Scientific Working Group on Digital Evidence

Best Practices for Radio Frequency Propagation Surveys

SWGDE 25-F-003-2.0

The version of this document is in draft form and is being provided for comment by all interested parties for a minimum period of 60 days.

Disclaimer Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish standards, requirements, best practices, guidelines, technical notes, positions, and considerations in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

SWGDE requests notification by email before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in such proceeding. The notification should include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be submitted via the SWGDE Notice of Use/Redistribution Form or sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, deprecated, or sunsetted. Readers are advised to verify on the SWGDE website (https://www.swgde.org) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

Redistribution Policy

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain this SWGDE cover page containing the Disclaimer Regarding Use.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or creation date) of the document and also indicate if the document is in a draft status.

Requests for Modification

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be submitted via the SWGDE Request for Modification

DRAFT

Form or forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of any suggested modification:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) SWGDE Document title and version number
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

All images, tables, and figures in SWGDE documents are developed and owned by SWGDE, unless otherwise credited.

Unauthorized use of the SWGDE logo or document content, including images, tables, and figures, without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or overrepresent 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.

DRAFT

Scientific Working Group on Digital Evidence

Best Practices for Radio Frequency Propagation Surveys

Table of Contents

1. Purpose **2**
2. Scope **2**
3. Definitions **2**
4. Synopsis **3**
5. Equipment Types **4**
6. Survey Methodologies **5**
6.1 Route or Scenario Survey 6
6.2 Location Survey 6
6.3 Cell Mapping 7
6.4 Surveys at Height 7
6.5 Attenuation 7
6.6 Area Survey 8
6.7 Proactive Survey 8
6.8 Records Verification 8
7. Data Analysis **8**
8. Timeliness **9**
9. Calibration **9**
10. Limitations **9**
11. Recommended Survey Actions **10**
12. Documentation **12**
12.1 Additional Documentation **12**
12.1.1 SDR Scanner Documentation 12
12.1.2 SIM-Based Documentation 12
12.1.3 Installed Mobile Device Applications Documentation 13
13. Future Considerations **13**
14. Additional Resources **13**
15. History **15**

DRAFT

1. Purpose

The purpose of this document is to provide best practices for Radio Frequency Propagation Surveys (RFPS), which includes the information collected, and recommendations on obtaining, interpreting, and analyzing available data.

2. Scope

This document provides recommended guidelines for the acquisition, interpretation, and analysis of RFPS data. The intended audience for this document is practitioners who have training, knowledge, and experience in working with this data, including investigators, analysts, and attorneys. This document is not intended to be a training manual or to replace standard organizational procedures. This document is not all-inclusive and does not account for every possible scenario related to RFPS data, and it should not be confused with historical cell site location information analysis. Refer to *SWGDE 17-F-001-4.0 Best Practices for Historical Cell Site Analysis*.

3. Definitions

The following definitions are provided to assist with interpreting this document. For further details, readers may refer to more technical resources defining these terms, such as the Third Generation Partnership Project (3GPP) and European Telecommunications Standards Institute (ETSI).

- **Band Locking:** Band locking is an equipment-level configuration that restricts a mobile device application or SIM-based survey equipment to operate only on one or more specified frequency bands, preventing it from automatically switching to other available bands, even if those bands are stronger or preferred by the network.
- **Drive Scan Test:** See Radio Frequency Propagation Survey.
- **Handover:** When the network chooses to move an active session on a mobile device from one cell to another. Sometimes called a handoff.
- **Neighboring Cell Sites:** Cell sites that are in close proximity to the target cell site. Neighboring Cell Sites can affect the outer boundaries of a target cell site's serving coverage area.
- **Radio Frequency Propagation Survey (RFPS):** The process of measuring and illustrating the full cellular radio spectrum occupied by 2G through 5G cellular and Wi-Fi technologies in a given area. This method is used by all cellular providers for the purpose of network optimization and can also be used by law enforcement to memorialize and forensically examine the characteristics of a cellular network in a given area.
- **Reselection:** When the mobile device, not actively transferring data, changes to a suitable cell from which to receive administrative and paging messages.

