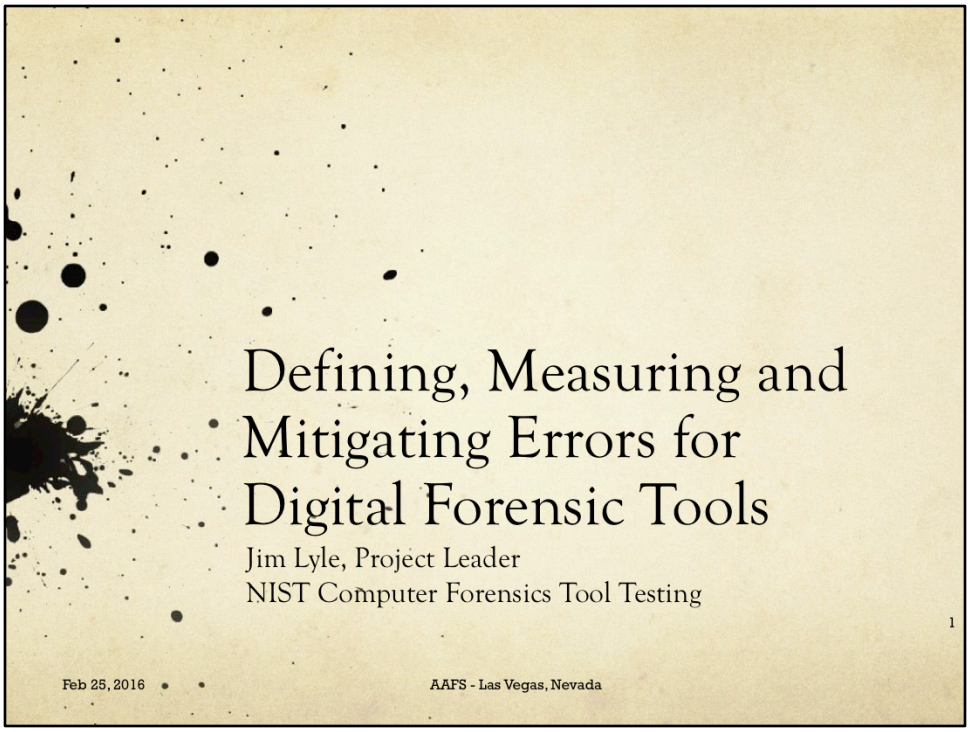
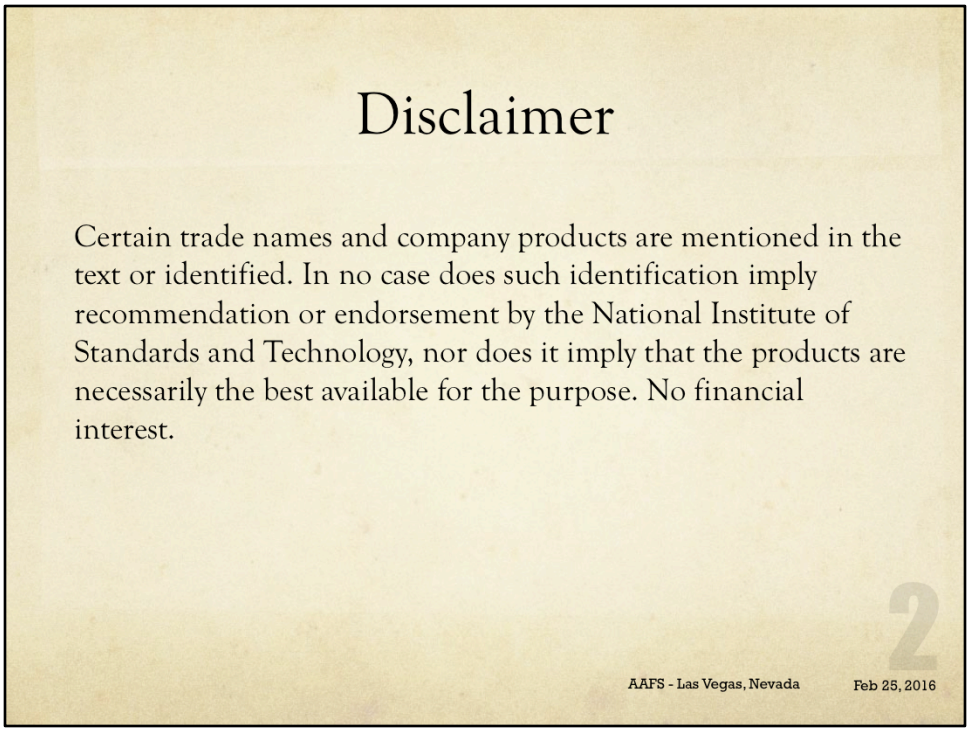
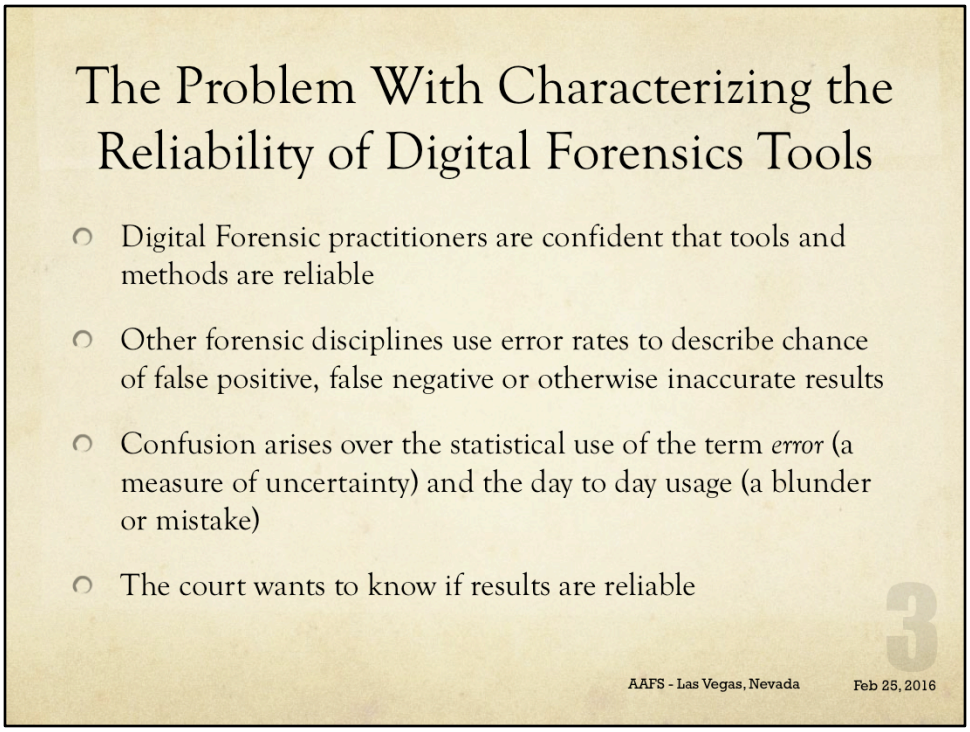


