Introduction to Digital Evidence

Prof. Josh Brunty
Department of Forensic Sciences
Marshall University

What is Digital Forensics?

Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in *digital evidence*, often in relation to computer crime.

Image credit: Marshall University Digital Forensics Laboratory

Digital Forensics ***IS*** a Scientific Process

- Like many other specializations within forensic science, the digital/multimedia discipline has been challenged with respect to demonstrating that the processes, activities, and techniques used are sufficiently *scientific.*
- In practice, digital/multimedia evidence serves investigative, procedural, and scientific functions, and the outcomes of these multiple modalities are synthesized into expert opinions and conclusions.

Image credit: Marshall University Digital Forensics Laboratory

Organization of Scientific Area Committees (OSAC)

- Created in 2014, part of an initiative by NIST and the Department of Justice to strengthen forensic science in the United States.
- The organization is a collaborative body of more than 600 forensic science practitioners and other experts who represent local, state, and federal agencies; academia; and industry.

Image credit: NIST

MARSHALL

Organization of Scientific Area Committees (OSAC)

- NIST has established OSAC to create a sustainable organizational infrastructure that produces consensus documentary standards and guidelines to improve quality and consistency of work in the forensic science community.

Image credit: NIST

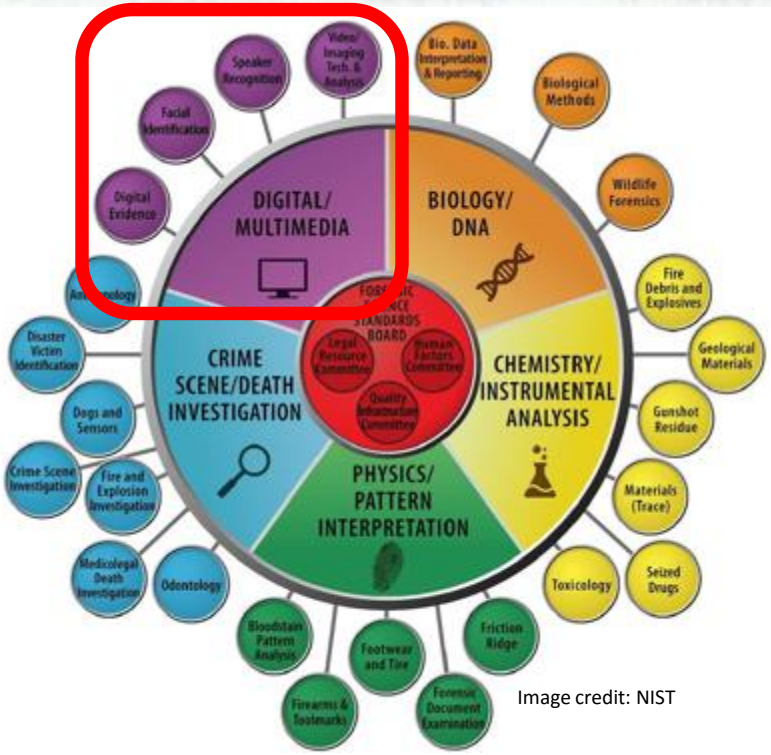
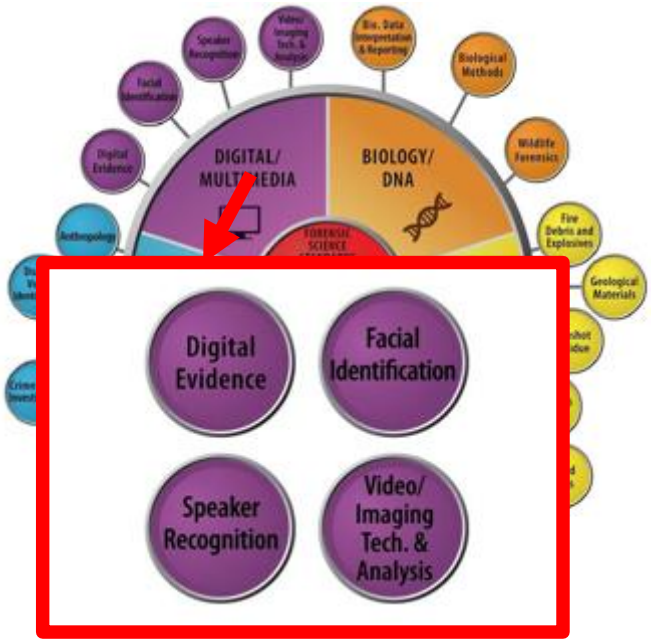


Image credit: NIST

https://www.nist.gov/topics/forensic-science/organization-scientific-area-committees-osac

To understand the scientific foundations of digital/multimedia evidence and how this fits into forensic science, it is necessary to consider the specializations of digital/multimedia evidence. Digital/multimedia evidence encompasses the following sub-disciplines, which are organized according to the current OSAC structure:

- Digital/Multimedia Evidence
- Speaker Recognition
- Facial Identification
- Video/Image Technology & Analysis



Digital Evidence

- Digital/Multimedia evidence involves handling digital traces for forensic purposes, including classification and identification of items, activity reconstruction, detection of manipulation (e.g., authentication of digital document, concealment of evidence).
- Within the current OSAC structure, audio recordings are treated as a form of digital evidence for enhancement and authentication purposes.

