ASTM INTERNATIONAL
Helping our world work better

E30.12 Digital Multi-media: Training on E3016-18 *Standard Guide for Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis*

E30.12 Digital Multi-media

TUESDAY, OCTOBER 19, 2021

Barbara Guttman and James Lyle,
National Institute of Standards and Technology

www.astm.org

Disclaimer

Certain trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose. We have no financial interest.

Overview – A Problem for Digital Evidence

How can you communicate confidence in the results of a digital investigation?

There is an ASTM Standard for that:

E3016 – 18 Standard Guide for Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis

Talk Outline

- Some Background
- Digital Forensics Tasks (what has to be done)
- Types of mistakes (what can go wrong)
- How to mitigate errors, what is the strategy

ASTM INTERNATIONAL
Helping our world work better

Section 1
Background & Overview

It’s All About Measurement

- Can you measure it? Can you express it in figures? Can you make a model of it? If not, your theory is apt to be based more upon imagination than upon knowledge.

- Nothing can be more fatal to progress than a too confident reliance on mathematical symbols; for the student is only too apt to take the easier course, and consider the formula not the fact as the physical reality.

- Lord Kelvin

The Problem With Characterizing the Reliability of Digital Forensics Tools

- Digital Forensic practitioners are confident that tools and methods are reliable
- Other forensic disciplines use error rates to describe chance of false positive, false negative or otherwise inaccurate results
- Confusion arises over the statistical use of the term *error* (a measure of uncertainty) and the day-to-day usage (a blunder or mistake)
- The court wants to know if results are reliable

Guidelines, Not Rules

Daubert – criteria to help assess reliability & admissibility of scientific testimony

- Tested
- Peer review
- Error rate
- Standards & controls
- General acceptance

Daubert, Kuhmo Tire & GE v. Joiner.

FRE 702

Some Forensic Tests try to Match two Samples

- Fingerprint matching:
  - –Suspect vs crime scene
  - –Suspect vs data-base
- Same for DNA
- Tire tread
- Footprints
- Tool marks & ballistics

Trying for a Match

A technique declares a match or not
The result and reality agree or not

And we get the usual 2x2 result table with type I and type II errors
Statistical analysis can give error rates

Testing a Hypothesis –
Does entity X have attribute A?

Statistical process, assumptions about randomness
A Matrix of possibilities

Test Result	Reality	
	X has A	X does not have A
X has A	Accept	False Positive aka Type I Error
X does not have A	False Negative aka Type II Error	Reject

Error rate for each type of error is the probability of the error occurring.

ASTM INTERNATIONAL
Helping our world work better

Section 2
Digital Tasks & Where They Can Go Wrong

Digital Usually Has Lots of Questions

Simplest question is: do two files match?

Other questions:

- Time line of events
- Event reconstruction
- Searching for strings
- Document retrieval
- Identifying file types
- Recovering deleted files
- Identifying deleted software

Digital-World vs Real-World

Digital is not as daunting as it seems!

Correspondence of Real (non-digital) World to Digital World Evidence	
Real-World	Digital-World
Crime scene or a place to search for evidence: could be a small site like an apartment or a large site like a farm or business.	Computer, mobile device, storage device: a device to be examined; a server farm with many computers
An item of evidence that is fragmented: shredded document, buried body	Deleted data: evidence that isn’t apparent with the usual computer user tools and can’t be examined without some reassembly
On site records such as a filing cabinet or desk	Files stored on the computer hard drive, removable media.
Offsite records such as at a business branch office, a summer home, or a storage locker	Files stored on a cloud server, or off-line on removable media
Burglar tools or weapons	Hacking tools
Names, phone numbers and addresses from a list of contacts, e.g., address book on paper.	Contact list from a mobile device

Digital Tasks

Getting Started

1. Protection of data during access by write blocking.
2. Acquisition of data stored on a device.
3. Verification of data integrity.
4. Recovery of deleted data.