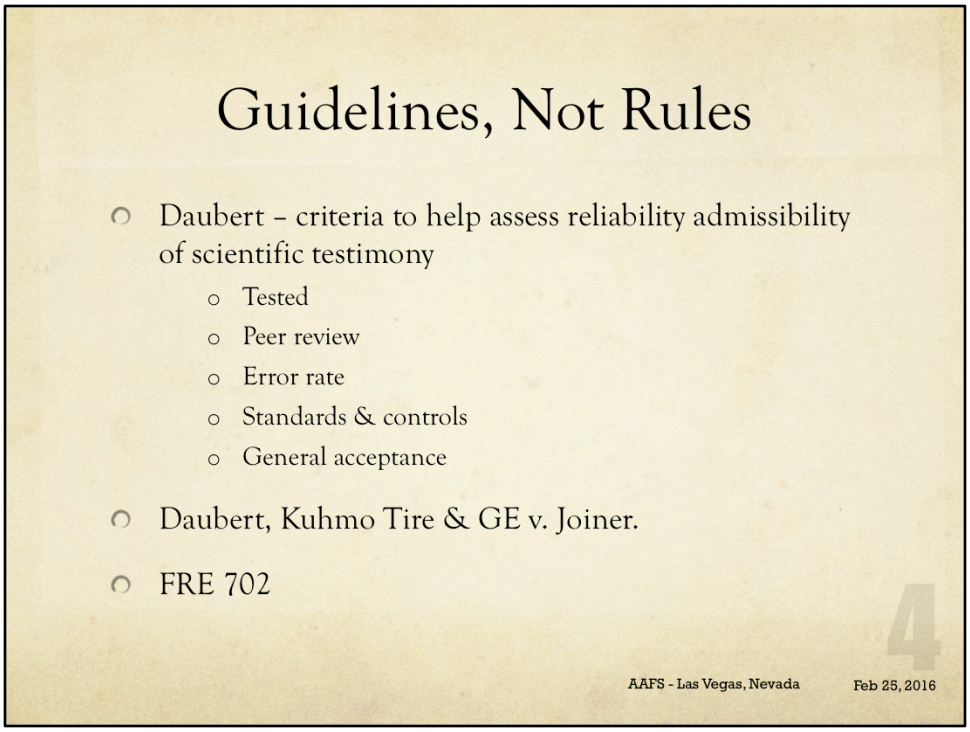
Good morning thanks for coming to my talk. The slides will be posted to the NIST CFTT website in the near future. www.cftt.nist.gov



I will try not to mention any specific products in my talk. If I do mention something I do not have any financial interest in any of these products.

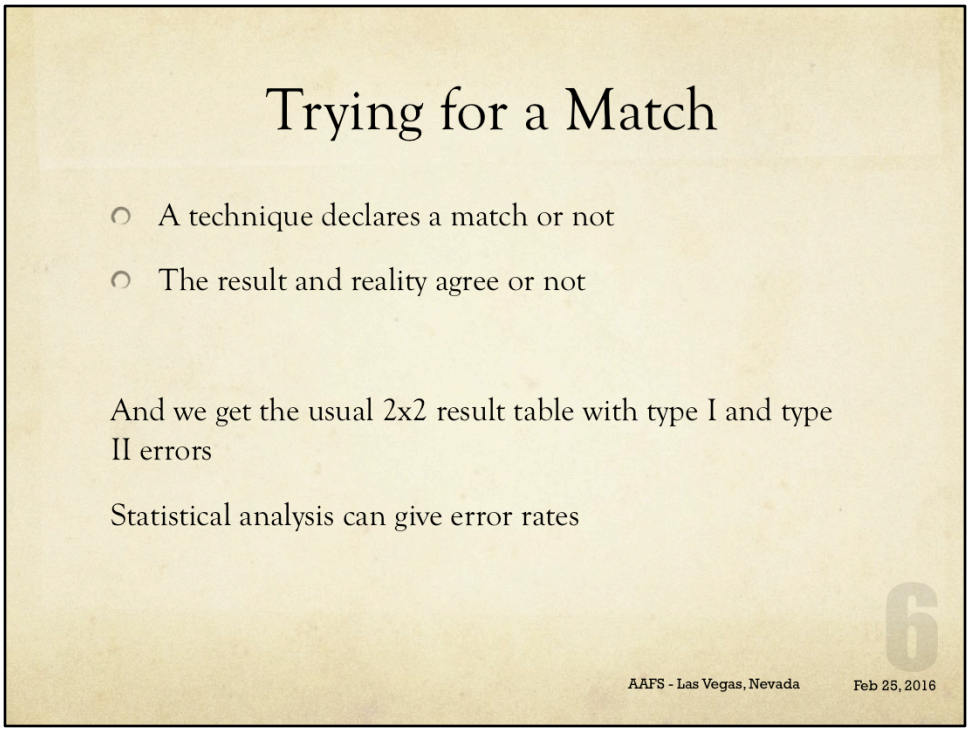


The court wants to know if the results presented are reliable. We know that our results are reliable. How can we communicate this to the court. Other disciplines can use error rates to describe the chance of false positives false negatives or otherwise in accurate results but we do not always have that. The term error often causes a problem because the statistical meaning is a measure of uncertainty while the day-to-day usage is a blender or mistake. This talk is based on the SWGDE document establishing confidence in digital forensic results by error mitigation analysis.