DRAFT

- **Reference Signal Received Power (RSRP):** The standard measure of cellular signal power strength in 4G LTE and 5G networks.
- **Reference Signal Received Quality (RSRQ):** The overall clarity and quality of an LTE or 5G cellular signal by comparing the useful signal strength against total noise and interference.
- **Serving Cell:** The primary cell site(s) providing coverage to specific locations of interest. This can be one singular cell site or multiple secondary cell sites.
- **Survey:** See Radio Frequency Propagation Survey.
- **Technical Review:** A qualified second party's evaluation of reports, notes, data, and other documentation to ensure there is appropriate and sufficient support for the actions, results, conclusions, opinions, and interpretations. Sometimes referred to as a peer review.

4. Synopsis

Radio Frequency Propagation Surveys (RFPS) are sometimes called *drive scans*, *cellular network surveys,* or *drive test scans*. A RFPS is the process of measuring and illustrating the full cellular radio spectrum occupied by 2G through 5G cellular in a given area. This method is traditionally used by all cellular providers for the purpose of network optimization and can also be used by practitioners to memorialize and forensically examine the characteristics of a cellular network in a given area. The survey equipment gathers its own location data via a global navigation satellite system (GNSS) receiver. By conducting a RFPS, cellular service coverage can be determined at locations of interest. RFPSs are performed with equipment such as SIM-based phone emulators, installed mobile device applications, or software-defined radios (SDR), more commonly known as drive test scanners.

With this data, the practitioner can identify the cellular service provider, the Tracking Area Code (TAC), eNodeB/gNodeB, ECGI/NCGI, sector orientation, channels, bands, radio frequencies, and received signal strengths and qualities of cell sites providing coverage to surveyed locations. Some equipment can collect Timing Advance data. This allows a RFPS practitioner to determine the cellular coverage provided at specific locations (a location survey), the service area of a given cell site (a cell coverage survey), and coverage along a route during a specific scenario (a route or scenario survey).

The results of RFPSs can be used in conjunction with Cell Site Location Information (CSLI) as part of historical cell site analysis. RFPS data can show whether it's possible for a device to have been connected to a particular cell site at or near a location of interest at the time of the survey.

5. Equipment Types

Types of RFPS equipment include: SDR, installed mobile device applications, and SIM-based equipment.

Survey equipment based on a software-defined radio receiver operates utilizing software that scans a wide range of radio frequencies. This equipment is passive in nature and only acts as a receiver of signals from cell sites. The SDR scanner cannot make test calls or otherwise connect to the surveyed cellular network. These types of equipment survey the entire geographic area for a specific subset of network providers and technologies (*e.g.*,3G, 4G, & 5G), capturing all channels, bands and frequencies, depending upon the capability of specific survey equipment, up to and including mmWave frequencies. The output of a SDR survey usually consists of details of all serving and non-serving (*e.g.*, neighbor) cell sites detected at a location. SDR equipment uses algorithms to rank serving cells to identify which cell site would be the server and which would be a neighbor. The survey may also include Cell ID, cell site details, signal strength, and quality. Some SDR equipment can decode additional network data, which can be helpful with analysis.

An installed mobile device application is software installed on a test mobile device. Since this is a mobile device, the cellular radios would be the same or very similar to that of a target mobile device. This style of scanning would be limited to the networks assigned to the SIM card(s) or e-SIM(s) installed in the mobile device. The application acts as a network monitor for the mobile device and can provide serving cell measurements, neighboring cell measurements, Timing Advance measurements, GNSS positioning, and data logging. Outside of these basic capabilities, each specific application can provide different capabilities such as test calls, importing cell site lists, different styles of export reports, etc. Different hardware and software can also affect the capabilities of mobile device applications in RFPSs.

SIM-based survey equipment uses the same types of cellular radios used by mobile devices by utilizing SIM cards, similar to those used in consumer mobile devices, which allow it to connect to and conduct RFPSs of the various cellular networks on various technologies. They can be configured to undertake surveys of all technologies on all networks or to target just one specific technology and/or one specific network. SIM-based survey equipment is capable of connecting to the cellular networks, allowing them to both passively survey local cellular coverage and make connections to the cellular network. SIM-based survey equipment is sometimes referred to as a *phone emulator*. Dedicated equipment has multiple radio units and SIMs that can survey multiple networks/technologies simultaneously.

