Priority Action Report

Digital Evidence

Digital / Multimedia SAC

James Darnell

2/13/2017

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

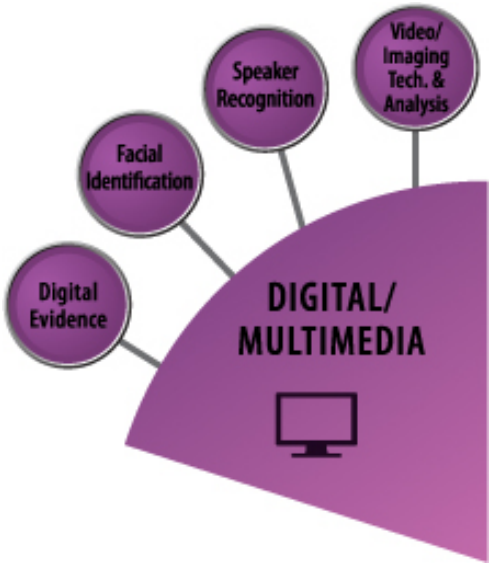
Subcommittee Leadership

Position	Name	Organization	Term	Email
Chair	James Darnell	U.S. Secret Service	2	james.darnell@usss.dhs.gov
Vice Chair	John Duckworth	U.S. Postal Investigation Service	2	jduckworth@uspsoig.gov

Subcommittee Members

#	Name	Organization	Term	Email
1	Bill Eber	Department of Defense	2	buzzbill@gmail.com
2	Mark Phillips	Johnson County Sheriffs Office	4	mark.phillips@jocogov.org
3	Mary Horvath	Federal Bureau of Investigation	4	mary.horvath@ic.fbi.gov
4	Ryan Pittman	NASA, OIG	4	ryan.d.pittman@nasa.gov
5	Sabrina Feve	U.S. Atty Office, San Diego, CA	3	sabrina.feve@usdoj.gov
6	Ovie Carroll	Department of Justice	4	ovie.carroll@usdoj.gov
7	Dave Hallimore	Houston Forensic Science Ctr	4	forensicaudio@gmail.com
8	Jeff Taylor	Arkansas State Crime Lab	4	jeff.taylor@crimelab.arkansas.gov
9	Jim Lyle	NIST	3	Jlyle@nist.gov
10	Marcus Rogers	Purdue University	3	rogersmk@purdue.edu
11	Joshua Brunty	Marshall University	4	josh.brunty@marshall.edu
12	James Adam Holland	Wal-Mart Stores, Inc.	3	James.A.Holland@walmart.com
13	David Papagiris	Iron Mountain	2	David.Papargiris@ironmountain.com
14	Joseph Cassilly	State's Atty, Harford County, MD	2	jicassilly@harfordcountymd.gov
15	Daren Ford	Weld County Sheriff's Office	2	dford@co.weld.co.us
16	Paul Reedy	Washington D.C. Lab	3	paul.reedy@dc.gov
17	Steve Watson	VTO Labs	2	stevewatson@vtolabs
18	Andrew Neal	TransPerfect	2	aneal@transperfect.com

Discipline Description



The Digital Evidence Subcommittee focuses on standards and guidelines related to information of probative value that is stored or transmitted in binary form.

Summary of Standards/Guidelines Priority Actions

Priority	Working Title of Document
1	Framework of a Quality Management System for Digital and Multimedia Evidence Forensic Science Service Practitioners
2	Establishing Confidence in Digital Forensics Results by Error Mitigation Analysis
3	ASTM E2678-09 Standard Guide for Education and Training in Computer Forensics
4	Forensic Audio Examination, Retrieval, Workflow; new standards derived from SWGDE Best Practices for Forensics Audio (3 new documents)
5	Best Practices for Preservation, Isolation, Acquisition of Mobile and other Embedded Systems, three new guidelines derived from NIST SP 800-101 Revision 1 - Guidelines on Mobile Device Forensics

Standards/Guidelines Development Priority 1 Document

Document Title: Framework of a Quality Management System for Digital and Multimedia Evidence Forensic Science Service Practitioners

