Cell-ID: Mobilfunkzellen-Analyser

Entwickler: M. Trojan

Einführung:

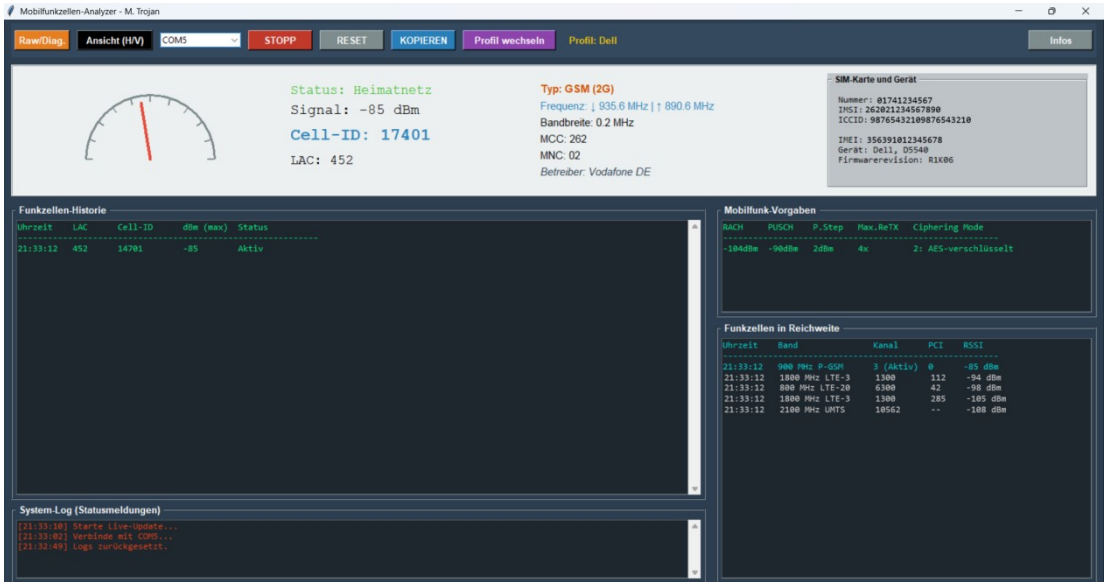
Das Programm ist ein hochspezialisiertes Werkzeug zur technischen Diagnose von Mobilfunknetzen über serielle AT-Kommandos. Es ist darauf ausgelegt, mit internen PC-Modems (z.B. Dell, HP) oder externen Geräten (Handys im Diagnosemodus) zu kommunizieren.

---

1. Programmzweck & Systemvoraussetzungen

Der Analyzer dient der Echtzeit-Auswertung von Mobilfunkdaten. Er liest technische Parameter wie Signalstärke, Zell-Identifikation (Cell-ID) und Frequenzen direkt von der Hardware aus.

- **Unterstützte Hardware:** Modems von Ericsson, Huawei, Qualcomm, Intel, MediaTek, Samsung, Sierra, Quectel u.v.m.
- **Schnittstelle:** Serieller COM-Port (USB oder intern).
- **Besonderheit:** Automatische Speicherung der Port-Wahl, des Geräte-Profils und der Fenster-Ausrichtung in einer config.txt.



2. Die Benutzeroberfläche (Hauptfenster)

- **Raw/Diag. (Button):** Öffnet das Experten-Terminal für Rohdaten (siehe Sektion 4).
- **Ansicht (H/V) (Button):** Schaltet das Layout zwischen horizontaler (breit) und vertikaler (schmal) Darstellung um.
- **Port-Auswahl (Combobox):** Hier wird der COM-Port dees Modems aus.
- **START / STOPP (Button):** * **Start:** Initiiert die Verbindung, liest IMEI/IMSI/ICCID aus und startet den automatischen Update-Loop (alle 1,0–1,2 Sek.).
    - **Stopp:** Beendet die serielle Kommunikation.
- **RESET (Button):** Löscht alle Tabellen (Historie, Reichweite) und das System-Log.
- **KOPIEREN (Button):** Kopiert den gesamten Text der Zell-Historie in die Zwischenablage.
- **Profil wechseln (Button):** Schaltet durch 16 herstellerspezifische Befehlssätze (z.B. Huawei AT^HCSQ?, Sierra AT!GSTATUS?), um die Zell-Details korrekt auszulesen.
- **Infos (Button):** Zeigt die integrierte Hilfe und rechtliche Hinweise an.

B. Live-Status-Panel (Zentral)

- **Analoge Anzeige (Gauge):** Ein Zeigerinstrument visualisiert die Signalstärke in dBm (berechnet aus (CSQ + 113) * 1.6).
- **Status:** Zeigt den Registrierungszustand (z.B. *Heimatnetz, Roaming, Netzsuche*).
- **Signal:** Exakter Wert in dBm.
- **Cell-ID & LAC:** Die eindeutige Kennung der aktiven Funkzelle und der Location Area Code.
- **Typ:** Funktechnologie (z.B. *E-UTRAN/LTE (4G), UTRAN (3G), GSM*).
- **Frequenz:** Zeigt den Downlink- und Uplink-Wert in MHz sowie den Kanal (ARFCN/EARFCN) an.
- **Bandbreite:** Ermittelt die Kanalbreite (z.B. 10 MHz oder 20 MHz).
- **MCC / MNC / Betreiber:** Identifiziert das Land (262 für DE) und den Anbieter (z.B. *Telekom, Vodafone, O2, 1&1*) anhand einer internen Datenbank (mnc_dict).

C. SIM- & Geräte-Info (Rechts oben)

Liest beim Start einmalig folgende Hardware-Daten aus:

- **Nummer:** Eigene Telefonnummer (falls auf SIM hinterlegt).
- **IMSI/ICCID:** Eindeutige SIM-Karten-Kennungen.
- **IMEI:** Seriennummer des Modems.
- **Gerät:** Hersteller, Modellname und Firmware-Revision.

---

3. Daten-Tabellen & Protokolle

Funkzellen-Historie

Listet chronologisch jeden Zellwechsel auf.

