The DNAForge Vulnerability

Identification, Exploration, Reporting, & Disclosure

Click here for August 3, 2026 recording
Passcode, if prompted: m09bxO#y

Responsibilities & Accountabilities

We are researchers and subject matter experts, unaffiliated with the commercial vendor, and we do not have financial disclosures regarding these materials.

Vulnerability disclosures are voluntary processes.

As members of the forensic science community, we recognized the significance of a potential exploit and chose to report it in consultation with appropriate experts.

Although downstream controls can help mitigate the risk, only the vendor can properly mitigate the vulnerability.

The end users are ultimately accountable for their data management practices.

Researchers Affiliations & Disclosures

Nathan Adams* - Systems Engineer, Forensic Bioinformatic Services

Laura Gaydosh Combs* - Associate Professor, University of New Haven

Dan Krane* - Professor, Wright State University

Kevin Dyer - Cryptographer & Cybersecurity Expert

The materials provided resulted from our contributions to research activities as scientists and do not represent the official position, policy, or views of the affiliated organizations, employers, or vendor.

*Nathan, Laura, and Dan provide expert consulting services including testimony

“Vulnerability” & Disclosure Process

“An instance of one or more weaknesses in a Product that can be exploited, causing a negative impact to confidentiality, integrity, or availability; a set of conditions or behaviors that allows the violation of an explicit or implicit security policy.”

-CVE Program™

If they are not mitigated, vulnerabilities may be exploited. However, a disclosed vulnerability does not mean an exploit has occurred.

Coordinated disclosure is process allowing finders/reporters (internal or external) to communicate to the vendor the details of a vulnerability.

There is an intentional delay between report and public disclosure to provide time for product or service updates to mitigate the vulnerability; typically 45 days, 92 days in this case due to prevalence.

The DNAForge Vulnerability

1. Forensic DNA profiling data file types .fsa/.hid contents can be modified.
2. Insufficient controls exist to detect and alert users to modifications.

In essence, forensic DNA profiling data is susceptible to tampering.

This threat is real, though we believe it can be mitigated.

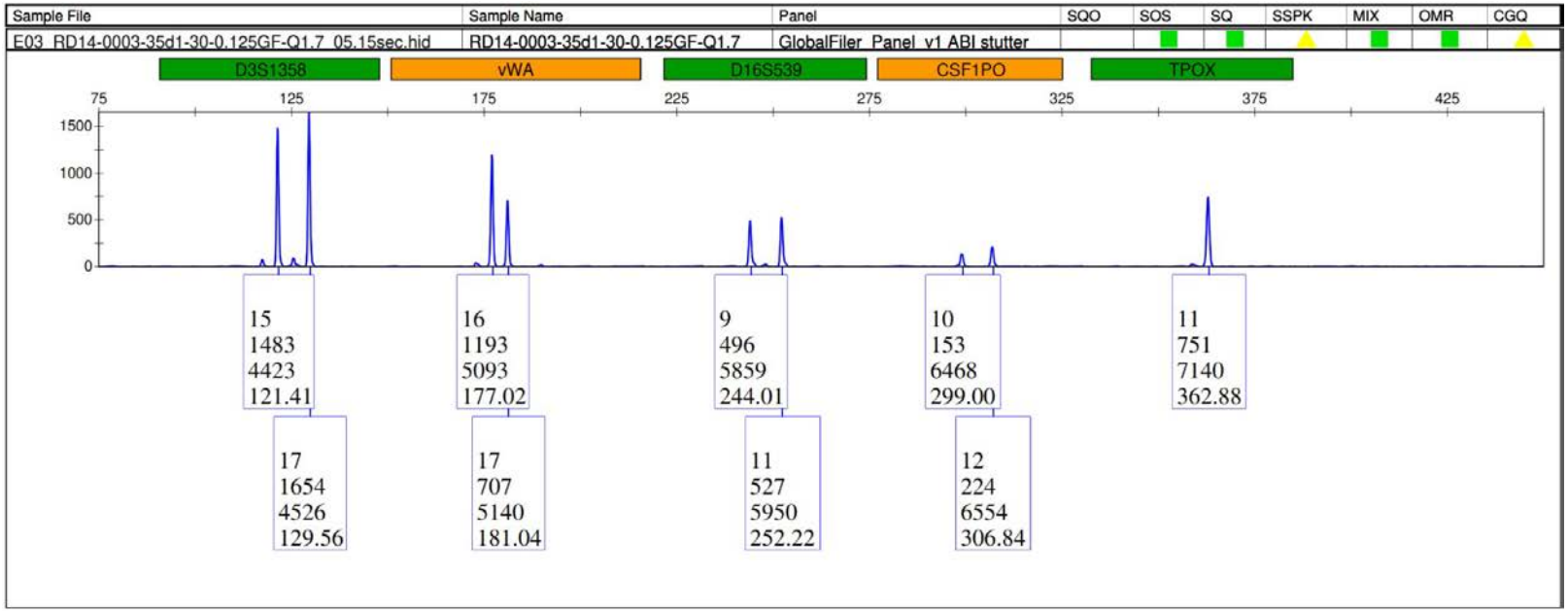
The vendor released a security bulletin July 31, 2026, linked in our accompanying materials. This presentation should be jointly considered with the bulletin.

Overview

- Background on .fsa/.hid files
- This vulnerability
- Exploit demonstration
- Timeline of discovery
- Detection
- Prevention
- Impact
- What next?

