Forensic Analytics

Digital Forensic Experts

White Paper

LIMSRV

THE QUEEN'S AWARDS FOR ENTERPRISE: INNOVATION 2021

Introduction

This white paper is designed to offer a technically complete definition of a Modem state recorded by Quectel Modems (which are installed in Lima CM) called LIMSRV. This Modem state may periodically be recorded in RF Survey results. There are currently questions and some confusion in relation to how LIMSRV rows of data should be interpreted and whether LIMSRV measurements are representative of viable serving cells or not and most importantly whether LIMSRV measurement rows can be considered evidentially sound.

It is important to acknowledge that any cellular Modem which adheres to 3GPP Specifications will have exactly the same the LIMSRV state condition which could be seen in the same way that Lima CM displays it if a device makes this data available (which generally they don't). This LIMSRV state is therefore not limited to Quectel Modems, it exists in every standards compliant cellular Modem on the planet and will record this state within their log files if and when they occur.

The overall objective of this paper is to ensure that the RF Community have absolute confidence in the evidential veracity of radio surveys undertaken and the data recorded by Lima CM.

Executive Summary

LIMSRV is a record of a cell found to provide dominance in an area according to a set of metrics which are very clearly defined for each radio technology (2G – 5G) in 3GPP Technical Specification (TS) and which have to be satisfied in order to record a specific cell as serving in terms of a signal strength and a set of signal quality.

Whether a cell ID is recorded under the Modem conditions LIMSRV, NOCONN or CONNECT the interpretation of the RF Technician is the same. A serving cell has been recorded.

This has nothing to do with whether a cell has the capacity to carry a transaction in active or connected mode or not, it has everything to do with recording dominance at a location. In the same way that it is not possible to say with absolute certainty whether a serving cell measured in idle mode will be the cell selected by the network to carry call or data traffic, the fact that a cell has been recorded as providing dominance to an area is often sufficient to draw a conclusion.

LIMSRV and NOCONN Modem states record RF data for cells exhibiting dominance to an area – that is all they are – accurate and evidentially sound records of cellular dominance.

It would be wrong to remove LIMSRV rows from any network survey results as what you would be removing is evidential records of cells found to provide serving coverage at locations within a radio survey and arguable this could be considered tampering with the evidence unless you can provide a rationale for doing so. Either way you would be diminishing the granularity of a radio survey for no discernible benefit.

What is LIMSRV?

Cellular Modems including the Quectel Modems utilised within Lima CM have four operating states.

- SEARCH – Search for a "suitable" Cell
- LIMSRV – Camped On, Not Registered with the Network
- NOCONN – Camped On, Registered with the Network
- CONNECT – Connected in a voice or data call

NOCONN is the prevalent state of a Modem measuring RF readings in the idle condition. CONNECT is a state recorded when the Lima CM is in the middle of an active or connected mode survey undertaking calls and/or generating data. LIMSRV can periodically appear within RF Readings and should be considered the same as a NOCONN state in terms of how it must be interpreted.

It is important to note that LIMSRV is not the same as Limited Service (although at first glance you could be forgiven for thinking so as they seem to be related). Limited Service has a very specific meaning within cellular engineering and concerns devices which can only use the emergency services and can therefore attach to an "acceptable cell" on any network to do so. An acceptable cell in this case means a cell which is supplying serving coverage independently of whichever Cellular Service Providers' cell it is – in other words a viable cell from any network.

LIMSRV is not related to a service – it is merely a Modem state, which when recorded indicates that the Modem has successfully completed the cell selection/reselection activity and has not completed the network attach procedure or that the attach procedure has not completed successfully. The Modem remains camped on a "suitable cell", but the registration process is incomplete. The Modem will continue to actively monitor the radio environment for other suitable cells should the radio conditions change, in the same way as any idle mode survey. If a Lima CM was moving around an area for example, even in the LIMSRV state a Modem would continue to undertake the cell selection/reselection process based upon the prevailing radio conditions.