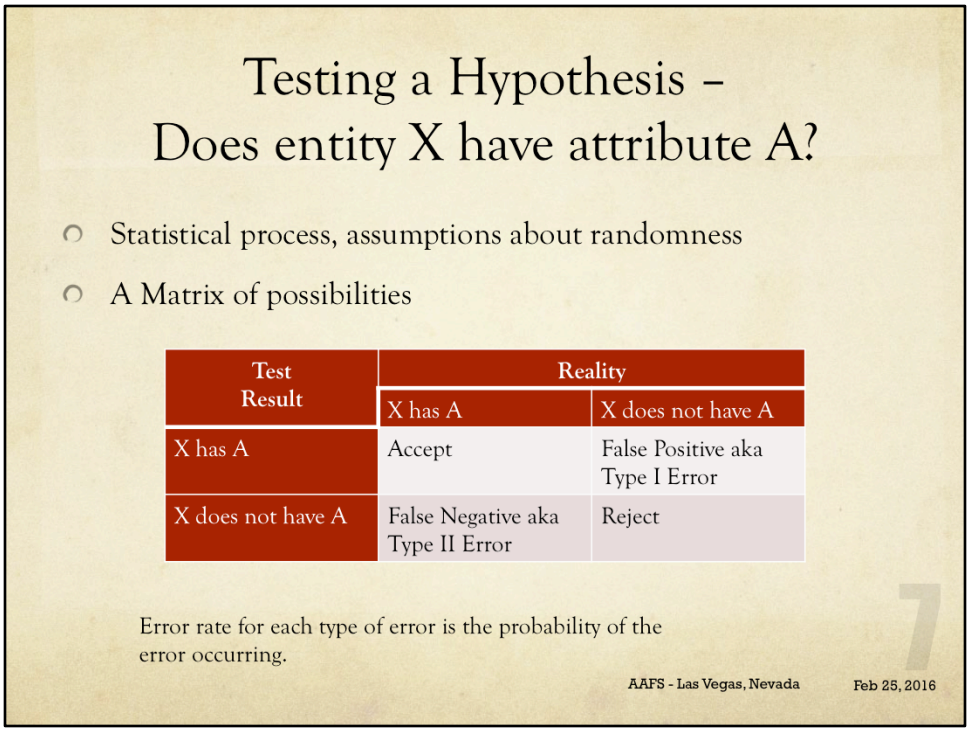


Remember these are guidelines and not rules it's nice to be able to meet all of them but you don't have to.

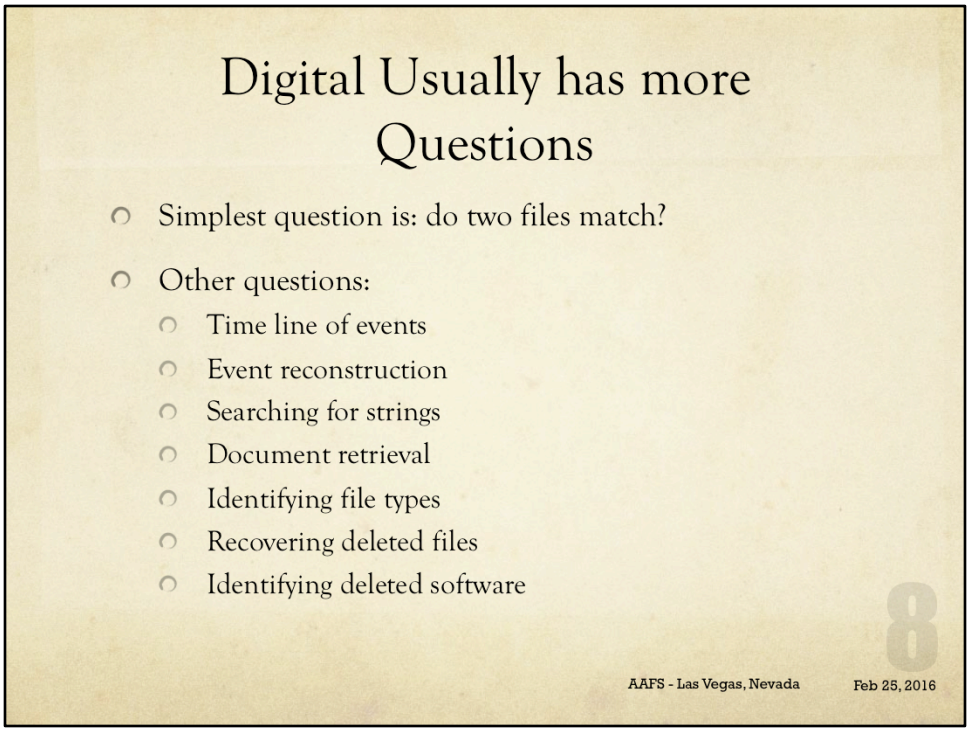
Other disciplines often focus on a single task such as matching one sample from the crime scene and a sample from a suspect.