- **Spalten:** Uhrzeit, LAC, Cell-ID, Maximalpegel (dBm max) während des Aufenthalts und die Verweildauer.
- **Aktive Zelle:** Wird in der obersten Zeile live aktualisiert.

Mobilfunk-Vorgaben (Netz-Parameter)

Überwacht kritische Netzvorgaben. Werte werden orange (Warnung), wenn sie Grenzwerte überschreiten:

- **RACH/PUSCH:** Sendeleistungsparameter.
- **P.Step:** Leistungsregelungsschritte.
- **Max.ReTX:** Maximale Anzahl der Sende-Wiederholungen.
- **Ciphering Mode:** Zeigt den Verschlüsselungsstatus an (z.B. *A5/3* für LTE/GSM oder *AES/ZUC*). Warnung bei unverschlüsselten Verbindungen!

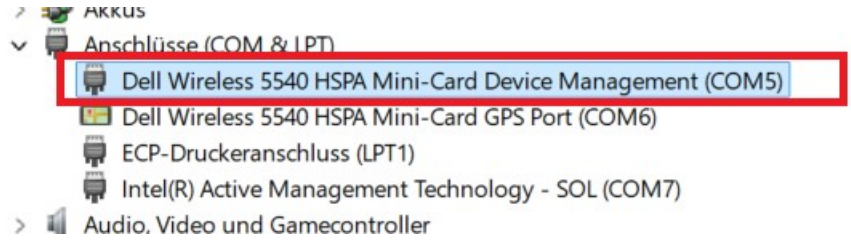
Funkzellen in Reichweite

Scannt (sofern vom Modem unterstützt) die Umgebung nach Nachbarzellen ab.

- **Türkis:** Die aktuell verbundene Zelle.
- **Grau:** Andere empfangbare Zellen mit Angabe von Band, Kanal, PCI (Physical Cell ID) und Signalstärke.

---

4. Vorbereitung



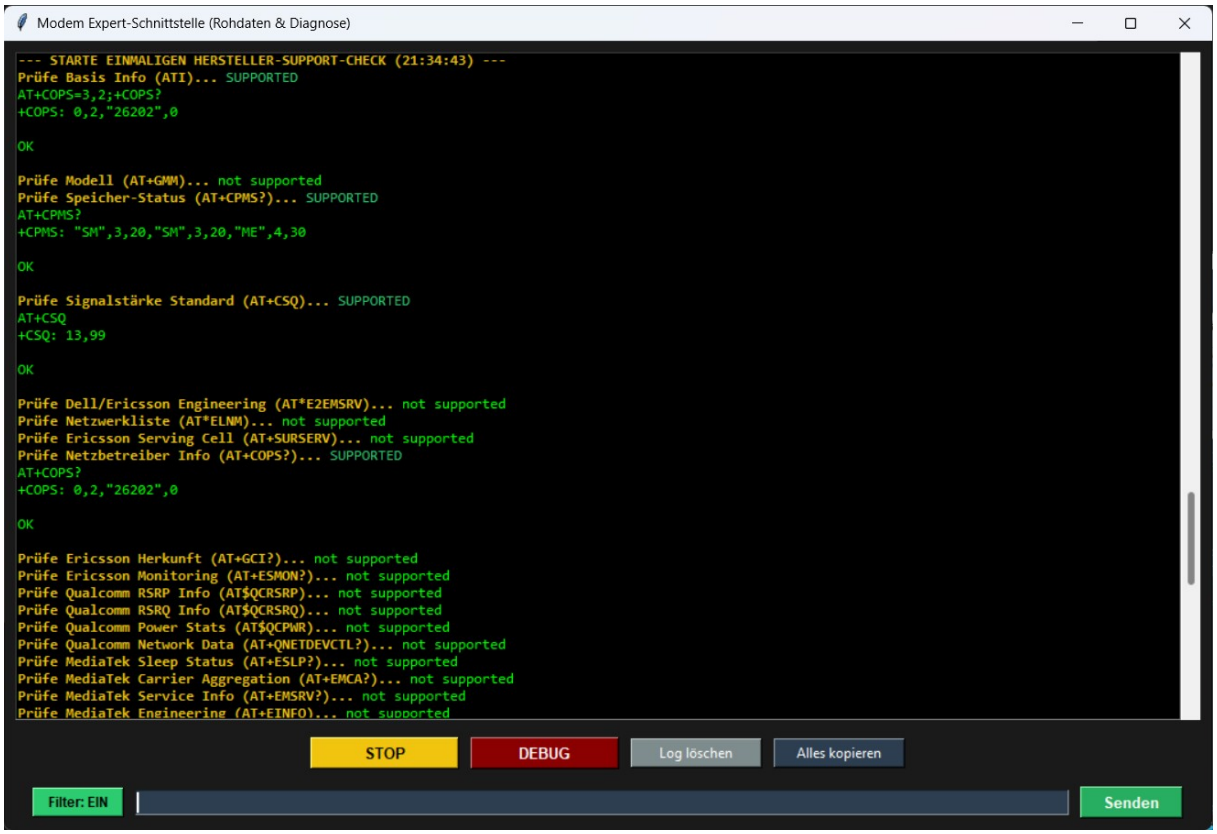
Über den Gerätemanager den COM-Port des WWAN-Moduls herausfinden

Sollte dies nicht möglich sein, dann kann man auch verschiedene aufgelistete COM-Ports probieren und „START“ drücken. Sobald Daten angezeigt werden (insbesondere Cell-ID, IMSI usw.) ist das Programm mit dem richtigen COM-Port verbunden.

Über die Schaltfläche „Profil wechseln“ werden herstellerspezifische Abfragebefehle umgeschaltet, um die passende *Sprache* zu finden.

Über „Ansicht H/V“ kann man das Programm für horizontale Ansicht (z.B. Computer) oder vertikale Ansicht (z.B. Tablet / Handy) umschalten.

Diese Einstellungen werden in der „config.txt“ nach Beenden des Programmes gespeichert.