Scope: This document proposes minimum requirements regarding training/education, examiner certification, examination requirements and lab requirements

Objective/rationale: Describe the minimum requirements necessary to achieve quality assurance in regard to completing digital evidence forensic examinations

Issues/Concerns: The minimum bar may be too high for some to achieve

Task Group Name: Training/Certification
Task Group Chair Name: Andrew Neal
Task Group Chair Contact Information:
aneal@transperfect.com
Date of Last Task Group Meeting: 1/10/2017

National Institute of Standards and Technology
U.S. Department of Commerce

Standards/Guidelines Development Priority 1 Document

Key Components of Standard:

- Employment Qualifications
- DME Training / Certification
- Apprenticeship
- Ongoing Training
- Competency and Proficiency Assessments
- Laboratory Standards
- Examination Procedures
- Review
- Reporting

Task Group/Subcommittee Action Plan

Planned Actions	OSAC Process Stage (e.g., SDO 100)	Assignee	Estimated Completion Date
Assess SWGDE's revisions that were requested by OSAC, DE Sub	SDO 100	Andrew Neal	8/1/2017
Continue to seek DMSAC and resource committee review			
If acceptable to OSAC, encourage SWGDE to push to SDO			
Once published by SDO, seek acceptance into OSAC Registry			

Standards/Guidelines Development Priority 2 Document

Document Title: Establishing Confidence in Digital Forensics Results by Error Mitigation Analysis

Scope: This document presents an error mitigation analysis process for practitioners

Objective/rationale: The purpose of this document is to provide a process for recognizing and describing both errors and limitations associated with tools used to support digital forensics

Issues/Concerns: Gaining acceptance by the courts

Task Group Name: Training/Certification
Task Group Chair Name: Andrew Neal
Task Group Chair Contact Information:
aneal@transperfect.com
Date of Last Task Group Meeting: 1/10/2017

National Institute of Standards and Technology
U.S. Department of Commerce

Standards/Guidelines Development Priority 2 Document

Key Components of Standard:

- Error mitigation analysis
- Error mitigation techniques
  - Tool testing
  - Performance verification
  - Training
  - Review

Task Group/Subcommittee Action Plan

Planned Actions	OSAC Process Stage (e.g., SDO 100)	Assignee	Estimated Completion Date
Assess SWGDE's revisions that were requested by OSAC, DE Sub	SDO 100	Andrew Neal	8/1/2017
Continue to seek DMSAC and resource committee review			
If acceptable to OSAC, encourage SWGDE to push revision to SDO			
Once published by SDO, seek acceptance into OSAC Registry			

Standards/Guidelines Development Priority 3 Document

Document Title: ASTM E2678-09 Standard Guide for Education and Training in Computer Forensics

Scope: This standard is specific to the computer forensics sub discipline of digital and multimedia evidence.

Objective/rationale: Improve and advance computer forensics through the development of model curricula consistent with other forensics science programs

Issues/Concerns: Work with organizations to adopt the model curricula

Task Group Name: Education
Task Group Chair Name: Marcus Rogers
Task Group Chair Contact Information:
rogersmk@purdue.edu
Date of Last Task Group Meeting: 7/10/2016

National Institute of Standards and Technology
U.S. Department of Commerce

Standards/Guidelines Development Priority 3 Document

Key Components of Standard:

- Qualifications
- Core Competencies
- Model curriculum
- Implementation including assessment, faculty, and facilities

Task Group/Subcommittee Action Plan

Planned Actions	OSAC Process Stage (e.g., SDO 100)	Assignee	Estimated Completion Date
Continue to seek DMSAC and resource committee review	RA-100	Marcus Rogers	4/1/2017
Send proposed edits to ASTM committee to update standard			
Once updated by SDO, seek acceptance into OSAC Registry			

Standards/Guidelines Development Priority 4 Documents

Document Title: Forensic Audio Examination, Retrieval, Workflow, three new standards derived from SWGDE Best Practices for Forensics Audio

