NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

CFFLD Virtual Meeting
8 September 2022

Digital Investigation Techniques:

A NIST Scientific Foundation Review

John M. Butler, PhD
NIST Special Programs Office
john.butler@nist.gov

1

Press Release
(with GovDelivery email push)

NEWS

NIST Publishes Review of Digital Forensic Methods

Report documents the scientific foundations of digital evidence examination and recommends ways to advance the field.

May 10, 2022

NISTIR 8354-DRAFT

Digital Investigation Techniques:
A NIST Scientific Foundation Review

Draft Report (82 pages)

James R. Lyle
Barbara Guttman
John M. Butler
Kelly Sauerwein
Christina Reed
Corrine E. Lloyd

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8354-draft

Public Comments Received

on NISTIR 8354-DRAFT
Digital Investigation Techniques: ***A NIST Scientific Foundation Review***

Published July 18, 2022

Compiled Public Comments (15 sets, 88 pages)

NISTIR 8354-DRAFT: Digital Investigation Techniques: ***A NIST Scientific Foundation Review*** was released for public comment on May 9, 2022. That draft document is available at https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354-draft.pdf.

A public comment period was held from May 9, 2022, to July 11, 2022. This document lists all 15 public comments in the chronological order in which they were received. Submitter email addresses and phone numbers have been redacted.

NIST hosted a webinar on June 1, 2022, to review the content of the draft report and address questions. A recording of the webinar can be found at https://www.nist.gov/news-events/events/2022/06/webinar-digital-investigation-techniques-nist-scientific-foundation. The 24 questions/comments received during the Q&A portion of the webinar are included in the public comments as PC7.

See https://www.nist.gov/forensic-science/digital-investigation-techniques-nist-scientific-foundation-review

2

NIST Process

Initial Input
(Resource Group, Workshop, Interlab Study, etc.)

DRAFT Report

Consider Public Comments Received

FINAL Report

Public Comments on Draft Report

3

Steps in Digital Forensic Investigations

Collect potential evidence

Protect → **Acquire** → **Ensure**

Collection — Gathering the Data

Recover → **Navigate** → **Identify/Extract** → **Analyze**

Interpretation — Understanding Data Obtained

reported result

Written Report

From the draft report Executive Summary: There are many ways to organize tasks performed in digital investigations; for this report, the following grouping of tasks is used:

1. Protect data from modification.
2. Acquire digital data.
3. Ensure integrity of acquired data.
4. Recover deleted data.
5. Navigate the acquired digital data.
6. Identify and extract data artifacts.
7. Analyze. Examination of extracted artifacts can help develop a narrative or reconstruction of relevant events for inclusion in a final written report.

4

From the Executive Summary of NISTIR 8354-DRAFT

Every interaction with a digital device has the potential to leave a trail of what we did, who we did it with, where we were, and when the event took place. This trail is made up of digital artifacts, which are created in the routine operation of a digital device. This trail can assist an investigator to discover and explain what happened. Computers generate many artifacts, most of which do not contribute to understanding what happened. The challenge is finding useful information and separating it from irrelevant information. Digital investigation techniques can extract this information and construct a narrative of the events. The analysis of digital devices for investigative purposes is widely practiced and, as this report shows, **there are at least 11,000 digital forensic laboratories in the United States.**

5

From the Executive Summary of NISTIR 8354-DRAFT

The overall finding of this report is that digital evidence examination rests on a firm foundation based in computer science. Several of the techniques had already been extensively studied and documented in the peer-reviewed literature. Others are documented more informally through community discussion forums. The application of these computer science techniques to digital investigations is sound, only limited by the difficulties of keeping up with the complexity and rapid pace of change in IT.

6

Key Takeaways from DRAFT Report on Digital Investigation Techniques

1. **KEY TAKEAWAY #2.1**: In routine operations computers store much more data than what is presented to the user. Examples include storing time and location data on photos, extra copies of data, and data about system activities. Forensic tools and techniques can reveal this data to provide a window into activities that have taken place on a computer or other digital device.
2. **KEY TAKEAWAY #2.2**: Digital forensics is dependent on an understanding of computers and how they work. Any activity that is performed by a computer can potentially be a target for a forensics tool or technique.
3. **KEY TAKEAWAY #2.3**: Computer technology evolves rapidly but sporadically. Some attributes of computers last for decades and some only for a few weeks.
4. **KEY TAKEAWAY #2.4**: The forensic examiner needs to be aware of key changes in computing technology relevant to the examination being performed. Frequent changes in digital technology introduces the possibility for incomplete analysis or for misunderstanding of the meaning of artifacts.
5. **KEY TAKEAWAY #2.5:** Not every digital forensic technique undergoes a peer review, formal testing, or error rate analysis. In general, the digital forensics community performs an informal review by providing feedback about the usefulness of techniques. This general acceptance process allows for techniques to be quickly evaluated and revised.

