

THE JOURNAL OF  
**DIGITAL FORENSICS,  
SECURITY AND LAW**

**Journal of Digital Forensics,  
Security and Law**

Volume 14 | Number 2


Article 5

6-30-2019

## Forensic Cell Site Analysis: Mobile Network Operator Evidence Integrity Maintenance Research

John B. Minor  
[jminor@johnbminor.com](mailto:jminor@johnbminor.com)

Follow this and additional works at: <https://commons.erau.edu/jdfsl>

 Part of the [Computer Law Commons](#), and the [Information Security Commons](#)

### Recommended Citation

Minor, John B. (2019) "Forensic Cell Site Analysis: Mobile Network Operator Evidence Integrity Maintenance Research," *Journal of Digital Forensics, Security and Law*. Vol. 14 : No. 2 , Article 5. Available at: <https://commons.erau.edu/jdfsl/vol14/iss2/5>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact [commons@erau.edu](mailto:commons@erau.edu).



(c)ADFSL



# FORENSIC CELL SITE ANALYSIS: MOBILE NETWORK OPERATOR EVIDENCE INTEGRITY MAINTENANCE RESEARCH

John B. Minor  
johnbminor.com  
jminor@johnbminor.com

## ABSTRACT

Mobile Network Operator (MNO) and Mobile Virtual Network Operator (MVNO) evidence have become an important evidentiary focus in the courtroom. This type of evidence is routinely produced as business records under U.S. Federal Rules of Evidence for use in the emerging discipline of Forensic Cell Site Analysis. The research was undertaken to determine if evidence produced by operators should be classified as digital evidence and, if so, what evidence handling methodologies are appropriate to ensure evidence integrity. This research project resulted in the creation of a method of determining if business records produced by MNO/MVNO organizations are digital evidence and whether evidentiary integrity is maintained in the conveyance of evidence between MNO/MVNO records custodians, law enforcement investigators and attorneys in criminal and civil cases. Block-chain based Distributed Ledger Technology was examined as a feasible evidence integrity maintenance solution.

**Keywords:** Distributed Ledger Technology, DLT, Block-chain, Openchain, Charging Data Records, Call Data Records, Call Detail Records

## 1. INTRODUCTION

A cell phone subscription in the United States is activated with either a Mobile Network Operator (MNO) or Mobile Virtual Network Operator (MVNO), which includes a variety of business models variously termed Virtual Network Operator or Mobile Other Licensed Operator. MNO/MVNO subscriber activity records, technically defined in 3G standards as Charging Data Records, are “a formatted collection of information about a chargeable event (e.g. time of call set-up, duration of the

call, amount of data transferred, etc) for use in billing and accounting” (ETSI, 2015) and commonly referred to as Call Detail Records (CDR), fall into a class of evidence called digital evidence. This type of evidence has traditionally been introduced in the courtroom as business records evidence. Citing the Federal Rules of Evidence, Rule 803, exceptions to the rule against hearsay, courts have, with rare exception, accepted CDRs as business records evidence. FRE 803 states in part:

“The following are not excluded by the rule against hearsay, regardless of whether the declarant is available as a witness:” . . .

(6) Records of a Regularly Conducted Activity. A record of an act, event, condition, opinion, or diagnosis if:

- (A) the record was made at or near the time by—or from information transmitted by—someone with knowledge;
- (B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit;
- (C) making the record was a regular practice of that activity;
- (D) all these conditions are shown by the testimony of the custodian or another qualified witness, or by a certification that complies with Rule 902 (11) or (12) or with a statute permitting certification; and
- (E) the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness.”

Note that under rule 803, (6), Records of a Regularly Conducted Activity, MNO/MVNO produced evidence including Call Detail Records and other records meet the requirements as business records, if, according to (6)(E) the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness. (Federal Rules of Evidence, 2019) This analysis will test the trustworthiness of MNO/MVNO records production as business records under FRE803(6)(E).

The key questions that this research analysis project seek to answer are: 1) whether MNO/MVNO records should be recognized by courts as digital evidence and 2) whether

the records should be subject to the same fundamental evidence handling standards and rules as any other digital evidence.

The research for this project is based upon patented scientific concepts and peer reviewed research as well as standards derived from the 3<sup>rd</sup> Generation Partnership Project (3GPP), International Organization for Standards (ISO), European Telecommunications Standards Institute (ETSI) and the Internet Engineering Task Force (IETF), The 5G Public Private Partnership (5G-PPP), the American Society for Testing and Materials (ASTM) and the Institute of Electrical and Electronics Engineers (IEEE) .

## 1.1 Digital Evidence Test

A four-part test was devised and applied to MNO/MVNO evidence to determine if this type of evidence should be subject to digital evidence handling and analysis standards. The devised test is as follows:

- Is mobile network subscriber communications activity record keeping a computer driven digital process?
- Are subscriber communications activity records maintained by MNOs/MVNOs and extracted for litigation purposes classified as digital evidence?
- Is this type of evidence subject to digital evidence handling standards?
- Do the same rules for spoliation determination apply to this type of evidence?

When applied to a control group of MNO/MVNO records produced as evidence from a pool of 100 civil and criminal cases the four-part test resulted in a positive determination that this class of evidence is indeed digital evidence.

This conclusion led to an evidence spoliation analysis of the control group of evidence,

consisting of over 700 evidence items, to determine if any evidence items were tainted during initial production and postproduction conveyance between parties.

## 1.2 Evidence Spoliation/Taint Analysis

The evidence spoliation analysis consisted of a multi-part test applied to determine if any evidence items exhibit positive indications for spoliation. The test was designed to answer the following questions:

- Is chain of custody documentation present for the conveyance from the producing MNO/MVNO to recipient(s)?
- What are the metadata creation and modification dates of each evidence artifact received?
- Is a modification date present indicating post creation modification to the evidence artifact?
- What are the metadata creation dates and authorship of the content of each evidence artifact?
- Is a modification date present indicating post creation modification to the evidence artifact and by whom?
- Has all metadata been removed from any analyzed evidence artifact?
- Is a verification function cryptographic hash value present for the original production evidence artifacts (ASTM, 2018)?

## 2. BACKGROUND

Mobile Network Operators (MNO)/Mobile Virtual Network Operators (MVNO) initiated subscriber activity tracking for

billing purposes when analogue cellular was launched in 1979. In 1996, the Federal Communications Commission (FCC) issued an order for the Enhanced 911 initiative, augmenting mobile network billing records to include location information. Phase 1 required that the location of the cell site to which a subscriber device was registered during communications be documented as part of the record keeping process.

Multiple technologies are utilized within mobile networks including radio frequency isotropic propagation technologies, Public Switched Telephone Network (PSTN) communications standards-based technologies, patented communications flow technologies, and a variety of data recording and gathering technologies. This section will not attempt to reiterate the corpora addressing the MNO/MVNO technology layers utilized in what are commonly referred to as 1G, 2G, 3G, 4G and 5G cellular communications but rather will address the science and methodology more directly applicable to the accounting and billing for subscriber communications activities of a mobile phone.

CDRs as evidence were made available from MNO/MVNO in response to the Communications Assistance for Law Enforcement Act (CALEA) (1994), Wireless Communication and Public Safety Act (911 Act) and Electronic Communications Privacy Act (ECPA) (1986) acts. This type of evidence has become an important evidentiary focus in the courtroom.

In the late twentieth century, Mobile Network Operators (MNO)/Mobile Virtual Network Operators (MVNO) began to produce subscriber device activity records, otherwise known as, Call Detail Records (CDR)/Cell Site Location Information (CSLI) as evidence in response to subpoena, search warrants and court orders. The primary focus of the analysis of this type of evidence is two-fold: 1) analysis of who was communicating with the

subscriber and 2) where the subscriber device was located during communications.

## 2.1 Forensic Cell Site Analysis

Forensic cell site analysis is a developing forensic analysis discipline requiring foundation knowledge of mobile network infrastructure and operations as well as an ability to analyze and interpret Call Detail Record/-Cell Site Location Information (CDR/CSLI) and other Mobile Network Operator (MNO) produced evidence. Forensic cell site analysis is a complex field incorporating radio, atmospheric, photonic, wave propagation, metrology and computer sciences, and is primarily reliant on human estimations aided by network testing, basic mapping, spreadsheet and word processing software tools. Under-developed algorithms embedded in automated tools currently used to process evidence and perform a preliminary analysis have resulted in a developing analysis capability in its nascent stage. Deficiencies in knowledge, skills and abilities (KSAs) or errors in algorithms, tools, and processes leads to incorrect findings, hence the necessity for standard analysis, validation and error mitigation protocol development. The scientific disciplines upon which forensic cell site analysis is dependent are often interlaced in complex scenarios due to various factors including:

- MNO infrastructure conditions and utilization loading.
- Cell site to mobile switching core backhaul issues.
- Subscriber and public event crowd behavior.
- Atmospheric events.
- Global network cyber-security events.

Basic understanding of the following areas of science should be requisite to every practitioner's KSAs.

## 2.2 Radio Science

Radio science is central to forensic cell site analysis despite the fact that typically less than 5% of the communications path between subscriber device and mobile switching core consists of a radio connection. Radio frequencies in use, communications technologies utilized, electromagnetic radiation physics, antenna radiation behaviors and other fundamental radio issues must be considered during an analysis.