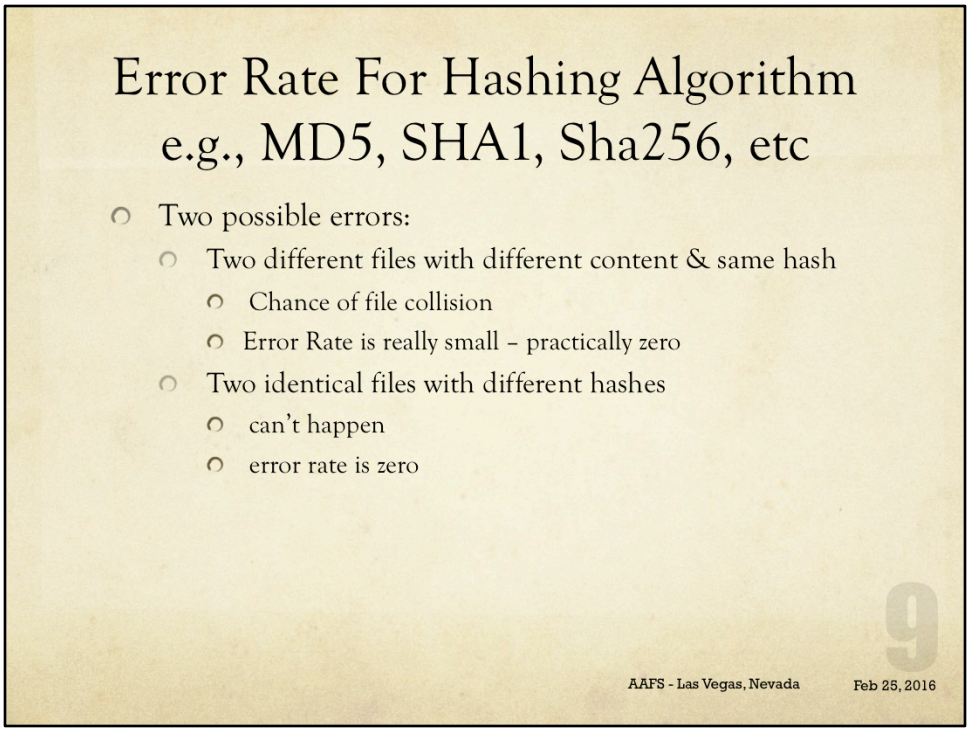
Matching is a natural for error rates



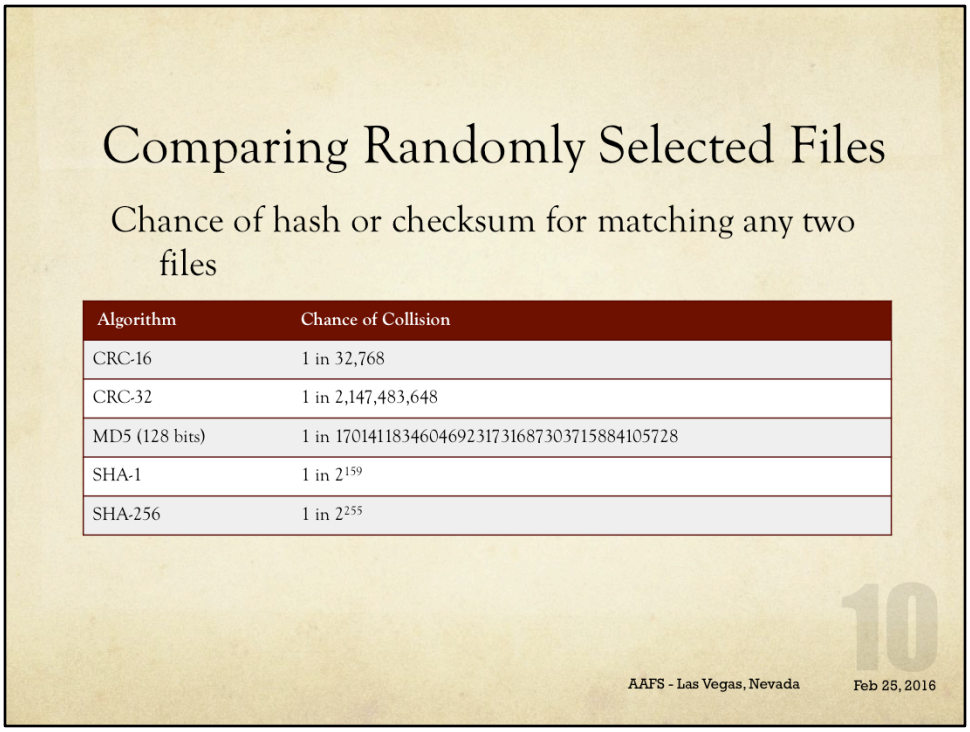
Matching is like a hypothesis test. Reliability can be measured with probablity.



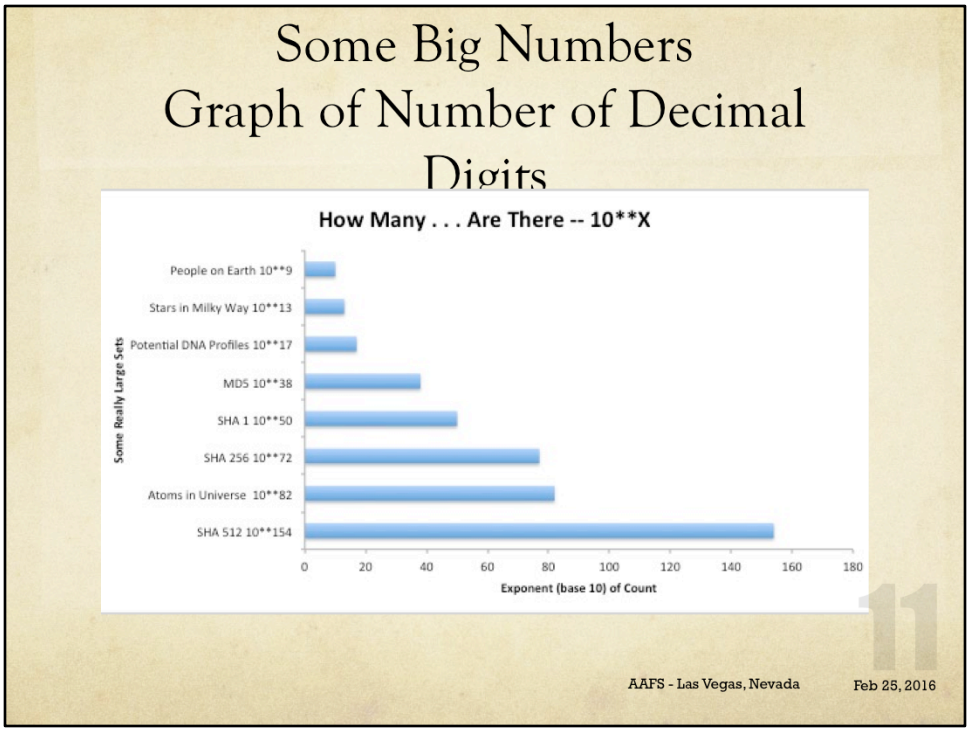
A digital investigation is more than a single test.



