Ing. Mag. Horst Greifeneder
Allgemein beeideter und gerichtlich zertifizierter Sachverständiger, Fachgebiet Informationstechnik;
Computer-Forensik-Spezialist

Forensische Auswertung von Call Detail Records

1. Einleitung

Die Verbreitung von Endgeräten mit SIM-Karte[1] für mobile Telefon- und Datenanschlüsse (Mobilfunkgeräte wie Handy, Smartphones, Tablets oder Ähnliches) ist in Österreich in den letzten Jahren stark gewachsen. Statistisch gesehen kamen 2014 in Österreich auf jeden Einwohner mehr als 1,5 SIM-Karten. Davon entfielen 10,7 Mio (83 %) auf 3G-SIM-Karten.[2]

Die zunehmende Verbreitung und Nutzung von Mobilfunkgeräten, insbesondere mit Zugang zum Internet, bewirken, dass immer häufiger damit in Verbindung stehende forensische Fragenstellungen in straf- oder zivilrechtlichen Rechtssachen eine Rolle spielen:

- Besitz von strafrechtlich relevantem Bild- oder Videomaterial am Handy;
- Aufenthaltsort eines Verdächtigen zum Zeitpunkt einer Straftat;
- Telefon- und Internetnutzung bei Mahnklagen.

Grundsätzlich lassen sich zur Beantwortung von forensischen Fragestellungen im Zusammenhang mit der Nutzung von Endgeräten mit Mobilfunkanschlüssen zwei Untersuchungsansätze unterscheiden:

- Die am mobilen Endgerät gespeicherten Daten werden sichergestellt und ausgewertet oder
- die im Zusammenhang mit der Nutzung des Endgeräts beim Mobilfunkanbieter angefallenen Daten werden analysiert.

Der vorliegende Artikel beschäftigt sich mit den, bei der Nutzung der mobilen Endgeräte in einem modernen Mobilfunknetz anfallenden Abrechnungsdaten (Call Detail Records – CDR) und deren Verfügbarkeit und Aussagekraft für eine forensische Untersuchung.

2. Daten der Mobilfunknutzer

Ausgangspunkt für Untersuchungen sind in der Regel die von den Mobilfunkanbietern im Zusammenhang mit dem Erwerb und der Nutzung von Mobilfunkgeräten gespeicherten Daten wie Stamm-, Verkehrs-, und Inhaltsdaten, welche nur für Zwecke der Besorgung eines Kommunikationsdienstes ermittelt oder verarbeitet werden dürfen.

2.1. Stammdaten

Unter Stammdaten versteht man die Angaben, die der Mobilfunkanbieter dauerhaft vom Kunden speichert. Dazu gehören unter anderem Name, Adresse, Teilnehmernummer sowie Informationen über Art und Inhalt des Vertragsverhältnisses.

Stammdaten sind spätestens nach Beendigung der vertraglichen Beziehungen mit dem Teilnehmer vom Betreiber zu löschen. Ausnahmen sind nur so weit zulässig, als diese Daten noch benötigt werden, um Entgelte zu verrechnen oder einzubringen, Beschwerden zu bearbeiten oder sonstige gesetzliche Verpflichtungen zu erfüllen.

2.2. Verkehrsdaten

2.2.1. Allgemeines

Verkehrsdaten sind jene Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Verrechnung dieses Vorgangs verarbeitet werden. Gespeichert wird unter anderem, wer mit wem, wann und wie lange telefoniert hat, bei Mobiltelefonen auch, von welchem geografischen Standort aus der Verbindungsaufbau erfolgte.

Anbieter dürfen Verkehrsdaten nur in bestimmten Fällen speichern oder übermitteln. Sie sind grundsätzlich unverzüglich nach Beendigung der Kommunikation zu löschen oder zu anonymisieren. Eine Ausnahme für die zulässige Speicherung von Verkehrsdaten stellt der Zweck der Verrechnung dar. Sobald dieser wegfällt, besteht eine Löschungs- bzw Anonymisierungsverpflichtung.

Sofern dies für Zwecke der Verrechnung von Entgelten erforderlich ist, hat der Betreiber Verkehrsdaten bis zum Ablauf jener Frist zu speichern, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann.[3] Diese Daten sind im Streitfall der entscheidenden Einrichtung sowie der Schlichtungsstelle unverkürzt zur Verfügung zu stellen.