## 2.3 Atmospheric Science

Atmospheric science impacts the airgap of mobile network linkage between subscriber device and cell site. Antenna radiation pattern and sizing in mobile subscriber devices such as cell phones and mobile network access points (Base Transceiver Station, NodeB, eNodeB, gNodeB) may be affected by heightened solar activity, certain precipitation events, lightning strikes or near strikes, and extremely high winds often affect mobile network operation and radio signal propagation. Atmospheric impact can reduce, block, destabilize or skew cell site coverage.

## 2.4 Photonic Science

Photonic science is the foundation of the communications transportation infrastructure utilized in the remaining 95% of the communications path between subscriber device and mobile switching core. Interruption or congestion in segments of the photonic network used as backhaul between cell sites and mobile switching core may disrupt or reroute communications, resulting in intermittent re-pathing, often manifested as slowdowns or interruptions in mobile communications that result in dropped calls, out of sequence communications events, or other anomalies.

## 2.5 Wave Propagation Science

Wave propagation science has a direct bearing on how radio signals propagate between subscriber device and cell site. The wave function is a key feature of quantum mechanics and radio wave scintillations including reflection, diffraction, refraction, absorption and other scattering of radio signal propagation at various frequencies, affected by objects in the path between a subscriber device and cell site, determine the extent and quality of cell coverage. Defined as manmade or naturally occurring objects varying in density and height, morphologies include vegetal, geographic, building or other structures, streets, waterways, and much more. Morphologies impact wave propagation and thereby cell site coverage. Antenna wave propagation behaviors must be considered during an analysis.

## 2.6 Metrology Science

Metrology, the science of measurement, is utilized in forensic cell site analysis to elevate the accuracy of analytical outcomes. An obvious example is the use of time and frequency metrology in performing radio surveys for mobile network testing. The units of measurement result in a standard, meaningful measurement of mobile network element performance and impact the radio link analysis between subscriber device and cell sites.

The photonic backhaul link between the mobile network cell site and the mobile network core is similarly subjected to link integrity quantification.

Location determination technologies utilized by mobile network operators to geolocate a subscriber device, the algorithms for which utilize a variety of measurements, offer another example of how the science of metrology influences forensic cell site analysis outcomes.

Standardized measurement units are critical to experimental and theoretical determi-

nations. Metrology establishes a standard measurement basis for discussion of analysis outcomes and resulting opinions.

From the evaluation of communications session metadata to radio frequencies in use during communications, time and frequency metrology plays a primary role in forensic cell site analysis.

The airgap between mobile network subscriber device and cell site consists of less than 5% of the path to the mobile network core. The measurement of various radio signal parameters and the associated formulae for determining cell site coverage, quality of service, handoff, and likelihood of service outages are critical to determining analysis outcomes and the formation of expert opinions. Examples include use of several formula models including Okumura-Hata Model, COST 231-Walfisch-Ikegami Model, COST 207 GSM Model, ITU-R Models, 3GPP Spatial Channel Model, ITU-Advanced Channel Model, and 802.15.4a UWB Channel Model to determine pathloss

Dimensional Metrology is the science of using measurement equipment to quantify the distance from an object. Examples of the use of measurement equipment in forensic cell site analysis illustrate this usage.

Subscriber device location quantification in forensic cell site analysis is dependent upon location determination technology ranging from highly accurate, finite location determination to wide-ranging, general location determination.

Radio surveys of the network segments under analysis, utilizing radio survey methodologies including idle mode and dynamic mode, and specific location, cell, and wide area mapping utilize precise dimensional metrology to determine handoff zones, sector coverage limits, and mobile network void coverage boundaries.

Optical metrology is the science and technology of measurements with photons. In forensic cell site analysis 95% of the communications linkage between subscriber device and mobile switching core is composed of photonic links. Understanding the measurement unit and normal link loss over segments of the photonic networks employed to transport communications sessions for a subscriber device on the mobile network is essential to calculating probabilities of network latency issues that may cause dropped calls, out of sequence text messaging, and other irregularities in communications sessions.

Metrology assists decision making in the analytical process by quantifying measurements and depending on type I (false positive) and type II (false negative) error rate determination.

Systematic errors usually originate within test and measurement instruments and occur due to instrument malfunction or improper use. Random errors occur by unknown and often unpredictable factors such as atmospheric conditions or morphologies introducing reflection, refraction or absorption of radio signals.

## 2.7 Computer Science

Computer science is fundamental to how the network elements that comprise the mobile network function and how accurately the MNO/MVNO subscriber device activities are logged to eventually become evidence in criminal or civil litigation. A thorough understanding of the Transmission Control Protocol/Internet Protocol, addressing schemes, composition of the Internet including network elements, switched packet flow, and routing protocols is essential to understanding both computer and photonic sciences. An understanding of peering, transit and service level agreements enhances understanding and lucidity regarding potential pathing issues that sometimes result in communications session sequencing irregularities.

## 2.8 MNO/MVNO Charging/Billing Architecture

Mobile network subscriber activity records are created during the usage of a subscriber device, while registered to the MNO/MVNO infrastructure and during communications sessions transporting voice calls, SMS text messages and data usage. Multiple mobile network elements, including Home Location Register (HLR), Visitor Location Register (VLR), Charging Gateway Function (CGF), and Policy and Charging Rules Function (PCRF) are tasked with documenting device usage and sending the activity records to a Billing/Charging Gateway and subsequently on to the Billing Domain, thereby creating records that become the basis of customer billing.

Charging Data Records, known as Call Detail Records (CDRs), are subscriber communications activity records produced from the billing information database and are typically considered to be higher accuracy accounts of device usage than a cell phone bill, e.g. metadata time stamp accuracy to the second rather than rounded to the minute, etc.

The functional output of the charging/-billing architecture has remained fundamentally the same during the evolution from 2G to 5G. The result has been highly accurate recordkeeping of subscriber activities during communications sessions, absent any errors in recordkeeping resulting from network documentation or functionality issues, network or billing domain configuration errors, or data storage failures.

A logical diagram of 2G, 3G, 4G and 5G architecture including an overview of the basic network elements and reference connectivity to the billing domain elucidates the concept that mobile networks are complex systems. These systems require significant knowledge

by analysts of the differences and complexities within each network generation.

The CDRs are extracted from larger database systems within the mobile network charging/billing infrastructure. The integrity of evidence extracted from this data repository is dependent upon the extraction methodology employed by mobile network legal production personnel and the handling of the evidence post extraction. Mobile

network records custodians do not produce any chain of custody documentation, however, in many instances the records custodian prepares a notarized certification of records, indicating, for example, that “such records were kept in the course of regularly conducted business activity”, that “the business activity made such records as a regular practice” and that “if such record is not the original, such record is a duplicate of the original”. Typically, the certification letter lists the phone number(s) and start and end dates of records produced without listing, by name or other means, the digital evidence items accompanying the certification.

Various other records are also maintained by various MNO/MVNO departments including billing records, network maintenance logs, real time and near real-time subscriber device location tracking logs, cell site database records that include technical data about each access point in the mobile network, configuration data regarding how the mobile network is configured, mobile network radio survey or drive test data, key performance indicator data that exhibits the coverage and health of the mobile network and other technical information about subscriber activities or network conditions. All records, apart from handwritten logs from physical cell site access, of maintenance, upgrade and repair personnel, are digital in origin and should be considered digital evidence when produced in court as evidence.

In the digital forensic science discipline, digital evidence obtained from sources including computer hard drive evidence and mobile device (cell phone), is preserved using a chain of custody methodology and must be proven identifiable as true to the original evidence produced to avoid preclusion by the courts. Digital evidence integrity is assured with verification of metadata creation and modification date/time preservation along with verification function cryptographic checksum hashing of each digital evidence item.

The International Organization of Standards (ISO) and the Internet Engineering Task Force (IETF) have published standards for the acquisition, preservation and handling of digital evidence, including the establishment of chain of custody and evidence verification function. The National Institute of Standards and Technology (NIST) and the American Society for Testing and Materials (ASTM) International have published extensive forensic evidence guidance and standards documents for the acquisition, validation and analysis of computer and cell phone evidence. Curiously absent are standards for the handling, validation or error mitigation of CDR/CSLI evidence in any of the aforementioned standards bodies.

A method of validating cellular carrier records for forensic cell site analysis is defined in United States Patent US9113307 (Minor, 2015). Research has demonstrated that a method for validation and error mitigation of MNO/MVNO evidence should be utilized to accurately complete a forensic cell site analysis (Minor, 2017). As a prefatory to performing validation and error mitigation of a forensic cell site analysis, an examination of the condition of the MNO/MVNO evidence is an important step that should be performed prior to proceeding with analysis, validation and error mitigation steps.