The primary differences between SDR, installed mobile device applications, and SIM-based equipment is related to efficiency and functionality. Some SDR equipment can measure a large portion of the entire cellular environment in just a few seconds, meaning surveys can be conducted very quickly. SIM-based equipment measures the succession of primary serving cell sites for a given network/technology over a period of time, which takes longer to complete. SDR equipment is generally passive and cannot connect to the surveyed network to make test calls or other types of connections, whereas SIM-based equipment has the option to operate in both *idle* (passive) or *connected* (active) modes, giving practitioners the option to confirm the current serving cell by making test calls or establishing data sessions. Both system types have advantages and disadvantages. Practitioners should understand the capabilities and limitations of

their chosen system. Some practitioners advocate a hybrid survey strategy making use of both SDR and SIM-based equipment.

Many RFPS systems can be configured to scan both cellular networks and Wi-Fi networks, to offer a more complete view of the radio resources available at surveyed locations.

6. Survey Methodologies

This section provides a review of the methodologies that can be employed when conducting a RFPS. The specific method used is dependent on the practitioner's data collection goals, the facts of the investigation, and the questions they are seeking to answer.

A survey can be performed to identify which cell sites are likely to provide service along a given route of travel to define the approximate serving coverage area of an identified cell site or sector or to determine if a particular cell site and sector can provide service to a defined location.

Surveys may be able to determine the best serving cell sites for a geographic location. This type of survey includes all serving cells covering a location and may include a rank structure depending on equipment being utilized. Serving cell coverage maps traditionally are generated by cellular network engineers for network planning strategy, as they include a total picture of each network's propagated frequencies. Server maps generated by cellular networks are often created using RF prediction software in lieu of actual field testing.

RFPSs are sometimes called *drive scans, cellular network surveys,* or *drive test scans* because the survey equipment is most commonly mounted in a vehicle to allow the practitioner to cover a larger geographical area more efficiently. When undertaking a vehicle-mounted RFPS, consideration needs to be given to whether the survey equipment's cellular antenna is mounted inside or outside the vehicle (if the equipment offers a choice). There are limitations to each option. Mounting the antenna outside the survey vehicle can offer a better received signal and avoid attenuation caused by the vehicle's body. Mounting the antenna inside the survey vehicle might more closely mimic a mobile device being inside the car, including attenuation caused by the body of the vehicle, which could offer a more realistic emulation of the service provided to the mobile device. It is best practice to follow the manufacturer's instructions on antenna placement.

A walking RFPS is also common if the survey equipment is small enough to be portable. In these surveys, the survey equipment is often carried in a backpack or other bag and controlled by the practitioner using a handheld device, such as a small laptop or tablet. This method can be useful when focusing on a small geographic area or where investigation of cell site coverage at a very specific spot is required, and a survey vehicle cannot be placed there. Indoor surveys would also follow the walking scan methodology.

In any survey involving a static location, care should be taken to maintain the survey equipment in the immediate vicinity of that location for a reasonable period of time, as dictated by the facts

of the case and the equipment being used. This duration should be sufficient to allow the equipment to capture the range of RF conditions that are occurring at the time of the survey.

Each type of survey goal requires a different methodology. This document will seek to provide a recommended methodology for each type of survey.

6.1 Route or Scenario Survey

A route survey is performed to identify which cell site(s) and sector(s) provide service along a defined route or in a defined scenario. In such a scenario, a known or suspected travel route is identified from other information, such as eyewitness testimony, surveillance cameras, or other data sources. A RFPS can identify the sequence of cell sites providing service along that route and be compared to the sequence of cell sites listed in the CSLI provided for a specific device. Route survey results should be retained for later analysis so the serving cell sites can be identified for future legal processes, such as a tower dump, an area search, etc. A survey of this type would be mobile, as the practitioner would need to travel along the defined route, most likely vehicle-based, and would cover the route in question. It is best practice to drive a route in both directions and as slowly as is safely possible to ensure the best chance of detecting the set of serving cell sites.