Wird ein Verfahren über die Höhe der Entgelte eingeleitet, dürfen die Daten bis zur endgültigen Entscheidung über die Höhe der Entgelte nicht gelöscht werden. Der Umfang der gespeicherten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken.

2.2.2. Zugangsdaten

Zugangsdaten sind jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Anbieter entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für die Kommunikation

verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind (zB IP-Adresse).

2.2.3. Standortdaten

Standortdaten sind Verkehrsdaten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben.

2.3. Inhaltsdaten

Inhaltsdaten beinhalten die Inhalte übertragener Nachrichten.

Inhaltsdaten dürfen – sofern die Speicherung nicht einen wesentlichen Bestandteil des Kommunikationsdienstes darstellt – grundsätzlich nicht gespeichert werden. Sofern aus technischen Gründen eine kurzfristige Speicherung erforderlich ist, hat der Anbieter nach Wegfall dieser Gründe die gespeicherten Daten unverzüglich zu löschen.

3. Teilnehmer- und Geräteidentifikatoren

Damit ein mobiles Netzwerk effektiv betrieben werden kann, verfügt es über eine Reihe von Identifikatoren zur eindeutigen Bestimmung von Teilnehmern und Geräten.

3.1. Mobile Station-ISDN

Die Mobile Subscriber Integrated Services Digital Network Number (MS-ISDN) ist die weltweit eindeutige Rufnummer, welche der Anrufer wählt, um einen Mobilfunkteilnehmer zu erreichen.

In Österreich sind die nationalen Rufnummern für mobile Dienste in der Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung 2009 (KEM-V 2009)[4] festgelegt. Mobile Rufnummern bestehen aus einer dreistelligen Bereichskennzahl und einer sieben- bis neunstelligen Teilnehmernummer. Die Teilnehmernummern sind in den einzelnen Mobilfunkanbietern zugeordneten Vorwahlbereichen 650 bis 653, 655, 657, 659 bis 661 und 663 bis 699 zugeteilt.

Die Zuteilungsinhaber aller österreichischen Rufnummern können per Online-Rufnummernsuche der RTR-GmbH abgefragt werden.[5]

3.2. International Mobile Station Equipment Identity

3.2.1. Allgemeines

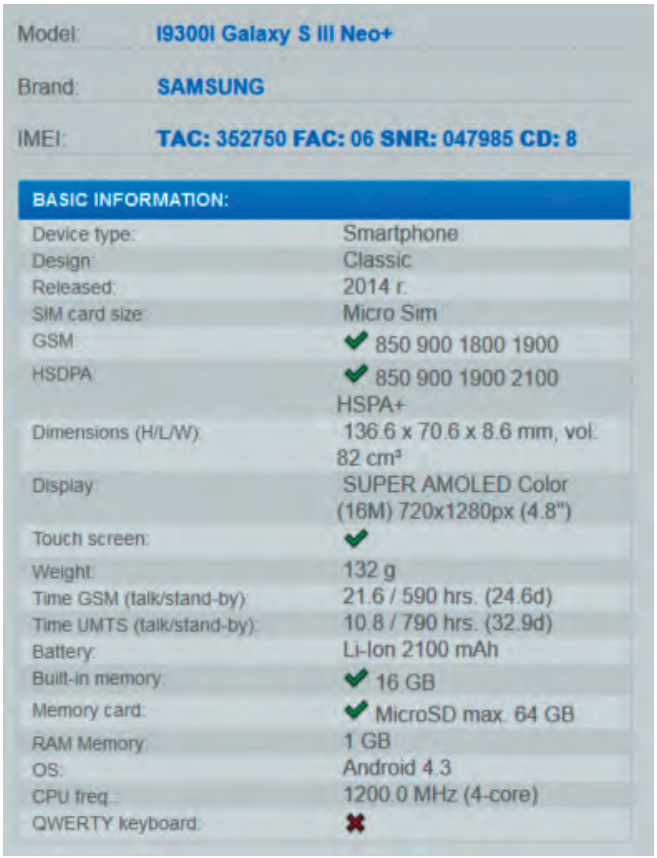
Die International Mobile Station Equipment Identity (IMEI) ist eine eindeutige 15-stellige Seriennummer(zB 352750006 – XXXXXX – 8), mit der ein GSM- oder UMTS-Endgerät weltweit eindeutig identifiziert werden kann.[6]