5. Experten-Schnittstelle (Raw/Diag. Fenster)

Dies ist das Herzstück für Profis und interessant, um das Modem zu testen oder weitere Informationen abzurufen.

Am Ende dieses Dokumentes findet sich eine Liste mit gängigen Befehlen.

1. **RawData (Button):** Schaltet den Live-Stream der Kommunikation ein. Man sieht genau, was das Programm sendet ([OUT]) und was das Modem antwortet ([IN]).
2. **Filter (Button):** Blendet bei Bedarf die automatischen Hintergrund-Abfragen aus und zeigt nur die eigens eigenebenen Befehle an, um die Übersicht zu behalten. Ein erneuter Druck auf den Filter-Knopf schaltet diesen Filter wieder aus.
3. **Manuelle Eingabe:** Über die untere Zeile können eigene AT-Befehle direkt an das Modem gesendet werden.
4. **DEBUG (Support-Check):** Dies ist eine mächtige Funktion. Das Programm rattert über 40 verschiedene Profi-Befehle ab (von AT!GSTATUS? bis AT$QCRSRP), um zu prüfen, welche "Geheimbefehle" das spezielle Modem unterstützt. Es markiert diese mit **SUPPORTED** oder **not supported**. Die Erkenntnisse daraus lassen auf das richtige Profil und den Umfang des Modem-Datenservice schließen.

   Info: Es ist nicht ungewöhnlich, wenn das Programm dabei für einige Sekunden eingefroren zu sein scheint, während es die Befehle testet und ausgibt.

Log löschen bereinigt das Fenster von allen Daten.

Alles kopieren kopiert den Inhalt des Fensters, um diese Daten z.B. in Editor, Notepad++ oder anderen Programmen einzufügen, wie wenn man Strg+A und Strg+C drückt.

5. Technische Logik

Das Programm nutzt komplexe mathematische Formeln zur Frequenzberechnung. Es erkennt automatisch anhand der Kanalnummer, ob es sich um:

- 900 MHz (P-GSM/E-GSM/LTE Band 8)
- 1800 MHz (GSM/LTE Band 3)
- 2100 MHz (UMTS/LTE Band 1)
- 800 MHz (LTE Band 20)
- 700 MHz (5G/LTE Band 28)

... handelt und berechnet daraus die exakte Downlink- und Uplink-Frequenz.

Insgesamt gibt es 12 unterschiedliche Bänder:

- **700 MHz (Kanal 9210–9659): LTE 5G**
  - Das "Flächenband" (Band 28). Wird oft für 5G via DSS genutzt, um ländliche Gebiete schnell zu versorgen.
- **800 MHz (Kanal 6150–6449): 800 MHz LTE-20 (Band 20)**
  - Das Standard-Band für LTE in Deutschland (ehemalige TV-Frequenzen). Bietet die beste Durchdringung von Gebäudewänden.
- **900 MHz (Kanal 0–124): 900 MHz P-GSM**
  - Das klassische "D-Netz" Ur-Band. Wird heute noch für Basis-Telefonie und SMS (2G) genutzt.
- **900 MHz (Kanal 975–1023): 900 MHz E-GSM**
  - Die Erweiterung des 900-MHz-Bands (Extended), um mehr Kapazität für GSM bereitzustellen.
- **900 MHz (Kanal 2937–3088): 900 MHz UMTS 3G**
  - Früher als 3G-Erweiterung auf dem Land genutzt; heute meist für LTE (Band 8) umgewidmet.
- **900 MHz (Kanal 3450–3799): 900 MHz LTE-8 (Band 8)**
  - Modernes LTE-Band 8. Die Telekom nutzt dies sehr effizient für 4G-Telefonie (VoLTE) in Gebäuden.
- **950 MHz (Kanal 3257–4458): 950 MHz UMTS**
  - Ein eher ungewöhnlicher Bereich für Europa; technisch gesehen eine Verschiebung innerhalb des 900er Segments.
- **1800 MHz (Kanal 512–885): 1800 MHz GSM**
  - Das alte "E-Netz". Wird heute kaum noch für GSM genutzt, sondern fast überall für LTE freigemacht.
- **1800 MHz (Kanal 1200–1949): 1800 MHz LTE-3 (Band 3)**
  - Das Haupt-Band für LTE in Städten. Bietet eine sehr gute Mischung aus Reichweite und hoher Datengeschwindigkeit.
- **2100 MHz (Kanal 0–599): 2100 MHz UMTS**
  - Theoretische Kanaldefinition für das 2100-MHz-Band (Band 1); in der Praxis selten mit diesen niedrigen Kanalnummern belegt.
- **2100 MHz (Kanal 10562–10838): 2100 MHz UMTS**
  - Der klassische UMTS-Bereich (3G). Fast alle deutschen Anbieter haben diesen Bereich mittlerweile auf LTE Band 1 umgestellt.
- **2600 MHz (Kanal 2400–2649): 2600 MHz LTE-7 (Band 7)**
  - Das High-Speed-Band für Hotspots (Bahnhöfe, Stadien). Enorme Kapazität, aber sehr geringe Reichweite.

6. Layer-Design, Layers mit dem das Programm arbeitet

Im Mobilfunk (und in der gesamten Telekommunikation) versteht man unter **Layern** (Schichten) eine hierarchische Struktur, die komplexe Aufgaben in kleine, spezialisierte Ebenen unterteilt. Das gängigste Modell ist das **OSI-Referenzmodell** mit 7 Schichten.

Das Programm fungiert als Schnittstellen-Monitor, der Informationen aus den unteren Ebenen (Layer 1–3) abgreift und auf Layer 7 (Anwendungsschicht) visualisiert. Da die Kommunikation mit dem Modem über AT-Kommandos erfolgt, wird der Status der tieferen Schichten direkt von der Hardware abgefragt. Die Verteilung innerhalb der Software stellt sich wie folgt dar:

Layer 1 (Physical Layer) – Die Funk-Ebene

- In dieser Schicht wird die Physik der Funkwellen behandelt. Das Programm liest diese Daten über Befehle wie AT+CSQ oder herstellerspezifische Profile aus.
- Anzeige im Programm: Die Signalstärke (dBm) im analogen Zeigerinstrument, die Frequenzen (MHz), die Kanalnummern sowie die Bandbreite (z. B. 10 MHz).
- Bedeutung: Es wird aufgezeigt, ob die physikalische Funkverbindung stabil genug für eine Datenübertragung ist.