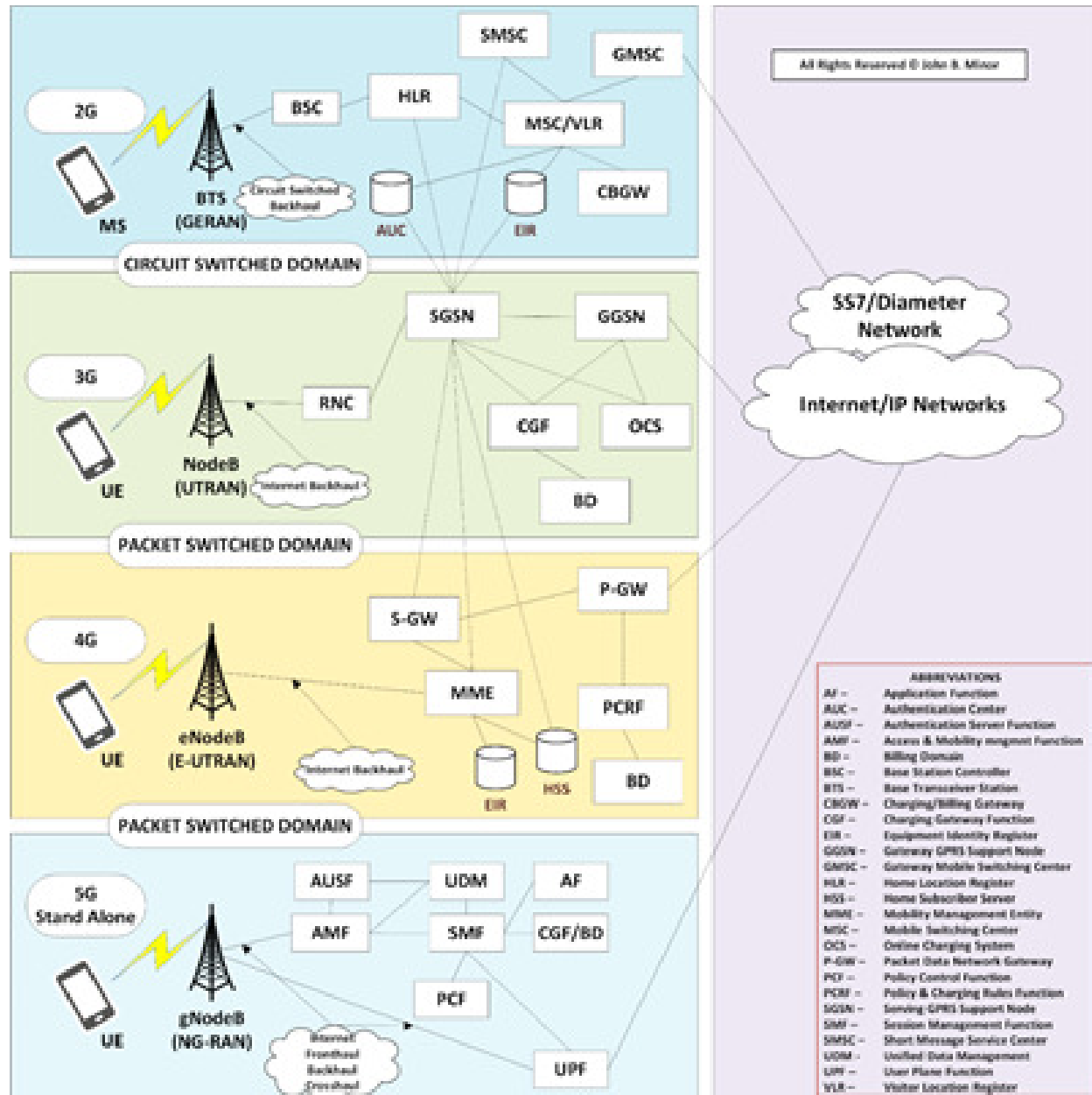


Figure 1. 2G-3G-4G-5G Mobile Network / Charging/Billing Architecture

## 2.9 Mobile Network Toll & Call Data Records Are a Computer Driven Process

The basis for all mobile network CDRs is the toll or billing record database sourced from the MNO/MVNO charging/billing system. The CDR is the primary subscriber record produced for criminal and civil cases.

Other records are produced by MNO/MVNO include a variety of logs, technical configuration data for segments of the mobile network, test data from radio survey results, and billing records.

## 2.10 Charging and Billing System

The MNO/MVNO charging/billing system necessarily maintains careful accounting of subscriber communications activities. The charging/billing system of each MNO/MVNO is operated according to standards established by a variety of organizations, including national and international bodies.

Charging Data Records, commonly known as Call Detail Records (CDRs) are maintained and produced from a standards based data flow to the Charging Gateway Function and into the CDR database in a format established by standards.

## 2.11 3GPP/ETSI Standards

One of the applicable standards related to billing and charging functionality, for example, are specified within 3GPP TS 32.299 V12.6.0 (2014-10)(ETSI, 2014) 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release 8). These standards among others are followed by MNO/MVNO in the United States and virtually all other MNO/MVNO.

The 3rd Generation Partnership Project (3GPP) – European Telecommunications Standards Institute (ETSI) TS 32.297 v13.2.0 (2016-06) standard addresses Charging management; Charging Data Record (CDR) file format and transfer, thereby clearly demonstrating that MNO/MVNO records are digital evidence.

In Chapter 6 of TS 32.297 v13.2.0, CDR file format specification, 6.1.1.0, General, the exact format of the CDR file header is given in table 6.1.1.1. This record keeping format is indicative of entirely digital content. Note that timestamps, file sequence numbers and

other important information is maintained, according to this standard. (ETSI, 2016)

The following table, from chapter 6, provides the data repository record layout for CDR data:

Bits	8	7	6	5	4	3	2	1
1..4	File length							
5..8	Header length							
9	High Release Identifier				High Version Identifier			
10	Low Release Identifier				Low Version Identifier			
11..14	File opening timestamp							
15..18	Timestamp when last CDR was appended to file							
19..22	Number of CDRs in file							
23..26	File sequence number							
27	File Closure Trigger Reason							
28..47	IP Address of Node that generated file							
48	Lost CDR indicator							
49..50	Length of CDR routing filter							
51..xy	CDR routing filter							
xy+1..xy+2	Length of Private Extension							
xy+3..n	Private Extension							
n+1	High Release Identifier extension							
n+2	Low Release Identifier extension							

Table 6.1.1.0.1: Format of CDR file header (p.21)

CDRs are addressed extensively in the file header and a variety of key indicators of the digital nature of this record keeping activity includes timestamp metadata, record numbers, file sequence numbers, record extension information and IP addressing of the node generating the CDR file. The specification concisely addresses how information is recorded and integrity is maintained.

Metadata timestamps include when a CDR file was opened, the local time differential offset from Universal Coordinated Time (UTC), append and closure times.

Information integrity is addressed in this format standard including number of CDRs in a file, file sequence numbers, file closure triggering and reasons for closure.

Finally, the specification provides for the IP address of the Charging Gateway Function creating the CDR file and a Lost CDR Indicator providing traceability of any error conditions detected.

The specification continues below (p.22):

**6.1.1.5 File opening timestamp** These parameters indicate the time when the file was opened, according to the following binary format:

- The first four binary bits indicate the month (1 .. 12), according to the CGF's(ETSI, 2005) local time zone;
  - The next five binary bits contain the date (1 :: 31), according to the CGF's local time zone;
  - The next five binary bits contain the hour (0 .. 23), according to the CGF's local time zone;
  - The next six binary bits contain the minute (0 .. 59), according to the CGF's local time zone;
  - The next bit indicates the sign of the local time differential from UTC (bit set to "1" expresses "+" or bit set to "0" expresses "-" time deviation), in case the time differential to UTC is 0 then the sign may be arbitrarily set to "+" or "-";
  - The next five binary bits contain the hour (0 .. 23) deviation of the local time towards UTC, according to the CGF's local time zone;
  - The next six binary bits contain the minute (0 .. 59) deviation of the local time towards UTC, according to the CGF's local time zone;
- Note that the CDR file name contains detailed date and time information related to file closure (see clause 6.2)

**6.1.1.6 Last CDR append timestamp**

This parameter is formatted the same as in clause 6.1.1.5, and indicates the time when the last CDR was appended to the file in UTC format. In case of an empty file (i.e. no CDRs included), the value of the parameter is "0".

**6.1.1.7 Number of CDRs in file** This parameter contains a binary value that specifies the total number of CDRs that are included in the file.

The value with all bits set to "1" is reserved for future extensions (e.g. for CDR files con-

taining more CDRs than represented by that value) and shall therefore not be used.

**6.1.1.8 File sequence number** This parameter is a value in binary that contains a running number of the CDR file generated by the same CGF. The first file of a CGF is indicated by the value "0". When the maximum number of file is reached (all bits set to "1"), the sequence shall be restarted with "0".

**6.1.1.9 File closure trigger reason** The file closure reason provides a means to determine the reason that the file was closed by the CGF. It is encoded as a single octet as follows:

Normal closure reasons (Binary values 0 to 127):

0 = Normal closure (Undefined normal closure reason).

1 = File size limit reached (OAM&P configured).

2 = File open-time limit reached (OAM&P configured).

3 = Maximum number of CDRs in file reached (OAM&P configured).

4 = File closed by manual intervention.

5 = CDR release, version or encoding change.

6 to 127 are reserved for future use.

Abnormal closure reasons (Binary values 128 to 255):

128 = Abnormal file closure (Undefined error closure reason).

129 = File system error.

130 = File system storage exhausted.

131 = File integrity error.

132 to 255 are reserved for future use.