Let me start with the easy example. Hashing algorithms have a built in chance of a false positive error that is unimaginably small. The algorithm is immune to false negative errors.

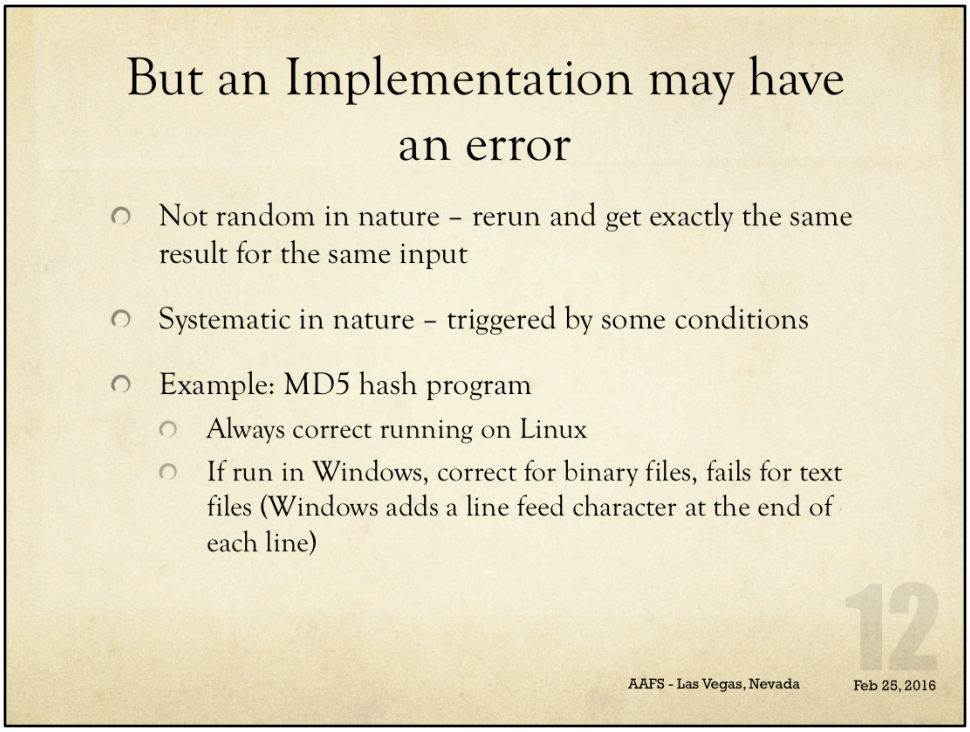


The CRC checksums lack some desirable properties of the cryptographic hash algorithms like randomization of the output so that similar files (even one bit different) produce very different cryptographic hashes.



The probability of a hash collision is unimaginably small. MD5, considered “not good enough” by some, has a chance of hash collision better than one in the number of people that there would be if every star in the milky way galaxy had 10 planets with earth size populations (10**9 x 10**13 x 10 is only 10**23, this is far less than 10**38).

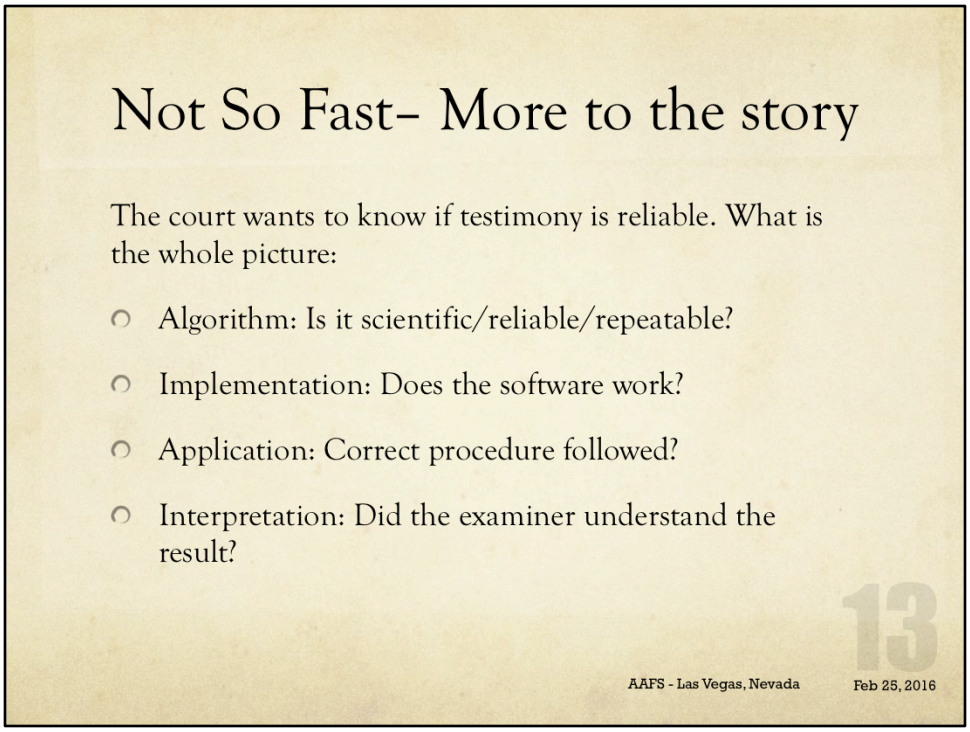
SHA512 is just overkill that’s been overkilled.