Background

Background on .fsa/.hid Files - Electropherograms

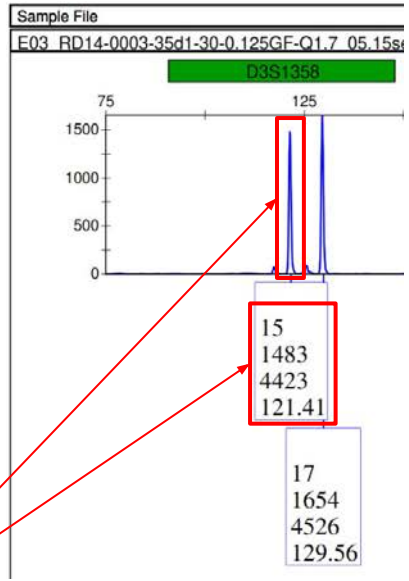


Electropherograms are produced by analyzing raw signal data.

Background on .fsa/.hid Files - Peak Data

Each “peak” consists of a short sequence of integers stored in a data channel within the .fsa/.hid file.

The raw data channel is processed and visually represented as an electropherogram.



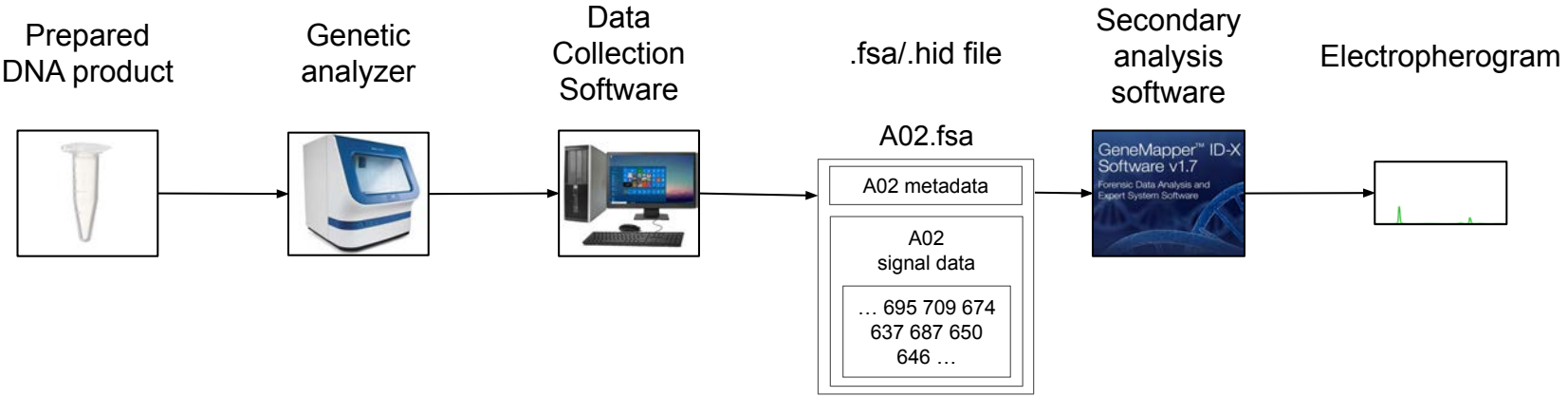

```
-7 -10 -10 -10 8 33 103 228 423 714 991 1292 1517 1542 1435 1209 951 642 435 286 179 89 74 43 38 21 20 1 18 8 -7 -9 -13 -15
```

Background on .fsa/.hid Files - Metadata

Metadata are also stored within the file:

- Sample name
- Well/tube identifier
- Date and time of analysis
- Additional fields include instrument and assay/protocol parameters, may also include consumable reagent information and expiration dates, in addition to run information

Background on .fsa/.hid Files - Origination



The electropherogram is a plot of signal detected over time and serves as the foundation for forensic DNA interpretations.

Background on .fsa/.hid Files - .fsa File Characteristics

- Produced by genetic analyzers widely used in casework labs until mid-2010s
- Also used in new systems, including deployable rapid DNA instruments, and subsequent laboratory-based systems
- Unencrypted

Background on .fsa/.hid Files - .hid File Characteristics

- Produced by the 3500 series genetic analyzers (circa 2010s-present)
  - Also, some 31XX series genetic analyzers (apparent function of data collection software)

- Partially encrypted using Data Encryption Standard (DES)
  - Widely used cipher first broken in mid-1990s
  - .hid file encryption broken by 2013 with decryption key posted online
  - DES is symmetric encryption, so the decryption key can also be used to re-encrypt data

Vulnerabilities vs Exploits

Vulnerability - a weakness in security

Ex. A hole in a fence.

Exploit - taking advantage of that weakness

Ex. Walking through that hole to bypass a locked gate and razor wire.