6.2 Location Survey

A location survey is conducted to identify the set of cell sites and sectors providing service to a specific location or to indicate whether a specific previously identified cell site and sector of interest provide service to a specific location. Location surveys are performed at identified crime scenes, alibi locations, suspect residences, or other locations of investigative interest. A survey of this type would likely cover a smaller geographic area than a route survey and consist of surveying only the immediate area in question. It is recommended that all sides of a building be surveyed, if possible.

The survey should also include the vicinity of the location of interest – the size of the ‘vicinity’ around a location of interest can vary. Widening the area surveyed to include the vicinity will provide details of cells that may have been used shortly before or after an incident occurred. The vicinity is at least partly determined by the subject’s potential mode of travel – if they were walking, the vicinity might be quite small but if they were travelling in a vehicle, the vicinity might be larger. The size of the vicinity should be clearly stated in the accompanying documentation.

When undertaking RFPS in relation to incidents that occurred at an indoor location, practitioners should also consider surveying inside the property, on all floors and rooms, if safe, lawful access is possible. GNSS location data may not be available for an indoor survey. There are techniques that can be used to accommodate this which are beyond the scope of this document.

DRAFT

6.3 Cell Mapping

A RFPS for cell site mapping, also known as a cell coverage survey, can be performed to measure the service area (or serving "footprint") of an entire cell site or sector. In this type of survey, the surveying equipment is moved, either on foot or in a vehicle, throughout the entire possible or suspected service area of the given cell site, allowing the core serving coverage area of the specific cell and the approximate handover areas to neighboring cell sites to be identified. RFPS practitioners should be aware that cell coverage areas can be non-contiguous; there may be gaps in coverage or areas where neighboring cell sites provide serving coverage. The practitioner should ensure that the full extent of the required cell is surveyed. The results of a survey may be processed to create varying illustrations of the collected data. These illustrations for a specific cell can be used to collectively indicate the extent of the area served by that cell.

6.4 Surveys at Height

When RFPSs are performed at ground level, signals from distant cell sites may be attenuated by the clutter of surrounding buildings and geographical features. The coverage measured at an elevated location or on an upper floor of a tall building can differ from the coverage measured at ground level of that building due to the lack of clutter at height. Signals from more distant cell sites may be detectable, and may be a serving cell, at an elevated location. If an incident under investigation occurred at height, the RFPS practitioner should attempt to undertake the RFPS at the same height as the incident location.

6.5 Attenuation

Attenuation is the natural reduction in radio signal strength as it propagates through space or passes through materials such as air, walls, and water. Thus, the extent of coverage measurable for a cell site is often limited by surrounding structures and other obstructions such as geography, buildings, hills, and the curvature of the Earth. These can block and attenuate radio signals, limiting the distance radio signals can travel. RFPS practitioners should be aware that signals transmitted by cell sites located near water often travel further than might be expected due to the lack of obstructions over open water.

Other causes of attenuation include induction along overhead power lines, transmission through transportation tunnels, or others that can result in coverage from cell sites being detected in unexpected areas. If one or more cells consistent with the survey strategy aren't detected during a survey, RFPS practitioners should make efforts to explain how or why the cells in question were not detected.

6.6 Area Survey

A RF area survey can be used to differentiate cell service between two different locations. For example, this technique can be used to indicate the differences or similarities in serving coverage between locations of interest. When the survey is completed, the serving cell sites at each location are compared to see if the service is different at each location.

6.7 Proactive Survey

Proactive radio surveys can be conducted regularly to compile details of the changing (or unchanging) cellular coverage provided to an area or a region. An organization may decide to proactively survey their service area at appropriate intervals to compile a database of historical coverage data that can be used to determine whether the serving coverage of specific cells has changed over time.

A proactive RFPS can also be conducted in advance of large-scale events where temporary portable cellular sites, or Cell on Wheels (COWs), are deployed to accommodate the increase of devices in a specific area. Examples of these events include annual championship sporting events or emergency situations where the cellular network has been damaged. Due to the temporary nature of these events, it becomes necessary to survey the cellular environment for later analysis and comparison to CSLI should an incident occur. RFPS practitioners should coordinate with event personnel to confirm the temporary cells are active.