Layer 2 (Data Link Layer) – Die Sicherungsschicht

- Diese Schicht regelt den Zugriff auf das Übertragungsmedium.
- Anzeige im Programm: Die PCI (Physical Cell ID) in der Nachbarzellen-Liste sowie Parameter wie RACH (Random Access Channel) oder PUSCH in der Tabelle „Mobilfunk-Vorgaben“.
- Bedeutung: Es wird ersichtlich, wie das Modem mit dem Sendemast interagiert, um Sendeplätze zu belegen und Fehler zu korrigieren.

Layer 3 (Network Layer) – Die Vermittlungsebene

- Dies ist die logische Ebene, auf der die Bewegung innerhalb des Netzwerks stattfindet.
- Anzeige im Programm: Cell-ID (CID), LAC (Location Area Code), der Registrierungsstatus (Heimatnetz, Roaming) sowie MCC/MNC (Landes- und Netzkennung).
- Bedeutung: Auf dieser Ebene wird analysiert, in welcher logischen Zelle das Gerät eingebucht ist und welcher Provider genutzt wird. Die Zell-Historie stellt eine reine Layer-3-Protokollierung dar.

Layer 4 (Transport / Application Layer) – Die Transportschicht / Anwendungsebene

- Diese Schicht ist für die Steuerung der Datenströme und die Sicherstellung einer vollständigen Übertragung zwischen Sender und Empfänger verantwortlich.
- Kernaufgabe: Segmentierung der Daten und Protokoll-Zuweisung (z. B. TCP für garantierte Zustellung oder UDP für Geschwindigkeit).
- Mobilfunk-Bezug: Hier wird geregelt, wie Web-Pakete oder Streaming-Daten trotz möglicher Funklöcher lückenlos beim Endgerät ankommen.
- Dies umfasst die Software selbst und die grafische Benutzeroberfläche.
- Funktionsweise: Hier erfolgt die Umrechnung der technischen Modem-Antworten (z. B. +CSQ: 25,0) in lesbare Werte (z. B. -63 dBm) sowie die grafische Aufbereitung innerhalb der Tkinter-Oberfläche.

Layer 5 (Session Layer) – Die Sitzungsschicht

- Die Sitzungsschicht organisiert die Verbindung zwischen zwei Endsystemen.
- Kernaufgabe: Aufbau, Aufrechterhaltung und Beendigung von Kommunikationssitzungen (Dialogsteuerung).
- Mobilfunk-Bezug: Sie sorgt dafür, dass eine Verbindung (z. B. ein Telefonat oder eine App-Anmeldung) bestehen bleibt, auch wenn kurzzeitig die Funkzelle gewechselt wird.

Layer 6 (Presentation Layer) – Die Darstellungsschicht

- Diese Ebene übersetzt die Daten in ein Format, das die Anwendung (Layer 7) versteht.
- Kernaufgabe: Datenkompression, Verschlüsselung (z. B. SSL/TLS) und Konvertierung von Zeichensätzen.
- Mobilfunk-Bezug: Hier findet beispielsweise die Dekodierung von Videostreams oder die Verschlüsselung vertraulicher Informationen statt, bevor sie auf dem Display erscheinen.

7. Aufbau des Mobilfunknetzes

Ein Mobilfunknetz besteht im Wesentlichen aus drei Hauptkomponenten:

1. Das Endgerät (User Equipment / UE): Das Smartphone oder – im Falle dieses Programms – das interne WWAN-Modem eines PCs.
2. Das Zugangsnetz (Radio Access Network / RAN): Dies umfasst die Basisstationen (Sendemasten), die eine geografische Region in "Funkzellen" unterteilen und die Funkverbindung zum Endgerät halten.
3. Das Kernnetz (Core Network / CN): Das "Gehirn" des Netzes, das Teilnehmer authentifiziert (über die SIM-Karte), Anrufe und Datenströme vermittelt und die Verbindung zum Internet herstellt.

8. Kommunikation zwischen Modem und Netz

- Die Kommunikation erfolgt in einem ständigen Dialog über definierte Protokolle:
- Einbuchung: Beim Einschalten sucht das Modem nach dem stärksten Signal einer passenden Kennung (MCC/MNC). Es sendet seine Identität (IMSI) an das Kernnetz, welches die SIM-Karte validiert.
- Signalisierung: Auch wenn keine Daten fließen, tauschen Modem und Basisstation permanent Kontrollnachrichten aus (Layer 3), um die Signalqualität zu überwachen und bei Bewegung den Wechsel zur nächsten Zelle vorzubereiten (Handover).
- Datenübertragung: Fordert ein Dienst Daten an, weist die Basisstation dem Modem spezifische Funkressourcen (Frequenzen und Zeitschlitze auf Layer 1 & 2) zu, über die die Informationen als verschlüsselte Bitströme übertragen werden.

9. Praktische Anwendungen

Die Bewertung von Mobilfunknetzen und SIM-Karten sowie die Einordnung von Sicherheitsrisiken durch IMSI-Catcher lassen sich anhand der technischen Parameter des Programms wie folgt beschreiben:

Mobilfunknetz

Die Qualität und Leistungsfähigkeit eines Mobilfunknetzes wird im Programm durch drei Hauptfaktoren bestimmt:

- **Signalqualität (Layer 1):** Das analoge Zeigerinstrument und die dBm-Anzeige geben Aufschluss über die Empfangsstärke. Werte zwischen -50 dBm und -80 dBm gelten als exzellent, während Werte unter -110 dBm auf eine instabile Verbindung hindeuten.
- **Netzkapazität und Technologie:** Die Anzeige des Typs (z. B. E-UTRAN/LTE) und der Bandbreite (z. B. 20 MHz) lässt Rückschlüsse auf die mögliche Datengeschwindigkeit zu. Ein breiteres Frequenzband (höhere MHz-Zahl) bietet in der Regel stabilere Datenraten bei vielen gleichzeitigen Nutzern.
- **Zell-Stabilität (Layer 3):** Die Zell-Historie dokumentiert, wie oft das Gerät zwischen verschiedenen Zellen (Handover) wechselt. Häufige Wechsel bei Stillstand des Geräts können auf ein überlastetes Netz oder eine ungünstige Positionierung zwischen Funkzellen hindeuten.