**6.1.1.10 Node IP address** This parameter indicates the IP address of the CGF generating the file. For both IPv4 and IPv6 CGF addresses, the parameter is encoded in IPv6 representation. The first four bytes of the parameter, which are [preceding] this IPv6 address, are insignificant, e.g. filled with 'FF'.

**6.1.1.11 Lost CDR indicator** This parameter indicates if and how many CDRs were lost during their processing in the CGF (see clause 5.1.1). The term "lost" implies that the CDR(s) could not be placed into the destination file due to irrecoverable errors.

Due to the possibility that the irrecoverable CDR errors may have impacted CDR parameters that are relevant for CDR routing, it is possible that the CGF cannot determine for a particular file whether CDRs have been lost. Appropriate indication shall be given according to the following encoding of the "lost CDR indicator".

- MSB bit "0", all other bits "0": no CDRs have been lost;
- MSB bit "0", all other bits set to a value corresponding to decimal 1 to decimal 126: CGF has identified that a number of CDRs corresponding to the value of the lower 7 bits were lost, while it is unknown whether more CDRs were lost;
- MSB bit "0", all other bits set to "1": CGF has identified that 127 or more CDRs were lost, while it is unknown whether more CDRs were lost;
- MSB bit "1", all other bits "0": CDRs have been lost but CGF cannot determine the number of lost CDRs;
- MSB bit "1", all other bits set to a value corresponding to decimal 1 to decimal 126: CGF has calculated the number of lost CDRs as indicated in the value of the lower 7 bits;
- MSB bit "1", all other bits set to "1": CGF has calculated the number of lost CDRs to be 127 or more." (ETSI, 2016)

## 2.12 Digital Evidence Integrity Maintenance Standards

ISO (The International Organization for Standardization) and IEC (The International Electrotechnical Commission) form the spe-

cialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with specific fields of technical activity. (ISO, 2012)

ISO 27037, Section 5.4, titled "Digital evidence handling processes", Section 6 titled "Key components of identification, collection, acquisition and preservation of digital evidence", and Section 6.1, titled "Chain of custody" (ibid), address the global standards for digital evidence handling including collection, acquisition, preservation and chain of custody.

The introduction to ISO 27037 states in part . . . "These processes are required in an investigation that is designed to maintain the integrity of the digital evidence – an acceptable methodology in obtaining digital evidence that will contribute to its admissibility in legal and disciplinary actions as well as other required instances. This International Standard also provides general guidelines for the collection of non-digital evidence that may be helpful in the analysis stage of the potential digital evidence."

The standard continues with the following statement: "This International Standard also intends to inform decision-makers who need to determine the reliability of digital evidence presented to them. It is applicable to organizations needing to protect, analyze and present potential digital evidence." . . . "Due to the fragility of digital evidence, it is necessary to carry out an acceptable methodology to ensure the integrity and authenticity of the potential digital evidence."

Under Section 1, Scope, the standard delineates applicable devices as " . . . devices and/or functions that are used in various circumstances:

— Digital storage media used in standard computers like hard drives, floppy disks, optical

- and magneto optical disks, data devices with similar functions,
- Mobile phones, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards,
  - Mobile navigation systems,
  - Digital still and video cameras (including CCTV),
  - Standard computer with network connections,
  - Networks based on TCP/IP and other digital protocols, and
  - Devices with similar functions as above.”

MNO/MVNO networks are a composite of several of the listed devices including “networks based on TCP/IP and other digital protocols”, “digital storage media used in standard computers”, “mobile navigation systems”, “mobile phones, personal digital assistants”, “standard computer with network connection”, and “devices with similar functions as above”.

Under Section 3, Terms and Definitions, several definitions were found to be relevant to this analysis, including:

### “3.1 acquisition

process of creating a copy of data within a defined set Note 1 to entry: The product of an acquisition is a potential digital evidence copy.”

### “3.5 digital evidence

information or data, stored or transmitted in binary form that may be relied on as evidence”

### “3.6 digital evidence copy

copy of the digital evidence that has been produced to maintain the reliability of the evidence by including both the digital evidence and verification means where the method of verifying it can be either embedded in or independent from the tools used in doing the verification”

### “3.1 preservation

process to maintain and safeguard the integrity and/or original condition of the potential digital evidence”

### “3.19 spoliation

act of making or allowing change(s) to the potential digital evidence that diminishes its evidential value”

### “3.22 timestamp

time variant parameter which denotes a point in time with respect to a common time reference

[SOURCE: ISO/IEC 11770-1:1996]”

### “3.25 verification function

function which is used to verify that two sets of data are identical

Note 1 to entry: No two non-identical data sets should produce an identical match from a verification function.

Note 2 to entry: Verification functions are commonly implemented using hash functions such as MD5, SHA1, etc., but other methods may be used.”

ASTM International establishes that “confidence in digital and multimedia evidence forensic results is best achieved by using an error mitigation analysis approach that focuses on recognizing potential sources of error and then applying techniques used to mitigate them, including trained and competent personnel using tested and validated methods and practices”. (ASTM, 2018)

All MNO/MVNO networks are pervasively integrated into the network of networks commonly called the Internet. Voice, text and data communications over the cellular network traverse the Internet from cell sites to MNO/MVNO network core (Cisco, 2011).

The Scientific Working Group on Digital Evidence (SWGDE) discipline guidance in Recommendations for Cell Site Analysis confirms that “if use of the records [CDRs] in court is anticipated, it is important to prepare to meet any applicable rules of evidence requirements”. (SWGDE, 2017)

The Internet Engineering Task Force (IETF) provides guidance and standardization for handling digital evidence in RFC 3227. The standard states in part "... you should consider generating checksums and cryptographically signing the collected evidence, as this may make it easier to preserve a strong chain of evidence. In doing so you must not alter the evidence." (IETF, 2002)

The National Institute of Standards and Technology (NIST), in the publication "Guidelines on Mobile Device Forensics" (NIST, 2007), verifies that all digital evidence must be handled using an appropriate chain of custody and a forensic hash validation of the evidence. NIST defines each of the procedures as follows:

- "Forensic Hash Validation: A forensic hash is used to maintain the integrity of an acquisition by computing a cryptographically strong, non-reversible value over the acquired data. After acquisition, any changes made to the data may be detected, since a new hash value computed over the data will be inconsistent with the old value. For non-forensic tools, hash values should be created using a tool such as sha1sum and retained for integrity verification. Even tools labelled as forensic tools may not compute a cryptographic hash, and (in these cases an integrity hash should be computed separately)."
- "Chain of Custody – A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for any transfers."

The Forensic Hash Validation is an integral part of the scientific digital forensics step process.

The verification function mentioned in ISO 27037 is best performed by comparing two digital evidence artifacts using a forensic hash validation.

### 2.13 Role of Metadata Date & Time

An important method of determining if digital evidence is spoliated is to analyze metadata creation and modification times and authorship of digital evidence artifacts. Documents such as Microsoft Word, Excel Spreadsheets or Adobe PDF's can also be analyzed for content creation and modification metadata, including authorship to further enhance the accuracy of digital evidence spoliation analysis.

Metadata creation and modification dates/-times should be identical if copies of digital evidence have not been tainted. Absence of this information is an important positive indicator of spoliation, absent the presence of verification function hash values.

NIST publication "Guide To Integrating Forensic Techniques Into Incident Response" describes external file metadata as follows - File Modification, Access and Creation Times.

It is often important to know when a file was created, used, or manipulated, and most OSs keep track of certain timestamps related to files. The most commonly used timestamps are the modification, access, and creation (MAC) times, as follows:

- **Modification Time.** This is the last time a file was changed in any way, including when a file is written to and when it is changed by another program.
- **Access Time.** This is the last time any access was performed on a file (e.g., viewed, opened, printed).
- **Creation Time.** This is generally the time and date the file was created; how-

ever, when a file is copied to a system, the creation time will become the time the file was copied to the new system. The modification time will remain intact.

Different types of filesystem may store different types of times. For example, Windows systems retain the last modified time, the last access time, and the creation time of files. . .” (NIST, 2006)

## 2.14 Error Rates

MNO/MVNO have documented error rates in subscriber activity records that, to date, have not been publicly disclosed. Research performed during validation and error mitigation testing on over 300,000 pages of MNO/MVNO produced evidence realized error rates that approach 2% in some cases (Minor, 2017).

The previously mentioned 3GPP/ETSI TS 32.297 standard, Section 6.1.1.11 Lost CDR indicator, mentions error rates; however, in hundreds of cases analyzed, and many cases in which a MNO/MVNO employee testified, none has ever disclosed any error rate information. The standard states in part ”This parameter indicates if and how many CDRs were lost during their processing in the CGF (see clause 5.1.1). The term ”lost” implies that the CDR(s) could not be placed into the destination file due to irrecoverable errors.”

Studies performed on the Movistar - Telefonica Chile Mobile Network Operations resulted in creation of a methodology to analyze time accuracy in post-mediation (postpaid billing) CDRs (Peredo, 2017). In this study, recorded CDR events were compared with actual logging events using a network event measurement tool. Although the analysis results were inconclusive, the methodology exhibits promise that more accurate error models for the CDR record keeping function are arriving and that error rates are quantifiable.

A method of validating cellular carrier records accuracy for forensic cell site analysis is defined in United States Patent US9113307. The process includes a multi-part test to validate CDR/CSLI records and an analysis error mitigation methodology.

