Validating Evidence for Courtroom Testimony

Heather Mahalik, Senior Instructor

Jessica Hyde, Magnet Forensics, Hexodia, GMU

Mattia Epifani, Instructor

Ian Whiffin, Senior Digital Intelligence Expert, Cellebrite

Paul Lorentz, Technical Account Expert - Canada, Cellebrite

Alexis Brignoni, Special Agent, Federal Law Enforcement

John Bair, Senior Consultant, Digital Forensics; Testifying Expert, Lighthouse

Mike Williamson, Forensic Consultant, Magnet Forensics

Christophe Poirier, Cybersecurity Team Leader, Edvance

*Additonal paper author – **Lee Reiber**, Oxygen Forensics

Cellebrite

ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

MAGNET FORENSICS

OXYGEN FORENSICS

MSAB

paraben corporation

GRAYSHIFT

Belkasoft
forensics made easier

SANS DFIR

Check out our paper:
https://www.sans.org/white-papers/six-steps-to-successful-mobile-validation/

6 Steps to Mobile Validation: Coming together for the common Good

6 Steps

1 Determine all possible extraction methods for your search authority

2 Process the data in more than one tool

3 Deep dive forensics:

4 Validation

5 Reporting / Sharing your findings

6 Education

Step 4: Validation

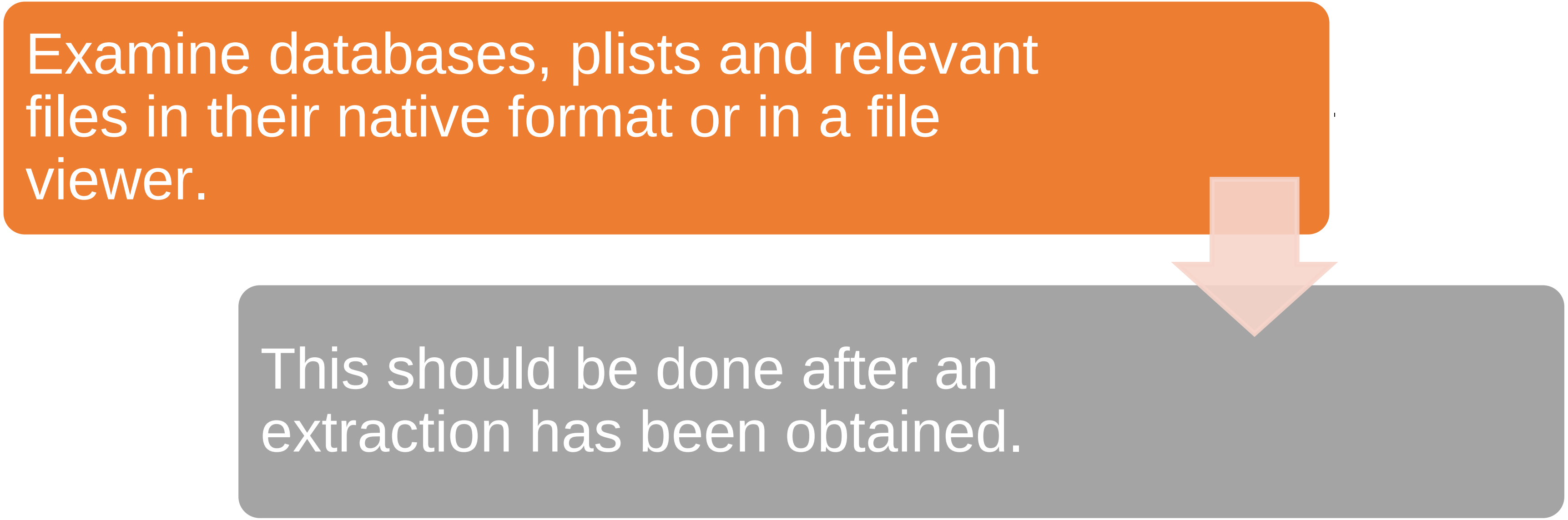
Types:

- Visual
- Cross-Tool
- Call Data Records
- CCTV
- Carving
- Replication

Follow the source file for the artifact

- The source should be identified and reported if the artifact is important to your investigation.
- The source file should be followed and verified for critical evidence.
- The source should be provided for future validation/verification purposes.
- On encrypted devices, tracing the data to its source hex data, is not trivial. Be prepared to answer questions on why decoded data can not be viewed in hex viewer in the raw data dump. The same might apply on translation layers as well.

Explore relevant files



Examine databases, plists and relevant files in their native format or in a file viewer.

This should be done after an extraction has been obtained.

Validate timestamps

Are the timestamps shown in the device local time or UTC?

Cross check for daylight saving time, time zone changes, time sync, etc.

Know where the timestamp comes from (handset vs mobile network).

Time zones can be tricky. Make sure you do not assume the user stayed in one location.

Make sure your tool is extracting relevant timestamps.

Verify on the device, if necessary.

Don’t fear the hex!

Don’t fear Hex and know how to keyword search in Hex.

If you are not familiar with looking at raw data with Hex viewers, find training that will further your understanding in this area.

This applies to other structures found on mobile devices including SQLite databases, plists, Realm and Level databases, Protobuf and others you may encounter on the device.

Reach out to support

Reach out for support and to get your questions answered (there is no stupid question as the field is wide and changing rapidly).

Be sure to use tool vendors support for any product-specific questions you have.

Reach out to the community

- SANS Listserv
- Digital Forensics Discord Server
- Twitter
- Other listservs and groups (IACIS, HTCIA, etc)

Create test data

Create test data to replicate your findings when the data may cause confusion.

Even more important when cross time zone data exists, you are reporting on/researching a non-supported application or when you have found “the smoking gun” and want to be sure to corroborate using all available sources of information.

Note taking

Take ample notes pertaining to validation steps taken.

Retain documentation

Retain all research and documentation created should it be required to be provided or referred to at a later stage by a third party.

Understand Recovered Data

Ensure understanding of recovered data.

Not all recovered data is user deleted.

A great reference for this is: Standardization of File Recovery Classification and Authentication

Questions