Image credit: Marshall University Digital Forensics Laboratory

Facial Identification

- Facial Identification involves the handling of photographs and videos containing an unknown face for comparison with facial images in a database or with a known subject for forensic identification purposes.
- Facial identification methods have been validated through empirical studies and found to be accurate.

Image credit: Marshall University Digital Forensics Laboratory

Speaker Recognition

- Speaker Recognition involves handling voice recordings in analog or digital form, including comparison of voice recordings with a known speaker for forensic purposes, comparison of voice recordings of unknown speakers, counting the number of speakers on a voice recording, and segmenting a voice recording into segments by speaker (“diarization”).

Image credit: Marshall University Digital Forensics Laboratory

Speaker Recognition

- In addition, principles developed for testing the performance of speaker recognition software have evolved into an international standard for all biometric modalities and applications.

Image credit: Marshall University Digital Forensics Laboratory

Video/Image Technology & Analysis

- Video/Image Technology & Analysis involves the handling of images and videos for forensic purposes. This includes classification and identification of items, such as comparing an item in an image or video with a known item (e.g., car, jacket).

Image credit: Marshall University Digital Forensics Laboratory

Video/Image Technology & Analysis

- This also includes authentication of images and videos, metadata analysis, Photo Response Non-Uniformity (PRNU) analysis, image quality assessment, and detection of manipulation.
- Operational techniques include image and video enhancement and restoration.

Image credit: Marshall University Digital Forensics Laboratory

Many Different Tools… Many Different Methods…

- No single forensic acquisition tool can obtain all of the data on a phone or digital device, especially if it has been deleted.
- To get necessary data, an examiner may turn to a variety of tools and processes.
- Even though litigators have familiarity with many of these tools, knowing “why” the examiner used that particular tool or method may be just as important.

Image credit: Marshall University Digital Forensics Laboratory

Get Granular: Knowing the Methods & the Tools…

To these ends, any examiner should be prepared to discuss:

- what tools he/she uses
- whether he/she is certified and/or trained to use the tools
- how often he/she validates and tests the tools
- how he/she handles chain of custody
- how he/she documents his/her processes
- where these processes/practice were taken from (i.e., SWGDE, OSAC Registry)

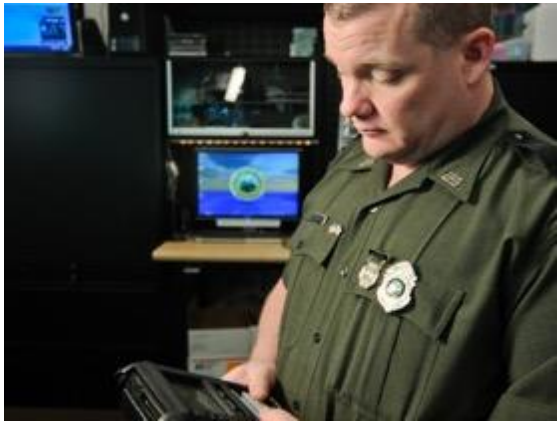


Image credit: Marshall University Digital Forensics Laboratory

Get Granular: Knowing the Methods & the Tools…

- A good examiner will document everything he/she did to recover and extract data.
- Good documentation of the process will look like a narrative of what was done.
- Things such as: make, model, serial numbers, software versions should be included for evidentiary items, hardware/software tools used, and collection repositories.
- This historical data may be valuable in older capital case litigation, where data was not accessible during initial trial, but technological advances allow such access much later (i.e. encryption/password bypass or chip-read in mobile device forensics).

Image credit: Marshall University Digital Forensics Laboratory

Scientific Working Group on Digital Evidence (SWGDE)

- The Scientific Working Group on Digital Evidence (SWGDE) brings together organizations actively engaged in the field of digital and multimedia evidence to foster communication and cooperation as well as to ensure quality and consistency within the forensic community.

http://www.swgde.org

MARSHALL

Scientific Working Group on Digital Evidence (SWGDE)

- SWGDE focuses on the development and publishing of cross-disciplinary guidelines and standards for the recovery, preservation, and examination of digital evidence, including audio, imaging, and electronic devices.
- SWGDE also serves as a forum to discuss, share, and evaluate methods, training, and research to enhance the digital evidence field.

http://www.swgde.org

MARSHALL

OSAC Registry

- The OSAC Registry is a published repository of consensus standards, best practices, and other guides that members of the respective OSAC subcommittee and standards board have recommended for inclusion.

Image credit: NIST

https://www.nist.gov/topics/forensic-science/organization-scientific-area-committees-osac/osac-registry

OSAC Registry

- Many existing standards are not included on the OSAC Registry. That does not necessarily mean that OSAC considers them invalid. The absence of a standard from the Registry may simply mean that the standard has not yet been recommended, or that it meets only some of OSAC's criteria for inclusion.
- To exemplify, some, but not all, documents from SWGDE are included in the OSAC Digital Evidence Registry.

OSAC REGISTRY

OSAC

Image credit: NIST

https://www.nist.gov/topics/forensic-science/organization-scientific-area-committees-osac/osac-registry

MARSHALL