SIM-Karte

Die SIM-Karte wird primär auf ihre Identitätsmerkmale und hinterlegten Informationen geprüft:

- **Identifikation:** Das Auslesen von IMSI (International Mobile Subscriber Identity) und ICCID bestätigt die korrekte Funktion des SIM-Controllers.
- **Provider-Zuordnung:** Über die MCC/MNC-Daten wird geprüft, ob die Karte im Heimatnetz oder im Roaming-Modus operiert.
- **Hinterlegte Daten:** Das Feld „Eigene Nummer“ zeigt an, ob der Provider die Rufnummer direkt auf dem Speicher der Karte (EF-MSISDN) hinterlegt hat, was für bestimmte automatisierte Dienste von Bedeutung ist.

Standortanalyse und Gebäudeplanung (Site Survey)

Das Programm dient als Werkzeug zur Ermittlung des idealen Standorts für Mobilfunk-Hardware in Innenräumen.

- **Ermittlung von Totzonen:** Durch Beobachtung der Signalstärke (dBm) in verschiedenen Räumen können "Funklöcher" innerhalb eines Gebäudes präzise lokalisiert werden.
- **Platzierung von Routern/Gateways:** Anstatt sich auf die grobe Balkenanzeige eines Geräts zu verlassen, ermöglicht die exakte dBm-Anzeige die Positionierung eines Modems am Punkt des absolut stärksten Empfangs.
- **Antennenausrichtung:** Bei Verwendung von externen Richtantennen kann das Programm genutzt werden, um die Antenne durch Drehung exakt auf das Maximum der Signalstärke oder auf eine spezifische Cell-ID auszurichten.

IMSI-Catcher

Ein IMSI-Catcher ist ein Gerät, das eine legitime Funkzelle (Basisstation) simuliert, um Mobiltelefone in der Umgebung zur Einbuchung zu bewegen.

- **Funktionsweise:** Der Catcher sendet ein stärkeres Signal als die echten Masten aus. Sobald sich ein Gerät einbucht, kann der IMSI-Catcher die eindeutige Identifikationsnummer (IMSI) der SIM-Karte auslesen.
- **Ziel:** Lokalisierung von Personen, Erstellung von Bewegungsprofilen oder – bei älteren Standards wie GSM – das Abhören von unverschlüsselter Kommunikation durch das Erzwingen einer Deaktivierung der Verschlüsselung.

Das vorliegende Programm kann als "Frühwarnsystem" dienen, da IMSI-Catcher oft technische Anomalien verursachen, die in den Tabellen sichtbar werden:

- **Überwachung der Verschlüsselung:** In der Tabelle „Mobilfunk-Vorgaben“ wird der *Ciphering Mode* angezeigt. Wechselt dieser plötzlich auf „No Ciphering“ (A5/0), ist dies ein starkes Indiz für einen IMSI-Catcher, der die Verschlüsselung unterdrückt.
- **Beobachtung der Cell-ID:** Ein IMSI-Catcher hat oft eine Cell-ID oder einen LAC (Location Area Code), der nicht zum restlichen Standort-Muster passt.
- **Analyse der Nachbarzellen:** IMSI-Catcher erscheinen oft als extrem starke Zellen ohne logische Nachbarzellen in der Umgebung. Wenn eine Zelle plötzlich mit maximalem Pegel erscheint, aber keine korrekten Nachbardaten liefert, ist Vorsicht geboten.

5. Praktischer Nutzen des Programms

Der praktische Nutzen lässt sich in drei Anwendungsbereiche unterteilen:

1. **Technische Diagnose:** Techniker können die Hardware-Kommunikation des Modems überwachen und feststellen, ob Verbindungsfehler an der Antenne (Layer 1), der SIM-Karte oder dem Netzwerk-Protokoll (Layer 3) liegen.
2. **Optimierung des Empfangs:** Durch die Echtzeit-Anzeige der Signalstärke kann der optimale Standort für externe Antennen oder Router ermittelt werden (z. B. Ausrichtung auf ein bestimmtes Frequenzband wie LTE-20 für Reichweite oder LTE-7 für Speed).
3. **Sicherheits-Audit:** Versierte Anwender können die Umgebung auf verdächtige Funkzellen scannen und sicherstellen, dass die Verbindung stets verschlüsselt erfolgt.

Geografische Lokalisierung (Cell Tower Mapping): Der Abgleich technischer Kennungen mit Datenbanken wie OpenCellID ermöglicht die präzise Standortbestimmung von Sendemasten zur optimalen Ausrichtung von Antennen.

Identifikation von „Fake-Zellen“ und IMSI-Catchern: Community-Projekte dienen als Referenz, um durch den Vergleich von Live-Daten mit registrierten Funkzellen verdächtige, nicht autorisierte Basisstationen im Umfeld zu identifizieren.

Analyse der Netzabdeckung (Coverage Analysis): Die Nutzung von Heatmaps erlaubt eine Vorabprüfung verfügbarer Frequenzen, wodurch Abweichungen zwischen Soll-Versorgung und tatsächlicher Modem-Leistung aufgedeckt werden können.

Beitrag zur Gemeinschaft (War-Driving / Stumbling): Durch den Export und Upload eigener Messdaten tragen Anwender zur Vervollständigung weltweiter Netzkarten bei und verbessern die Dokumentation der digitalen Infrastruktur.