Scope: These documents will comment on only those matters that may effect the audio forensic examination process

Objective/rationale: Provide forensic audio practitioners recommendations for the handling and examination of forensic audio evidence

Issues/Concerns: None

Task Group Name: Audio
Task Group Chair Name: David Hallimore
Task Group Chair Contact Information:
forensicaudio@gmail.com
Date of Last Task Group Meeting: 1/10/2017

Standards/Guidelines Development Priority 4 Documents

Key Components of Standard:

- Audio Laboratory Considerations
- Evidence Retrieval
- Receiving Evidence
- Examination
- Administrative and Technical Review

Task Group/Subcommittee Action Plan

Planned Actions	OSAC Process Stage (e.g., SDO 100)	Assignee	Estimated Completion Date
Original document broken into three sections; SWGDE to complete drafts using ASTM template	SD-100	David Hallimore	8/1/2017
Complete SDO packet and submit to DMSAC for review			
Review any DMSAC/resource committee edits			
Send to SDO			
Once published by SDO, seek acceptance into OSAC Registry			

Standards/Guidelines Development Priority 5 Documents

Document Title: Best Practices for Preservation, Isolation, Acquisition of Mobile and other Embedded Systems, three new guidelines derived from NIST SP 800-101 Revision 1 - Guidelines on Mobile Device Forensics

Scope: Organizations should find these documents helpful in establishing their policies and procedures.

Objective/rationale: Help organizations evolve appropriate policies and procedures for dealing with mobile devices and to prepare forensic specialists to conduct forensically sound examinations involving mobile devices.

Issues/Concerns: None

Task Group Name: Mobile Devices
Task Group Chair Name: Steve Watson
Task Group Chair Contact Information:
forensics@stevewatson.net
Date of Last Task Group Meeting: 1/10/2017

National Institute of Standards and Technology
U.S. Department of Commerce

Standards/Guidelines Development Priority 5 Documents

Key Components of Standard:

- Forensic tools and classification system
- Preservation
- Acquisition
- Examination and analysis
- Reporting

Task Group/Subcommittee Action Plan

Planned Actions	OSAC Process Stage (e.g., SDO 100)	Assignee	Estimated Completion Date
Original document broken into three sections; DE subcommittee to complete drafts using ASTM template	SD-100	Steve Watson	8/1/2017
Complete SDO packet and submit to DMSAC for review			
Review any DMSAC/resource committee edits			
Send to SDO			
Once published by SDO, seek acceptance into OSAC Registry			

Summary of Standards/Guidelines Priority Actions

Priority	Working Title of Document(s)
1	Framework of a Quality Management System for Digital and Multimedia Evidence Forensic Science Service Practitioners
2	Establishing Confidence in Digital Forensics Results by Error Mitigation Analysis
3	ASTM E2678-09 Standard Guide for Education and Training in Computer Forensics
4	Forensic Audio Examination, Retrieval, Workflow; new standards derived from SWGDE Best Practices for Forensics Audio (3 new documents)
5	Best Practices for Preservation, Isolation, Acquisition of Mobile and other Embedded Systems; new guidelines derived from NIST SP 800-101 Revision 1 - Guidelines on Mobile Device Forensics (3 new documents)

Standards/Guidelines Reviewed For Technical Merit

Title	Developing Organization	Status*	OSAC Process Stage (e.g., RA 100)
Framework of a Quality Management System for Digital and Multimedia Evidence Forensic Science Service Practitioners	ASTM	Complete revisions and move through SDO Process	SD-100
Establishing Confidence in Digital Forensics Results by Error Mitigation Analysis	ASTM	Complete revisions and move through SDO Process	SD-100
ASTM E2678-09 Standard Guide for Education and Training in Computer Forensics	ASTM	Complete revisions and update SDO	RA-100

Additional Items of Interest

- Short Term
  - SDO and tech merit forms completed
  - TGs working with both SWGDE and OSAC DE Sub revisions
  - Move through SDO/Registry process

- Long Term
  - Lab accreditation
  - Method / process validation
  - National examiner certification