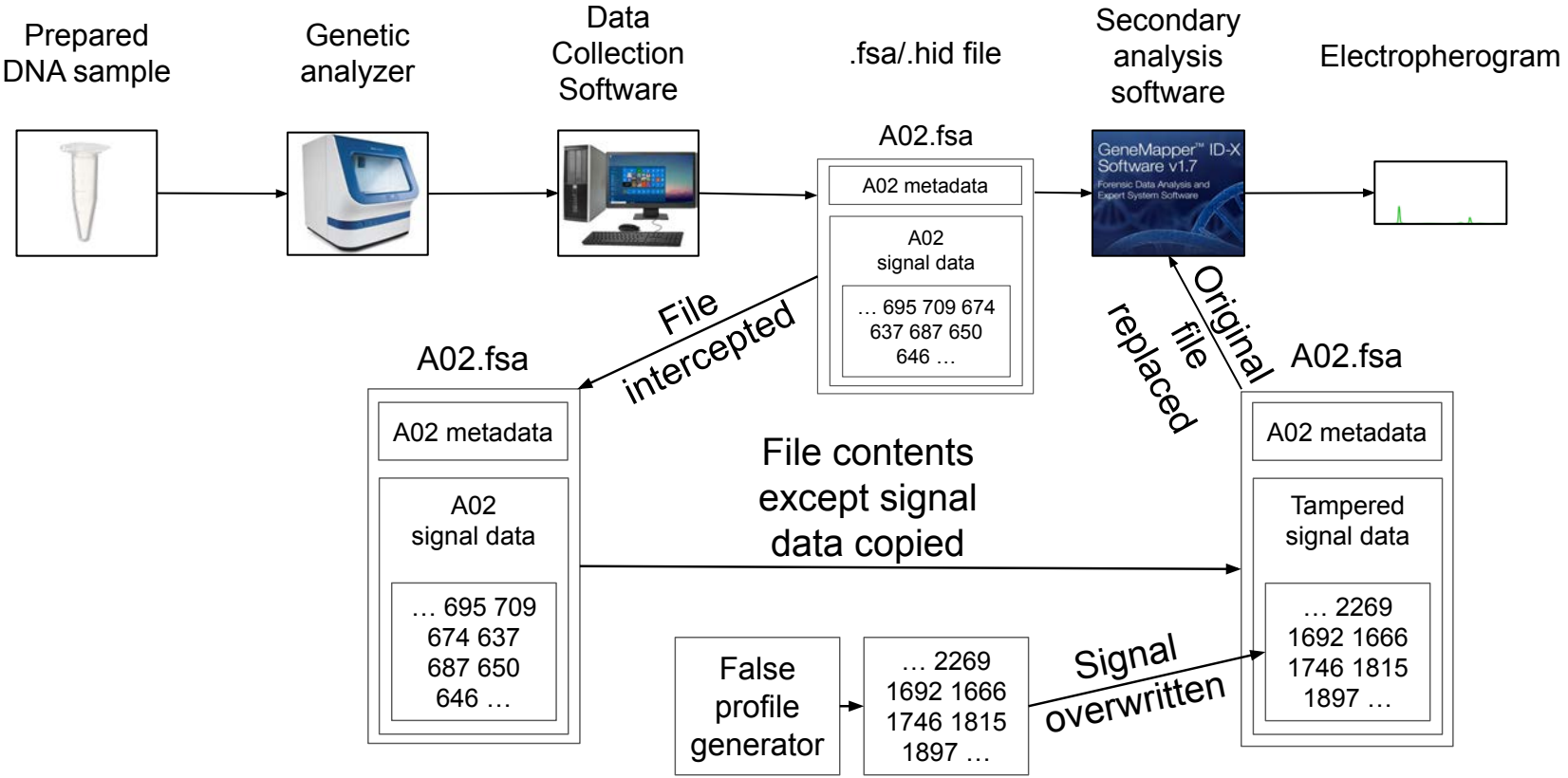
The DNAForge Vulnerability

The DNAForge vulnerability

Metadata or signal data can be modified.

Without data integrity checks, the modifications can be difficult to detect.

Exploited analysis process



Exploit examples

Proof-of-concept attacks performed

1. Summation
    - Adding signal from File A to signal from File B
2. Swap
    - Swapping signal data from File A to File B (optional - and vice versa)
3. Scaling
    - Raising or lowering signal

Hypothetical

4. Arbitrary
    - Inserting signal to artificially create any profile

Exploit demonstration
“Summation Attack”