Allgemeine standarisierte Befehle (nach 3GPP / TS 27.007, herstellerunabhängig)

1. Basis-Kontrolle (V.250 Standard)

`AT`: Der "Attention"-Präfix. Testet, ob das Modem bereit ist.
`A/`: Wiederholt den letzten Befehl (einziger Befehl ohne AT-Präfix).
`ATE[0|1]`: Echo-Modus, ob Modem die eingegebenen Zeichen zurücksendet.
`ATV[0|1]`: Ergebniscodes als Text (OK) oder Zahlen (0).
`ATZ`: Soft-Reset des Modems auf Benutzerprofil.
`AT&F`: Werkseinstellungen laden.
`AT+CFUN=[0|1|4]`: Modi 0 (Minimal), 1 (Vollfunktion), 4 (Flugmodus).
`AT+CPAS`: Abfrage des Aktivitätsstatus, ob Modem bereit oder besetzt ist.
`AT+CBC`: Abfrage des Batteriezustands und der Spannung.
`AT+CTZU`: Aktiviert die automatische Zeitzonen-Aktualisierung durch das Mobilfunknetz.

2. Identifikation (3GPP Standard)

`ATI`: Identifikations-String (Modell, Hersteller, Revision).
`AT+CGMI`: Abfrage des Herstellernamens.
`AT+CGMM`: Abfrage der Modellbezeichnung.
`AT+CGMR`: Abfrage der Firmware-Revision.
`AT+CGSN`: Abfrage der Seriennummer (IMEI).

3. SIM-Karte und Sicherheit

`AT+CPIN?`: Abfrage des PIN-Status (Antwortet mit READY, SIM PIN, SIM PUK).
`AT+CIMI`: Abfrage der IMSI– die eindeutige ID der SIM.
`AT+CCID`: Abfrage der ICCID (die physische Kartennummer der SIM).
`AT+CEER`: Der „Extended Error Report für den letzten Abbruch einer Verbindung.
`AT+CLCK`: Facility Lock. Erlaubt Sperren, wie z. B. SIM-Lock, Tasten- oder Anrufsperren.
`AT+CPWD`: Ermöglicht das Ändern von Passwörtern für die AT+CLCK Dienste.
`AT+CRSM=...`: Restricted SIM Access. Direkten Lese- und Schreibzugriff auf SIM-Karte.

4. Netzwerk-Registrierung und Signale

`AT+CSQ`: Signalstärke (RSSI) und Fehlerrate (BER).
`AT+COPS?`: Aktueller Netzbetreiber.
`AT+CREG?`: Registrierungsstatus im CS-Netz (Telefonie).
`AT+CREG=2`: LAC und Cell-ID.
`AT+CGREG?`: Registrierungsstatus im PS-Netz (GPRS/Edge).
`AT+CEREG?`: Registrierungsstatus im EPS-Netz (LTE).
`AT+CLCC`: Liste der aktuellen Gespräche/Verbindungen.
`AT+CSCON?`: Abfrage des Signalisierungsstatus.
`AT+CGERP`: Abfrage des GPRS-Fehlerberichts.
`AT+CESQ`: Die erweiterte Version von AT+CSQ. Liefert präzisere Werte für LTE und 5G.
`AT+COPS=?`: Der „Network Scan“. Das Modem sucht nach allen verfügbaren.

5. Daten-Grundfunktionen (TS 27.005)

`AT+CMGF=[0|1]`: Umschalten zwischen PDU-Mode (hexadezimal) und Text-Mode.
`AT+CPMS?`: Abfrage des SMS-Speicherstatus.
`AT+CGDCONT?`: Abfrage der definierten Zugangspunkte (APN).
`AT+CGACT?`: Prüft, welche Datenverbindung aktuell aktiv ist.
`AT+CGPADDR`: Zeigt die vom Netzwerk zugewiesene IP-Adresse des Modems an.
`AT+CGAUTH`: Definiert die Authentifizierungsdaten für den Internetzugang.
`AT+CNUM`: Liest die MSISDN (die eigene Telefonnummer) von der SIM-Karte aus.
`AT+CPBS`: Wählt den Speicherort für das Telefonbuch aus (SIM-Karte / Gerätespeicher).
`AT+CPBR`: Liest Einträge aus dem gewählten Telefonbuch aus.

Befehle für Netz- und Zelleninformationen (herstellerspezifisch)

Diese Befehle werden genutzt, um detaillierte Informationen über die aktive Zelle und Nachbarzellen abzurufen:

- Allgemein / Mobil: `AT+EINFO` (Standardbefehl für erweiterte Systeminformationen).
- Dell (Modems): `AT+COPS=3,0;+COPS?` (Setzt das Format auf alphanumerisch und fragt den Betreiber ab).
- Ericsson: `AT+SURSERV` (Startet die Abfrage von „Serving Cell“ und Nachbarzellen).
- Gemalto / Cinterion: `AT^SMONI` (Umfassender Monitor-Befehl für Zell-ID, Pegel und Netztyp).
- Huawei: `AT^HCSQ?` (Spezialbefehl für die Signalqualität in LTE/UMTS-Netzen).
- Intel: `AT+XMONI` (Intels Äquivalent für detailliertes Zellen-Monitoring).
- MediaTek: `AT+EMCI?` (Abfrage von „Mobile Cell Information“).
- Qualcomm: `AT$QCRSRP?` (Liest spezifische LTE-Referenzsignalwerte aus).
- Samsung: `AT+NRINFO` (Informationen über die aktuelle Netzwerkregistrierung).
- Sierra Wireless: `AT!GSTATUS?` (Der wohl mächtigste Befehl im Programm; liefert Band, Frequenz, Cell-ID und Empfangswerte auf einen Blick).
- Telit: `AT#SERVINFO` (Spezifischer Befehl für Service-Zellen-Daten).
- U-blox: `AT+UCEDATA` (Abfrage von Zell-Umgebungsdaten).
- ZTE: `AT+ZCELLINFO` (Spezifischer Befehl für detaillierte Zell-Parameter).
- Quectel: `AT+QENG="servingcell"` (Engineering-Mode-Abfrage für LTE/5G-Parameter).

