Mobile Forensics

Digital Forensics

University of Genoa 2025

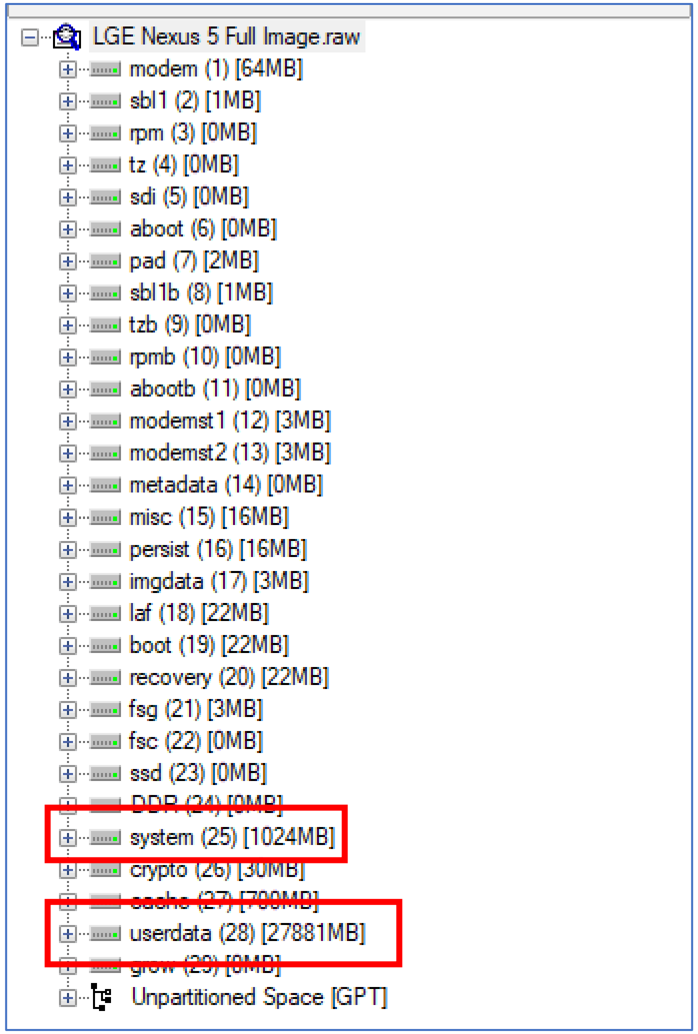
Requirements

- **Exterro FTK Imager**
  https://www.exterro.com/ftk-imager

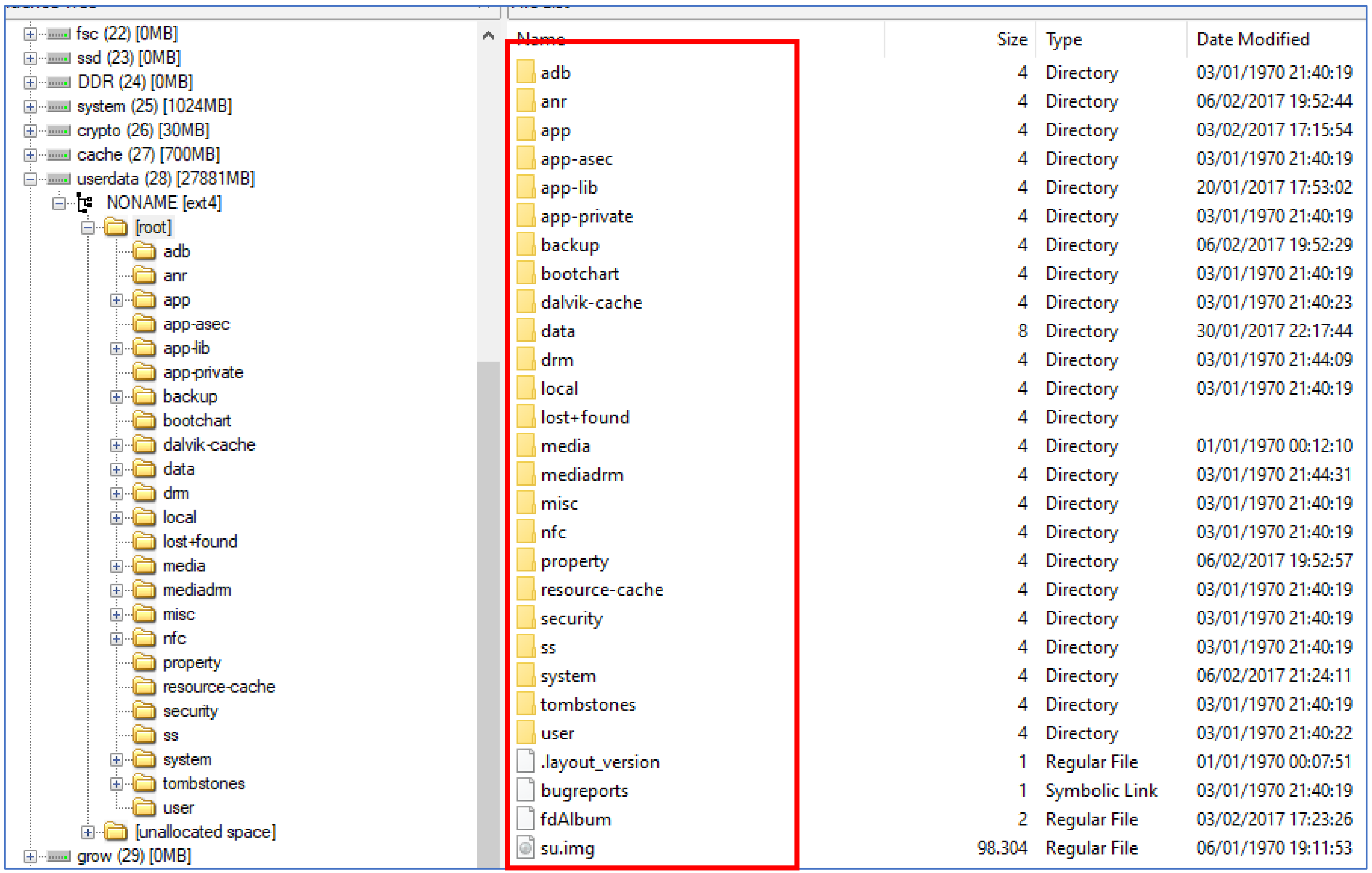
- **aLEAPP**
  https://github.com/abrignoni/ALEAPP

- **UFED Reader and Report**

Android OS – Partitions



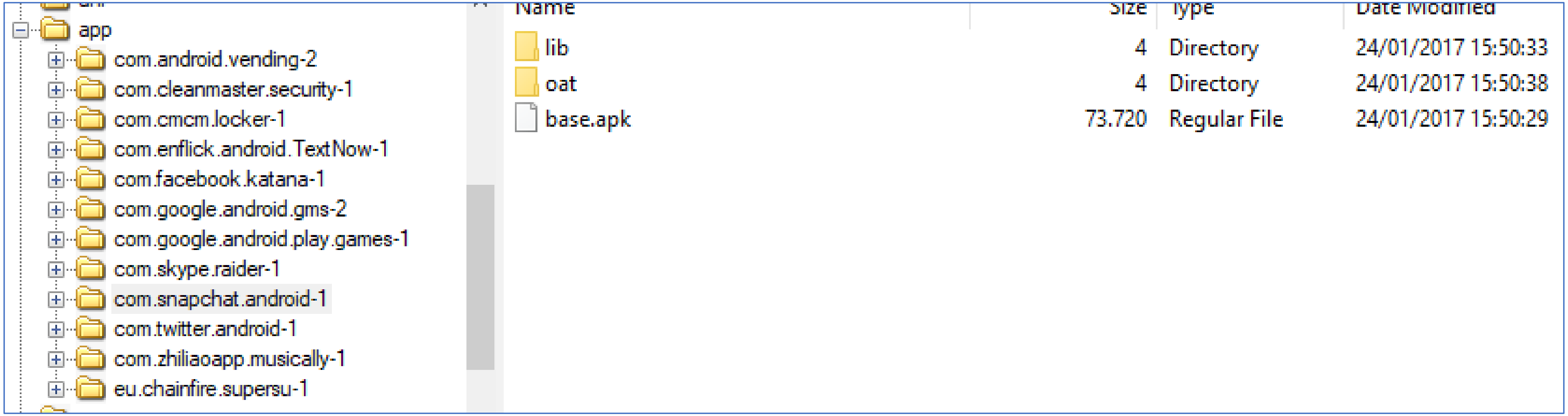
```
LGE Nexus 5 Full Image.raw
    modem (1) [64MB]
    sbl1 (2) [1MB]
    rpm (3) [0MB]
    tz (4) [0MB]
    sdi (5) [0MB]
    aboot (6) [0MB]
    pad (7) [2MB]
    sbl1b (8) [1MB]
    tzb (9) [0MB]
    rpmb (10) [0MB]
    abootb (11) [0MB]
    modemst1 (12) [3MB]
    modemst2 (13) [3MB]
    metadata (14) [0MB]
    misc (15) [16MB]
    persist (16) [16MB]
    imgdata (17) [3MB]
    laf (18) [22MB]
    boot (19) [22MB]
    recovery (20) [22MB]
    fsg (21) [3MB]
    fsc (22) [0MB]
    ssd (23) [0MB]
    DDR (24) [0MB]
    system (25) [1024MB]
    crypto (26) [30MB]
    cache (27) [700MB]
    userdata (28) [27881MB]
    grow (29) [0MB]
    Unpartitioned Space [GPT]
```



```
fsc (22) [0MB]
ssd (23) [0MB]
DDR (24) [0MB]
system (25) [1024MB]
crypto (26) [30MB]
cache (27) [700MB]
userdata (28) [27881MB]
    NONAME [ext4]
        [root]
            adb
            anr
            app
            app-asec
            app-lib
            app-private
            backup
            bootchart
            dalvik-cache
            data
            drm
            local
            lost+found
            media
            mediadrm
            misc
            nfc
            property
            resource-cache
            security
            ss
            system
            tombstones
            user
        [unallocated space]
grow (29) [0MB]
```