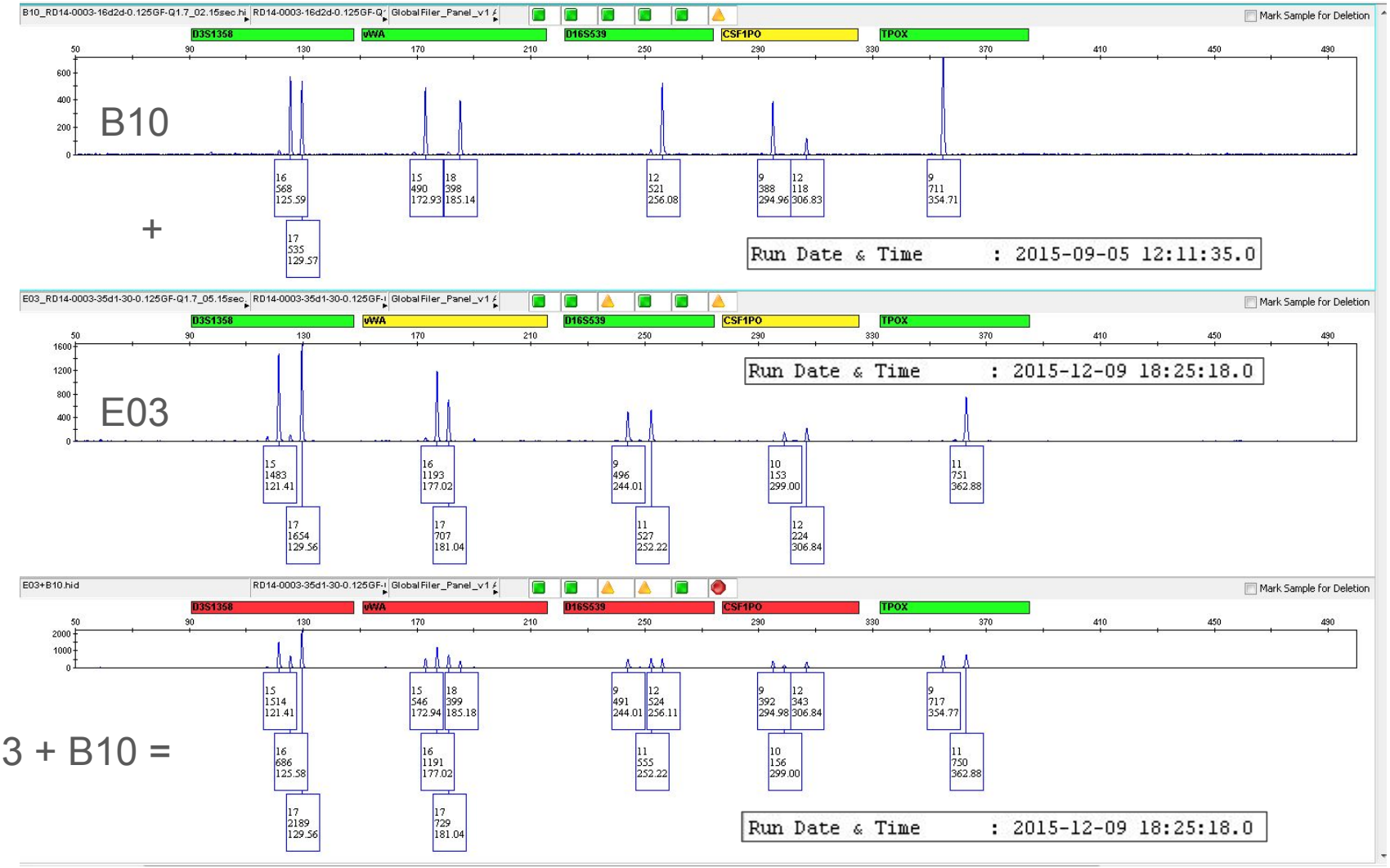
Summation attack

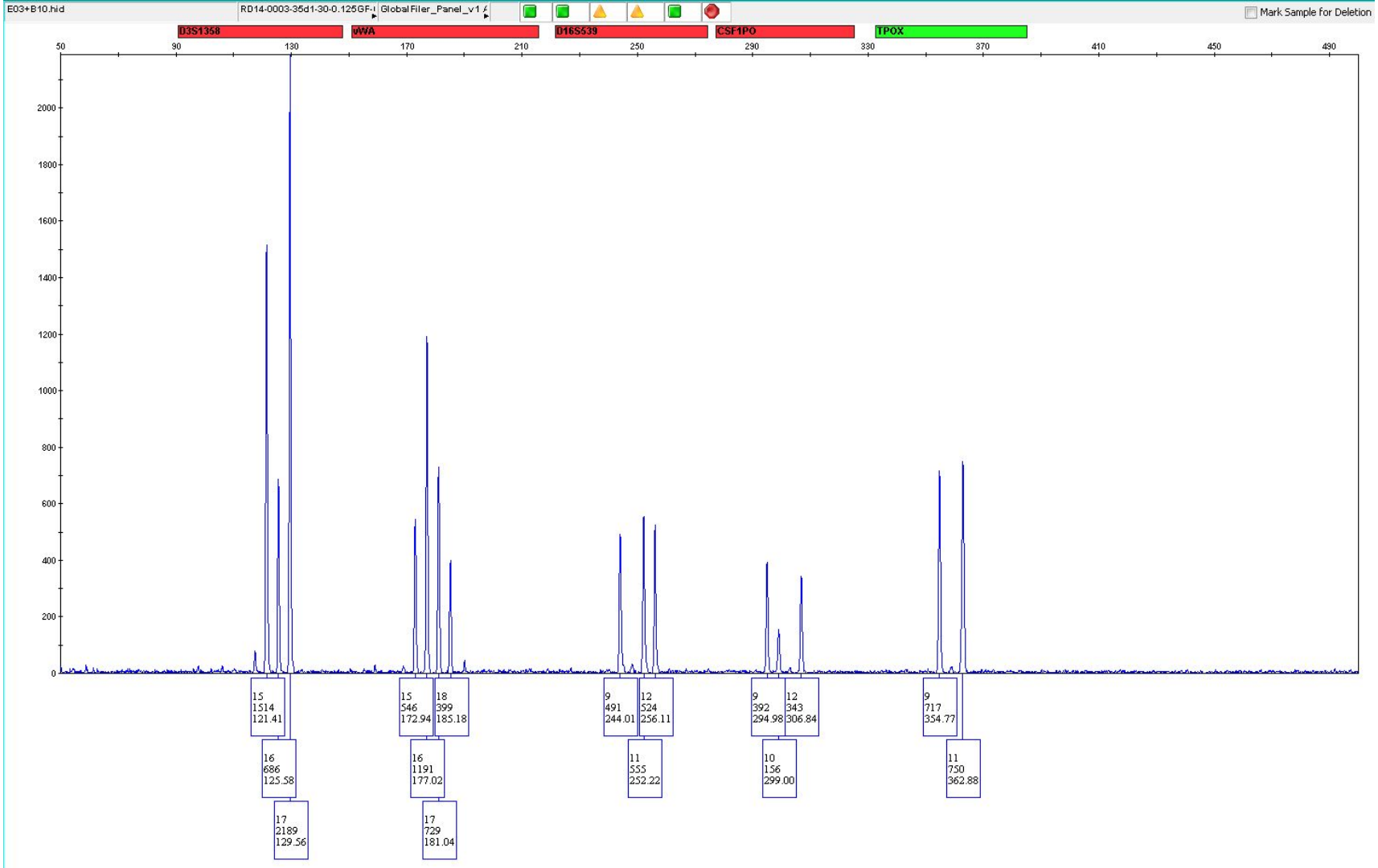
Source data:

- Single-source “B10”
- Single-source “E03”

Goal:

- Add B10 signal into E03 file


B10_RD14-0003-16d2d-0.125GF-Q1.7_02.15sec.hi
RD14-0003-16d2d-0.125GF-Q
GlobalFiler_Panel_v1
Mark Sample for Deletion
D3S1358
vWA
D16S539
CSF1PO
TPOX
B10
16 568 125.59
17 535 129.57
15 490 172.93
18 398 185.14
12 521 256.08
9 388 294.96
12 118 306.83
9 711 354.71
+
Run Date & Time : 2015-09-05 12:11:35.0
E03_RD14-0003-35d1-30-0.125GF-Q1.7_05.15sec.
RD14-0003-35d1-30-0.125GF-
GlobalFiler_Panel_v1
Mark Sample for Deletion
D3S1358
vWA
D16S539
CSF1PO
TPOX
E03
Run Date & Time : 2015-12-09 18:25:18.0
15 1483 121.41
17 1654 129.56
16 1193 177.02
17 707 181.04
9 496 244.01
11 527 252.22
10 153 299.00
12 224 306.84
11 751 362.88
E03+B10.hid
RD14-0003-35d1-30-0.125GF-
GlobalFiler_Panel_v1
Mark Sample for Deletion
D3S1358
vWA
D16S539
CSF1PO
TPOX
E03 + B10 =
15 1514 121.41
16 686 125.58
17 2189 129.56
15 546 172.94
18 399 185.18
16 1191 177.02
17 729 181.04
9 491 244.01
12 524 256.11
11 555 252.22
9 392 294.98
12 343 306.84
10 156 299.00
9 717 354.77
11 750 362.88
Run Date & Time : 2015-12-09 18:25:18.0


E03+B10.hid
RD14-0003-35d1-30-0.125GF-I
GlobalFiler_Panel_v1
Mark Sample for Deletion
D3S1358
vWA
D16S539
CSF1PO
TPOX
50
90
130
170
210
250
290
330
370
410
450
490
2000
1800
1600
1400
1200
1000
800
600
400
200
0
15
1514
121.41
16
686
125.58
17
2189
129.56
15
546
172.94
18
399
185.18
16
1191
177.02
17
729
181.04
9
491
244.01
12
524
256.11
11
555
252.22
9
392
294.98
12
343
306.84
10
156
299.00
9
717
354.77
11
750
362.88


B10_RD14-0003-16d2d-0.125GF-Q1.7_02.15sec.hi
RD14-0003-16d2d-0.125GF-Q
GlobalFiler_Panel_v1
Mark Sample for Deletion
Yi...
AMEL
D8S1179
D21S11
D18S51
DYS391
50 90 130 170 210 250 290 330 370 410 450 490
800 600 400 200 0
2 853 86.86
X 737 98.97
Y 997 105.07
13 497 147.03
14 661 151.24
28 366 199.65
29 294 203.66
16 293 297.71
18 296 305.71
9 777 373.37
E03_RD14-0003-35d1-30-0.125GF-Q1.7_05.15sec.
RD14-0003-35d1-30-0.125GF-
GlobalFiler_Panel_v1
Mark Sample for Deletion
Yi...
AMEL
D8S1179
D21S11
D18S51
DYS391
50 90 130 170 210 250 290 330 370 410 450 490
1600 1200 800 400 0
2 1782 86.71
X 1661 98.82
Y 1523 104.89
10 1383 134.55
15 1958 155.22
Spike 103 5244
30 220 207.51
28 707 199.57
12 431 281.72
20 169 313.81
10 80 377.47
E03+B10.hid
RD14-0003-35d1-30-0.125GF-
GlobalFiler_Panel_v1
Mark Sample for Deletion
Yi...
AMEL
D8S1179
D21S11
D18S51
DYS391
50 90 130 170 210 250 290 330 370 410 450 490
2000 0
2 2562 86.79
X 2361 98.90
Y 2477 104.97
10 1392 134.55
13 500 147.02
14 796 151.15
15 1961 155.22
Spike 104 5244
29 321 203.66
28 1052 199.57
30 222 207.60
12 436 281.72
16 289 297.72
18 310 305.73
20 172 313.81
9 782 373.40
10 85 377.47

Timeline

Timeline - Historical Context

1995 (approx.): **ABI PRISM 310 Genetic Analyzer** **(**Applied Biosystems) released, producing .fsa files.