Befehle für Verschlüsselung (Ciphering) & Sicherheit

- `AT+CRSM=176,28448,0,0,9`: Ein spezieller SIM-Lese-Befehl (EF-Ciphering Indicator), der prüft, ob die Verschlüsselungsanzeige auf der SIM-Karte aktiviert ist.
- `AT+CPOL?`: Fragt die Liste der bevorzugten Netze ab, was indirekt Aufschluss über Roaming-Sicherheitsvorgaben gibt.
- `AT+clck="PN",2`: Prüft den Status der Personalisierung (Netz-Sperren), was wichtig für die Integrität der Verbindung ist.
- `AT!KCFG?`: (Sierra Wireless) Prüft spezifische Konfigurations-Flags, die auch Sicherheitsaspekte betreffen können.
- `AT+CRSM=176,28448,0,0,9`: Greift direkt auf das Filesystem der SIM-Karte zu (EF-AD = Administrative Data), um den „Ciphering Indicator“ auszulesen (ob das Handy ein Symbol für unverschlüsselte Verbindungen anzeigen muss).
- `AT+clck="PN",2`: Prüft den Status der Personalisierung des Netzwerks (Sperren).
- `AT+CPOL?`: Liest die Liste der bevorzugten Betreiber aus – wichtig, um manipulierte Prioritäten durch IMSI-Catcher zu erkennen.

  `AT+CEER`: „Extended Error Report“. Gibt den Grund für den letzten Verbindungsabbruch an (z.B. vom Netz abgewiesen wegen ungültiger Authentifizierung).

Die "Geheim-Befehle" für 5G & LTE-Advanced

- `AT+QENG="servingcell"`: Quectel-Befehl für 5G-NR (New Radio) Informationen.
- `AT+QCAINFO`: Abfrage von Carrier Aggregation (wenn das Modem mehrere LTE-Bänder gleichzeitig nutzt, um die Geschwindigkeit zu erhöhen).

Diagnose- & Identifikationsbefehle (Experten-Modus)

- `AT+GMI` / `AT+GMM`: Abfrage von Hersteller und Modellname.
- `AT+CGSN`: Abfrage der IMEI (Seriennummer des Modems).
- `AT+CIMI`: Abfrage der IMSI (Identität der SIM-Karte).
- `AT+CCID`: Abfrage der ICCID (Seriennummer der SIM-Karte).
- `AT+CNUM`: Abfrage der eigenen Rufnummer (falls auf der SIM gespeichert).
- `AT+CREG?` / `AT+CGREG?` / `AT+CEREG?`: Prüfung des Registrierungsstatus in GSM-, UMTS- und LTE-Netzen.

Netzwerk-Konfigurationsbefehle (Low-Level)

- `AT+COPS=3,2`: Schaltet den Operator-Modus auf das numerische Format um (zeigt 26201 statt „Telekom“), was für Datenbankabfragen wie OpenCellID essenziell ist.
- `AT+CEREG=2` / `AT+CREG=2`: Aktiviert den erweiterten Registrierungsstatus, damit das Modem bei jedem Zellwechsel sofort die neue Cell-ID und den LAC ungefragt meldet (Unsolicited Result Codes).
- `AT+CSCON=1`: Aktiviert die Signalisierungs-Verbindungsüberwachung (zeigt an, ob das Modem im „Idle“ oder „Connected“ Modus ist).

Hardware-Eingeweide (Modem-Status)

- `AT+CGMR`: Zeigt die exakte Revisionsnummer der Firmware an (wichtig für die Kompatibilität mit den AT-Befehlssätzen).
- `AT+CGSN`: Liest die Seriennummer (IMEI) aus – das Programm nutzt dies zur Identifikation des Geräts.
- `AT+CCID`: Liest die eindeutige ID des SIM-Chips aus (ICCID).
- `AT+CPIN?`: Prüft den Status der SIM-PIN (ob das Modem überhaupt bereit ist, mit dem Netz zu reden).

Hardcore-Diagnose & System-Stacks (aus der Debug-Routine)

- `AT!DALPOCW?`: Ein spezialisierter Sierra-Wireless-Befehl zur Abfrage von Hardware-Konfigurationen.
- `AT!GSTATUS?`: Liefert den kompletten Protokoll-Stack (Band, Channel, Port-Status, Temperatur des Modems).
- `AT$QCRSRP?` & `AT$QCRSRQ?`: Qualcomm-spezifische Befehle für die exakten Signalqualitätswerte von LTE-Referenzsignalen (RSRP/RSRQ).
- `AT+XMONI`: Ein Intel-spezifischer Befehl, der nicht nur die eigene Zelle, sondern detaillierte Informationen über das gesamte Funkumfeld liefert.
- `AT+EMCI?`: MediaTek-Befehl für „Enhanced Mobile Cell Information“ – liefert tiefere Layer-3-Daten als der Standard.
- `AT^HCSQ?`: Huawei-Befehl, der differenziert zwischen GSM, UMTS und LTE Signal-Metriken ausgibt.

Die vollständige Liste der Steuerbefehle für die jeweilige Hardware kann in den offiziellen „AT Command Set Manuals“ (oder auch AT Command Interface Guide) der jeweiligen Hersteller bezogen werden, welche die spezifischen Implementierungen des 3GPP-Standards (z. B. TS 27.007 und 27.005) detailliert dokumentieren.

Technische Systemdokumentation: Funkzellen-Netzwerkanalyzer (© 2026 – V 1.0)

Software-ID: FZ-NA-2026-MT

Entwickler: M. Trojan (Trojanix Lab int.)

Klassifizierung: Fernmelde-Diagnose-Software

Status: Revision 1.0 (Final Code Analysis)

---

1. Systemübersicht und Zweckbestimmung

Der Funkzellen-Netzwerkanalyzer ist eine forensische und diagnostische Anwendung zur Echtzeit-Analyse von Mobilfunkschnittstellen. Das System agiert als passiver und aktiver Monitor zwischen dem Betriebssystem und der WWAN-Hardware (Modem). Es dient der Identifikation von Netzinfrastrukturen, der Überwachung von Sicherheitsparametern (Ciphering) und der Detektion von Anomalien in den Schichten 1 bis 3 des OSI-Modells.