Finding Evidence

5. Locating artifacts.
6. Extracting artifacts.
7. Interpretation of results.

Protection of data during access by write blocking

- Connecting a storage device to a computer may be necessary to acquire the data. If possible, techniques should be employed that do not allow any changes to the original data and allow the acquisition of the storage device contents accurately.
- Not always possible to use write blocking, sometimes a small program needs to be installed that overwrites some of the data to be acquired. This is often the case when acquiring computer memory. Sometimes the case when acquiring mobile device memory.

Acquisition of data stored on a device

- This task is simple in concept, just make a copy of the data, but subtle in execution. There is a short list of considerations that must be addressed to succeed in data acquisition without changes.
- The algorithms for reliable data copying go back to the 1950’s and are well understood. Google Hamming and ”error correcting codes”

Verification of data integrity

- After the digital data is acquired, it should not be changed, but if there is a change it must be detected.
- Consider algorithms for detecting if a digital object has changed.
- Candidates: CRC16, CRC32, MD4, MD5, SHA-1, SHA-2.
  - CRC algorithms have been used for decades (since the 1950’s) to check if a block of data has been transmitted without an error
  - CRC is fit for detecting changes caused by random noise
  - But, a malicious actor can easily change anything in the file and then modify a tiny section of the file in such a way that the CRC can match an arbitrary value (it is trivial to generate a hash collision).
- Some additional requirements are needed for a hash algorithm to be fit for purpose in a forensic context:
  - Can be computed quickly.
  - Collision resistance, i.e., requires an unreasonable amount of computation to find a hash collision.
  - Original message cannot be recovered.
  - Any change to the original brings about changes in the hash output value.

Error Rate For Hashing Algorithm e.g., MD5, SHA1, Sha256, etc

Two possible errors:

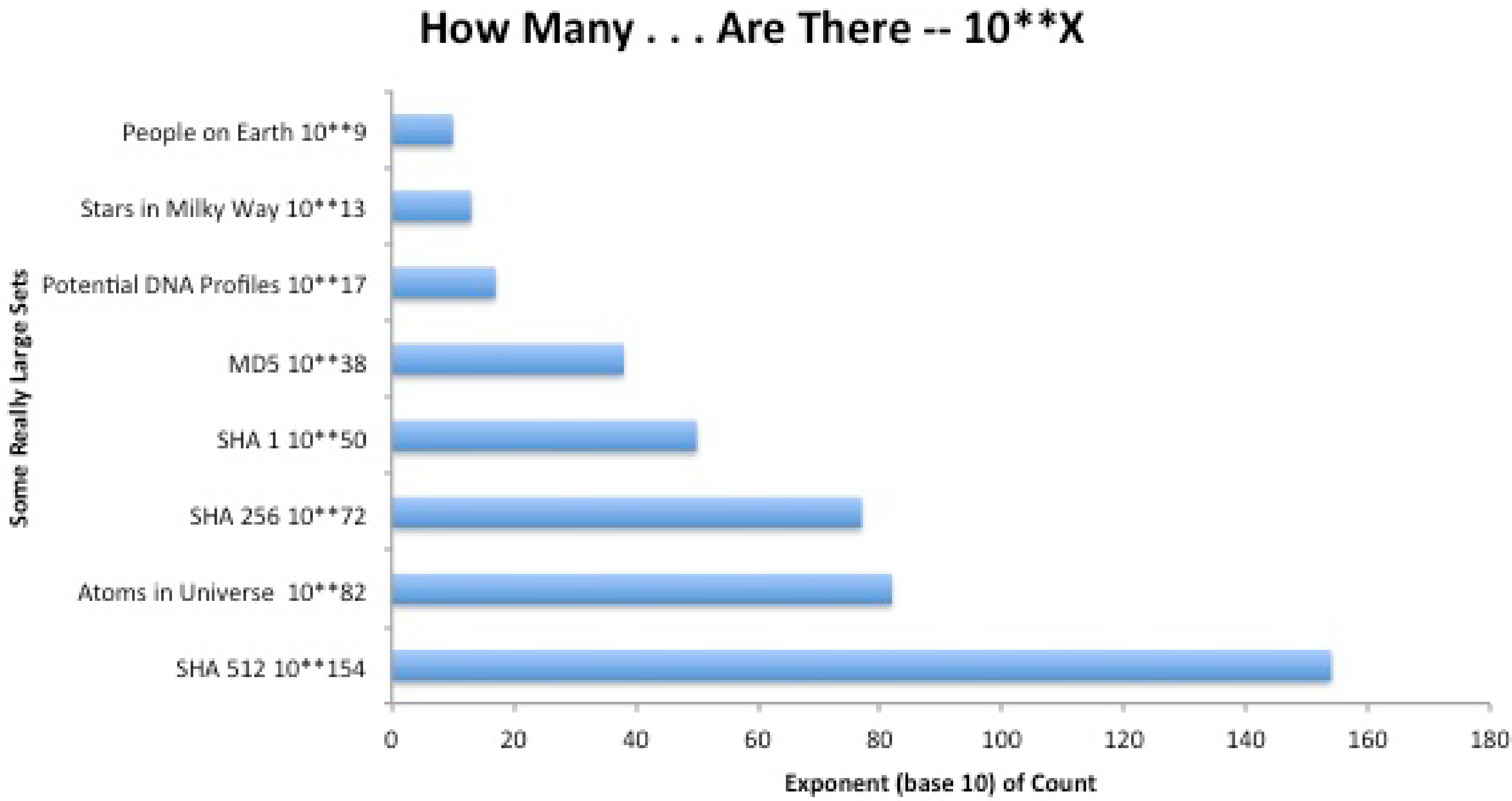
- Two different files with different content & same hash
  - Chance of file collision
  - Error Rate is really small – practically zero
- Two identical files with different hashes
  - can’t happen
  - error rate is zero