Name	Size	Type	Date Modified
adb	4	Directory	03/01/1970 21:40:19
anr	4	Directory	06/02/2017 19:52:44
app	4	Directory	03/02/2017 17:15:54
app-asec	4	Directory	03/01/1970 21:40:19
app-lib	4	Directory	20/01/2017 17:53:02
app-private	4	Directory	03/01/1970 21:40:19
backup	4	Directory	06/02/2017 19:52:29
bootchart	4	Directory	03/01/1970 21:40:19
dalvik-cache	4	Directory	03/01/1970 21:40:23
data	8	Directory	30/01/2017 22:17:44
drm	4	Directory	03/01/1970 21:44:09
local	4	Directory	03/01/1970 21:40:19
lost+found	4	Directory	
media	4	Directory	01/01/1970 00:12:10
mediadrm	4	Directory	03/01/1970 21:44:31
misc	4	Directory	03/01/1970 21:40:19
nfc	4	Directory	03/01/1970 21:40:19
property	4	Directory	06/02/2017 19:52:57
resource-cache	4	Directory	03/01/1970 21:40:19
security	4	Directory	03/01/1970 21:40:19
ss	4	Directory	03/01/1970 21:40:19
system	4	Directory	06/02/2017 21:24:11
tombstones	4	Directory	03/01/1970 21:40:19
user	4	Directory	03/01/1970 21:40:22
.layout_version	1	Regular File	01/01/1970 00:07:51
bugreports	1	Symbolic Link	03/01/1970 21:40:19
fdAlbum	2	Regular File	03/02/2017 17:23:26
su.img	98.304	Regular File	06/01/1970 19:11:53