6.8 Records Verification

A RFPS may be completed to verify the lawfully obtained CSLI. For example, suppose CSLI identifies a particular cell site that was used by a specific device at or around the time of an incident. In that case, a RFPS can be performed to verify the cell site is located in and provides service to that area. It can also be done to confirm whether a particular cell site and sector faces the direction stated in CSLI. For example, if the CSLI states the azimuth of a cell is 90°, a RFPS can be performed to verify the strongest signal from the given sector is located at or near the stated azimuth.

7. Data Analysis

Data collected during a RFPS will vary depending on the equipment used to perform the survey. Collected data can include locations, identifiers of cell sites being measured or connected to, Reference Signal Receive Power (RSRP) and Reference Signal Receive Quality (RSRQ).
It is beyond the scope of this document to provide step-by-step instructions as to how to analyze and interpret the collected RFPS data.

8. Timeliness

The question of when a RFPS can and should be conducted is often contingent upon the facts of the underlying investigation. It is best practice to conduct a RFPS as close in time as practicable to when an incident occurred. This helps to obtain survey data when similar cellular and environmental conditions existed. RFPS practitioners recognize it is impossible to recreate the exact conditions that existed when an incident occurred. A RFPS is a sample of cellular coverage found on the date and at the time the survey is performed. Therefore, conducting the RFPS closest in time to the incident may help to capture similar conditions.

RFPS practitioners are often requested to conduct surveys weeks, months, and even years after an incident occurred. There is still significant value to conducting RFPSs long after an incident

DRAFT

occurred, but the RFPS practitioner needs to recognize the limitations. Known cellular network changes (new cell sites added, old cell sites removed), time of year, and environmental conditions should be considered and documented when conducting a RFPS a significant amount of time after the underlying incident.

If historical survey data is available (*e.g.* from previous surveys or proactive surveys), it is acceptable to use that to demonstrate the historical coverage of cells of interest.

9. Calibration

An SDR scanner shall be calibrated or tested according to manufacturer recommendations and/or agency policy. SIM-based survey equipment does not need to be calibrated; the reasons for this are beyond the scope of this document.

Frequency calibration, which ensures the equipment is surveying the correct radio channels, is handled automatically by the cellular network, recalibrating to a serving cell's frequency multiple times every second.

Power measurement calibration, which ensures the equipment applies the correct power measurements to received signals, isn't possible with the majority of survey equipment. The receiver sensitivity is a fixed consequence of the characteristics of the specific receiver circuitry and cannot be altered. Survey equipment applies the same sensitivity to all received signals, so although two different types of survey equipment might register slightly different received signal strengths for a set of measured cell sites, the set of detected cell sites and their relative signal strength ranking is likely to be proportionally the same for those two types of survey equipment.

10. Limitations

Network configurations, the built environment, and geographic landscapes can change over time, so the practitioner should consider what changes might have occurred, particularly when there is an extended time between the event and the survey. This can be addressed by comparing cell site lists from the time of the incident and the time of the survey in order to determine if network changes have occurred and by determining whether any significant changes in the physical landscape have occurred.

Data collected as part of RFPSs is often stored and maintained by the investigating agency and not submitted to a central repository. Such a central repository of historical RFPS data, whether maintained on a local, state, or national level, could be useful for use in future investigations, but the establishment of such a repository is outside the scope of this document.

SIM-based and SDR equipment both have limitations in their use. SIM-based surveys can result in false negatives, where a cell site that is capable of serving at a location isn't "seen" or detected by the SIM-based equipment. The mitigation for this issue is usually to survey for an extended period and to move within the vicinity of the surveyed location to ensure the maximum opportunity to detect all serving signals.

With SIM-based equipment the device may retain connection from different cell sites depending on the direction the equipment entered the location of interest from. This is due to the serving cell site not meeting the threshold for reselection or handover immediately upon entering the location of interest. SIM-based equipment practitioners should conduct RFPSs entering the location of interest from multiple different directions.

Conversely, SDR equipment is not a normal mobile device and does not interact with the network in the same way a mobile device does. This means SDRs use algorithms to determine whether a specific cell serves at a location and cannot make test connections to confirm the usability of the estimated serving cell sites. Practitioners should be aware of the algorithms used to rank serving cells. A limitation of a SDR is a risk of false positives, where a cell determined as serving may not be.