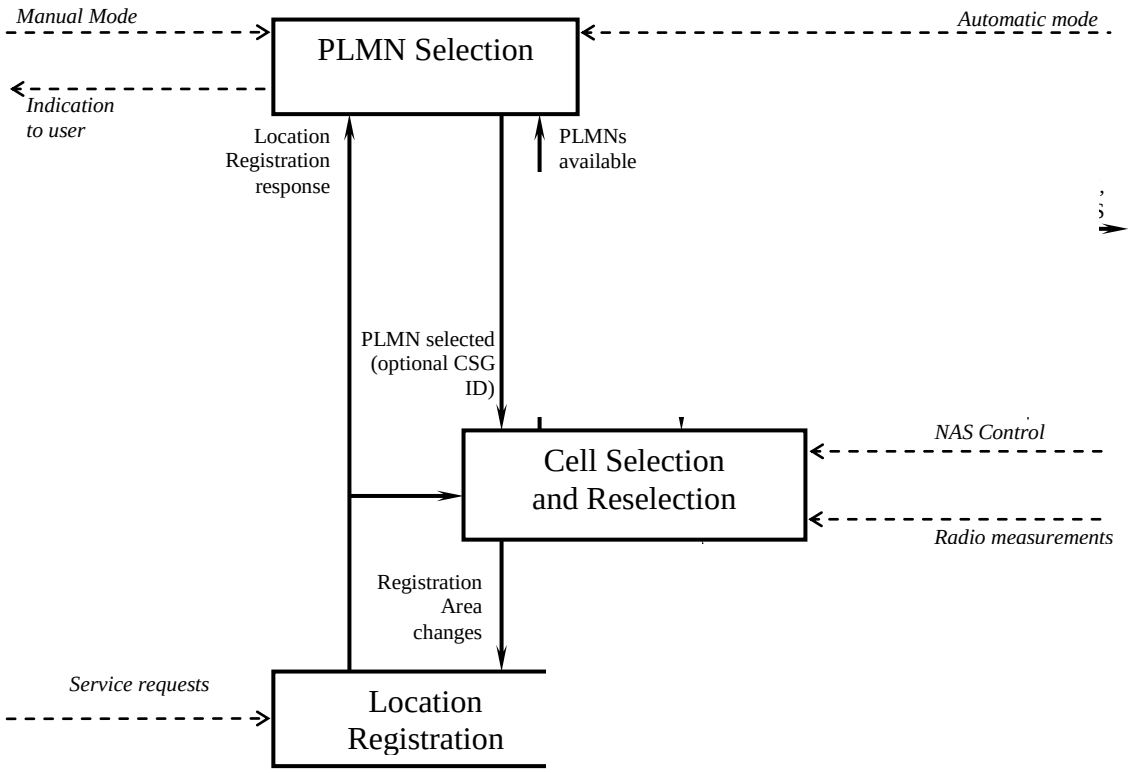
The key issue here is that a suitable cell (which has a specific definition in cellular engineering, meaning serving cell) is one which has been selected over others. A Modem has therefore rejected other cells in an area on the basis that they don't offer better signal strength and/or signal quality. It is a serving cell and therefore a LIMSRV reading in a set of RF readings may be considered a state whereby the Modem has not yet successfully completed the network registration process and attach to the network, but it is not a failed RF reading and it is not indicative of a cell which is incapable of carrying traffic.

Quectel define the condition LIMSRV in an unhelpful way as it does not offer sufficient clarity and there is room for misinterpretation. In order to understand what is meant by the LIMSRV state it is worth interrogating the 3GPP specifications and consider the activity undertaken by any mobile device in order to select a suitable cell and to camp on to the network.

Given that 2G, 3G, 4G and 5G are all fundamentally attempting to achieve the same thing – successful end to end mobile communication. Despite of the various radio access technologies (the

Access Stratum (AS)) being different the general principles of network selection and attachment are largely the same so for brevity I will focus in detail on 4G only.

As detailed within 3GPP TS 36.304 V16.7.0 (2022-03), a mobile handset will go through the steps detailed below and in the associated diagram in Idle mode in order to register with the network.



Modified diagram from 3GPP TS 36.304 V16.7.0 (2022-03)

In the diagram above details the process a mobile device will go through as it attempts to select, camp on, and register with a network:

- PLMN Select – Public Land Mobile Network (a generic term for a cellular network). Cellular Network Select can be manual or automated.
- Cell Select/Reselect – This may involve interaction via the Non-Access Stratum (NAS) (Core Network) as part of determining which PLMN to attach to, and it will always involve RF measurements once a PLMN has been determined. With cell selection, the UE (User Equipment) searches for a suitable cell of the selected PLMN and chooses that cell to provide available services, further the UE shall tune to its control channel. This choosing is known as "camping on the cell". I'll consider what is meant by a "suitable cell" later in the paper. If the UE finds a more suitable cell, according to the cell reselection criteria, it reselects onto that cell and camps on it.

- Location Registration – The UE shall, if necessary, then register its presence, by means of a NAS (Core Network) registration procedure, in the tracking area of the chosen cell and as outcome of a successful Location Registration the selected PLMN becomes the registered PLMN TS 23.122.

Cell Selection Criteria

The UE shall use one of the following two cell selection procedures:

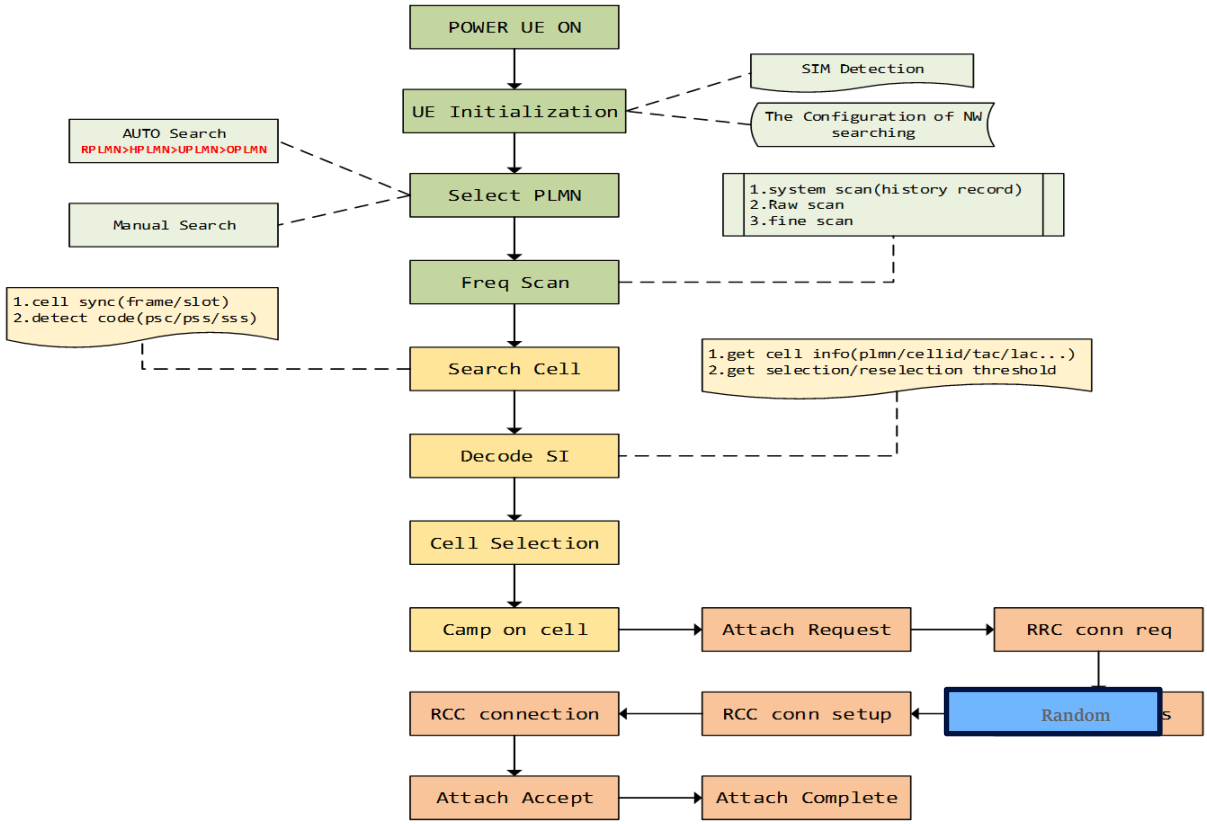
Initial Cell Selection

This procedure requires no prior knowledge of which RF channels are Evolved Universal Terrestrial Radio Access (E-UTRA) carriers. The UE shall scan all RF channels in the E-UTRA bands according to its capabilities to find a suitable cell. On each carrier frequency, the UE need only search for the strongest cell. Once a suitable cell is found this cell shall be selected.

Stored Information Cell Selection

This procedure requires stored information of carrier frequencies and optionally also information on cell parameters, from previously received measurement control information elements or from previously detected cells. Once the UE has found a suitable cell the UE shall select it. If no suitable cell is found the Initial Cell Selection procedure shall be started once more.

If we consider the process undertaken by the Quectel Modems we can see that the process followed is entirely consistent with the 3GPP Specifications.



Note that there are a number of processes undertaken before the Modem camps on to a cell. This will include synchronising up to the air interface and reading system information packets (MIBs and SIBs) which will allow the Modem to determine which networks, channels, and cells it can see.

Whilst determining which network it can connect to it can also be controlled to ensure that it also knows which ones it can't connect to. With a standard commercial off the shelf mobile handset with a national SIM card installed, there is a forbidden list (dependent upon which UK network). The forbidden list determines which PLMNs (mobile networks) a handset can attach to outside of an emergency situation, in which it simply requires access via an "acceptable cell". This means that if I have a Vodafone SIM card deployed within my handset, even though my handset would be capable of seeing all the other UK networks, and measuring their radio signals – my handset would in effect be barred from connecting to those networks. This is not done for technical reasons (although there are some good ones) it is done for commercial reasons to lock in revenue to the Cell Service Provider of choice, Vodafone in this case.

Lima CM SIMs do not have a forbidden list as they are designed to attach to every network as determined by the Lima CM operator on demand – which of course gives great flexibility to the RF Surveyor. Through the user interface, Lima CM can be locked to a specific network which will inhibit Lima CM from attaching to other networks, which achieves the same outcome as would a forbidden list.

I'd like to focus on the three boxes labelled Decode SI, Cell Selection and Camp on Cell as this is critical to understanding the LIMSRV Modem state.

Decode SI – Decode System Information – which means to read broadcast channels to determine Cellular Service Provider, Radio Channels, Cell Configurations, Common Identifiers – such as PLMN, LAC/TAC, Cell ID (CGI), cell configuration parameters which can be used in the cell selection process.