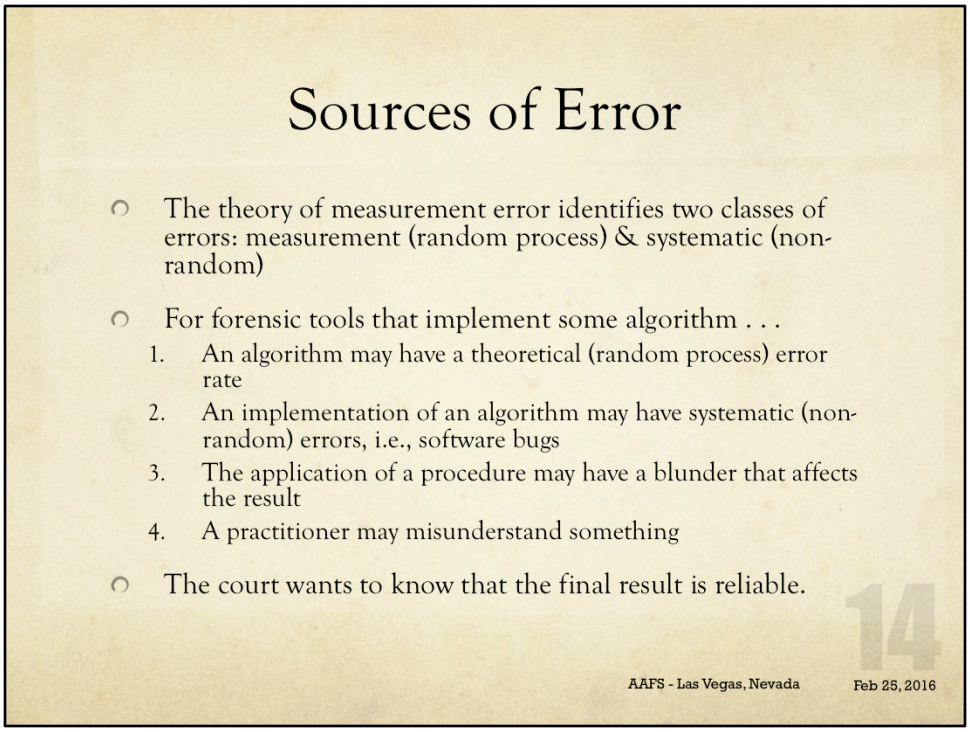
Here comes the rub, and it applies to any forensic process that uses computer software to calculate a result. A hypothesis test or a probability value depends on a random variable with a known probability distribution (usually Gaussian, aka Normal). The (random) error rate is a measure of uncertainty.

The software that makes the calculation can have a software error that is not random in nature. This is a systematic error, nothing random here. Same input yields same output.

BTW, I wrote this program on Linux and moved the software to windows. The software error quickly showed up in just a few test cases and was promptly fixed.



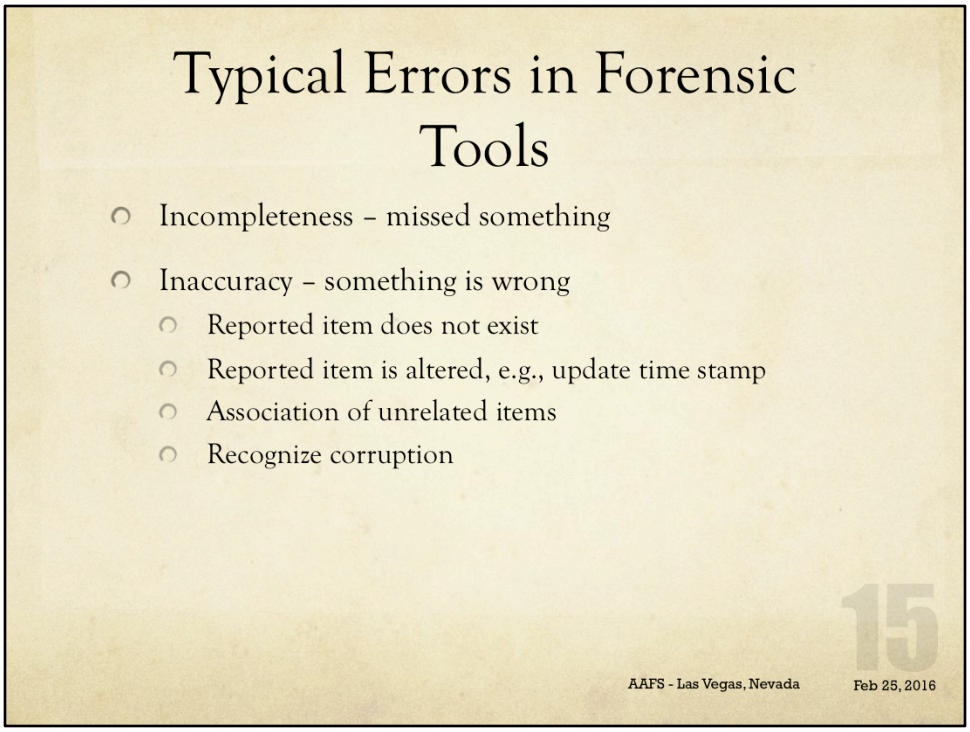
The algorithm has an error rate, but the tool may have systematic software errors and there are other broad paths to perdition. A practitioner might not follow the best practice and wind up comingling data from two cases. Or a practitioner may think that a file was accessed at 00:00 (midnight), but in reality it was zero because the "access" field was never updated by that particular OS.