Während der Standard vorsieht, dass eine IMEI eindeutig und vor Manipulation durch den Benutzer geschützt ist, ist dies in der Praxis nicht in jedem Fall gewährleistet. Die GSM Association (GSMA)[7] selbst legt die Verantwortung für die Einhaltung der Standards und somit die Eindeutigkeit der IMEI sowie den Schutz vor Manipulation dieser in die Hände der Gerätehersteller, räumt aber ein, dass die Standards besonders außerhalb der EU nur mangelhaft zur Anwendung kommen.

Die IMEI-Nummer eines Handys kann in der Regel über die Eingabe von *#06# am Tastenfeld des Telefons abgerufen werden. Ein Dual-SIM-Handy besitzt zwei IMEI-Nummern.

3.2.2. Gerät per IMEI identifizieren

Ist die IMEI bekannt, dann lassen sich über eine öffentlich zugängliche Datenbank[8] Hersteller, Modell und technische Informationen zu einem Gerät ermitteln (siehe Abbildung 1).



Model:	I9300I Galaxy S III Neo+
Brand:	SAMSUNG
IMEI:	TAC: 352750 FAC: 06 SNR: 047985 CD: 8
BASIC INFORMATION:	
Device type:	Smartphone
Design:	Classic
Released:	2014 r.
SIM card size:	Micro Sim
GSM:	✔ 850 900 1800 1900
HSDPA:	✔ 850 900 1900 2100 HSPA+
Dimensions (H/L/W):	136.6 x 70.6 x 8.6 mm, vol. 82 cm³
Display:	SUPER AMOLED Color (16M) 720x1280px (4.8")
Touch screen:	✔
Weight:	132 g
Time GSM (talk/stand-by):	21.6 / 590 hrs. (24.6d)
Time UMTS (talk/stand-by):	10.8 / 790 hrs. (32.9d)
Battery:	Li-Ion 2100 mAh
Built-in memory:	✔ 16 GB
Memory card:	✔ MicroSD max. 64 GB
RAM Memory:	1 GB
OS:	Android 4.3
CPU freq.:	1200.0 MHz (4-core)
QWERTY keyboard:	✖

Abbildung 1: Geräteidentifikation per IMEI

Die ersten acht Ziffern der IMEI bilden den Type Allocation Code (TAC). Der TAC ist für verschiedene Endgerätehardware eindeutig und kann zur Identifizierung eines Endgerätetyps herangezogen werden. Die nächsten sechs Ziffern bilden die eigentliche Seriennummer des Endgeräts (SNR). Die letzte Ziffer ist eine Prüfziffer Check Digit (CD).

3.3. International Mobile Subscriber Identity

Die International Mobile Subscriber Identity (IMSI) dient in GSM-, UMTS- und LTE-Mobilfunknetzen der eindeutigen Identifizierung von Netzteilnehmern.

Neben weiteren Daten wird die IMSI auf der SIM-Karte gespeichert. Die IMSI-Nummer wird weltweit einmalig pro SIM von den Mobilfunknetzbetreibern vergeben und hat nichts mit der Telefonnummer zu tun, die der SIM-Karte zugeordnet ist.[9]

Die IMSI besteht aus maximal 15 Ziffern und setzt sich folgendermaßen zusammen:

- Mobile Country Code (MCC): 3 Ziffern (232 für Österreich);
- Mobile Network Code (MNC): 2 oder 3 Ziffern, (01 für A1 Telekom);[10]
- Mobile Subscriber Identification Number (MSIN): 1 bis 10 Ziffern.

In der Praxis können einer Rufnummer (MS-ISDN) durchaus mehrere IMSI-Nummern zugeordnet sein.

4. Call Detail Records

4.1. Allgemeines

Die CDR enthalten Daten, welche von den Telekommunikationsanbietern für die teilnehmerbezogene Abrechnung der Services benötigt werden. Jedes Mal, wenn ein Benutzer einen Telefonanruf erhält oder tätigt, eine Textnachricht sendet oder empfängt oder sich mit einem mobilen Datendienst verbindet, wird ein CDR erzeugt.