Cell Selection – From all the cells which are visible to the Modem broadcast on the network that the Modem can "see" the Modem will determine which cell is the most attractive based upon criteria detailed below. For a cell to be selected by UE, it must meet the Cell Selection Criterion. This is set out in 3GPP Reference: GSM TS 43.022, 3G UTRAN TS 25.304, LTE TS 36.304 and 5G New Radio NR) TS 38.304.

This process involves the User Equipment (UE) looking at each cell that it can detect over the air interface and in effect giving them and strength and quality score. This can be influenced by a service provider as they may (for various reasons beyond the scope of this paper) wish to steer a handset to a particular cell.

The key parameter here is the S (Selection Criteria), this is a calculated value determined as a result of utilising over the air parameters broadcast by a cell and also as a function of the RF Signal readings that a Modem is measuring and is in effect a calculated number. A very poor signal is likely to produce an outcome for S which is less than 0 and therefore be unattractive to the Modem. A strong signal will produce an outcome which is greater than 0 and for all the viable cells that a Modem can detect, one will have a higher S value than any other.

The selection criteria if fulfilled if

Srxlev > 0 - where the quality as well as the signal strength are being consider then the following applies;

Srxlev > 0 AND Squal > 0 - where:

Srxlev = Qrxlevmeas – Qrxlevmin – Pcompensation - Qoffsettemp

Squal = Qqualmeas – Qqualmin - Qoffsettemp

A UE (User Equipment) will select the best cell whose Srxlev and Squal are greater than 0.

Srxlev = Qrxlevmeas – (Qrxlevmin + Qrxlevminoffset) – Pcompensation.

A definition of the parameters featured as part of cell selection are detailed below and whilst they do tend to be overly complex – cell selection is a matter of the dominant cell as determined by the RF measurements a Modem undertakes whilst factoring these against any service provider steering preferences;

Srxlev	Cell selection RX level value (dB)
Squal	Cell selection quality value (dB)
$Qoffset_{temp}$	Offset temporarily applied to a cell as specified in TS 36.331 (dB)
$Q_{rxlevmeas}$	Measured cell RX level value (RSRP)
$Q_{qualmeas}$	Measured cell quality value (RSRQ)
$Q_{rxlevmin}$	Minimum required RX level in the cell (dBm)
$Q_{qualmin}$	Minimum required quality level in the cell (dB)

Pcompensation	If the UE supports the additionalPmax in the NS-PmaxList-NB, if present, in SIB1-NB, SIB3-NB and SIB5-NB:
	$\max(P_{EMAX1} - P_{PowerClass}, 0) - (\min(P_{EMAX2}, P_{PowerClass}) - \min(P_{EMAX1}, P_{PowerClass}))$ (dB);
	else:
	if $P_{PowerClass}$ is 14 dBm:
	$\max(P_{EMAX1} - (P_{PowerClass} - Poffset), 0)$ (dB);
	else:
	$\max(P_{EMAX1} - P_{PowerClass}, 0)$ (dB)

P_{EMAX1}, P_{EMAX2}	Maximum TX power level an UE may use when transmitting on the uplink in the cell (dBm) defined as P_{EMAX} in TS 36.101. P_{EMAX1} and P_{EMAX2} are obtained from the p-Max and the NS-PmaxList-NB respectively in SIB1-NB, SIB3-NB and SIB5-NB as specified in TS 36.331.
$P_{PowerClass}$	Maximum RF output power of the UE (dBm) according to the UE power class as defined in TS 36.101

Camping on a Cell

Camp on a Cell – In line with the state diagram above. The next stage is for a Modem to register and attach to the network. Once this has been completed, the Modem will be in the NOCONN state. It is in the idle condition, it is attached to the network, but it is not in a position whereby it is in a call or sending data (connected state) The NOCONN state is the condition that the Modem is in for the majority of the time when surveying.

Whether a Modem is successful with the registration process or not, the handset remains camped on a cell selected for dominance on a specific network which is capable of cell reselection. This means that another cell can be chosen when the prevailing radio conditions trigger cell reselection.

Cell Reselection – As the name suggests, a cell reselection process will occur if the radio conditions change. Periodically the Modem will do the following;

- Monitor relevant System Information as specified in TS 36.331.
- Perform necessary measurements for the cell reselection evaluation procedure.
- Execute the cell reselection evaluation process on the following occasions/triggers:
    - UE internal triggers, so as to meet performance as specified in TS 36.133
    - When information on the BCCH used for the cell reselection evaluation procedure has been modified.

Cell reselection is a constant, ongoing part of mobile device behaviour and is fundamental to ensure optimal cell selection, mobility and to ensure continuity of service.

Cell Categories

Different types of Cell Categories have been defined which are useful for definition purposes:

Acceptable cell: An “acceptable cell” is a cell on which the UE may camp to obtain limited service (originate emergency calls and receive Earthquake, Tsunami, Warning System (ETWS) notifications). An example of where this could be used is where either no SIM card exists, and an emergency call is necessary. The other example is where a SIM card does exist, but there is no viable cellular signal from the incumbent network and an emergency call is necessary.