At least one MNO/MVNO has concluded that this evidence is digital evidence and should be treated as such. In 2013, AT&T Mobility acquired Cricket Wireless, a prepaid mobile network provider (Mobile Virtual Network Operator or MVNO). Cricket Wireless uses the AT&T infrastructure to process communications for its subscribers and the

AT&T Mobility charging/billing system provides usage records to Cricket Wireless. Cricket produces CDR/CSLI evidence for its subscribers in response to legal requests and offers the following disclaimer when digital copies of CDR/CSLI evidence is produced and emailed to a requesting party:

***“At the request of the law enforcement agency receiving the following Subpoena Compliance information, Cricket Communications (“Cricket”) provides the following information electronically in a searchable, manipulable form. Although Cricket verifies the authenticity of the information attached to this e-mail as sent, Cricket cannot and will not testify to the authenticity of this information after it is received by the recipient law enforcement agency. This is because the attached information electronically sent by Cricket is manipulable.”*** (Pennsylvania Superior Court, 2016)

## 3. RESEARCH METHODOLOGY

The analysis was performed in four phases as follows:

### 3.1 Phase I

A four-part test was applied to first determine if MNO/MVNO subscriber activity records should be subjected to digital evidence handling and analysis standards as follows:

- Is MNO/MVNO subscriber communications activity record keeping a computer driven digital process?
- Are subscriber communications activity records, extracted for litigation purposes, digital evidence?
- Is this type of evidence subject to digital evidence handling standards?
- Do the same rules for spoliation determination apply to this type of evidence?

### 3.2 Phase II

The control group of MNO/MVNO digital evidence was reviewed for the presence of any chain of custody documents. Note that any certification letters provided by records custodians do not list evidence items by document name, number or other confirmable identifier.

### 3.3 Phase III

The MNO/MVNO CDR evidence was then subjected to a five-part metadata analysis using the following protocol:

- Internally within each digital evidence item, any document “creation date” metadata including date and author. This portion of the analysis was documented under the Internal Document Metadata categorization.
- Internally within each digital evidence item, any document “modification date” metadata including date and author.

This portion of the analysis was documented under the Internal Document Metadata categorization.

- Internally within each digital evidence item, any document “last printed date” metadata including date and author. This portion of the analysis was documented under the Internal Document Metadata categorization.
- Externally, any valid original creation date metadata for each digital evidence item. This portion of the analysis was documented under the External File Metadata categorization. (NIST, 2006)
- Externally, any valid original modification date metadata for each digital evidence item. This portion of the analysis was documented under the External File Metadata categorization.

### 3.4 Phase IV

Finally, a verification function analysis was performed to determine that the copy of the evidence is identical to the evidence produced by the MNO/MVNO custodian of records in the following manner:

- Each evidence item was scrutinized for a verification function cryptographic checksum hash value. A cryptographic checksum hash value should have been calculated on the original and any copy of the evidence item.
- If a verification function cryptographic hash value was found, then a cryptographic hash value was calculated for the produced evidence item for the purpose of comparison and final verification that the original evidence item and the evidence item produced are identical.



Microsoft Excel, a spreadsheet database software product, was utilized to document the chain of custody analysis, metadata analysis, verification function analysis outlined above and document the presence or absence of spoliation. All information in the matrix is independently verifiable.

## 4. OUTCOMES

### 4.1 Phase I - Business Records – The Question of Digital Evidence

Are Mobile Network Records Produced as Evidence Actually Digital Evidence?

Analysis of MNO/MVNO CDR evidence was undertaken from the research control group of cases to determine if each evidence artifact should be classified as digital evidence by applying the devised four-part test. All evidence items tested positive as digital evidence.

The following outcomes were observed for Phase I:

1. Is MNO/MVNO subscriber communications activity record keeping a computer driven digital process? Yes, standards for digital record keeping methods and formats clearly affirm this question.
2. Are MNO/MVNO subscriber communications activity records, extracted for litigation purposes, classified as digital evidence? Yes, the records are created digitally by computing-based methods and the extracted reports produced are digital evidence and, thus, are purely digital from inception to production.
3. Is this type of evidence subject to digital evidence handling standards? Yes, all digital evidence is subject to the same evidence handling standards.

4. Do the same rules for evidence spoliation determination apply to this type of evidence? Yes, no exceptions to the standards are addressed.

### 4.2 Phase II - Chain of Custody Issue

No chain of custody documentation accompanied any of the evidence. Chain of custody documentation should have been created and forwarded with the CDR evidence from the MNO/MVNO legal department/custodian of records and all others conveying the evidence.

The Custodian of Records certification letters were present in many cases. When such documents were present, the certifications did not describe or specify which files, documents or other digital evidence were being provided, by file name, traceable number or any other recognizable, traceable or accountable method.

The following outcomes were observed for Phase II:

None of the digital evidence items were accompanied by chain of custody documentation.

### 4.3 Phase III - Evidence Condition Observations and Findings

A spoliation analysis of the MNO/MVNO CDR evidence produced the following results:

1. Observation: MNO/MVNO CDR evidence within the control group was produced in a variety of digital formats including Microsoft Excel spreadsheet file, comma-separated values (CSV) file (IETF, 2005) (typically opened automatically by Excel), plain text file, Rich Text File (RTF) file, Adobe Portable Document Format (PDF) file, Joint Photographic Experts Group (JPEG) file, and Microsoft Word Document file.

OUTCOMES SUMMARY	
<b>Phase I</b>	The Four Part Test Result Was Affirmative for Digital Evidence
<b>Phase II</b>	Chain of Custody Documentation Was Not Present for Any Reviewed Evidence Item
<b>Phase III</b>	The Overall Spoilation / Taint Rate for All Reviewed Evidence was 74.07%
<b>Phase IV</b>	A Verification Function Cryptographic Checksum Hash Value Was Not Present for Any Reviewed Evidence Item

Figure 2. Outcomes Summary

2. Observation: MNOs/MVNOs began to offer degraded evidence production as pressure to respond to escalating demand during recent years. Observed manifestations were typically either removal of all creation/modification metadata, creation of documents using methods that produce no creation/modification metadata, multiple employee (author) creation/modification metadata, or removal of employee (author) metadata combined with differing creation and modification metadata. Examples of appropriate creation/modification metadata were rarely found within the control group.



Figure 4. MNO evidence item example internal metadata with proper artifact integrity

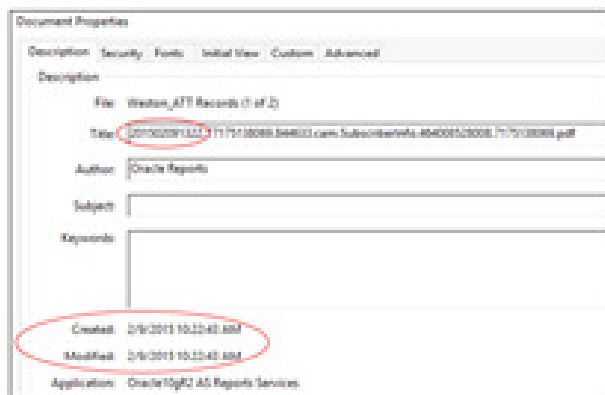


Figure 3. MNO evidence item example indicating appropriate evidence creation and handling

Examples of tainted evidence is indicated in significant percentages of MNO/MVNO ev-

idence when multiple authors are discovered during analysis of metadata.

1. Observation: MNO/MVNO CDR production formats vary widely in content and arrangement of data. Contrary to guidance provided in SWGDE Cell Site Analysis that states that “Even if CDRs are provided, which include specific latitude and longitude references to the antennas used by a target device, it is necessary to have the neighboring cell site locations and information to conduct CSA more thoroughly”, production

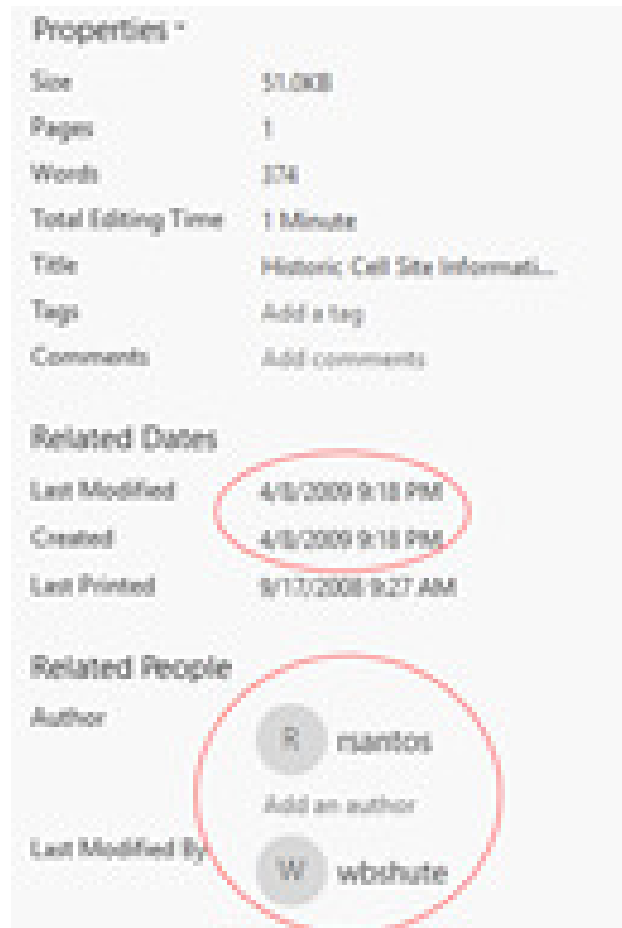


Figure 5. MNO evidence item example presenting multiple authors with no metadata date changes. The Last Modified by author is consistent with changes by a different author

from some MNOs/MVNOs do not provide neighboring cell site locations.