2. Architektur und Schnittstellen (Layer-Spezifikation)

2.1 Hardware-Kommunikation

Die Anwendung kommuniziert über die serielle Schnittstelle (**RS-232/USB-Serial**) mittels **AT-Kommandos** (V.250 Standard sowie herstellerspezifische Erweiterungen).

- **Baudrate:** 115200 (Standard)
- **Protokoll:** Asynchrone Datenübertragung
- **Anforderung:** Exklusiver Zugriff auf den Diagnose-Port des Modems.

2.2 Software-Stack

- **Frontend:** Python-basiertes GUI (Tkinter-Framework)
- **Multithreading:** Separater `Serial-Polling-Thread` zur Vermeidung von Interface-Blocking bei hoher Datenlast.
- **Persistenz:** Konfigurationsmanagement über `config.txt` zur Speicherung von Port-Zuweisungen und Geräte-Profilen.

---

3. Funktionsspezifikation der Analyse-Module

3.1 Physikalische Analyse (Layer 1)

Das System extrahiert und berechnet physikalische Parameter zur Bewertung der Funkschnittstelle:

- **RSSI/RSRP:** Signalstärke-Visualisierung via Analog-Instrument.

- **Frequenzanalyse:** Automatische EARFCN/UARFCN/ARFCN-Konvertierung in MHz-Werte für Downlink und Uplink.
- **Bandbreitenerkennung:** Detektion der Kanalbreite (LTE-Carrier-Width).

3.2 Netzwerk-Identifikation (Layer 3)

Eindeutige Identifizierung der Infrastruktur durch Extraktion von:

- **MCC (Mobile Country Code):** Länderidentifikation.
- **MNC (Mobile Network Code):** Betreiberidentifikation via interner Lookup-Tabelle (`mnc_dict`).
- **LAC/TAC:** Location Area Code / Tracking Area Code.
- **Cell-ID (CID):** Eindeutige Kennung der Funkzelle (GCI/ECI).

3.3 Sicherheits-Monitoring (Ciphering Indicator)

Überwachung der Luftschnittstellen-Verschlüsselung:

- **Modus:** Abfrage des Verschlüsselungsstatus (z. B. A5/3, AES, ZUC).
- **Alerting:** Visuelle Warnung bei unverschlüsselten Verbindungen (Potential IMSI-Catcher Alert).

---

4. Gerätespezifische Implementierung (Profile)

Das System verfügt über eine integrierte Bibliothek herstellerspezifischer Diagnose-Befehle, um die Datentiefe zu maximieren:

- **Sierra Wireless:** Nutzung von `AT!GSTATUS?` (Vollständiger Protokoll-Stack).
- **Qualcomm:** Extraktion von `RSRP/RSRQ` via `AT$QCRSRP`.
- **Huawei/Gemalto/Intel:** Herstellerspezifische Monitor-Kommandos (`^SMONI`, `+XMONI`, `^HCSQ`).

---

5. Datenverarbeitung und Logging

5.1 Zell-Historie (Event-Logging)

Chronologische Erfassung aller Zellwechsel mit Zeitstempel, Verweildauer und Maximalpegel. Diese Daten dienen der Erstellung von Bewegungsprofilen oder der Netzstabilitätsanalyse.

5.2 Nachbarzellen-Überwachung (Neighbor Cells)

Abfrage der `BCCH/Inter-Frequency`-Listen zur Identifikation benachbarter Zellen. Dies ermöglicht eine Triangulation des Standorts ohne GPS-Daten.

---

6. Diagnose- und Expertenmodus (Forensik)

Der integrierte **Raw-Debugger** erlaubt:

1. **Bit-Stream Monitoring:** Echtzeit-Anzeige der ein- und ausgehenden AT-Befehle.
2. **Manuelle Injektion:** Senden benutzerdefinierter Befehle zur Hardware-Manipulation oder Tiefendiagnose.
3. **Support-Matrix:** Automatisierter Scan (`run_full_diagnose`) zur Feststellung der Hardware-Fähigkeiten und unterstützter Sicherheits-Features.

---

7. Systemsicherheit und Integrität

- **Code-Sicherheit:** Verzicht auf externe Abhängigkeiten (außer `pyserial`), um die Angriffsfläche zu minimieren.
- **Datenlokalität:** Sämtliche Analysedaten verbleiben im flüchtigen Speicher (RAM) oder lokal im Anwendungsordner; keine Cloud-Anbindung oder Datenübermittlung. Es werden nur folgende Daten lokal gespeichert: Fenstergröße, Profil und COM-Port.
- **Fehlerbehandlung:** Robuste `try-except`-Blöcke bei der Port-Kommunikation zur Vermeidung von Systemabstürzen bei Hardware-Abbruch.

---

8. Abkürzungsverzeichnis (Behördenstandard)

- **EARFCN:** E-UTRA Absolute Radio Frequency Channel Number
- **IMEI:** International Mobile Equipment Identity
- **IMSI:** International Mobile Subscriber Identity
- **ICCID:** Integrated Circuit Card Identifier
- **RRC:** Radio Resource Control (Layer 3 Management)

Abschlussbewertung: Die Software erfüllt die Anforderungen an ein mobiles Netzwerkanalyse-Tool für behördliche Aufgaben im Bereich der Funküberwachung und technischen Aufklärung. Sie zeichnet sich durch eine hohe Hardware-Kompatibilität und eine präzise Layer-3-Datenerfassung aus nach BSI TR-03105 und ETSI TS 103 487. Das Programm ist 3GPP-konform in der Datenextraktion und erfüllt die Anforderungen der ITU-T V.250 für die Schnittstellensteuerung.

Eckernförde, den 26.02.2026

Mehmet S. Trojan

Software Engineering Research

Trojanix Lab int.