CDR bilden somit die Grundlage für die Erstellung des Einzelverbindungsnachweises der Teilnehmerrechnung. Im Unterschied zum Einzelverbindungsnachweis enthalten CDR aber zusätzliche Identifikatoren sowie die vollständige Teilnehmernummer des angerufenen Teilnehmers, welche unter Umständen für eine forensische Untersuchung von großem Interesse sein können.

Wichtig in diesem Zusammenhang ist, dass Telekommunikationsanbieter für die Speicherung der Daten unterschiedliche Datenstrukturen, -typen und -formate verwenden. So kann es sein, dass ein Anbieter die Daten zu allen verrechenbaren Ruftypen (Gespräch, Daten, SMS, MMS) in einem gemeinsamen Datensatz speichert, während ein anderer Anbieter die verrechneten Telefondienste (Gespräch, SMS, MMS) und Datendienste in unterschiedlichen Datensätzen speichert.

Aus forensischer Sicht ist es deshalb von entscheidender Bedeutung für die Befundaufnahme, in Absprache mit dem Mobilfunkbetreiber frühzeitig Klarheit über Inhalt und Struktur der gespeicherten Daten zu erlangen, damit durch die Auswertung unvollständiger Datenbestände nicht wertvolle Informationen verloren gehen.

4.2. Inhalt und Struktur von CDR-Datenbanken

Inhalt und Struktur der anbieterspezifischen CDR sind in der Regel nicht standardisiert und entsprechen vor allem den Anforderungen der jeweiligen Abrechnungssysteme der Mobilfunkbetreiber.

Im Allgemeinen werden CDR nachfolgende Informationen enthalten:

- Datum und Uhrzeit eines Verbindungsaufbaus;
- Dauer einer Gesprächs-, Nachrichten oder Datenverbindung;
- Art des genutzten mobilen Dienstes (zB Telefonat, SMS, MMS, Datenverbindung);
- Sender- und Empfänger-MS-ISDN;
- IMEI-Nummer des verwendeten Endgeräts;
- IMSI-Nummer der verwendeten SIM-Karte;
- Cell-ID und Location Area Code (LAC) beim Verbindungsaufbau;
- Cell-ID und LAC beim Verbindungsende.

Bei der Nutzung von mobilen Datendiensten enthält der CDR unter anderem auch Informationen über die vom mobilen Endgerät genutzte IP-Adresse bzw gesendete (Upload-) bzw empfangene (Download-)Datenmenge.

5. Forensische Auswertung von CDR

5.1. Allgemeines

Grundsätzlich können CDR aus dem Abrechnungssystem eines Mobilfunkanbieters nach unterschiedlichen, teilnehmerspezifischen Kriterien extrahiert und ausgewertet werden. In den meisten Fällen wird man als Auswahlparameter einen bestimmten Zeitraum und die Teilnehmernummer für die Auswertung der Daten heranziehen (siehe Abbildung 2).

Als in der Praxis vielfach bewährtes Tool für die Auswertung größerer Datenmengen eignen sich Pivot-Tabellen von Microsoft Excel sehr gut für die Analyse von CDR-Datenbeständen.

Datum	Time	A-Nummer	B-Nummer	Dauer	A-IMSI	A-IMEI	LAC	CellID	Ruftyp	A/P	B-IMSI	B-IMEI
12.11.2015	11:35:37	436641234567	436761234567	0	232011234567890	352750061234568	2107	2972311	SMS	A	232021234567890	355001071234561
13.11.2015	12:25:37	436641234567	436991234567	51	232011234567890	352750061234568	65406	18235	Telefon	A	232052123456789 0	012345678901234
14.11.2015	13:25:37	436641234567	436761234567	0	232011234567890	352750061234568	5522	16805	SMS	A	232021234567890	355001071234561
14.11.2015	14:25:37	436641234567	436761234567	0	232011234567890	352750061234568	5522	16805	SMS	A	232021234567890	355001071234561
14.11.2015	14:25:37	436641234567	436761234567	0	232011234567890	352750061234568	5522	16805	SMS	A	232021234567890	355001071234561
14.11.2015	14:26:37	436641234567	436761234567	756	232011234567890	352750061234568	5522	16805	Telefon	P	232021234567890	355001071234561