Comparing Randomly Selected Files

Chance of hash or checksum for matching any two files

Algorithm	Chance of Collision
CRC-16	1 in 32,768
CRC-32	1 in 2,147,483,648
MD5 (128 bits)	1 in 170141183460469231731687303715884105728
SHA-1	1 in 2^{159}
SHA-256	1 in 2^{255}

Some Big Numbers



Recovery of deleted data

- Data that has been deleted may be gone from access via the operating system, but the deleted data can be recovered with some caveats. Three types of data recovery are:
  - Meta-data based. Use remnants of information used to provide location data to partially reconstruct the deleted file. Some of the caveats are that the location data may be corrupt or file data may be overwritten.
  - File carving. There may not be any location remnants, but some files such as pictures or documents are highly structured and have identification codes at the beginning and the end of a file. After the file has been deleted, these codes can be found and the deleted file reconstructed. Similar caveats apply.
  - Deleted Record Recovery. Some files such as data bases are highly structured and frequently updated. Records (think of a line of data in a table) are created, updated or deleted. If the application leaves updated or deleted records in place they can be identified and retrieved.
- There is a lot of potential for misinformation; the investigators must their knowledge, skills and experience to examine the results of data recovery.

Locating artifacts

- As an investigation progresses questions arise that if they can be answered give a more complete view of events of interest.
- Some questions can be answered by finding a specific artifact. Some examples:
  - Keyword search locates files that contain a specific string.
  - Document retrieval locates files that discuss a specific topic.
  - Meta-data attribute matching locates files with meta-data matching given criteria, e.g., file updated on a given date.
  - Matching file properties can identify contraband.
  - Examining known files can identify needed information, e.g., contact list.
  - Examining recovered files or recovered data records.

Extracting artifacts

- After an artifact is located it must be extracted and decoded into a human readable form.