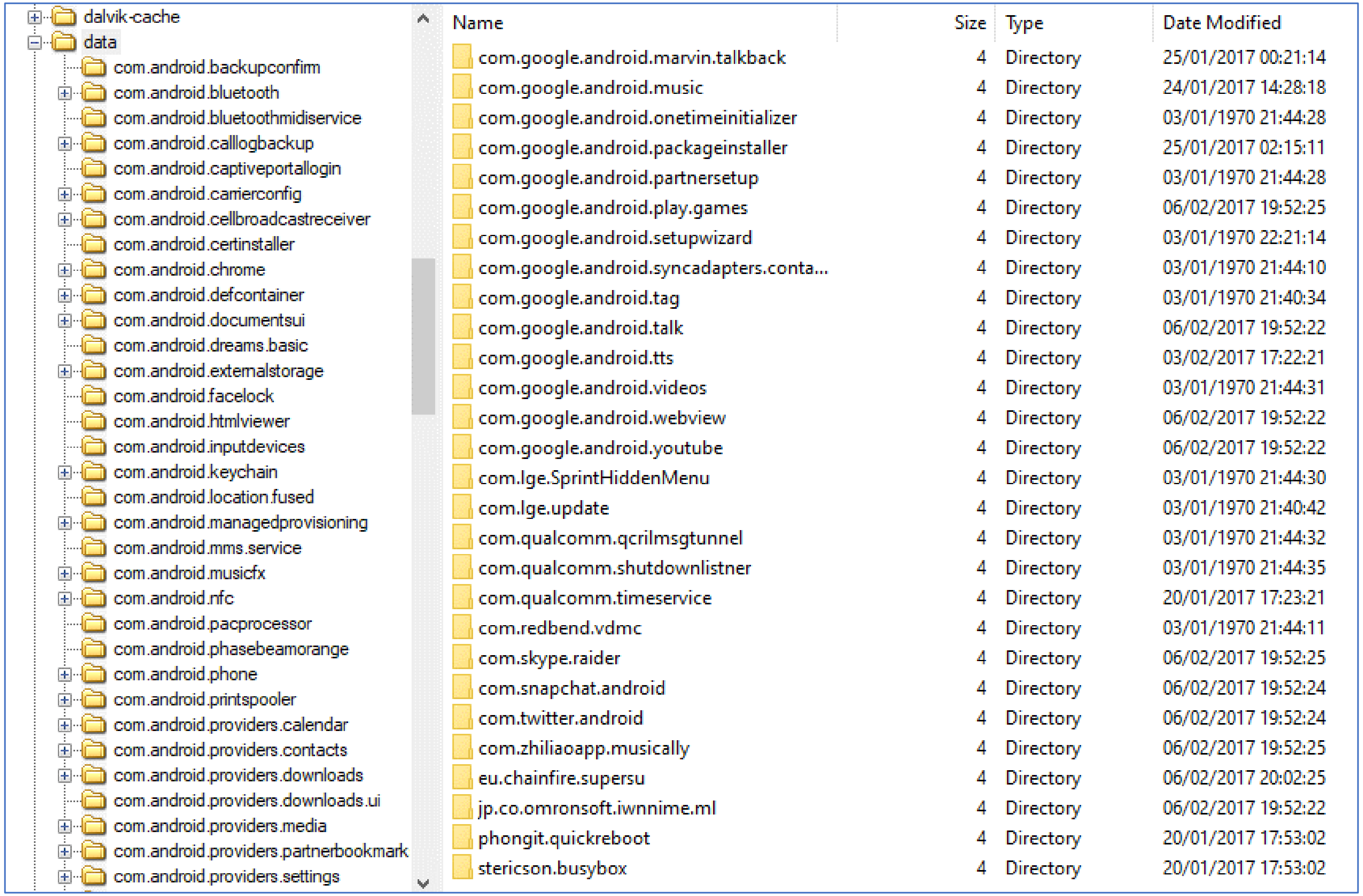
Android OS – Userdata Partition – «App» folder



- app
  - com.android.vending-2
  - com.cleanmaster.security-1
  - com.cmcm.locker-1
  - com.enflick.android.TextNow-1
  - com.facebook.katana-1
  - com.google.android.gms-2
  - com.google.android.play.games-1
  - com.skype.raider-1
  - com.snapchat.android-1
  - com.twitter.android-1
  - com.zhiliaoapp.musically-1
  - eu.chainfire.supersu-1

Name	Size	Type	Date Modified
lib	4	Directory	24/01/2017 15:50:33
oat	4	Directory	24/01/2017 15:50:38
base.apk	73.720	Regular File	24/01/2017 15:50:29