This is not the same as LIMSRV which could be a point of confusion. LIMSRV occurs as a result of a Modem having successfully camped on a cell but has not completed or failed to complete the registration process.

Suitable cell: A “suitable cell” is a cell on which the UE may camp on to obtain normal service. The term suitable here relates to a cell which has been selected as part of the cell selection/reselection process and as such is the cell which provides dominance to an area and can therefore be considered a serving cell.

Barred cell: A cell is barred if it is so indicated in the system information. This does not generally affect RF Surveying.

Reserved cell: A cell is reserved if it is so indicated in system information. This does not generally affect RF Surveying.

Quectel Specific Modem Sequence

A Quectel Modem will follow the following initiation process.

Modem Status - Search

The search state is described as the Modem searching for a **suitable cell**. As discussed, this has a specific definition which is detailed above. A suitable cell therefore is one which exhibits the minimum requirements for cell selection and one which provides service to an area – as serving cell.

After power-on and UE initialization, the first step is to Select PLMN:

- When starting up, the module will read NV (Non Volative RAM) to check user configuration.
- Then it will check whether COPS (Command OPerator Selection)/ nwscanmode (Network Scan Mode)/ nwscanseq (Network Scan Sequence) commands are configured. If not, it will be in auto mode and it will automatically select a dominant cell on the network of interest.
- Elementary Files (EF) files is a complex way of stating that a SIM contains configuration data which determines a number of things including the identifiers are of the SIM (EFIMSI) for example which contains the IMSI number. The module will then check whether the EFepsloci (Evolved Packet System Location Information) and EFpsloci (Evolved Packet Switched Location Information) files in the SIM card are valid. If they are valid, it will use the PLMN (or RemotePLMN) in the file; otherwise, it will use HomePLMN. These files are configured when you configure Lima CM through the companion app on the tablet.
- When the HomePLMN is used (as would be the case with a native SIM card in a home country), it will check whether RAT (Radio Access Technology) priority is configured – which again is configured through the companion app.
- When RemotePLMN is used, it will check the NV (Non rplmnact (system registered in the previous session) Information and use this to initiate network search.

Next steps are Frequency Scan & Search Cell.

Using Frequency Scan, the UE selects the frequency/EARFCN for camping:

- There are two types of frequency scan:
    - System scan, also known as history list frequency scan (scan using acquisition database, that is result of all previous scanning attempts)
    - Band scan, also known as Full Frequency scan
- If the UE can read one or several PLMN identities, each found PLMN shall be reported to NAS as a high-quality PLMN, provided the following criteria is fulfilled:
    - For an E-UTRAN cell, the measured RSRP value shall be ≥ -110 dBm.

Once the search stage is completed the Modem moves to the camping on stage. And only when a Modem has successfully camped on to a cell will it complete this stage. Any Modem which has moved from the search state to the camped-on state (which is true of the LIMSRV or NOCONN state) will have completed the search and camping on processes having found a suitable cell.

In 3GPP TS 36.304 V16.7.0 (2022-03) it states that if the UE is unable to find a suitable cell to camp on or if the location registration failed (except for LR rejected with cause #12, cause #14, cause #15 or cause #25, see TS 23.122 [5] and TS 24.301 [16]), it attempts to camp on a cell irrespective of the PLMN identity, and enters a "limited service" state.

This would be true were the SIM cards not locked to a specific PLMN. This means that even in the LIMSRV state the Modem continues to seek out the dominant cell of that PLMN selecting and reselecting cells accordingly.

Why is LIMSRV occurring?

To be clear an RF measurement recorded with a Modem in LIMSRV is as reliable as an RF measurement which has been taken in the NOCONN state. The difference between the LIMSRV state and the NOCONN state is found in the post processing after the completion of the camping on state. The difference is whether the cell registration (and attach) process has been successfully completed or not – which is a function of the signalling between a Modem and the core network rather then a measure of RF reliability.

In order to determine why this happens periodically we would need access to the TS 23.122 cause codes so we could see exactly where this occasional failure in registration was occurring. This has not been undertaken thus far so we wouldn't speculate. This does not undermine the validity of the RF reading, however.

After the Modem finds a suitable cell and camps on it (at this moment the module is connected to the specific base station), it will send the Attach Request over the NAS.

If the Network accepts this request,

- it will first send to the module Attach Accept message (among others, this message will carry on the IP address that is assigned to the module)
- and then it will send the Attach Complete message to the module.

At this point, the attach process is finished, and the module will have available services from the NW that are according to the agreement of the SIM provider and NW operator. In this case, the state can be "CONNECT" or "NOCONN", depending upon whether the Modem is active or idle.

Can we prove LIMSRV readings are reliable

We have undertaken a lot of testing around this area. Whilst there are only a small percentages of rows of entries within any data set, a LIMSRV reading could still be critical to an investigation and therefore a reading which has to be relied upon.