Here is a little clarification on the word error

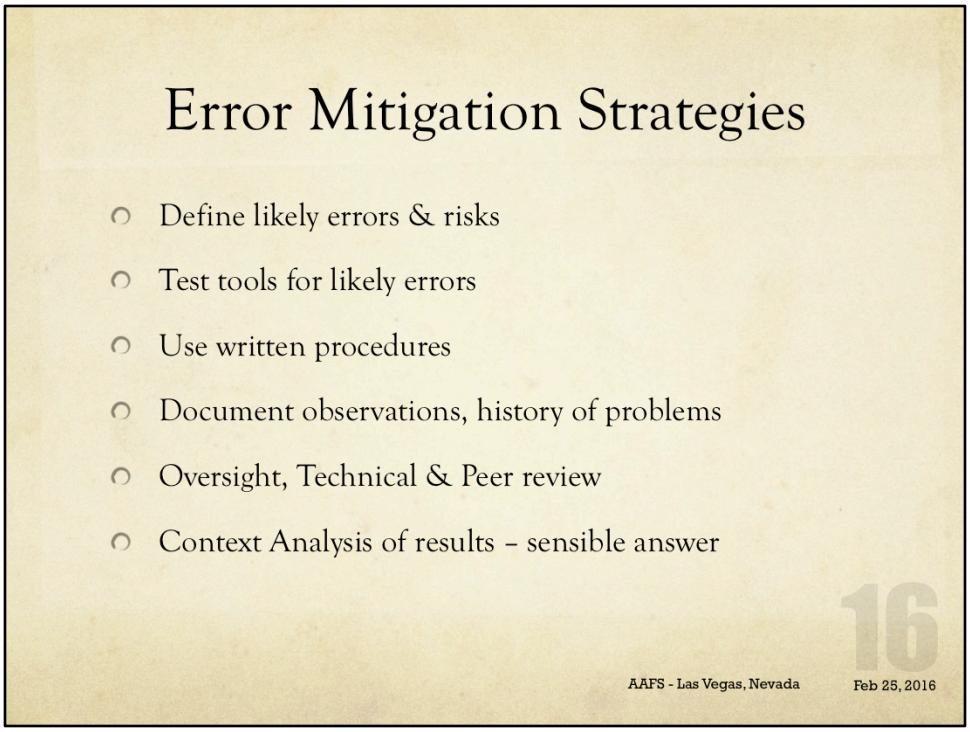
Statistical vs systematic

Again, the court wants to know the result is reliable



It helps to find errors if you can identify likely errors and then test for them.

These are the kinds of errors we have seen at CFTT



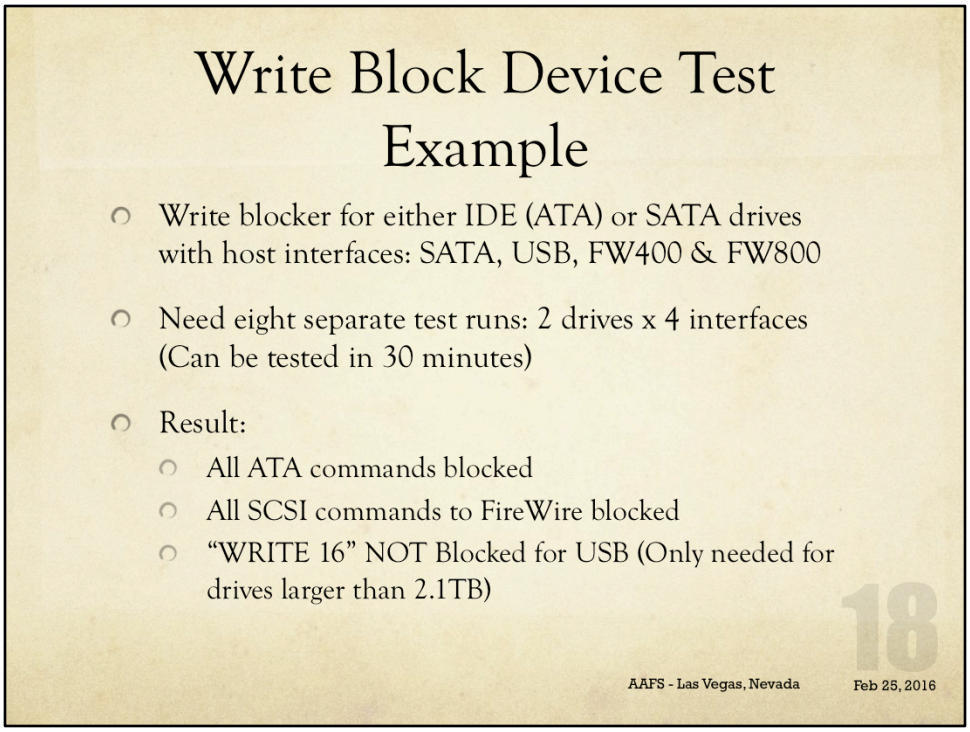
With all the sources of error, what to do . . .

Test for the software errors that are likely or you have seen before

Follow good quality assurance procedures and best practices (like published by SWGDE)

What Do Digital Tools Do?

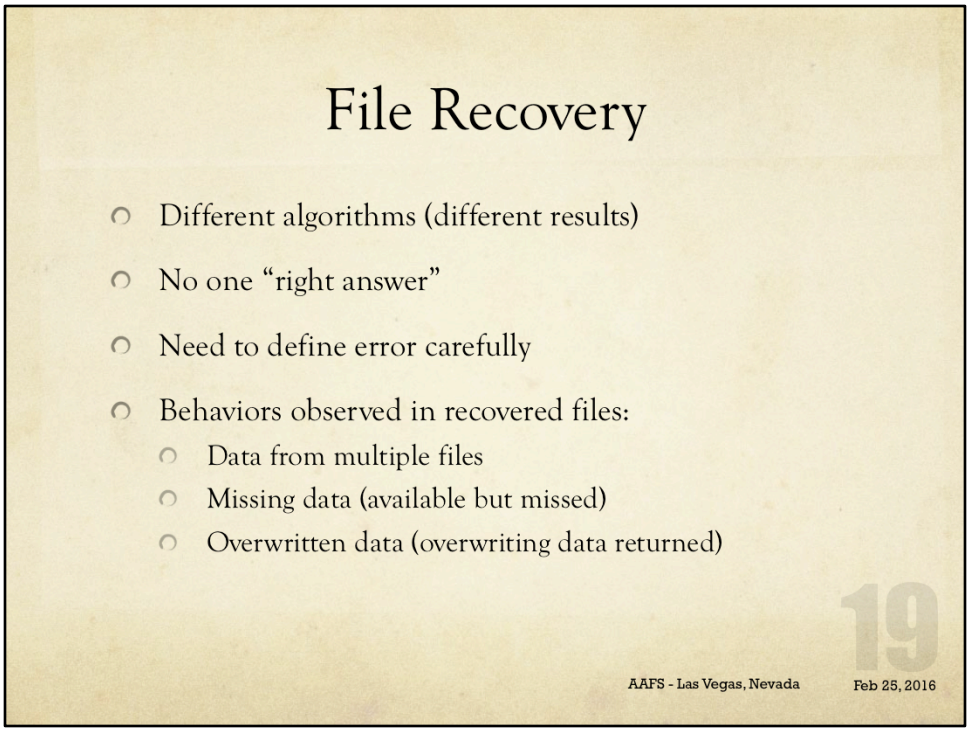
- Collection – disk imaging & write blocking
- Search – look for items that have properties of interest
- Reconstruction – Put things back together
- Time Line – When did events happen