Interpretation of results

- Linking artifacts to events, users, and activities can often answer questions relevant to an investigation.
- Some other aspects of interpretation include matching artifacts with a user id, identifying how a user id interacted with artifacts, putting events in a time sequence based on artifacts, analysis of whether artifacts have been contaminated or if there are missing pieces that may present an alternative explanation for the links.
- Other aspects of interpretation include understanding that deleted file recovery might be incomplete or might put things together that don’t belong together (such as a case where a tool puts attachments with the wrong email), determining if the system had been hacked, noting changes in usage patterns and so forth.

But an Implementation may have an error

Not random in nature – rerun and get exactly the same result for the same input

Systematic in nature – triggered by some conditions

Example: MD5 hash program

- Always correct running on Linux
- If run in Windows, correct for binary files, fails for text files (Windows adds a line feed character at the end of each line)

Not So Fast– More to the story

The court wants to know if testimony is reliable. What is the whole picture:
Algorithm: Is it scientific/reliable/repeatable?
Implementation: Does the software work?
Application: Correct procedure followed?
Interpretation: Did the examiner understand the result?

Sources of Error

The theory of measurement error identifies two classes of errors: measurement (random process) & systematic (non-random)

For forensic tools that implement some algorithm . . .

1. An algorithm may have a theoretical (random process) error rate
2. An implementation of an algorithm may have systematic (non-random) errors, i.e., software bugs
3. The application of a procedure may have a blunder that affects the result
4. A practitioner may misunderstand something

The court wants to know that the final result is reliable.

Typical Errors in Forensic Tools

- Incompleteness – missed something
- Inaccuracy – something is wrong
- Reported item does not exist
- Reported item is altered, e.g., update time stamp
- Association of unrelated items
- Recognize corruption

ASTM INTERNATIONAL
Helping our world work better

Section 3
Error Mitigation

Error Mitigation Strategies

- Define likely errors & risks
- Test tools for likely errors
- Use written procedures
- Document observations, history of problems
- Oversight, Technical & Peer review
- Context Analysis of results – sensible answer

Three Examples of Error Mitigation Report

See These Examples in The Standard

1. Intellectual Property Theft
2. New Technique Developed
3. Use of Tools Tested Elsewhere

A Tool Test Example: Write Block Device Test Example

Write blocker for either IDE (ATA) or SATA drives with host interfaces: SATA, USB, FW400 & FW800

Need eight separate test runs: 2 drives x 4 interfaces (Can be tested in 30 minutes)

Result:

- All ATA commands blocked
- All SCSI commands to FireWire blocked
- “WRITE 16” NOT Blocked for USB (Only needed for drives larger than 2.1TB)

File Recovery

Different algorithms (different results)

No one “right answer”

Need to define error carefully

Behaviors observed in recovered files:

- Data from multiple files
- Missing data (available but missed)
- Overwritten data (overwriting data returned)

Graphic File Carving Behaviors

- Success measured by ability to view returned file
- Beginning of file returned
- Only viewable in some file viewers
- Only one file viewable but additional graphics included in file
- File not viewable, only one sector missing
- Risk that recovered data already on storage device before used by current owner

Summary & Observations

- Distinguish between intended algorithm and actual implementation
- Algorithm may have an error rate (statistical in nature)
- Implementations have systematic errors
- Most digital forensic tool functions are simple collection, extraction or searching operations with a zero error rate for the algorithm.
- Tools tend to have minor problems, usually omitting data, sometimes duplicating existing data.
- An implementation's systematic errors can be revealed by tool testing.
- To satisfy the intent of Daubert, tools should have the types of failures and triggering conditions characterized.
- Error mitigation analysis involves recognizing potential sources of error
- Taking steps to mitigate any errors
- Employing quality assurance and continuous human oversight & improvement

References

This standard started as a SWGDE guideline document:

SWGDE Establishing Confidence in Digital Forensic Results by Error Mitigation Analysis

See www.swgde.org

ASTM INTERNATIONAL
Helping our world work better

Thank you

www.astm.org

Contact Information

Jim Lyle
jlyle@nist.gov

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