One of the challenges associated with attempting to prove the reliability of LIMSRV is to reproduce it consistently so that it can be tested in as close to a controlled environment as one can get with a highly dynamic radio environment. As it is something that occurs ocasionally and somewhat randomly, this presents a challenge. Even cells against which LIMSRV is recorded in one second, can then switch to NOCONN and maintain that condition henceforth.

Notwithstanding the above, we have managed to identify areas where LIMSRV has manifested itself and we have been able to test it.

Cell Selection/Reselection

Every Modem within Lima CM is constantly assessing and reassessing which cell is best placed to provide serving coverage at a given location and as radio conditions change then a new cell may be selected as the cell to camp on to.

This will occur whether or not a Modem is exhibiting LIMSRV or NOCONN.

The example below is from a set of readings for the same Modem wihtin Lima CM and in this case measuring UMTS. Note that the Modem state is LIMSRV and there is clearly a cell reselection which has taken place, as the LAC changes as we enter a new location area (LAC).

timestamp	longitude	latitude	tech_ce	type	cellid	lac_tac	band	channe	tech_as	net_ass	imei	slot	mode	signalst	encrypt	netnam	bsic	rnc_id	psc	serving	ecno
22/07/2022 13:49:11	000 10.7018W	51 35.5089N	3G	SERVING	42774	142	2100	10564	UMTS	23420	862348056533110	4	i	-115		23420		128	150	LIMSRV	-21
22/07/2022 13:49:12	000 10.7018W	51 35.5089N	3G	SERVING	41705	1217	2100	10588	UMTS	23420	862348056533110	4	i	-115		23420		125	89	LIMSRV	-21

If a Modem is in the LIMSRV state, that does not become the quiescent state for that Modem and is a state from which the Modem could change to NOCONN at any time as detailed in the two readings below:

timestamp	longitude	latitude	tech_ce	type	cellid	lac_tac	band	channe	tech_as	net_ass	imei	slot	mode	signalst	encrypt	netnam	bsic	rnc_id	psc	serving	ecno	rank
22/07/2022 13:49:21	000 10.7018W	51 35.5089N	3G	SERVING	41705	1217	2100	10588	UMTS	23420	862348056533110	4	i	-113		23420		125	89	LIMSRV	-19	
22/07/2022 13:49:22	000 10.7018W	51 35.5089N	3G	SERVING	41705	1217	2100	10588	UMTS	23420	862348056533110	4	i	-115		23420		125	89	NOCONN	-20	

A consideration for RF surveying is whether a Modem which is in the LIMSRV state is capable of carrying a call or not.

In the table below the Modem in slot 12 is in the CONNECT state as it is undertaking a call (highlighted in yellow), and at the same time as the call on slot 12, the Modem in slot 13 was recording cell 42772 as the serving cell (but still in a LIMSRV state):

13/07/2022 13:02:08	13/07/2022 13:02:08	3G	SERVING	42774	2100	23420	12	Id	CONNECT
13/07/2022 13:02:09	13/07/2022 13:02:09	3G	SERVING	42774	2100	23420	13	I	LIMSRV
13/07/2022 13:02:09	13/07/2022 13:02:09	3G	SERVING	42774	2100	23420	12	Id	CONNECT
13/07/2022 13:02:10	13/07/2022 13:02:10	3G	SERVING	42774	2100	23420	13	I	LIMSRV
13/07/2022 13:02:10	13/07/2022 13:02:10	3G	SERVING	42774	2100	23420	12	Id	CONNECT
13/07/2022 13:02:11	13/07/2022 13:02:11	3G	SERVING	42774	2100	23420	13	I	LIMSRV
13/07/2022 13:02:11	13/07/2022 13:02:11	3G	SERVING	42774	2100	23420	12	Id	CONNECT
13/07/2022 13:02:12	13/07/2022 13:02:12	3G	SERVING	42774	2100	23420	13	I	LIMSRV
13/07/2022 13:02:12	13/07/2022 13:02:12	3G	SERVING	42774	2100	23420	12	Id	CONNECT
13/07/2022 13:02:13	13/07/2022 13:02:13	3G	SERVING	42774	2100	23420	13	I	LIMSRV
13/07/2022 13:02:13	13/07/2022 13:02:13	3G	SERVING	42774	2100	23420	12	Id	CONNECT
13/07/2022 13:02:14	13/07/2022 13:02:14	3G	SERVING	42774	2100	23420	13	I	LIMSRV
13/07/2022 13:02:14	13/07/2022 13:02:14	3G	SERVING	42774	2100	23420	12	Id	CONNECT

We have again undertaken testing on this specific question.

On a recent survey we found a cell (41705) which was 3G H3G and which was tagged as LIMSRV at the location in which the survey was being undertaken. All the results were taken at the same spot.

The Lima CM was configured like so:

- Modem 1 – H3/3G (Tele2)
- Modem 2 – H3/3G (Native PAYG SIM)
- Modem 3 – H3/3G (Tele2)
- Modem 4 – H3/3G (Tele2)

In the data below, you can see that cell 41705 was recorded as LIMSRV on Modem 4 (Tele2 SIM) at around 13:49hrs.

