house I.T. person whatever it might be. In particular we do this to show that these people are qualified to do whatever part of the chain of custody they're involved in.
- And last is locations of the evidence. Evidence will move over time from the initial collection to being stored in a storage room to potentially be moved to law enforcement. We need to be able to document all of those steps.

When you approach a computer to begin gathering data, one big concern is the order of volatility. A computer has got all kinds of ones and zeroes start all over it. And our job is to try to grab as much of this data as we can. So the order volatility is basically a checklist that says what do you go to first, then what do you go to, and then what you do after that.

- So number one is going to be memory. Now when we're talking about memory certainly all the processes and services that are running on the computer are important, but there's a lot of other stuff in there too as well. For example caches. Even CPU caches can be absolutely critical. We could have routing tables which can change back and forth on a system. You could have an arp table. Wouldn't it be great to know the MAC addresses of everybody that that particular system has been talking to at just this very given moment. So dealing with memory is very very important.
    - Now luckily for us there are tons of great programs out there that are great at grabbing and dumping memory. Now they have very clever names like “dump it” or “volatility” and it's volatile volatility. OK funny joke. These are well-known programs and basically you just take a thumb drive you run the program they have a tiny tiny memory footprint and their job is just to grab everything in memory and dump it to a file.
- After memory is data on the disk itself. Now certainly when we talk about data on disk. And by the way this could be equally true for example optical media or flash drive whatever it might be. When a system is up and running there's a lot of data on that disk that will probably disappear when the system's shut down. For example things like cache files. You've got a big

swap file on there you might want to grab that data as well. There could be temp files that are very very important to whatever you're going to be doing with this. Now in this type of situation there literally hundreds of programs that are out there and designed to grab the data. All of these programs are designed to work in some form of what we call write block, something where you could say in a court of law it's impossible for me to write on the system because this piece of hardware for example will only grab data it's not capable of actually writing back to it. If you're looking for simple software even a program like Linux' wonderful dd program does a great job of doing a detailed grab of the entire image.

Now once we're done with the system you're not really done yet. The other thing you need to consider is remotely logged data. If something is going wrong here a lot of times there are two connections that are taking place. So if you're worried that someone's doing something on a website there might be logs on that remote web site. If you're worried that somebody is doing something on a file server there might be something on the file server in terms of when did they access it or something like that that can be very very important for you to grab. Logs tend to last a fairly good amount of time but it's important for you to grab it as quickly as possible.

The last part of order of volatility are backups. Backups are going to be terrible in telling you what happened right now, but they can be a wonderful tool for looking for trends. Oh this person has done this multiple times in the past. Ah, we've had this exact situation take place five times in the last year. However backups even though they have very low volatility it can often take a while to grab all of that data.

So be comfortable with the order of volatility.

All right.
I guess the last thing we need to do is actually take a look at the process of gathering this data.
So what I'm going to be doing here and this is not a particular order but basically a checklist of issues you should be thinking about when you're performing digital forensics.

- Number one capture the system image. You would be hard pressed to come up with a scenario where you're not grabbing the system image from whatever system is in question. What tool you use is up to you, but keep in mind write blocking tools are often very common for this type of situation.
- Number two grab network traffic and logs. Not only will the be some logs on the system itself but here's the opportunity to go over to the domain controller, to go over to what other servers that the system might be accessing and get an idea of where this person has been and what they're doing.
- Number three is capture video. Now that has two different meanings to me.
    - Number one if I'm in a forensic situation and I'm approaching the system I will videotape physically the workstation everything laying around it so that it's well-documented what I approached.
    - Secondly though capturing video can mean if you're finding media, and when I say video this could even include audio on a system, you would go ahead and want to capture all that too which would be normally part of the system image itself. Last you might want to look around for security cameras. Are there any other cameras that are part of a broader physical security system that might be appropriate to this particular situation?
    - Anytime you're dealing with video always record a time offset. Make sure people know what they're seeing and when it happened.
- Next take hashes. Take hashes of everything. Hash every file, hash every image, just keep on hashing. Most good forensics tools actually have built in auto hashing functions for you but the hash is your ultimate proof to show the integrity of any single piece of data that you've handled.
- Next take screenshots. When you walk up grab a screen capture, take a look at what's happening, and be sure to capture all these, and again be sure to record date and time.
- Next, interview witnesses. Anybody who's been nearby. Anybody who a communication was taking place. Get these interviews done quickly, get the documentation, contact information, and their job function within that organization so that, if necessary, law enforcement can speak to them.
- And the last one this is interesting is track the man hours. You are costing people money by doing these forensics. For example you might have budget issues in terms of how hard your organization is going to be defending a particular issue or you might have an insurance issue where your organization is going to be paid back for your hard work. The bottom line is every moment you're working, you're tracking those man hours.

The whole world of digital forensics is absolutely fascinating. I have spent decades working both in the public and private sector dealing with digital forensics. And I can tell you not only is it interesting it's also a very very good career.

So for the exam we're only doing the lightest of touches. You're not going to see much on there other than definitions of what is chain of custody, what is order of volatility, but if you really want to get into it I can't recommend it enough. It's actually a lot of fun.