Scientific Working Group on Digital Evidence

SWGDE Guidance for DME Labs on Addressing ANAB's 2020 Update on Field Sampling

f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for suggested modification

Intellectual Property:
Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

Scientific Working Group on Digital Evidence

SWGDE Guidance for DME Labs on Addressing ANAB's 2020 Update on Field Sampling

Table of Contents

1. Purpose

To provide guidance on aligning and developing policies and procedures that address the requirements for Field Sampling as part of an ANAB Scope of Accreditation under ISO/IEC 17025:2017 or ISO/IEC 17020:2012.

This document provides a mapping between how ANAB is defining Field Sampling and terms and activities familiar to the DME discipline. Once this mapping is understood, DME labs should be able to address Field Sampling as a scope of ANAB accreditation.

2. Scope

The scope of this guidance document is applicable to organizations seeking or maintaining accreditation from ANAB with a scope of accreditation that includes Field Sampling.

3. Background

Sampling is addressed in ISO/IEC 17025:2017 Section 7.3 and ISO/IEC 17020:2012 Section 7.1.2 and has been consistently considered outside the scope of the Digital and Multimedia Evidence (DME) disciplines by accreditation bodies including ANAB. However, on September 24, 2020, ANAB issued Guidance Document (GD) 3064, Forensic Guidance Document-Drafting a Scope of Accreditation, and applied the Sampling definition from ISO/IEC 17000:2020 ("collection of material and/or data") to all disciplines seeking accreditation under ISO/IEC 17020 or 17025 in the following guidance for the Field Sampling "Component/Parameter" scope of accreditation:

- Performed at a location other than the physical location listed on the scope of accreditation.
- Sampling - Selection of a sample for testing or inspection, according to a procedure (ISO/IEC 17000, modified). The approach to sampling can be either non-statistical or statistical.
    - Selection can be performed by different people in the same or different disciplines.
    - Collection can be part of selection but is not required. If collection of items occurs by the accredited forensic service provider, then Field Sampling will be listed on the scope of accreditation.
    - If the accredited forensic service provider selects sample(s) to be collected and the collection is conducted by another party, then Field Sampling will be listed on the scope of accreditation.

Until issuing GD 3064 in September 2019, ANAB offered the DME discipline scopes of accreditation that generally aligned with ISO/IEC 27037:2012 (Guidelines for the identification, collection, acquisition of digital evidence).

However, GD 3064 terms and definitions are aligned with ISO/IEC 17000:2020 and ASTM E2916 for the DME disciplines as it relates to Sampling and its applicability to the DME disciplines, as well as acquisition/extraction of digital data. Neither identification nor collection are defined in these documents. Therefore, ANAB classified these as Field Sampling which

refers to activities that occur outside of the location on an organization's scope of accreditation (i.e., laboratory facility or remote collections of data).

GD 3064 also provides a framework for defining how remote work and remote workers may be classified as performing Field Sampling as well as identifying activities that are laboratory administrative and support services that would fall outside of the scope of accreditation (*See* GD 3064 "How to Draft a Scope of Accreditation," page 1, bullet 3 "What is not a 'location' listed on the scope of accreditation").

Given the long history of Sampling being classified as not applicable to DME disciplines, which remains the case with other accreditation bodies (e.g., A2LA), this document is intended to provide guidance on aligning quality management systems in the DME disciplines with ANAB's definitions around the Field Sampling scope of accreditation.

4. Terms and Definitions: Bridging the Gap

This section provides a mapping between the GD-3064, ISO/IEC 17000:2020, and ASTM E2916 terms and definitions and their applicability to the DME discipline and the ISO/IEC 27037:2012 for:

- Sampling: The selection and/or collection of material or data regarding an object of conformity assessment. Note 1: Selection can be on the basis of a procedure, an automated system, professional judgement, etc. Note 2: Selection and collection can be performed by the same or different persons or organizations. (ISO/IEC 17000:2020 Section 6.1)
- Selection: The identification of data or devices as potential sources of digital evidence which may be acquired and/or collected. (ANAB GD 3064: 2020/09/24 - as interpreted for this document)
- Acquisition: The process of creating a copy of data within a defined set. Note 1: The product of an acquisition is a potential digital evidence copy. (ISO/IEC 27037:2012 Section 3.1)
- Collection: The process of gathering the physical items that contain potential digital evidence. (ISO/IEC 27037:2012 Section 3.3)
- Identification: The process involving the search for, recognition and documentation of potential digital evidence. (ISO/IEC 27037:2012 Section 3.12)

5. Common Scenarios

The following common scenarios illustrate how Field Sampling may apply to DME labs accredited by ANAB or seeking such accreditation. Appendix A describes types of activities that map to Field Sampling for identification and collection, and those activities that may fall under the Acquisition/Extraction scope of accreditation.

5.1 Incident Response Location

If lab personnel go to an incident response location and identify which digital devices should be collected or imaged, this is Field Sampling (identification). Creating an image onsite is

acquisition. Bringing the image or computers/media back to the lab is Field Sampling (collection).