Here is an example of what testing can reveal

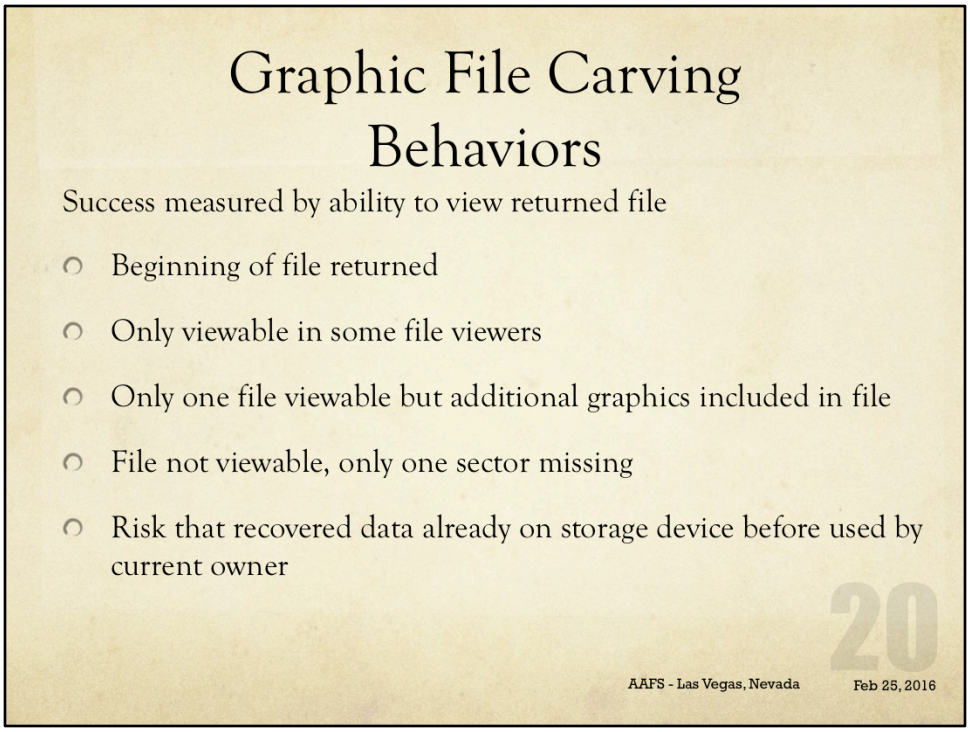
There are are about 5 write commands that a disk driver can choose from. A disk driver (software to access a storage device) usually has a preferred instruction for a given type of drive. In this case, on Windows XP, the write 10 command is preferred unless a disk address greater the 1.2TB is accessed. The "write 10" command has an address limit at that point and a command, like "write 16", with a larger address range must be used.

Note that this particular write block device works just fine except for "write 16" over the USB interface. "Write 16" is blocked on the firewire interface. The problem arose when a chip maker implemented a significant change without informing the write block vendor.

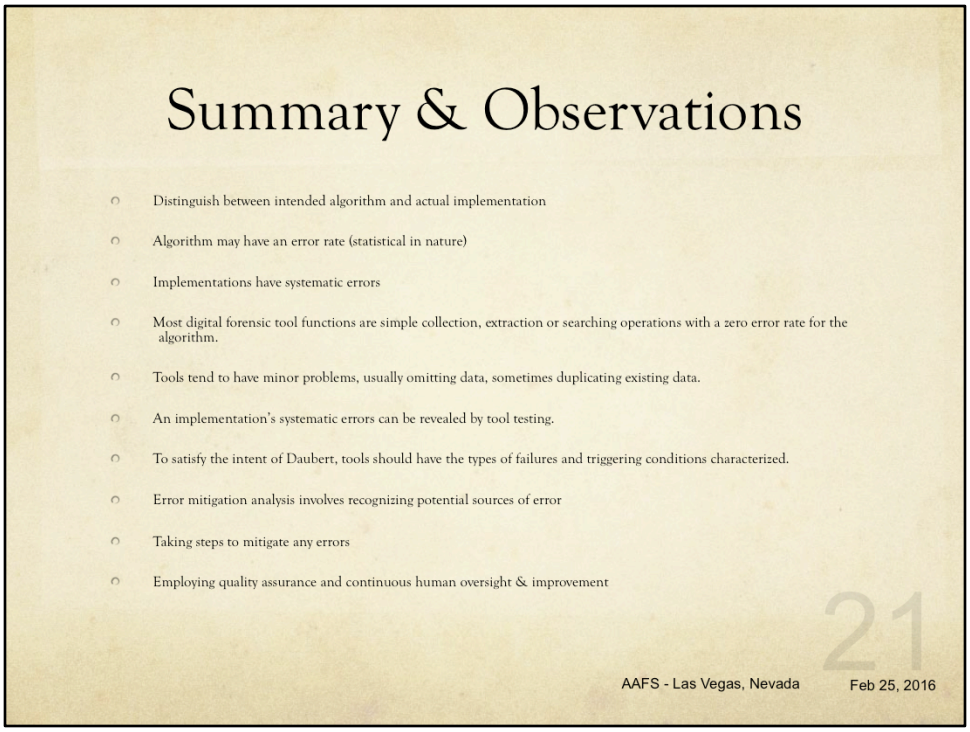


File recovery is one of the more challenging tasks

Recovered files need to be checked for mixing data clusters from multiple files together



Viewing a file usually makes any mixing of data from multiple sources stand out and easy to identify



The key message from the SWGDE document is to look at Error holistically – examine what kinds of errors can occur, which ones are likely. Then systematically take steps to address and reduce error and to describe where potential errors (especially the likely ones) remain.

References

- See: *SWGDE Establishing Confidence in Digital Forensic Results by Error Mitigation Analysis* at www.swgde.org
- CFTT: www.cftt.nist.gov

Contact Information

Jim Lyle
jlyle@nist.gov

Sue Ballou
Susan.ballou@nist.gov

Barbara Guttman, Software and Systems Division
bguttman@nist.gov