There were successful test calls on this cell using slot 4 (Tele2 SIM) at 13:56hrs and 13:58hrs (however, the Lima CM was not recording cell 41705 as LIMSRV at this time but did a few mins earlier at the same location).

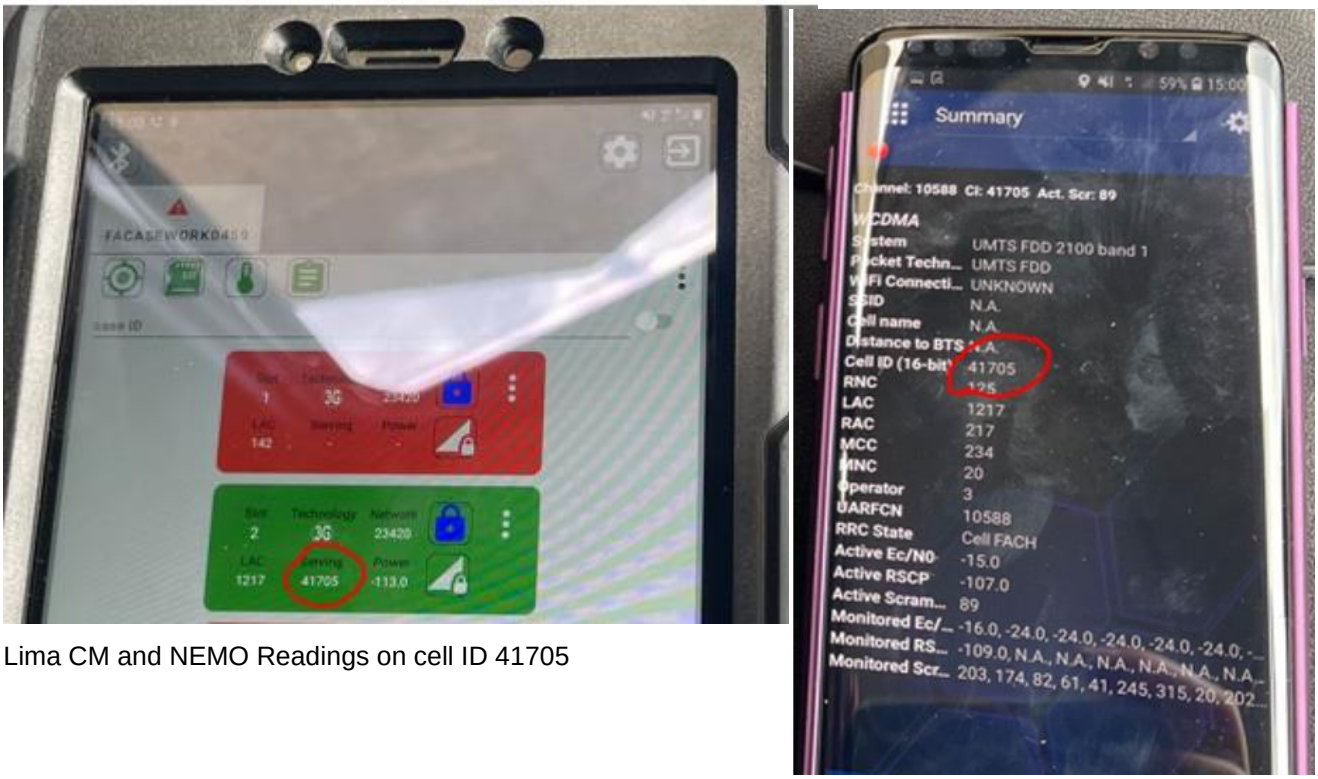
There was also a successful test call on this cell using slot 2 (H3G PAYG SIM) at 13:59hrs.

Calls were successfully completed on Tele2 SIMs and H3G PAYG SIMs at the same location where the Lima CM was recording cell ID 41705 as a LIMSRV cell.