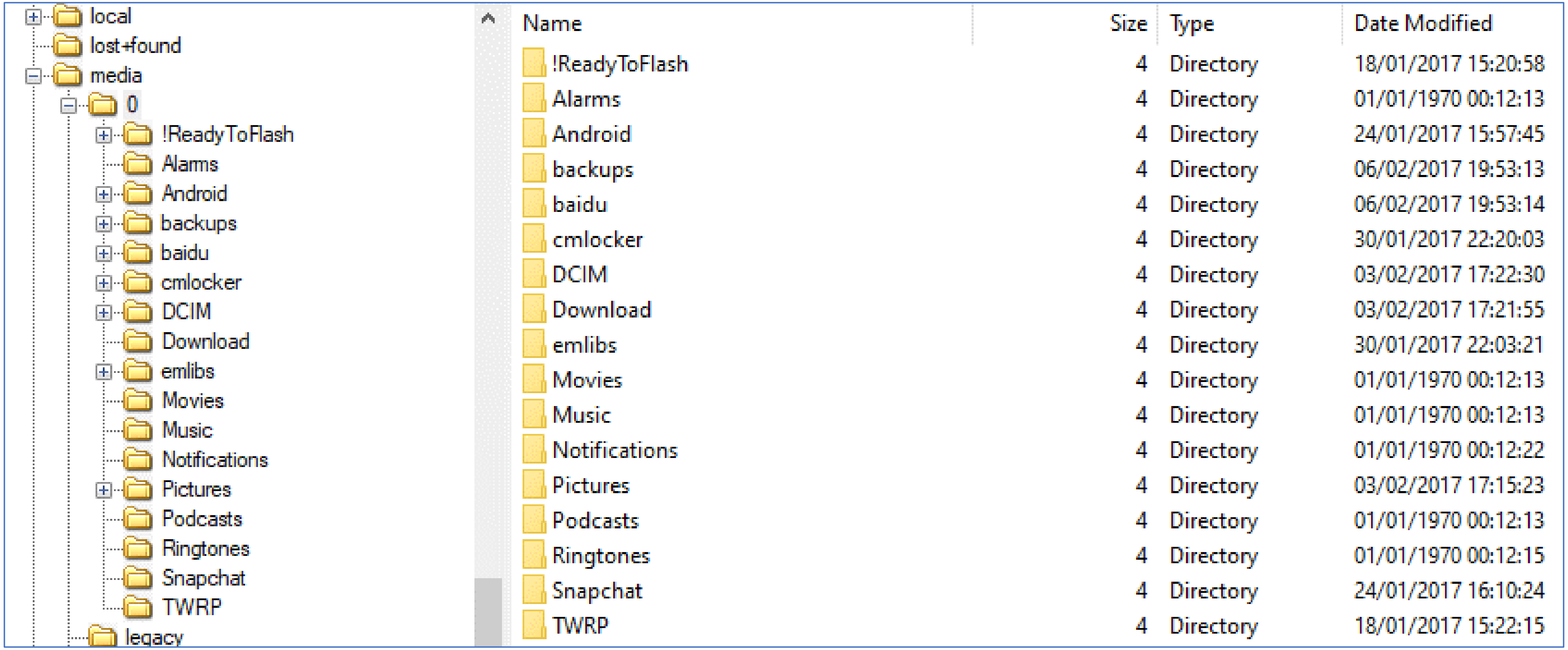
Android OS – Userdata Partition – «Data» folder



- ⊞ dalvik-cache
- ⊟ data
  - com.android.backupconfirm
  - ⊞ com.android.bluetooth
  - com.android.bluetoothmidiservice
  - ⊞ com.android.calllogbackup
  - com.android.captiveportallogin
  - ⊞ com.android.carrierconfig
  - ⊞ com.android.cellbroadcastreceiver
  - com.android.certinstaller
  - ⊞ com.android.chrome
  - ⊞ com.android.defcontainer
  - ⊞ com.android.documentsui
  - com.android.dreams.basic
  - ⊞ com.android.externalstorage
  - com.android.facelock
  - com.android.htmlviewer
  - com.android.inputdevices
  - ⊞ com.android.keychain
  - com.android.location.fused
  - ⊞ com.android.managedprovisioning
  - com.android.mms.service
  - ⊞ com.android.musicfx
  - ⊞ com.android.nfc
  - com.android.pacprocessor
  - com.android.phasebeamorange
  - ⊞ com.android.phone
  - ⊞ com.android.printspooler
  - ⊞ com.android.providers.calendar
  - ⊞ com.android.providers.contacts
  - ⊞ com.android.providers.downloads
  - com.android.providers.downloads.ui
  - ⊞ com.android.providers.media
  - ⊞ com.android.providers.partnerbookmark
  - ⊞ com.android.providers.settings