Abbildung 2: CDR-Rohdaten (Musterformat, mit teilweise anonymisierten Daten)

5.2. Quantitative und qualitative Auswertung der CDR-Rohdaten

Die CDR-Rohdaten bilden die forensische Grundlage für eine ganze Reihe von quantitativen und qualitativen Auswertungen zur Nutzung von Telekommunikationsdiensten durch einzelne Teilnehmer. So ist es unter anderem möglich, die Anzahl, das Datum und die Uhrzeit von Telefonaten, Nachrichtenübermittlungen oder Datenverbindungen einer bestimmten Teilnehmernummer zu ermitteln.

Ebenso kann natürlich festgestellt werden, wer mit wem, wann und wie oft telefoniert bzw SMS-Nachrichten ausgetauscht hat. In Hinblick auf Datenverbindungen lassen sich Zeitpunkt und die Menge der empfangenen bzw gesendeten Daten eruieren. Eine Auswertung der CDR-Daten in Hinblick auf besuchte Websites ist nicht möglich. Diese Daten werden von den Telekomanbietern aus rechtlichen Gründen nicht gespeichert.

Dem in Abbildung 2 dargestellten Auszug der CDR-Daten der Teilnehmernummer 0664-1234567 lassen sich unter anderem nachfolgende Informationen entnehmen:

- Das Telefon wurde im Beobachtungszeitraum (11. bis 14. 11. 2015) unter anderem für Telefonate und Textnachrichten (SMS) mit mehreren Teilnehmern in verschiedenen Teilnehmernetzen verwendet.
- Im dargestellten Beobachtungszeitraum kommunizierte der untersuchte Teilnehmer fünfmal mit der Teilnehmernummer 0676-1234567. Versandt wurden unter anderem mehrere SMS. Der letzten SMS am 14. 11. 2015 und 14:25:37 Uhr folgte ein 756 Sekunden lang dauernder Rückruf des Empfängers der Textnachrichten.
- Anhand der aufgezeichneten IMEI-Nummer lässt sich auch das vom untersuchten Teilnehmer verwendete Endgerät als Samsung S3 Neo identifizieren.

5.3. Geo-Location mittels Global Cell-ID

Die CDR-Rohdaten eigenen sich unter Umständen auch zur nachträglichen Standortbestimmung des aktiven Teilnehmers. In der Praxis erfolgt die Standortbestimmung durch die Global Cell-ID,[11] diese besteht dem MCC,[12] dem MNC,[13] dem LAC[14] und der Cell-ID (CID)[15] (siehe Abbildung 3).

Die Position eines Mobiltelefons ist für den Mobilfunkbetreiber durch die permanente Anmeldung am Netz in gewissen Genauigkeitsgrenzen bekannt. Im Bereitschaftsbetrieb ist sie zumindest durch die Zuordnung zur aktuell verwendeten Location Area gegeben. Diese Information wird bei Bewegung der Mobilstation regelmäßig aktualisiert und in einer Datenbank, dem Home Location Register (HLR), gespeichert. Im Gesprächsbetrieb kann die Position eines Mobiltelefons genauer bestimmt werden, da hier zumindest die Cell-ID der aktiven Basisstation bekannt ist.[16]

Abbildung 3: Aufbau der Global Cell-ID

Mit der Global Cell-ID lässt sich in Verbindung mit öffentlich zugänglichen Datenbanken wie OpenCellID[17] der ungefähre Standort des Mobilfunkgeräts zum Zeitpunkt der Verbindungserstellung ermitteln (siehe Abbildung 4).

Die Lokalisation bezieht sich auf den baulichen Standort der Funkzelle, in der sich das Endgerät zum Zeitpunkt der Messung aufhält. Die erzielte Genauigkeit ist von mehreren Faktoren abhängig und steht im direkten Zusammenhang mit der Verbreitungsdichte der Funkzellen im Aufenthaltsbereich des Benutzers.

Mit den in Abbildung 2 ersichtlichen Standortdaten lässt sich über die Global Cell-ID (232-01-2107-2972311) der ungefähre Aufenthaltsort des Teilnehmers am 12. 11. 2015 um 11:35:37 Uhr mit den Positionsdaten eines Senders in der Wiener Innenstadt verknüpfen.

