
# AURORAGOLD

# WORKING AID (UPDATED 17 MAY 2012)


(U//FOUO) AURORAGOLD is a team of SSG4 analysts, developers and wireless SMEs working on:

- (S//SI//REL) Database of Mobile Network Operators (MNOs), networks, and PWIDs collected from GSM/UMTS/LTE roaming documents (IR.21s),
- (S//SI//REL) Target development effort against MNOs, roaming hubs, and GSM Association (GSMA) working groups, and
- (U) Fusion of open source, licensed, commercial data with SIGINT to answer wireless needs.

## (S//SI//REL) Sample SIGINT (IR.21) Queries

- (S//SI//REL) What IR.21s have we seen for networks within a country or set of countries?
- (S//SI//REL) What IR.21s have we seen for networks managed by a mobile network operator?
- (S//SI//REL) What IR.21s have we seen for a particular network or set of networks?

## (U) Sample Open Source (Licensed Commercial Data) Queries

- (S//SI//REL) What are all of the cellular network operators within a country currently in service?
- (S//SI//REL) What suppliers have sold equipment to which operators within a country?
- (S//SI//REL) What networks are currently in service/planned within a country for each operator?
- (S//SI//REL) Which network technology equipment exists within a country for each operator?

- (S//SI//REL) What is the network name for each network within a country for each operator?
- (S//SI//REL) When was each network placed into service for each operator within a country?
- (S//SI//REL) What cellular network technology (e.g., GSM, W-CDMA, HSPA, etc.,) is in service for each operator in a country?
- (S//SI//REL) Which frequency spectrum bands are being used by which operators in a country?
- (S//SI//REL) What 4G/LTE networks are currently in service/planned for each operator within a country?
- (S//SI//REL) What CDMA or CDMA Wireless Local Loop networks are currently in service/planned for each operator within a country?
- (S//SI//REL) What network license auctions are planned within a country?

Derived From:
NSA/CSSM 1-52
Dated: 20070108

## (S//SI//REL) Some IR.21 Fields Useful to SIGINT

| (U) IR.21 Field | (U) What is it? | (U) How is it used? |
|---|---|---|
| **Mobile Country Code (MCC)/ Mobile Network Code (MNC)** | (U) A decimal digit code which uniquely identifies a mobile network. The MCC which identifies the country is used as the first three digits of any user's IMSI, followed by the two digit MNC which identifies the network within that country. | (U) Provide unique identification of networks to identify network boundaries, interfaces, protocols, software, hardware, etc. |
| **Mobile Subscriber Integrated Services Digital Network Number (MSISDN)** | (U) A number uniquely identifying a subscription in a GSM or a UMTS mobile network (the telephone number to the SIM card in a mobile/cellular phone). | (U) Allow identification of real phone number dialed |
| **TADIG codes** | (U) A number allocated by the GSMA for use as primary identifiers, both within file contents and file names. Also used as a more generic entity identifier in the mobile industry | (U) Identify the network for billing purposes and help identify targets |
| **Signaling Connection Control Part (SCCP)** | (U) A network layer protocol that provides extended routing, flow control, segmentation, connection-orientation, and error correction facilities in Signaling System 7 telecommunications networks | (U) Provides routing information within the Public Land Mobile Network and provides access to applications such as 800-call processing and calling card processing to identify targets and other information |
| **Subscriber Identity Authentication** | (U) This field indicates whether or not authentication is performed for roaming subscribers at the start of GSM service and the type of A5 cipher algorithm version in use. | (S//SI//REL) It would also show the emergence of new cipher algorithms and support target analysis, trending and the development of exploits. |
| **Mobile Application Part (MAP)** | (U) A SS7 protocol which provides an application layer for the various nodes in GSM and UMTS mobile core networks and GPRS core networks to communicate with each other in order to provide services to mobile phone users. The Mobile Application Part is the application-layer protocol used to access the Home Location Register, Visitor Location Register, Mobile Switching Center, Equipment Identity Register, Authentication Centre, Short message service center and Serving GPRS Support Node (SGSN). | (S//SI//REL) Provides a clearer understanding of network features when roaming agreement information is published. Current information about subscribers, mobility management and applications can be used for targeting and target development. |
| **Network Element** | (U) Specific network components, their manufacturer, software & hardware versions, etc. | (S//SI//REL) This specific information is necessary for targeting and exploitation. Includes core and |

| | | |
|---|---|---|
| **Information** | | radio interface information. |
| **Packet Data Services Information** | (U) Packet Data Services identifies the affected GPRS networks. An Access Point Name is also included in this information. APNs can identify the type of service provided by GPRS networks provided to mobile users. APNs also help identify the network and operator's packet network involved in the IR.21 and could be used for targeting. | (S//SI//REL) This data element also provides information on the WAP gateway being access and multimedia messaging services gateway IP addresses which is useful for target development. Insight into the GPRS Tunneling Protocol versions being used within the networks is provided as well. GPRS, EDGE and HSPA technologies are covered. |