2. The National Domestic Communications Assistance Center (NDCAC, 2018) is provided extensive support by MNOs/MVNOs, specifically supplying lists of cell sites with technical configurations for each site to NDCAC. A request to NDCAC for access to the cell site database receives an access denial from NDCAC personnel with the message “Users who access our systems must acknowledge and attest they are an employee of a law enforcement or

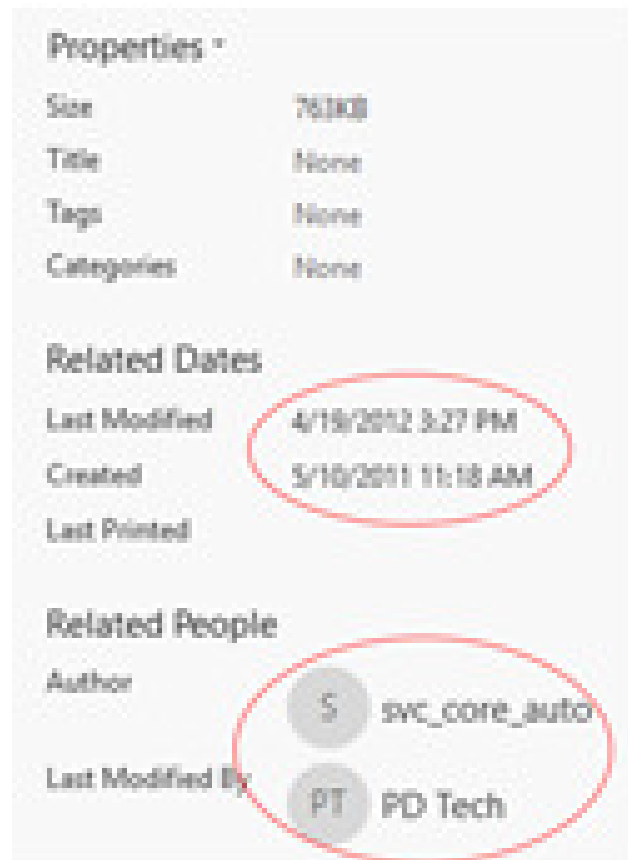


Figure 6. MNO evidence item example presenting multiple authors and disparate creation and modification dates metadata evidence taint

criminal justice agency, in good standing and are accessing this U.S. Government system for official use only”. Until MNOs/MVNOs provide the information produced in a data repository that is accessible to all stakeholders / practitioners, or, an acceptance of MNO/MVNO evidence as digital evidence transpires, performing any verification of authenticity or validation of the condition of this category of evidence will continue to be a challenge.

The following outcomes were observed for Phase III:

<b>MNO/MVNO EVIDENCE SPOILIATION ANALYSIS</b>	
<b>Category of Spoliation</b>	<b>Percentile</b>
Internal Metadata Creation Date	0.41%
Internal Metadata Author Modification	10.90%
Internal Metadata Last Modified Date	23.17%
Internal Metadata Removed	20.41%
External File Creation Date	0.14%
External File Last Modified Date	37.79%
<b>Overall Evidence Taint Rate (Excluding Chain of Custody &amp; Hash Value Presence Tests)</b>	<b>74.07%</b>
No Chain of Custody Present	100.00%
No Verification Function Hash Value Present	100.00%

Figure 7. Results of the Phase III Analysis

1. Analysis of the internal file metadata present within the evidence revealed that only 0.41% of the internal metadata creation dates had been altered.
2. Various authorship was indicated in internal file creation and modification metadata in 10.9% of the control group analysis.
3. The last modified date, according to internal file metadata, was not consistent with pristine evidence condition in 23.17% of the evidence.
4. 20.14% of the evidence was found to have been scrubbed of internal file metadata creation / modification information, thus rendering the evidence subject to undetectable, inappropriate alteration. The most commonly observed evidence with such missing metadata was Comma Separated Values or CSV data, a method of saving spreadsheet files, commonly used to eradicate any indications of authorship or metadata creation/modification information. CSV format evidence from the control group is from more recent cases.
5. External file metadata for last modified date was found to be tainted in 37.79% of the evidence.
6. Overall, excluding the tests for chain of custody and verification function hash value presence, 74.07% of evidence reviewed from the control group were found to be tainted.
7. Evidence taint was introduced either carelessly or nefariously by MNO/MVNO employees, law enforcement investigators, attorney staff or others involved in handling and conveyance of evidence.
8. 100% of the evidence was found to have no chain of custody documentation.
9. 100% of the evidence was found to have no calculated verification function cryptographic checksum hash values.

#### **4.4 Phase IV – Verification Function Calculated Hash Value Analysis**

The following outcomes were observed for Phase IV:

None of the digital evidence items were accompanied by a cryptographically calculated verification function checksum hash value.

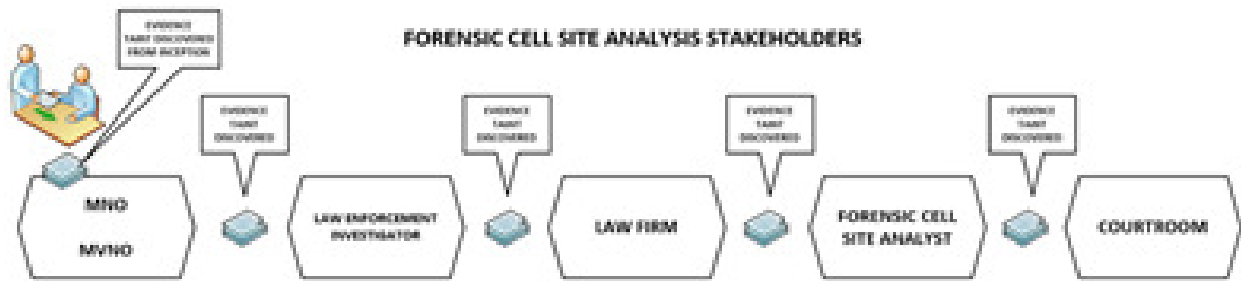


Figure 8. Evidence Spoliation/Taint was Discovered Throughout the Stakeholder Spectrum

## 5. EVIDENCE INTEGRITY MAINTENANCE SOLUTIONS

MNOs/MVNOs do not currently utilize a mechanism to properly preserve the integrity of evidence produced in criminal or civil case requests. Research into multiple existing or emerging chain of custody/verification function technologies resulted in potential solutions to the evidence integrity maintenance challenge.

### 5.1 Background and Incentives

Key incentives for MNO/MVNO adoption of a solution are likely to be the following:

- Ease of integrating a solution into existing charging/billing architectures.
- Judicious Capitalization (CAPEX) and Operating (OPEX) Expenses.
- Timeliness and performance speed of evidence integrity preservation processing.
- Ability for the solution to be assimilated by each successive generation of the mobile network.

Numerous proven and patented methods for evidence integrity maintenance currently exist and this paper explores one such solution.

MNO/MVNO evidence production is clearly a process lacking uniformity between operators, varying widely in internal evidence extraction techniques. Format and content of evidence production also varies widely.

Standards are non-existent for uniform MNO/MVNO evidence extraction, format, integrity assurance or delivery methods. The widespread use of this type of evidence in criminal and civil cases necessitates an urgent need for evidence production and management protocols that incorporate chain of custody, verification function hash value generation and maintenance of evidence integrity assurance, none of which are currently utilized by MNO/MVNO nor other digital platforms such as social network, search engine, or other digital service providers during evidence production.

This research project undertook development of a simplified solution to MNO/MVNO evidence production protocols that would provide a relatively low cost, state of the art evidence integrity assurance mechanism that meets basic digital evidence handling standards. MNO/MVNO operations are complex, ultra-busy environs with an exponential rise in communications volume and evidence production expected in the coming years, consequently any solution would necessarily be efficient and effective.

## 5.2 Distributed Ledger Technology/Block-chain Research

Block-chain/Distributed Ledger Technology (DLT)(Gramoli, 2018) offers a promising solution to digital document authentication and verification. Block-chain paradigms such as Bitcoin and other open source technologies, e.g. Openchain (Openchain, 2019), provide for a distributed ledger-based chain of custody and verification function checksum hash value generation for each evidence artifact, enabling an analyst to verify evidence integrity.

Numerous service providers currently offer document authentication and verification services that utilize Block-chain/DLT protocols.

Incorporating a built-in Block-chain/DLT client during the evidence production process would eliminate the evidence spoliation/taint issues discovered during this research project and would introduce readily validated evidence that is synonymous with digital evidence in all other digital forensics disciplines. Block-chain/DLT provides key elements of a functional architecture that ensure validity and integrity of digital evidence.