Name	Size	Type	Date Modified
com.google.android.marvin.talkback	4	Directory	25/01/2017 00:21:14
com.google.android.music	4	Directory	24/01/2017 14:28:18
com.google.android.onetimeinitializer	4	Directory	03/01/1970 21:44:28
com.google.android.packageinstaller	4	Directory	25/01/2017 02:15:11
com.google.android.partnersetup	4	Directory	03/01/1970 21:44:28
com.google.android.play.games	4	Directory	06/02/2017 19:52:25
com.google.android.setupwizard	4	Directory	03/01/1970 22:21:14
com.google.android.syncadapters.conta...	4	Directory	03/01/1970 21:44:10
com.google.android.tag	4	Directory	03/01/1970 21:40:34
com.google.android.talk	4	Directory	06/02/2017 19:52:22
com.google.android.tts	4	Directory	03/02/2017 17:22:21
com.google.android.videos	4	Directory	03/01/1970 21:44:31
com.google.android.webview	4	Directory	06/02/2017 19:52:22
com.google.android.youtube	4	Directory	06/02/2017 19:52:22
com.lge.SprintHiddenMenu	4	Directory	03/01/1970 21:44:30
com.lge.update	4	Directory	03/01/1970 21:40:42
com.qualcomm.qcrilmsgtunnel	4	Directory	03/01/1970 21:44:32
com.qualcomm.shutdownlistner	4	Directory	03/01/1970 21:44:35
com.qualcomm.timeservice	4	Directory	20/01/2017 17:23:21
com.redbend.vdmc	4	Directory	03/01/1970 21:44:11
com.skype.raider	4	Directory	06/02/2017 19:52:25
com.snapchat.android	4	Directory	06/02/2017 19:52:24
com.twitter.android	4	Directory	06/02/2017 19:52:24
com.zhiliaoapp.musically	4	Directory	06/02/2017 19:52:25
eu.chainfire.supersu	4	Directory	06/02/2017 20:02:25
jp.co.omronsoft.iwnnime.ml	4	Directory	06/02/2017 19:52:22
phongit.quickreboot	4	Directory	20/01/2017 17:53:02
stericson.busybox	4	Directory	20/01/2017 17:53:02

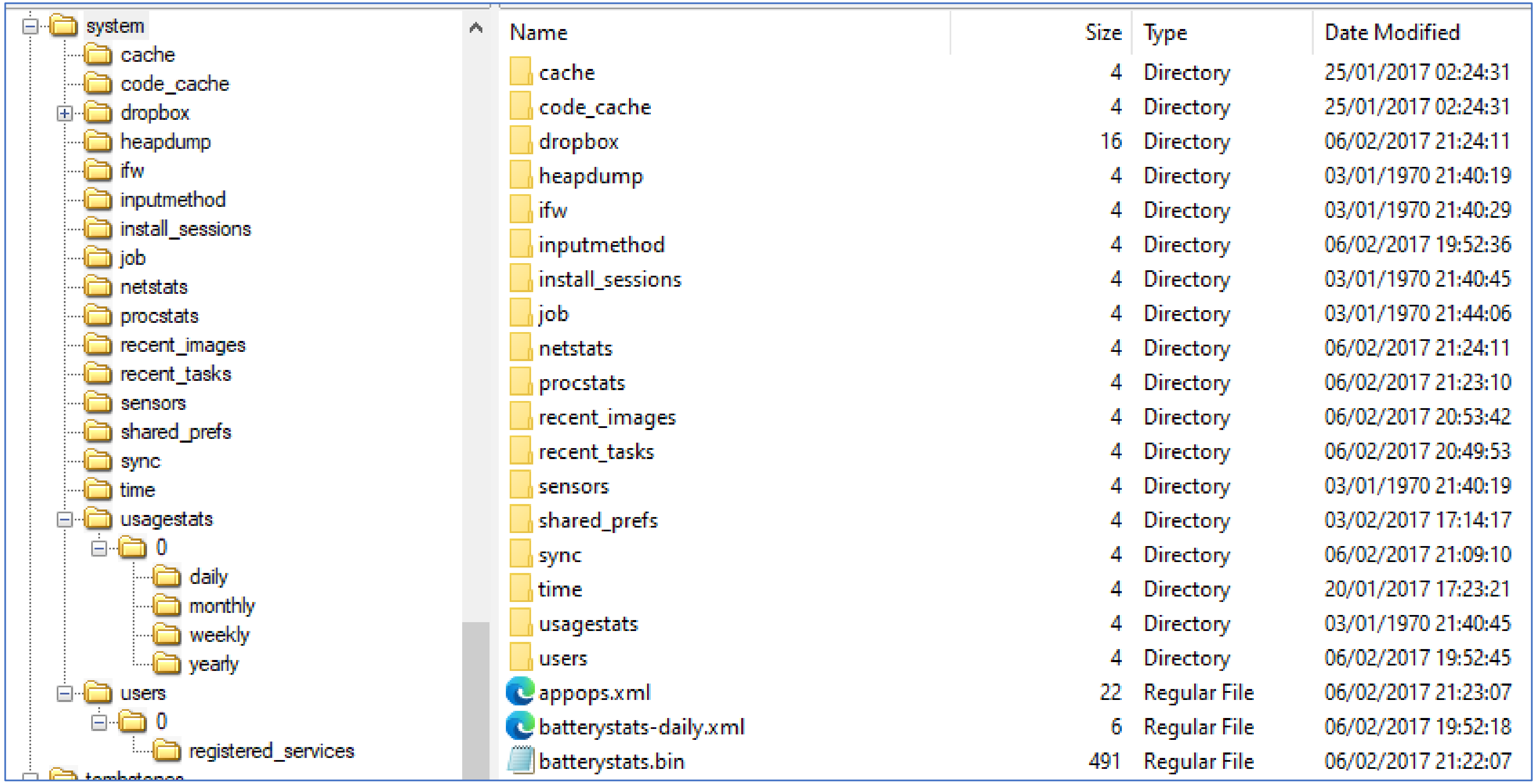
Android OS – Userdata Partition – «Media» folder



