Legal Standards Covering Forensics Tools

In this video we're going to start to transition away from the Civics Lessons about laws and our system of justice and talk about the legal standards that apply to forensics tools. There are two main items you'll learn about in this video, what forensics tools do, and the legal standards related to selecting and using a forensic tool.

The first thing to look at is what do forensics tools do in a general sense. You'll learn a ton about the exact steps for using these tools to do things like crack passwords or find hidden files later in the class, but for now you just need to know the general function.

So, forensics tools, like any computer tool, allow you a human to make sense of binary data. Remember that everything on a computer is stored in binary, which is easy for the computer and it's components to read or store or interpret, but binary is very difficult for humans to work with. You did this once in a previous video, but let's do it again because it really illustrates what the forensics tools do for you. Look at the following string of binary digits. Do you have any idea what this represents or means?

I know most of you aren't even going to try and figure this out. Heck, I don't recognize it and I'm the one who created it. But just in case you're curious I'll give you a a hint, it's ASCII text. You can pause the video if you want to try and figure it out, but don't knock yourself out because it's not important that you interpret it. The important thing you need to get out of this is that binary is ~~censored~~ very hard for humans to work with. You need to know what type of data is being stored, where the data starts and ends, which end to start reading from, etc.

```
010101110110100101101110011101000110010101110010001000000110100101110011
100100000011000110110111101101101011010010110111001100111
```

When this binary data is decoded it ends up being the following text:

> Winter is coming

There are more factors that make reading and understanding the data on a computer even more difficult including:

1. The data is being stored (at rest), in memory (in use) or being transferred between computers (in motion). The data may have extra meta-information added to it in each of these states. For example a hard drive has meta information at the start and end of each sector that is separate from the data being stored in that sector. Or data being sent across a network will be encapsulated in TCP/IP packets (or other protocols) which divide the data into chunks and add header and footer information to each chunk.
2. While all of the data is stored in binary, the actual encodings will be much different. There are different data formats such as ASCII for plain text, RGB or other image formats, 2's complement for integers, etc. Some formats are public domain like ASCII or JPG, while others such as Photoshop are proprietary.
3. In addition, different types of devices encode data differently. For example, some devices store the data in straight binary where a zero is a zero and 1 is a one. But other devices such as hard drives may use other encodings such as Run Length Encoding (RLE) where a 1 means the current bit is different than the previous bit and a 0 means the bit is the same as the last bit.
4. The data may not be stored in contiguous sectors. Storage devices such as hard drives use something called interleaving which skips physical sectors in the numbering and access scheme

> to reduce latency, while drives that use flash memory are constantly moving data between different cells in a process called load levelling. So if you get a set of bits from contiguous sectors on a device there's no guarantee that they will be from the same file.

What all of this means is that when you look at the bits on a device you'll need some way to determine which bits are actual data bits, which of those data bits you need to reconstruct each file, and how the bits are stored and encoded. You could do all of this by hand if you had a lot of time, a lot, and the requisite knowledge; but it would be technically difficult, maybe even impossible for most people, and even if you had the knowledge to decipher the bits is would be very time consuming.

Luckily someone has developed different tools to perform these tasks, and in some cases gathered large suites of tools into a program. These forensics tools make it possible for an investigator to make sense of the mountains of data that will be gathered in an investigation.

While the forensics tools make it possible to perform an investigation, there is no guarantee that the results you generate with the tools will be allowed in court. So let's finish our discussion about forensics and our justice system by taking a look at the legal standards that any forensics tool must meet.

The first thing to note is that forensics tools are relatively new. In the 1980s there wasn't a digital forensic tool. Investigators who were faced with making sense out of millions of bytes of 0's and 1's either repurposed tools originally designed for other tasks or wrote their own utility programs. For example they would use backup software to make copies of hard drives and then use data recovery tools to find deleted files. But while the repurposed tools may have helped investigators find evidence they also presented a problem anytime the evidence had to be presented in court.