Installed mobile device app-based surveys are less robust than surveys conducted with SIM-based or SDR-based equipment. They collect less data and are limited to the carrier of the phone on which the app is installed.

These limitations should be mitigated by practitioners receiving comprehensive training.

11. Recommended Survey Actions

A survey conforming to recommended best practice includes the following actions:

- **Comparative Survey Strategy:** Once a mobile device has been identified and corresponding CSLI has been obtained, the practitioner should compile a list of cell sites and locations of interest to survey. The investigation and analysis of a cell site connection at a specific date and time as documented by CSLI may require specific band locking when using SIM-based equipment. Upon completion of the RFPS, the practitioner then conducts a comparative analysis of the gathered data.
    - This analysis answers the following questions:
        - During the RFPS, did the equipment identify the expected cell site(s) in the same or similar manner as documented by the CSLI?
        - Does an expected cell site provide service to the geographic area specific to the case scenario?
        - Does the RFPS data confirm or deny case-specific information?
        - Does the RFPS data confirm the expected configuration of the cell site, i.e. physical location by latitude and longitude or address, sector orientation by azimuth, and beamwidth?

- **Missing Cell Sites:** If expected cell sites aren't detected at a surveyed location, the practitioner should attempt to determine why. They should visit the cell site (if the site location is known) and check to see if the cell can be detected there. If the cell can be detected at the cell site, the practitioner should travel back towards the survey location and note where the serving coverage for that cell ends. If an expected cell can't be detected at the site, the practitioner should check with the network provider to find out whether the cell still exists or had been taken off the air.

- **Survey Data:** Unprocessed copies of the raw survey data should be retained as source evidence in accordance with agency policy and applicable laws and should be available for reprocessing or disclosure if required by the court.

- **Review:** It is recommended that reports, statements, and other products created as a result of RFPSs are reviewed by a competent third party. Technical reviews should be completed to ensure that the conclusions reached in a report are supported by the RFPS results. Technical checks can be completed to ensure that details such as cell IDs, dates/times, signal strength measurements, etc. have been correctly transposed into the report. Each organization that conducts RFPSs may have its own processes and definitions of both of these checking activities, so the specific nature of the checks to be performed are outside the scope of this document.

12. Documentation

Practitioners shall document the methodology used to conduct RFPSs, including where, when, and by whom the data was obtained. Additionally, documentation shall include specifically what data was obtained and how the data was archived.

12.1 Additional Documentation

The wide range of hardware and software used to conduct RFPSs can make it difficult for others to review, validate, or challenge the resulting data. To address this, practitioners shall disclose the details of their data and methodology as set out below.

12.1.1 SDR Scanner Documentation

When using an SDR scanner, practitioners shall provide all locations recorded and all cellular signals identified by the scanner at that location. This unfiltered, original data shall be provided in a readable format such as a text document or CSV file detailing the date, time, location coordinates, the cell site(s) seen at that location, RSRP and RSRQ for the cell site(s) seen at that

DRAFT

location. If data is binned, aggregated, grouped, or averaged into geographic areas, the size of that geographic area and the exact methodology of compiling that data shall be disclosed.

In the event that SDR data is used to create a map, including one utilizing propagation, predictive, extrapolation, or interpolation, practitioners shall provide the base level empirical data described above. Additionally, the methodology in creating the propagation, predictive, extrapolation, interpolation style map shall be disclosed, including any filters or algorithms used to rule in or out cell site usability.

All imagery created as a result of SDR scans shall include a non-proprietary file of the route driven or walked during the scan. If the imagery displays one or more specific cell sites from a scan, it must clearly label the site or sites shown.

12.1.2 SIM-Based Documentation

When using a SIM-based scanner, practitioners shall provide all locations recorded and all cell sites captured by the scanner at that location. This unfiltered original data shall be provided in a readable format such as a text document or CSV file detailing the date, time, location coordinates, cell site(s) captured, RSRP and RSRQ for the captured cell site, whether the device was in idle or connected mode, timing advance values, subcarrier carrier spacing (SCS), and whether any band locking or other type of cell selection/reselection or handoff restriction was used.