7

Key Takeaways from DRAFT Report on Digital Investigation Techniques

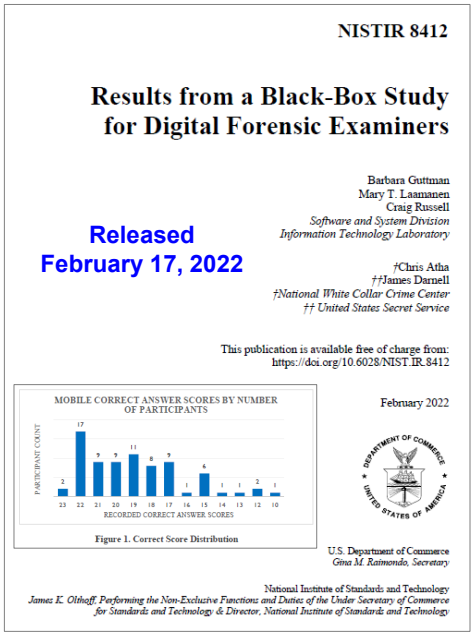
6. **KEY TAKEAWAY #4.1:** When using techniques to recover deleted or hidden artifacts the examiner must determine the relevance of the recovered information as it may be incomplete or improperly merged with irrelevant information.
7. **KEY TAKEAWAY #4.2:** Searching tools have limitations based on the multiple ways that computers store information. Limitations include the type of files, types of encoding, and many other parameters. In general search tools are very effective at finding information, but there is a possibility that data will be missed because a tool does not have the capability to find it.
8. **KEY TAKEAWAY #4.3:** If someone has taken steps to change information in digital evidence to mislead an examiner, it may be difficult to detect the changes. Depending on the sophistication of the manipulation, identification of the changes relies on the skill of the examiner.
9. **KEY TAKEAWAY #4.4:** Digital processes tend to have systematic errors rather than random errors. Therefore, an error mitigation analysis provides more information and is the correct way to manage uncertainty. Asking for an error rate is only useful where there are random errors.
10. **KEY TAKEAWAY #4.5:** When error rates are provided, it is important for the user to understand the context of the numbers. Errors in computer science techniques tend to be so small as to be negligible. For some forensic techniques, the error rates may vary significantly based on attributes of the technology and usage patterns.
11. **KEY TAKEAWAY #4.6:** It is not feasible to test all combinations of tools and digital evidence sources.
12. **KEY TAKEAWAY #4.7:** Extensive tool testing of over 250 widely used digital forensic tools showed that most tools can perform their intended functions with only minor anomalies.

8

From the Executive Summary of NISTIR 8354-DRAFT

In addition to addressing the scientific foundation of digital investigation, it is critical that digital findings are communicated clearly. **Because of the breadth of digital evidence tools and techniques, it is challenging to properly communicate the results of a digital examination.** Some of the basic topics are familiar to most lay people, but the more advanced topics can be rather difficult to understand. Hopefully this report will be helpful in communicating the underlying science and its limitations.

9


NISTIR 8412

Results from a Black-Box Study for Digital Forensic Examiners

Barbara Guttman
Mary T. Laamanen
Craig Russell
Software and System Division
Information Technology Laboratory

†Chris Atha
††James Darnell
†National White Collar Crime Center
†† United States Secret Service

Released February 17, 2022

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8412

Figure 1. Correct Score Distribution

February 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

https://doi.org/10.6028/NIST.IR.8412 (58 pages)

Digital Forensic Interlaboratory Study

- Part of the NIST Scientific Foundation Review on Digital Investigation Techniques (NISTIR 8354-DRAFT)
  - This study was open to anyone in the public or private sectors who work in the field of digital forensics
- Evaluated accuracy of volunteer digital examiners with **24 questions using case scenarios and test artifacts for mobile devices and computer hard-drives**
  - Tests were developed in collaboration with the U.S. Secret Service and the National White Collar Crime Center
- Study participants:
  - **77 mobile device** and **102 hard-drive analyses**
  - Demographic data collected related to an individual's workplace environment, education, and work experience

10

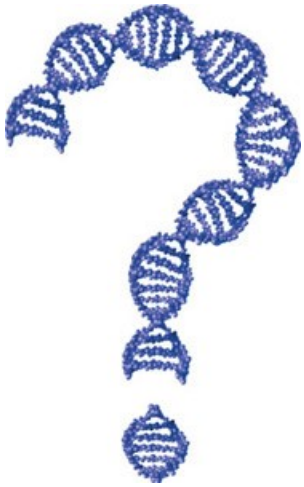
Results & Findings (per Barbara Guttman, ITL)

- It was really hard to get people to participate
  - Pandemic/all electronic outreach was suboptimal
  - Fear of participation (even anonymous) was higher than I anticipated
  - Getting approval was difficult even if people wanted to participate
- It was harder than we thought to verify people
  - Full police departments and local governments are working off of gmail addresses
- Ideas for further studies
  - Used controlled group of participants (would need a lot of lead time)

11

Thank you for your attention!

John Butler
john.butler@nist.gov



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Questions?

12