Priority Action Report

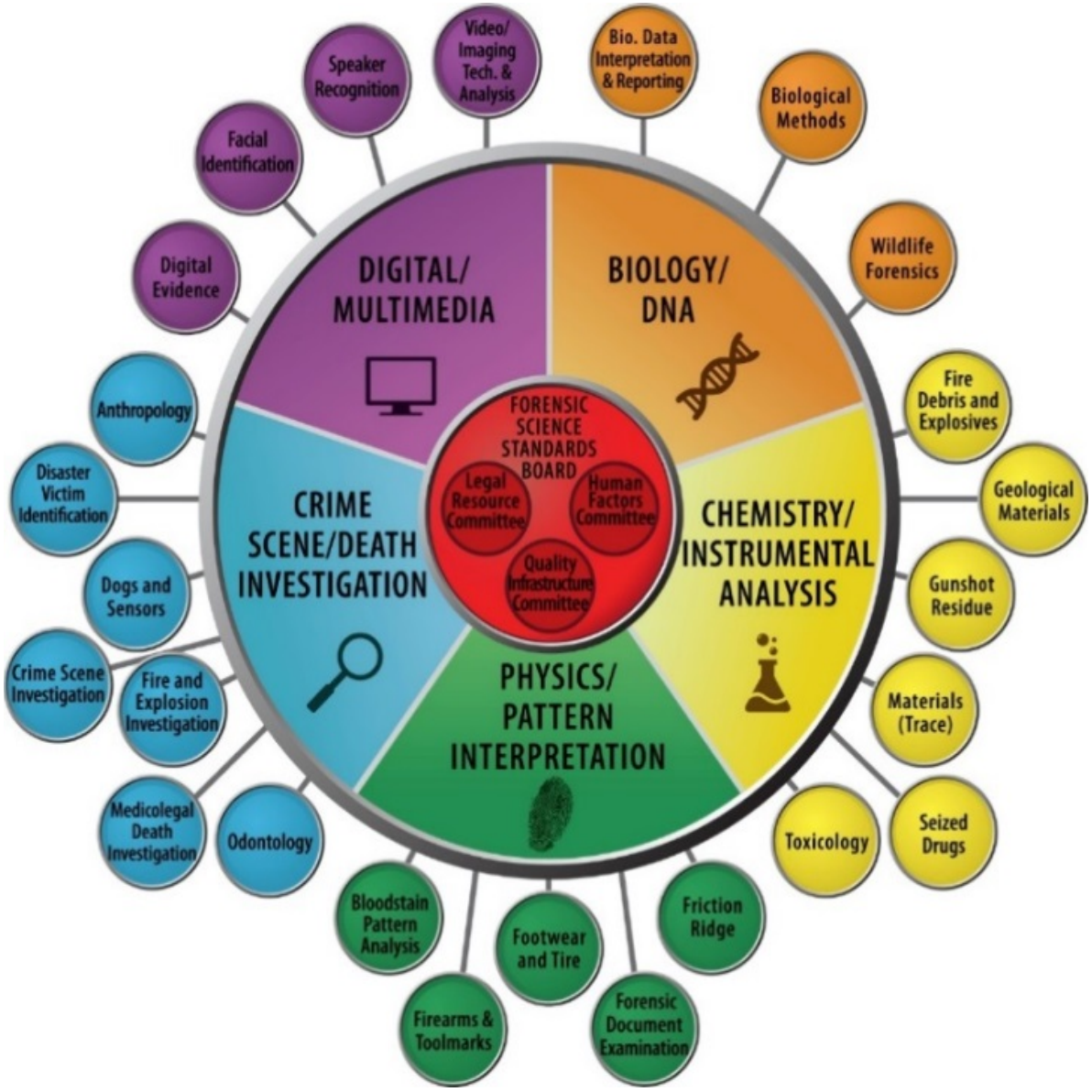
Digital Evidence

Digital / Multimedia SAC

James Darnell

2/13/2017

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



National Institute of Standards and Technology
U.S. Department of Commerce