All imagery created as a result of SIM-based scans shall include a non-proprietary file of the route driven or walked during the scan. If the imagery displays one or more specific cell sites from a scan, it must clearly label the site or sites shown.

12.1.3 Installed Mobile Device Applications Documentation

When using an installed mobile device application scanner, practitioners shall provide the following scanner details: make and model of the user equipment (UE), the UE operating system, if the UE is rooted, and the mobile device application being used. In addition, the following base-level empirical data shall be provided: identify all GNSS or locations scanned and identify all cell sites captured by the scanner at that location. This unfiltered original data shall be provided in a readable format such as a text document or CSV file detailing the date, time, location coordinates, cell site recorded, RSRP and RSRQ for the recorded cell site, whether the device was in idle or connected mode, timing advance values, and whether band locking or any other type of reselection or handoff restriction deployed.

All imagery created as a result of SDR scans shall include a non-proprietary file of the route driven or walked during the scan. If the imagery displays one or more specific cell sites from a scan, it must clearly label the site or sites shown.

13. Future Considerations

5G mmWave is a wireless communication technology currently using high-frequency electromagnetic waves above 24 GHz. This is also referred to as Frequency Range 2 (FR2), with the more traditional spectrum employed by cellular systems in a range between 410 MHz and 7.125 GHz, known as Frequency Range 1 (FR1). High-frequency mmWave FR2 radio signals are typically usable over shorter distances as compared to FR1 cell site; FR2 cell site will generally be much smaller than traditional lower-frequency cell sites using FR1. mmWave signals do not penetrate buildings as efficiently as lower frequency signals, meaning mmWave/FR2 cell sites transmitted from traditional outdoor sites are less likely to offer indoor coverage. Because of the newness of mmWave technologies, the effects of mmWave/FR2 cell sites on the best practice recommendations for RFPSs are yet to be determined.

14. Additional Resources

- 3GPP. https://www.3gpp.org/. Accessed 14 Jan. 2025.
- Hoy, Joseph. *Forensic Radio Survey Techniques for Cell Site Analysis*. Second Edition, Wiley, 2026.
- Jovanovic, Vladen M., and Brian. T. Cummings. "Analysis of Mobile Phone Geolocation Methods Used in US Courts." *IEEE Access*, vol. 10, 2022, pp. 28037-28052, https://ieeexplore.ieee.org/document/9729192. Accessed 23 Oct. 2025.
- Scientific Working Group on Digital Evidence. *Best Practices for Historical Cell Site Analysis*. SWGDE 17-F-001-4.0, *SWGDE*, 2025, https://www.swgde.org/documents/published-complete-listing/17-f-001-4-0/
- Horan, Kevin R. "Drive Testing in Cellular Analysis: Why Multi-Platform Capability Sets PCA Apart." *Precision Cellular Analysis,* 9 December 2025, https://www.pcaexperts.com/post/drive-testing-in-cellular-analysis-why-multi-platform-capability-sets-pca-apart. Accessed January 12, 2026.
- Griffiths, Martin and Nuttall. "The need for an evolving Radio Frequency Propagation Survey (RFPS) methodology in law enforcement investigations – a hybrid concept." *Forensic Analytics,* 13 March 2024, https://www.forensicanalytics.io/us/knowledge-hub/csas-v3-13-1-enhanced-features-and-performance-1/. Accessed January 12, 2026.

DRAFT

15. History

Revision	Issue Date	History
1.0 DRAFT	1/15/2025	SWGDE voted to release as a Draft for Public Comment.
1.0 DRAFT	2/10/2025	Formatted for release as a draft for public comment.
1.0 DRAFT	10/22/2025	Response to public comments and additional content added. Formatted for release as a draft for public comment.
1.0 DRAFT	1/15/2026	Response to public comments; substantive changes made throughout the document.
1.0 DRAFT	2/18/2026	SWGDE voted to approve as Draft for Public Comment. Formatted for release as a Draft for Public Comment.
1.0	7/16/2026	SWGDE voted to publish as an Approved document (Version 1.0).
2.0 DRAFT	9/2/2026	Section added on Documentation (Section 12).
2.0 DRAFT	9/10/2026	SWGDE voted to approve as Draft for Public Comment. Formatted for release as a Draft for Public Comment

DRAFT