- local
- lost+found
- media
  - 0
    - !ReadyToFlash
    - Alarms
    - Android
    - backups
    - baidu
    - cmlocker
    - DCIM
    - Download
    - emlibs
    - Movies
    - Music
    - Notifications
    - Pictures
    - Podcasts
    - Ringtones
    - Snapchat
    - TWRP
  - legacy

Name	Size	Type	Date Modified
!ReadyToFlash	4	Directory	18/01/2017 15:20:58
Alarms	4	Directory	01/01/1970 00:12:13
Android	4	Directory	24/01/2017 15:57:45
backups	4	Directory	06/02/2017 19:53:13
baidu	4	Directory	06/02/2017 19:53:14
cmlocker	4	Directory	30/01/2017 22:20:03
DCIM	4	Directory	03/02/2017 17:22:30
Download	4	Directory	03/02/2017 17:21:55
emlibs	4	Directory	30/01/2017 22:03:21
Movies	4	Directory	01/01/1970 00:12:13
Music	4	Directory	01/01/1970 00:12:13
Notifications	4	Directory	01/01/1970 00:12:22
Pictures	4	Directory	03/02/2017 17:15:23
Podcasts	4	Directory	01/01/1970 00:12:13
Ringtones	4	Directory	01/01/1970 00:12:15
Snapchat	4	Directory	24/01/2017 16:10:24
TWRP	4	Directory	18/01/2017 15:22:15