5.4. Bezug der CDR-Daten

Die österreichische StPO verzeichnet mehrere, vom Tatbestand oder der Strafbedrohung abhängige Möglichkeiten, um die Daten aus der Nutzung von mobilen Endgeräten zur Aufklärung einer Straftat einzusetzen: Auskunft über Daten einer Nachrichtenübermittlung (Rufdatenauswertung) sowie die Überwachung von Nachrichten oder eines Fernmeldeverkehrs. Erstere bezieht sich in der Regel auf die CDR eines Teilnehmers. Die beiden anderen auf Inhaltsdaten.

Diensteanbieter und Netzbetreiber sind zur Rufdatenauswertung verpflichtet, wenn

- der Verdacht auf eine Entführung besteht und während dieser Zeit eine Nachrichtenübermittlung stattgefunden hat,
- die Auskunft der Aufklärung einer Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, dient und der Betroffene der Auskunftserteilung ausdrücklich zustimmt,
- die Auskunft der Aufklärung einer Straftat, die mit einer Freiheitsstrafe von mehr als einem Jahr bedroht ist, dient oder
- dadurch der Aufenthalt von flüchtigen oder abwesenden Beschuldigten ermittelt werden kann, die einer vorsätzlich begangenen mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig sind.

Die zu den CDR gespeicherten Stamm- und Verkehrsdaten sind im zivilrechtlichen Verfahren in der Regel auf richterliches Verlangen und mit der Zustimmung des Betroffenen direkt über den jeweiligen Telekomprovider erhältlich.