	A	B	C	D	E	F	G	H	I	J	K
	timestamp	gpstimestamp	tech_ce	type	cellid	band	channe	net_ass	slot	mode	serving	tate
4	22/07/2022 13:49:12	22/07/2022 13:49:11	3G	SERVING	41705	2100	10588	23420	4	i	LIMSRV	
6	22/07/2022 13:49:13	22/07/2022 13:49:12	3G	SERVING	41705	2100	10588	23420	4	i	LIMSRV	
8	22/07/2022 13:49:14	22/07/2022 13:49:13	3G	SERVING	41705	2100	10588	23420	4	i	LIMSRV	
0	22/07/2022 13:49:15	22/07/2022 13:49:14	3G	SERVING	41705	2100	10588	23420	4	i	LIMSRV	
1	22/07/2022 13:49:16	22/07/2022 13:49:15	3G	SERVING	41705	2100	10588	23420	4	i	LIMSRV	
3	22/07/2022 13:49:17	22/07/2022 13:49:16	3G	SERVING	41705	2100	10588	23420	4	i	LIMSRV	
4	22/07/2022 13:49:18	22/07/2022 13:49:17	3G	SERVING	41705	2100	10588	23420	4	i	LIMSRV	
5	22/07/2022 13:49:19	22/07/2022 13:49:18	3G	SERVING	41705	2100	10588	23420	4	i	LIMSRV	
6	22/07/2022 13:49:20	22/07/2022 13:49:19	3G	SERVING	41705	2100	10588	23420	4	i	LIMSRV	
7	22/07/2022 13:49:21	22/07/2022 13:49:20	3G	SERVING	41705	2100	10588	23420	4	i	LIMSRV	
7	22/07/2022 13:56:33	22/07/2022 13:56:33	3G	SERVING	41705	2100	10588	23420	4	d	CONNECT	
8	22/07/2022 13:56:34	22/07/2022 13:56:34	3G	SERVING	41705	2100	10588	23420	4	d	CONNECT	
9	22/07/2022 13:56:35	22/07/2022 13:56:35	3G	SERVING	41705	2100	10588	23420	4	d	CONNECT	
0	22/07/2022 13:56:36	22/07/2022 13:56:36	3G	SERVING	41705	2100	10588	23420	4	d	CONNECT	
1	22/07/2022 13:56:37	22/07/2022 13:56:37	3G	SERVING	41705	2100	10588	23420	4	d	CONNECT	
2	22/07/2022 13:56:38	22/07/2022 13:56:38	3G	SERVING	41705	2100	10588	23420	4	d	CONNECT	
3	22/07/2022 13:56:39	22/07/2022 13:56:39	3G	SERVING	41705	2100	10588	23420	4	d	CONNECT	
2	22/07/2022 13:58:11	22/07/2022 13:58:11	3G	SERVING	41705	2100	10588	23420	4	d	CONNECT	
3	22/07/2022 13:58:12	22/07/2022 13:58:12	3G	SERVING	41705	2100	10588	23420	4	d	CONNECT	
4	22/07/2022 13:58:13	22/07/2022 13:58:12	3G	SERVING	41705	2100	10588	23420	4	d	CONNECT	
5	22/07/2022 13:58:14	22/07/2022 13:58:14	3G	SERVING	41705	2100	10588	23420	4	d	CONNECT	
6	22/07/2022 13:58:15	22/07/2022 13:58:15	3G	SERVING	41705	2100	10588	23420	4	d	CONNECT	
6	22/07/2022 13:59:53	22/07/2022 13:59:52	3G	SERVING	41705	2100	10588	23420	2	d	CONNECT	
7	22/07/2022 13:59:54	22/07/2022 13:59:53	3G	SERVING	41705	2100	10588	23420	2	d	CONNECT	
8	22/07/2022 13:59:55	22/07/2022 13:59:54	3G	SERVING	41705	2100	10588	23420	2	d	CONNECT	
9	22/07/2022 13:59:56	22/07/2022 13:59:54	3G	SERVING	41705	2100	10588	23420	2	d	CONNECT	
0	22/07/2022 13:59:57	22/07/2022 13:59:56	3G	SERVING	41705	2100	10588	23420	2	d	CONNECT	
1	22/07/2022 13:59:58	22/07/2022 13:59:57	3G	SERVING	41705	2100	10588	23420	2	d	CONNECT	
2	22/07/2022 13:59:59	22/07/2022 13:59:58	3G	SERVING	41705	2100	10588	23420	2	d	CONNECT	
3												

In order to validate the results, a Nemo was utilised which also recorded cell 41705 as a serving cell at this location. Multiple test calls were undertaken on both devices and as can be seen above the Lima CM was able to utilise this cell in order undertake a call.

The images below records what the Lima CM was recording as a serving cell at the same time as a



Lima CM and NEMO Readings on cell ID 41705

Conclusion

LIMSRV is a Modem state which indicates that a Modem has found a serving cell and is yet to complete the registration process. LIMSRV is not a permanent Modem state, and Modems can move from LIMSRV to NOCONN autonomously.

Whether Lima CM is recording LIMSRV or NOCONN it is recording a serving cell at a location as a result of having successfully completed the search process for a “suitable cell”. A Modem in LIMSRV is capable of undertaking cell reselection when in either Modem state LIMSRV or NOCONN.

LIMSRV is a periodic state and should be considered an idle mode serving cell measurement as would be case with any other RF Survey equipment which doesn’t record this Modem state, where it occurs within its RF Log Files.

Whilst LIMSRV is small but potentially significant percentage of the RF readings in any survey file, to remove any rows containing LIMSRV from the survey data would be inappropriate and potentially have a detrimental affect on any conclusions that may otherwise have been drawn with the inclusion of these readings.

Forensic Analytics

Digital Forensic Experts

CSAS

CDAN
Nexus

ForensicRF
Services

Training
Services

Consultancy
Services

Forensic Analytics Ltd | Registered in England and Wales. Company No: 08606475
Pixmore Centre, Pixmore Avenue, Letchworth, SG6 1JG

+44 800 158 3830 | www.forensicanalytics.co.uk