### Fundamental DLT Architecture

The architecture of Distributed Ledger Technology is articulated in several elements. (Gramoli, 2018)

The Consensus Element (p.19) is a fundamental function of a Block-chain providing a “distributed voting process”. Protocols that are both scalable and secure will be required to accommodate the rapidly growing world of MNO/MVNO evidence production.

The Security Element (p.20) is critical to authentication and integrity, providing malicious user protections.

The Validation Element (p.20) is the asymmetric cryptographic system used to create necessary public and private key pairs, using technologies currently available including

Elliptic Curve Cryptography (ECC) (IETF, 2011) algorithms. Despite security concerns regarding early ECC algorithms adopted by NIST (NIST, 2000) almost 20 years ago, more current ECC including Curve 25519 (IETF, 2016) offer security levels with exponentiated Elliptical Curve Digital Signature Algorithm (ECDSA) protections.

The Ownership Element (Gramoli, p. 20) enables transfer of evidence copy while ensuring authenticity and integrity. DLT transaction language offers the opportunity for such transfer of digital assets between accounts while maintaining evidence integrity.

All entities requesting evidence production from an MNO/MVNO would be dealt with uniformly as follows:

1. As evidence extraction from the MNO/MVNO occurs a Block-chain/DLT process is incorporated during evidence production to create a chain of custody and a public key is utilized to encrypt each evidence item.
2. Using Block-chaining transaction techniques during the encryption process, a ledger-based chain of custody and verification function hash value calculation is automatically created.
3. Each evidence artifact is transmitted to an evidence portal to be accessed by the evidence requesting entity. Evidence items are decrypted by authorized parties, producing a chain of custody resulting in self-auditing evidence artifacts.
4. An evidence integrity checking mechanism is integrated into the same portal, resulting in the ability for anyone who has access to the evidence to determine the condition of the evidence.

To validate the effectiveness of the use of Block-chain/DLT protocols with



Figure 9. Comparison of Bitcoin Financial Transaction and MNO/MVNO Evidence Transaction Paradigms



Figure 10. Data Flow for the MNO/MVNO Compliance Center Evidence Production with Built-in Distributed Ledger

MNO/MVNO evidence, an experiment was conducted using MNO/MVNO produced evidence to authenticate and provide condition verification services for each evidence item.

The experiment consisted of several steps as follows:

1. Creation of a user ID on the website of a provider offering DLT digital document authentication and verification services.
2. Two MNO/MVNO evidence items were then processed into the portal. The time

to perform an intake varied from 15-45 seconds (processing time is primarily related to digital file size and Internet access bandwidth). Processing timeliness may be a critical function for MNOs as the volume of evidence requests soars.

3. The evidence artifacts were then digitally signed, creating the digital ledger-based chain of custody documentation required.

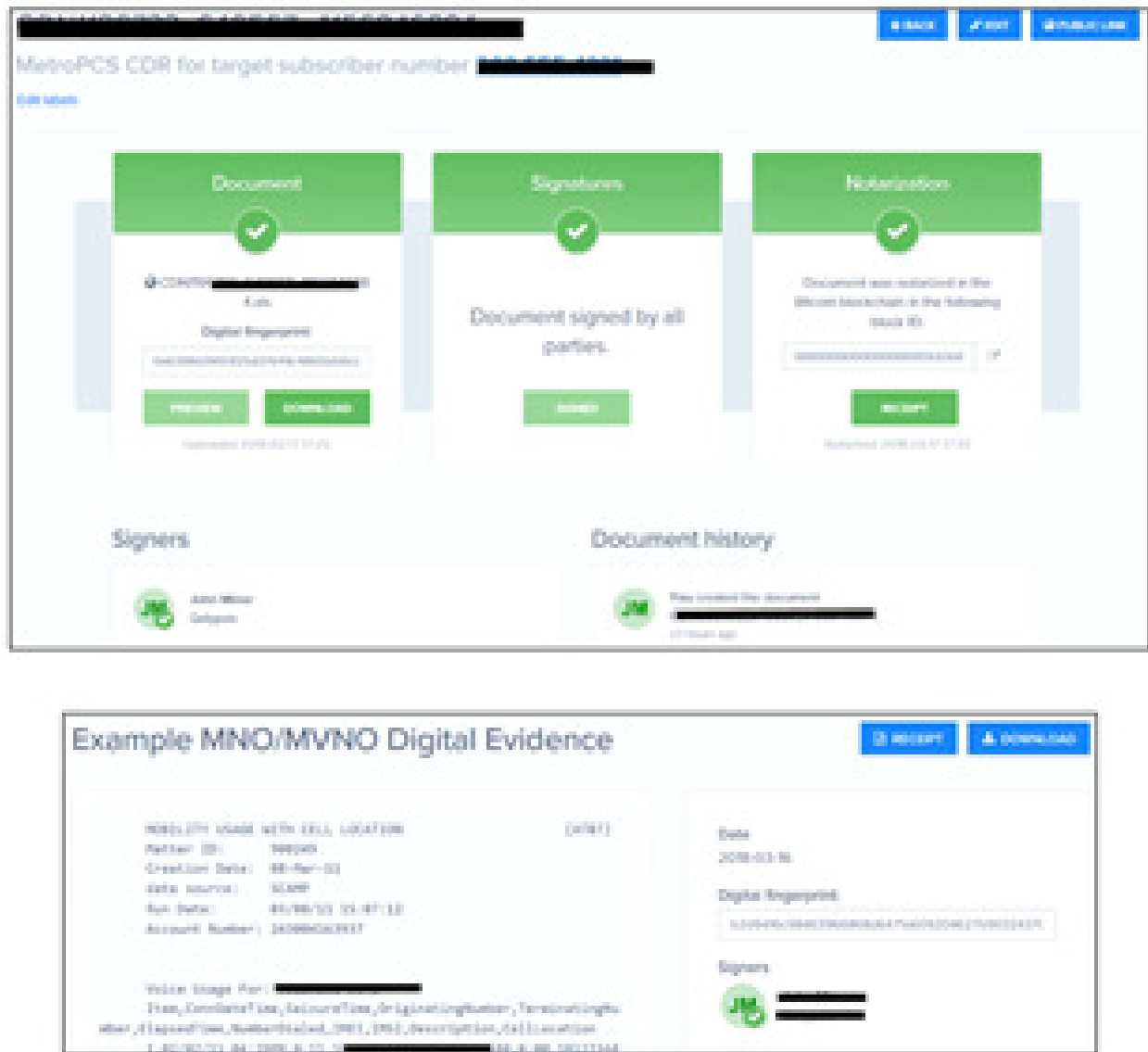


Figure 11. Example test Block-chain processing of MNO/MVNO evidence

4. The intake, verification function hash value calculation and signature process required a total of 1-2 minutes to perform for each evidence artifact. The final step in this process, notarization, required a short pause for verification of steps 1-3.
5. At this stage in the process the evidence receipt is available, and the evidence item is available to download by the requesting party.

Block-chain/DLT research (Bonomi 2018) (Lone 2019) has produced similar methods for evidence processing, demonstrating that at least conceptually, this is a potential solution that MNOs/MVNOs, and tech giants such as Facebook, Google and other technology platforms could readily integrate to introduce an evidence integrity maintenance process to legal records production as evidence.

Alternative solutions to the evidence integrity maintenance conundrum for



MNOs/MVNOs include the use of a digital certificate, by "[i]nserting the certification into the file", research of which has demonstrated, "is the only apparent reliable method and is the approach used by leading companies such as Microsoft and Adobe for digital signing of Office and PDF documents" (Curran 2017) offer potential resolution of this issue, however may be cumbersome to integrate.

## 6. CONCLUSIONS

The MNO/MVNO evidence analyzed during this research project was determined to be digital evidence. Subsequently, the evidence was subjected to a multi-part spoliation/taint test and examined to validate if each digital evidence artifact was identical to the evidence originally produced by the MNO/MVNO records custodian.

Over 74% of the evidence was determined to be spoliated/tainted based upon an analysis of the metadata creation/modification dates and/or authorship for each evidence artifact.

National and international standards for the preservation, integrity maintenance and handling of digital evidence were **not** followed in 100% of the evidence.

Neither chain of custody documentation nor verification function cryptographic hash values were found to be present within **any** of the evidence, further eliminating any opportunity to validate that the evidence analyzed was an exact copy of the original evidence produced by the MNO/MVNO.

If any evidence from the control group was offered as digital evidence in a court proceeding it should be precluded from admission as valid evidence based on the findings from this research. If challenged under FRE 806 (6)(E), absent adequate chain of custody documentation, verification function cryptographic checksum hash calculations ensuring evidence

integrity, and with affirmative evidence spoliation/taint indicators, such evidence should be precluded by a court.

The use of a variety of existing methods for maintaining the integrity of digital evidence offers an opportunity to bring much needed integrity to MNO/MVNO evidence production.

Use of Block-chain based DLT technology, researched and tested as an evidence integrity maintenance solution, would permit MNO/MVNO organizations to create chain of custody and verification function cryptographic hash value calculations during evidence production. The process could be performed with minimal human interaction, requiring no trusted third party while ensuring that evidence integrity endures during evidence conveyance among parties.

Further performance and conformity testing will ultimately evolve an adequately robust mechanism for preserving evidence integrity in MNO/MVNO environs. MNOs/MVNOs work together continuously to create global standards for the operation and inter-operation of mobile networks worldwide. No published standards work has occurred to jointly create a uniform evidence production format or evidence handling, integrity maintenance and conveyance protocols.