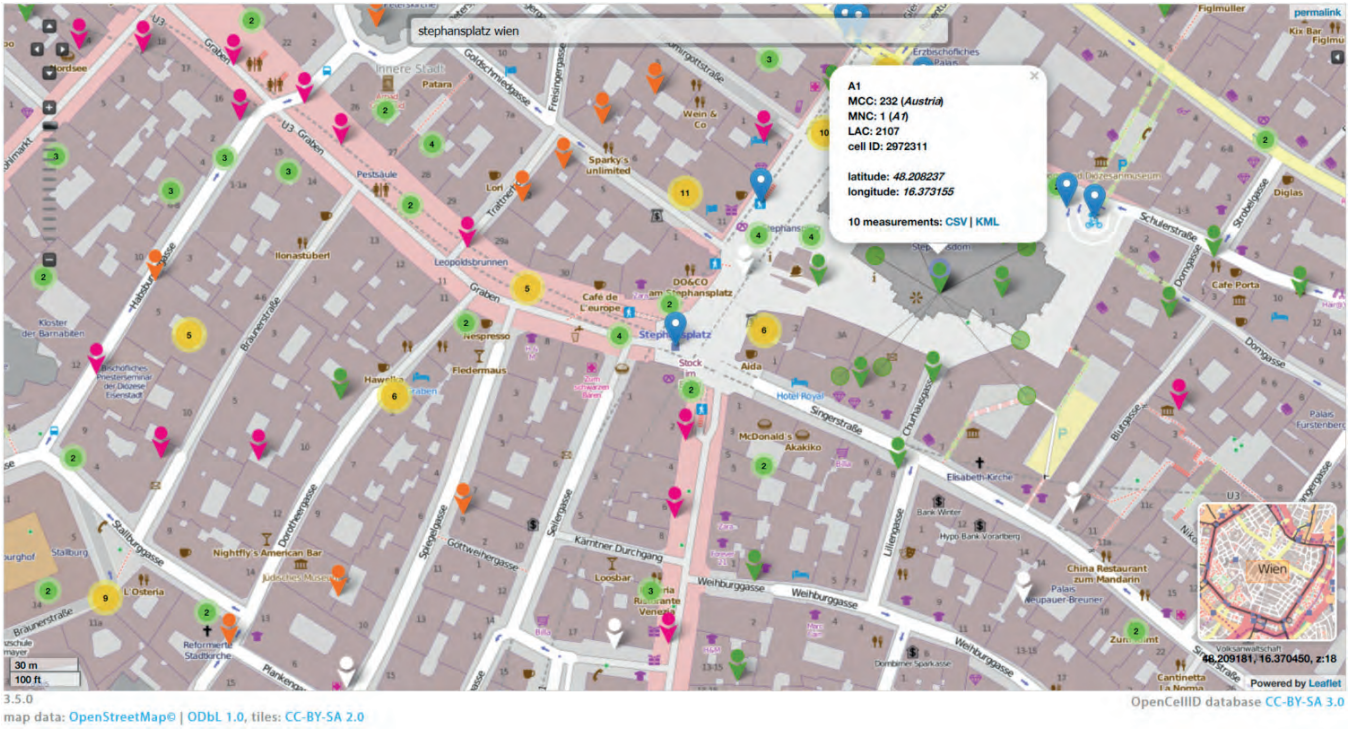


Abbildung 4: Standortbestimmung in OpenCellID mittels Global Cell-ID

6. Fazit

Bei der Nutzung von Telekommunikationsdiensten verarbeiten und speichern Netzbetreiber große Menge an Stamm-, Verkehrs- und Inhaltsdaten. Die für Abrechnungszwecke gespeicherten CDR enthalten für forensische Untersuchungen wertvolle Informationen. Über bestehende Teilnehmer- und Geräteidentifikatoren können eine ganze Reihe von quantitativen und qualitativen Auswertungen in Bezug auf einzelne Teilnehmernummern erstellt werden.

In Hinblick auf abweichende Standards bei der Verarbeitung und Speicherung der CDR durch einzelne Netzbetreiber ist eine möglichst frühzeitige und detaillierte Abklärung der beim jeweiligen Netzbetreiber verfügbaren Datenstrukturen, -typen und -formate im Vorfeld einer forensischen Untersuchung unbedingt empfehlenswert.

Anmerkungen:

1 Die SIM-Karte ist eine Chipkarte, die unter anderem in ein Mobiltelefon eingesteckt wird und zur Identifikation des Nutzers im Netz dient. Mit ihr stellen Mobilfunkanbieter Teilnehmern mobile Telefonanschlüsse und Datenanschlüsse zur Verfügung; siehe https://de.wikipedia.org/wiki/SIM-Karte.

2 RTR Telekom Monitor 1/2015, online abrufbar unter https://www.rtr.at/tr/inf/TKMonitor_1_2015/TM1_2015.pdf.

3 Nach Auskunft eines Telekomanbieters werden die entsprechenden Verkehrsdaten in der Regel nach sechs Monaten gelöscht.

4 Verordnung der Rundfunk und Telekom Regulierungs-GmbH, mit der Bestimmungen für Kommunikationsparameter, Entgelte und Mehrwertdienste festgelegt werden (Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung 2009 – KEM-V 2009), BGBl II 2009/212 idF BGBl II 2015/107.

5 Siehe https://www.rtr.at/de/tk/Rufnummernsuche?S=06&art=m.

6 Siehe https://de.wikipedia.org/w/index.php?title=International_Mobile_Equipment_Identity&oldid=143857212.

7 Die GSMA wurde im Jahre 1987 als die weltweite Industrievereinigung der GSM-Mobilfunkanbieter gegründet und vertritt heute mehr als 800 Mobilfunkanbieter.

8 Siehe http://www.imei.info.

9 Siehe https://de.wikipedia.org/w/index.php?title=International_Mobile_Subscriber_Identity&oldid=144741970.

10 In Österreich ist die Rundfunk- und Telekom Regulierungs-GmbH für die Vergabe zuständig.

11 Weltweit eindeutige Kennung einer Funkzelle.

12 Der MCC für Österreich lautet 232.

13 In Österreich werden MNC von der Rundfunk und Telekom Regulierungs-GmbH an die Betreiber vergeben, zB 01 für A1 Telekom.

14 Betreiberspezifische Kennung des Aufenthaltsbereichs eines Mobilfunkgeräts innerhalb eines Mobilfunknetzes.

15 Betreiberspezifische Kennung einer Funkzelle innerhalb eines Aufenthaltsbereichs.

16 Siehe https://de.wikipedia.org/w/index.php?title=GSM-Ortung&oldid=140535773.

17 Siehe http://www.opencellid.org.

Korrespondenz:
Ing. Mag. Horst Greifeneder
Schenkelbachweg 32, A-4600 Wels
Tel.: 07242 / 77715
Fax: 07242 / 77716
E-Mail: office@fds.at