2000 (approx.): **ABI PRISM 3100 Genetic Analyzer** (Applied Biosystems) released, producing .fsa files

2008-06-11: Invitrogen acquires Applied Biosystems, later rebranded as Life Technologies Corporation

2010 (approx.): **3500 Series Genetic Analyzers** (Life Technologies Corp.) released, producing .hid files

2013-10-04: **.hid encryption key is published online**

2014-02-03: Thermo Fisher Scientific acquires Life Technologies Corporation

2015-07-13: **Metadata edited to de-identify .fsa files using WinHex Hex Editor & Disk Editor (2012)**

2015-09-02: **ABIF Manager published online**

Pavel B, Mraz I. ABIF Manager: Simple Reading and Editing of ABIF Formatted Files. Bioinformatics. 2015 Sep 2;31(24):4012–3. Available from: https://doi.org/10.1093/bioinformatics/btv512

Timeline - Identification through Disclosure

2025-05-24: .hid file metadata test edit using Microsoft Visual Studio
This test was insufficient to determine if signal data were vulnerable

2026-04-21: Claude prompted to alter .fsa file signal data (random Tuesday)

2026-04-26: Claude prompted to alter .hid file signal data (Sunday)

2026-05-01: Vulnerability disclosure to vendor (Friday, **10d & 5d, respectively**)

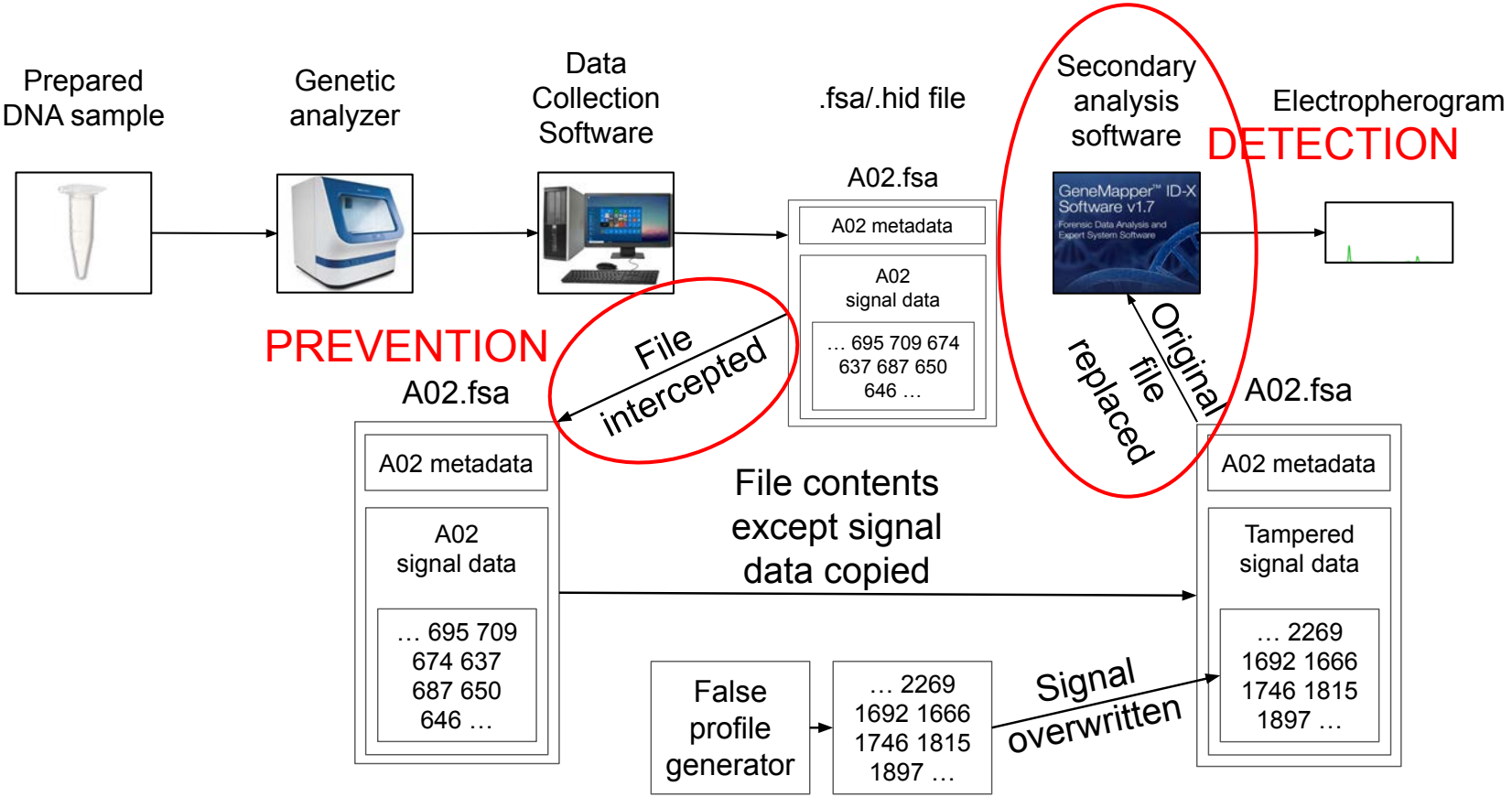
2026-07-31: Vendor security bulletin and software patches released (**91d TAT**)

2026-08-01: Public disclosure date, finders/reporters–>stakeholders

2026-08-04: Common Vulnerabilities and Exposures (CVE) publication anticipated

Detection and Prevention

Exploited analysis process



Exploration - Detection Overview

All files are inherently editable, so the question for us was really whether there appeared to be a reliable indicator of file modification (tampering).