5G and future Generations of mobile networks are expected to continue to produce increasing volumes of evidence as continuous connectivity between subscribers reaches ubiquity and use of this evidence in criminal and civil cases becomes ever more prolific.

MNOs/MVNOs cooperate with government and law enforcement entities necessarily as a requirement of CALEA and other acts. The Federal Communications Commission (FCC) regulates radio frequency spectrum in the United States yet has no oversight regarding evidence produced by MNOs/MVNOs. Determination whether evidence produced

by MNOs/MVNOs is permissible in a courtroom as business records under FRE 803 (6) or is required to be treated as digital evidence falls under the scope of the United States Federal Judiciary. A persuasive argument using FRE 803 (6)(E) could result in a judicial decision that the current practice of introducing this evidence in a court as business records is an obsolete paradigm for MNO/MVNO evidence acceptance by courts, resulting in a shift in judicial precedent for this issue. The increased use of this type of evidence in criminal and civil cases could also result in U.S. Congress deciding to regulate these decisions through legislation to ensure that constitutional rights are upheld.

Only when MNOs/MVNOs follow well established digital evidence preservation, integrity maintenance and handling protocols will pristine evidence be found throughout the life cycle of a civil or criminal case.

## REFERENCES

- [1] American Society for Testing and Materials (ASTM)(2018), Standard Terminology for Digital and Multimedia Evidence. Retrieved on December 15, 2018 from <https://compass.astm.org/EDIT/html.annot.cgi?E2916+13#s00007>
- [2] American Society for Testing and Materials (ASTM)(2018). ASTM E3016-18 Standard Guide for Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis. Retrieved on January 4, 2019, from <https://www.astm.org/Standards/E3016.htm>
- [3] Bonomi, Silvia & Casini, Marco & Ciccotelli, Claudio. (2018). B-CoC: A Block-chain-based Chain of Custody for Evidences Management in Digital Forensics. Retrieved on June 6, 2019, from [https://www.researchgate.net/publication/326681814\\_B-CoC\\_A\\_Block-chain-based\\_Chain\\_of\\_Custody\\_for\\_Evidences\\_Management\\_in\\_Digital\\_Forensics](https://www.researchgate.net/publication/326681814_B-CoC_A_Block-chain-based_Chain_of_Custody_for_Evidences_Management_in_Digital_Forensics)
- [4] Cisco (2011). The Case for IP Backhaul - The Internet Protocol Journal, Volume 14, No. 3. Retrieved on January 4, 2019, from <https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-53/143-backhaul.html>
- [5] Curran, Kevin, Harran, Martin, & Farrelly, William. (2017). A method for verifying integrity & authenticating digital media. Letterkenny Institute of Technology, Donegal, Ireland, Ulster University, Derry, United Kingdom. Retrieved on June 6, 2019, from <https://doi.org/10.1016/j.aci.2017.05.006>
- [6] European Telecommunications Standards Institute (ETSI). (2005). Universal Mobile Telecommunications System (UMTS); Telecommunication management; Charging management; Charging architecture and principles (3GPP TS 32.240 version 6.2.0 Release 6)
- [7] Retrieved on January 4, 2019, from [http://www.etsi.org/deliver/etsi\\_ts/132200\\_132299/132240/06.02.00\\_60/ts\\_132240v060200p.pdf](http://www.etsi.org/deliver/etsi_ts/132200_132299/132240/06.02.00_60/ts_132240v060200p.pdf)
- [8] European Telecommunications Standards Institute (ETSI). (2014) Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Charging management; Diameter charging applications. Retrieved on January 4, 2019, from <https://www.etsi.org/deliver/etsi-ts/132200-132299/132299/09.17.00-60/ts-132299v091700p.pdf>
- [9] European Telecommunications Standards Institute (ETSI). (2016). Digital cellular

- telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunications management; Charging management; Charging Data Record (CDR) file format and transfer (#GPP TS version 13.2.0 Release 13). Retrieved on January 4, 2019, from [http://www.etsi.org/deliver/etsi\\_ts/132200\\_132299/132297/13.02.00\\_60/ts\\_132297v130200p.pdf](http://www.etsi.org/deliver/etsi_ts/132200_132299/132297/13.02.00_60/ts_132297v130200p.pdf)
- [10] European Telecommunications Standards Institute (ETSI). (2017). ETSI Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Charging management; Charging Data Record (CDR) parameter description. Retrieved on January 4, 2019, from [http://www.etsi.org/deliver/etsi\\_ts/132200\\_132299/132298/12.06.00\\_60/ts\\_132298v120600p.pdf](http://www.etsi.org/deliver/etsi_ts/132200_132299/132298/12.06.00_60/ts_132298v120600p.pdf)
- [11] Gramoli, Vincent & Staples, Mark. (2018). Block-chain Standard: Can We Reach Consensus?. IEEE Communications Standards Magazine. 2. 16-21. 10.1109/M-COMSTD.2018.1800022.
- [12] International Organization for Standardization (ISO)(2012). Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Retrieved on January 4, 2019, from <https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en>
- [13] Internet Engineering Task Force (IETF)(2002). Guidelines for Evidence Collection and Archiving. Retrieved on January 4, 2019, from <http://www.ietf.org/rfc/rfc3227.txt>
- [14] Internet Engineering Task Force (IETF)(2005). Common Format and MIME Type for Comma-Separated Values (CSV) Files. Retrieved on January 4, 2019, from <https://tools.ietf.org/html/rfc4180>
- [15] Internet Engineering Task Force (IETF)(2011). Fundamental Elliptic Curve Cryptography Algorithms. Retrieved on January 4, 2019, from <https://tools.ietf.org/html/rfc6090>
- [16] Internet Engineering Task Force (IETF)(2016). Elliptic Curves for Security. Retrieved on January 4, 2019, from <https://tools.ietf.org/html/rfc7748>
- [17] Lone, Auqib Hamid & Mir, Roohie Naaz,. (2019). Forensic-chain: Block-chain based digital forensics chain of custody with PoC in Hyperledger Composer. Department of Computer Science and Engineering, NIT Srinagar, Jammu and Kashmir, 190006, India. Retrieved on June 6, 2019, from <https://www.sciencedirect.com/science/article/pii/S174228761830344X>
- [18] Minor, J. B. (2015). A method of validating cellular carrier records accuracy, U.S. Patent No. 9,113,307. Washington, DC: U.S. Patent and Trademark Office. Retrieved on January 4, 2019, from <https://www.google.com/patents/US9113307>
- [19] Minor, John B. (2017) "Forensic Cell Site Analysis: A Validation & Error Mitigation Methodology," *Journal of Digital Forensics, Security and Law*: Vol. 12: No. 2, Article 7. DOI: <https://doi.org/10.15394/jdfsl.2017.1474> Retrieved on January 4, 2019, from <https://commons.erau.edu/jdfsl/vol12/iss2/7>
- [20] National Institute of Standards and Technology (NIST)(2000). DIGI-

TAL SIGNATURE STANDARD (DSS). Retrieved on December 14, 2019, from <https://csrc.nist.gov/csrc/media/publications/fips/186/2/archive/2000-01-27/documents/fips186-2.pdf>

[21] National Institute of Standards and Technology (NIST)(2007). Guidelines on Cell Phone Forensics. Retrieved on December 14, 2019, from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf>

[22] National Institute of Standards and Technology (NIST)(2006). Guide to Integrating Forensic Techniques into Incident Response. Retrieved on December 14, 2019, from <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>

[23] Openchain. (2019) Openchain is an open source distributed ledger technology. Retrieved on January 4, 2019, from <https://www.openchain.org/>

[24] Pennsylvania Superior Court. (PSC)(2016). Commonwealth of Pennsylvania vs. Bryant Jones, No. 865 WDA 2015 (page 17). Retrieved on January 4, 2019, from <http://www.pacourts.us/assets/opinions/Superior/out/J-S37012-16m.pdf>

[25] Peredo, Oscar & Deschamps, Roman. (2017). Time Accuracy Analysis of Post-Mediation Packet-Switched Charging Data Records for Urban Mobility Applications. Retrieved on January 4, 2019, from [https://www.researchgate.net/publication/316921278\\_Time\\_Accuracy\\_Analysis\\_of\\_Post-Mediation\\_Packet-Switched\\_Charging\\_Data\\_Records\\_for\\_Urban\\_Mobility\\_Applications](https://www.researchgate.net/publication/316921278_Time_Accuracy_Analysis_of_Post-Mediation_Packet-Switched_Charging_Data_Records_for_Urban_Mobility_Applications)

[26] Scientific Working Group on Digital Evidence (SWGDE)(2017). SWGDE

Recommendations for Cell Site Analysis. Retrieved on January 4, 2019, from <https://www.swgde.org/documents/CurrentDocuments/SWGDERecommendationsforCellsiteAnalysis>.

[27] The National Domestic Communications Assistance Center. (NDCAC)(2018). Retrieved on January 4, 2019, from <https://ndcac.fbi.gov/>

[28] United States Courts Federal Rules of Evidence (FRE).(2019). Exception to the Rule Against Hearsay. Retrieved on January 4, 2019, from <https://www.rulesofevidence.org/article-viii/rule-803/>