Remember that the courts want expert witnesses to stick to presenting facts, and needed some way to decide how to define a fact. While the definition of a fact might seem obvious to us, creating a legal definition of a fact is a little trickier.

For example is something a fact if enough people believe it to be true? You can see how this could be a problem. I'm sure you can think of dozens of hoaxes or fake news stories that people have believed. Or facts like "Pluto is a planet" or "wait an hour after eating before swimming". Or how about if accepting something as a fact if someone is able to demonstrate it? This might be a little better, but I've been fooled by plenty of magicians who were able to demonstrate their magic with sleight of hand tricks.

> . It's get this name because it comes from case law, *Daubert v. Merrell Dow Pharmaceuticals*, (1993). We'll discuss the Daubert standard more in a later video.

The court's process for defining facts has been evolving and now most state courts use one of two systems for defining facts, the Frye Standard or the Daubert Standard. The Frye standard came first in 1923 and gets it's name because it comes from the case *Frye v. United States*, (1923). This case had to do with admissibility of polygraph, or lie detector, evidence. In the findings of this case the court wrote:

> Just when a scientific principle or discovery crosses the line between the experimental and demonstrable stages is difficult to define. Somewhere in this twilight zone the evidential force of the principle must be recognized, and while the courts will go a long way in admitting experimental testimony deduced from a well-recognized scientific principle or discovery, the thing

> from which the deduction is made must be *sufficiently established to have gained general acceptance* in the particular field in which it belongs. (Emphasis added.)

The definition of a fact in the Frye Standard basically gets back to popular opinion, but only checks the opinion of people working in a particular field. That is, it didn't ask if everyone in the US thought that the results of a polygraph test were infallible; the court was only interested in the opinion of people working with polygraphs. This means that if you want to introduce evidence in a court that uses the Frye Standard all you need to do is ensure that the programs or tools you use are generally accepted by the forensics community.

The Frye Standard is a little loose, so only a handful of states still use it (including Washington state.) In most states courts and in Federal court the Frye Standard has been superseded by the Daubert Standard. Remember from FRE if you go to court to testify you will considered an expert witness, which means that your testimony must be based on facts and that any tools you used must meet the Daubert Standard. The Daubert Standard was set in the case *Daubert v. Merrell Dow Pharmaceuticals*, (1993) and it increases the requirements for expert testimony. The court findings in Daubert state that the following non-exclusive requirements must be met:

1. Whether the expert's technique or theory can be or has been tested. (The court wanted to ensure that any technique or process would always return the same results given the same input.)
2. Whether the technique or theory has been subject to peer review and publication.
3. The known or potential rate of error of the technique or theory when applied. (For example science has shown the human DNA should be an excellent identifier of an individual. However, the lab processes for DNA matching have been shown to introduce errors and have generated many false positives.)
4. The existence and maintenance of standards and controls. (Are there any outside factors that may affect test outcomes? If so, what types of controls must be used to eliminate the influence of these factors.)
5. Whether the technique or theory has been generally accepted in the scientific community.

For more information on the Daubert standard see: https://www.law.cornell.edu/rules/fre/rule_702

There are two points you should take away from this. The first, is that you need to remember that the Daubert Standard sets the requirements for any expert testimony or tools used to analyze evidence. This applies to any tests for this class and every certification test I've ever taken. Even though some states, including Washington, still use the Frye Standard the Feds use the Daubert Standard so this has always been the correct answer on any test I've taken.

The second point, getting back to talking about forensics tools, is that the findings from the Daubert case made it much more difficult to use homegrown or repurposed tools for digital forensics analysis. However some enterprising individuals saw an opportunity and began developing tools that were specifically designed for forensics analysis such as Encase and AccessData's Forensic Tool Kit (FTK) These tools meet all of the Daubert requirements and their outcome has been accepted as evidence in many court cases.

It's important to note that there is **not** a list of approved programs or tools. There are programs that meet the Daubert Standard, but no court, at the Federal or state level, have ever created a list or approved tools. This is a semantics issue (and possibly a trick question on a test), yes there are tools you can use, but there is no list of these tools.