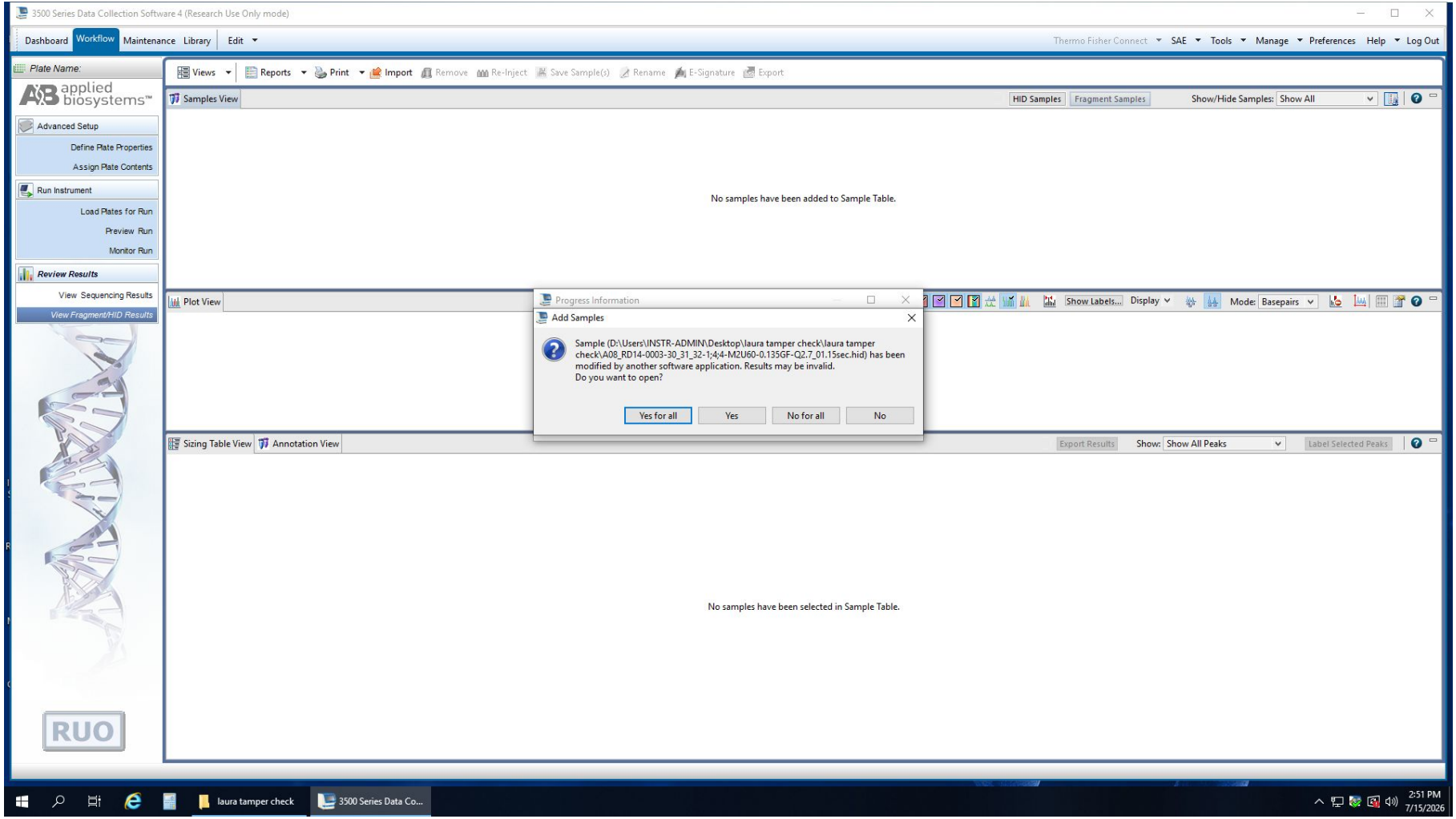
Simple inspection of files and electropherograms, no obvious tells.

Odd patterns in signal data might be suspicious but are difficult to conclusively show that tampering occurred.

It’s not clear to us that we currently have the tools necessary to detect tampering. Or that they could be developed easily.

Exploration - Detection Attempts

- “Date modified” in Windows file details
  - Not reliable, may update from benign activity, *e.g.* if a file unzipped from a compressed folder.
- Secondary analysis software (GeneMapper ID-X*, GeneMarker, & OSIRIS) did not reveal any indicators of modification to metadata and/or signal data
- No obvious irregularities in exported data from secondary analysis software
  - Inspection of txt/csv data appears as seamless modification of signal data
- Re-importing .fsa,.hid files generated with any 3500 series instrument into data collection (primary analysis) software will alert the user; however, it is a soft stop that does not prevent re-saving; subsequent imports lack warning
  - Not reliable, also appears when .fsa files generated by 310 and 3100 series instruments


3500 Series Data Collection Software 4 (Research Use Only mode)
Dashboard
Workflow
Maintenance
Library
Edit
Thermo Fisher Connect
SAE
Tools
Manage
Preferences
Help
Log Out
Plate Name:
applied biosystems
Advanced Setup
Define Plate Properties
Assign Plate Contents
Run Instrument
Load Plates for Run
Preview Run
Monitor Run
Review Results
View Sequencing Results
View Fragment/HID Results
RUO
Views
Reports
Print
Import
Remove
Re-Inject
Save Sample(s)
Rename
E-Signature
Export
Samples View
HID Samples
Fragment Samples
Show/Hide Samples:
Show All
No samples have been added to Sample Table.
Plot View
Show Labels...
Display
Mode:
Basepairs
Progress Information
Add Samples
Sample (D:\Users\INSTR-ADMIN\Desktop\laura tamper check\laura tamper check\A08_RD14-0003-30_31_32-1;4;4-M2U60-0.135GF-Q2.7_01.15sec.hid) has been modified by another software application. Results may be invalid.
Do you want to open?
Yes for all
Yes
No for all
No
Sizing Table View
Annotation View
Export Results
Show:
Show All Peaks
Label Selected Peaks
No samples have been selected in Sample Table.
laura tamper check
3500 Series Data Co...
2:51 PM
7/15/2026