5.2 Advising Incident Responders Remotely

If lab personnel remotely advise those at an incident response location about how to identify and/or collect specific items or data (i.e., via phone call, video call), this may be Field Sampling (identification and/or collection). General advice and guidance on identifying devices or physical collection methods (e.g., whether to turn off a phone or unplug a device) is general advice and not Field Sampling.

5.3 Remote Identification

Prior to acquiring data from a network environment, lab personnel may traverse the network to locate and identify data to be acquired. When this activity is conducted on a network controlled by the organization, this is not Field Sampling. When lab personnel traverse a network not controlled by the lab's organization, this is Field Sampling. Note: The process for identifying data relevant to the customer's request may include applying filters, search terms, date ranges, and other techniques to focus on the data to be acquired. These activities fall within the definition of Field Sampling (identification).

5.4 Remote Acquisition

When lab personnel collect data via a network this activity falls under the Acquisition/Extraction scope of accreditation. It is not Field Sampling.

5.5 Device delivered to Lab

If lab personnel receive a device from non-lab personnel for acquisition and analysis, this is not Field Sampling.

6. What does this mean to me and how do I deal with it?

Briefly, organizations that opt to add Field Sampling to their ANAB scope of accreditation should ensure that their management system addresses at least the following requirements:

- Have a written procedure for Field Sampling activities for:
  - Identification of physical items or digital data stored virtually
  - Collection of physical items
  - Preservation of physical items and digital data
  - (*See* ISO/IEC 17025:2017 Sections 7.2 and 7.4)
- Maintain records of Field Sampling activities, to include dates, identification of personnel and methods/equipment involved, and diagrams, sketches, and/or photos (*see* ISO/IEC 17025:2017 Section 7.3)
- Report Field Sampling activities, including any environmental conditions during the field sampling activities that impacted results (*see* ISO/IEC 17025:2017 Section 7.8.3.2 and 7.8.5)

For organizations that do NOT include Field Sampling to their scope of accreditation but may occasionally perform one or more of the activities described in the questions at the beginning of this section, the lab should identify those activities as outside the scope of their accreditation in accordance with ANAB policies.

APPENDIX A - Table of Example Scenarios

ANAB Scope of Accreditation for Field Sampling				
Scenario Examples	**Field Sampling?**	**Field Sampling Activity**	**Extract /Acquire**	**Notes**
Testing inside Laboratory	No	NA	NA	Lab location is on the Scope of Accreditation.
Activities Outside of Location on Scope of Accreditation (GD-3064)				**Includes scenarios for remote workers (see below).**
Incident Response Location – Lab Personnel Identifying	Yes	Identification	No	Lab personnel identify what to collect.
Incident Response Location – Lab Personnel Collecting Physical	Yes	Collection	No	Lab personnel collect physical items.
Incident Response Location - Lab Personnel Onsite Directing Identification	Yes	Identification	No	Lab personnel physically present and applying professional judgement to guide non-technical personnel on identification of items that may be relevant to the customer's request or legal authority.

Incident Response Location – Lab Personnel Onsite Directing Collection	Yes	Collection	No	Lab personnel physically present and applying professional judgement to guide non-technical personnel on collection of items that may be relevant to the customer's request or legal authority.
Incident Response Location - Lab Personnel Not Onsite Guiding Identification	Yes	Identification	No	Lab personnel not physically present, but are viewing the scene virtually (e.g., Facetime) and applying professional judgement to guide non-technical personnel on identification of items that may be relevant to the customer's request or legal authority.
Incident Response Location – Lab Personnel Not Onsite Directing Collection	Yes	Collection	No	Lab personnel not physically present, but are viewing the scene virtually (e.g., Facetime), and applying professional judgement to guide non-technical personnel on collection of items that may be relevant to the customer's request or legal authority.
Incident Response Location – Lab Personnel Not Onsite but providing general guidance	No	NA	NA	Providing general guidance and not directing identification nor collection of specific items.
Incident Response Location – Lab Personnel Onsite Imaging to External Media	Yes	Identification Collection	Extract /Acquire	Identifying data to be extracted/acquired. Collecting the physical external media use to extract/acquire.

Incident Response Location – Lab Personnel Imaging via network to lab or another controlled virtual environment	Yes	Identification	Extract /Acquire	Nothing physically collected.
Work from Home - Lab Personnel Traversing a Network to Identify and Acquire Data (virtual data)	Yes	Identification	Extract /Acquire	Assumes that the employee used approved network connections to identify, collect, and extract/acquire data.
Work from Home – Lab Personnel Testing Activities (physical devices)	Yes	NA	Extract /Acquire	If the physical item is delivered no identification or collection has occurred.
Work from Organization Controlled Space Outside Lab Scope of Accreditation for Location (virtual data)	Yes	Identification	Extract /Acquire	If the item is delivered no identification or collection may have occurred.
Work from Organization Controlled Space Outside the Lab's Scope of Accreditation for Location (physical devices)	Yes	NA	Extract /Acquire	If the physical item is delivered no identification or collection has occurred.

SWGDE Guidance for DME Labs on Addressing ANAB's 2020 Update on Field Sampling

History

Revision	Issue Date	Section	History
1.0 DRAFT	2021-06-17	Quality	Initial draft created and voted by SWGDE for release as a Draft for Public Comment
1.0	2022-01-13	Quality	Document voted for release as final publication