General Security Improvements Available - SAE Module

3500 Series Data Collection Software includes an SAE module, which does not prevent or identify our model exploits of this vulnerability; however, enabling this feature will allow the following functions that may assist in

- Security: admin controls for user access and define privilege levels
- Audit: enabling generates audit trails for features requiring e-signature
- E-Signature: define security policies requiring signatures for specific tasks
    - For example: modifying protocols or assays, approving plates, and renaming files

Refer to topic “Security” in the Data Collection Software manual via Help menu

Chapter in User Guide “Use Security, Audit, and E-Sig functions (SAE Module)”

Exploration - Some Potential Prevention Strategies

These are only ideas:

1. Cryptographic signing in hardware/software
    - Cryptographic tools support electronic signatures without encrypting (obscuring) the data.

2. Laboratory Information Management System integration
    - Close coupling of genetic analyzer with automated file management
    - Can (nearly) instantaneously take a snapshot/hash of a .fsa/.hid file for future comparison

Releasing the Exploits

1. Proof-of-concept is not “just a concept”
    - It is useful for demonstrating feasibility, appropriate risk mitigation, stakeholder engagement, resource optimization, and user feedback
    - Stakeholders are more likely to take a demonstration seriously than an idea
2. Exploits in the light are better than exploits in the dark
    - Expected attacks are easier to prevent and detect than surprise attacks
3. Low burden to replicate
    - A DNA analyst and a few hours with Claude and GeneMapper can get here

Impact

Impacts

Unclear

- This wasn’t a publicly known vulnerability
  - Existing checks for data authentication and integrity were developed without considering it
- Reviewing past work involves developing post-hoc audit methods.
  - Variable laboratory data retention policies and accessibility of previous primary and secondary analysis software versions routinely prevent examination, same issue applies there.
  - Might be complicated by relevant materials not retained
- Future work depends on both vendor responses and lab implementations.
  - The vendor is responsible for properly mitigating the vulnerability; however, laboratory end users are ultimately accountable for their data management practices and supplying documentation to authenticate and verify the integrity of their records.

What next?

Where do we go from here?

The vendor has already responded with a security bulletin.

A CVE report will be published (Aug. 4)

Security professionals are vital partners and must be consulted.

Stakeholder representatives should consider risks.

Standards, audit practices, IT policies, etc. may require review/revision.

Discovery, voir dire, and expert testimony might have to address this.

Procurement of new hardware and software systems should proactively consider data security with consideration made for all stakeholders (*e.g.* discovery).

Phase II of DNAForge - Public Discourse & Engagement

Sarah Chu - Director of Policy and Reform, Perlmutter Center for Legal Justice at Cardozo Law

Nicolas Hughes - Criminal Defense Attorney and Forensic Consultant

And perhaps, you?

Stakeholders Call to Action

Support initiatives to require digital evidence, including raw data, to meet the same level of security as physical items with a chain of custody and audit trail.

Consider including appropriate subject matter experts and members of other stakeholder groups when developing standards and policies.

Acknowledgments - Vulnerability Disclosure

We would like to thank the following:

The Cybersecurity and Infrastructure Security Agency (CISA) Cyber Systems Analyst

Computer Emergency Response Team Coordination Center (CERT CC) for facilitating reporting and coordination.

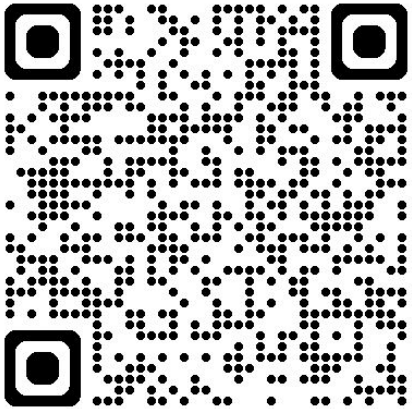
Thermo Fisher Scientific product security team for their response, including acknowledgment, customer communication, and software patches.

Thermo Fisher Scientific Human Identification team for disseminating information to end users as soon as they were available.

Acknowledgements - Unrelated to Disclosure

IEEE members Jeanna Matthews and Marc Canellas for sharing their subject matter expertise with forensic scientists

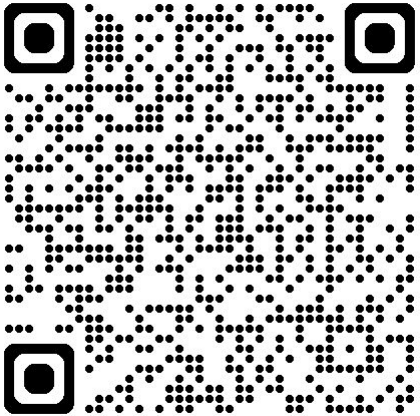
Rhonda Roby and Yogesh Prasad sharing their time and expertise regarding the CE platforms and related materials with students, trainees, and end users



ABIFtampering, GitHub Public Repository

Thank you!

Questions?



Security Bulletin, Thermo Fisher Scientific

dnaforge.cve@gmail.com