Android OS – Userdata Partition – «System» folder



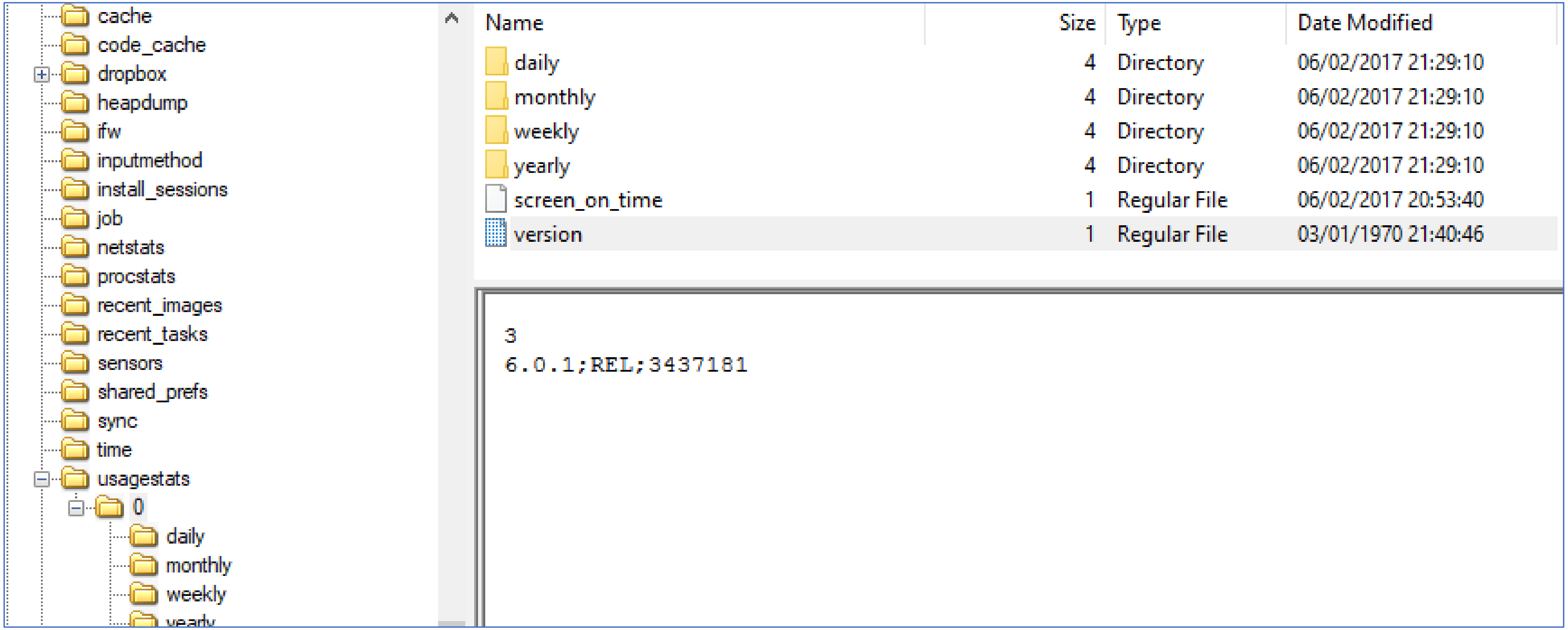
- system
  - cache
  - code_cache
  - dropbox
  - heapdump
  - ifw
  - inputmethod
  - install_sessions
  - job
  - netstats
  - procstats
  - recent_images
  - recent_tasks
  - sensors
  - shared_prefs
  - sync
  - time
  - usagestats
    - 0
      - daily
      - monthly
      - weekly
      - yearly
  - users
    - 0
      - registered_services
- tombstones

Name	Size	Type	Date Modified
cache	4	Directory	25/01/2017 02:24:31
code_cache	4	Directory	25/01/2017 02:24:31
dropbox	16	Directory	06/02/2017 21:24:11
heapdump	4	Directory	03/01/1970 21:40:19
ifw	4	Directory	03/01/1970 21:40:29
inputmethod	4	Directory	06/02/2017 19:52:36
install_sessions	4	Directory	03/01/1970 21:40:45
job	4	Directory	03/01/1970 21:44:06
netstats	4	Directory	06/02/2017 21:24:11
procstats	4	Directory	06/02/2017 21:23:10
recent_images	4	Directory	06/02/2017 20:53:42
recent_tasks	4	Directory	06/02/2017 20:49:53
sensors	4	Directory	03/01/1970 21:40:19
shared_prefs	4	Directory	03/02/2017 17:14:17
sync	4	Directory	06/02/2017 21:09:10
time	4	Directory	20/01/2017 17:23:21
usagestats	4	Directory	03/01/1970 21:40:45
users	4	Directory	06/02/2017 19:52:45
appops.xml	22	Regular File	06/02/2017 21:23:07
batterystats-daily.xml	6	Regular File	06/02/2017 19:52:18
batterystats.bin	491	Regular File	06/02/2017 21:22:07

Android OS relevant information

- **Android OS Version**
- **Installed Apps**
  - **Localappstate.db**
  - **Gass.db**
- **Permissions**
- **Contacts**
- **Call Log**
- **SMS/MMS Messages**
- **Downloads**
- **Wi-Fi Profiles**

Android OS Version (\usagestats\0\version)

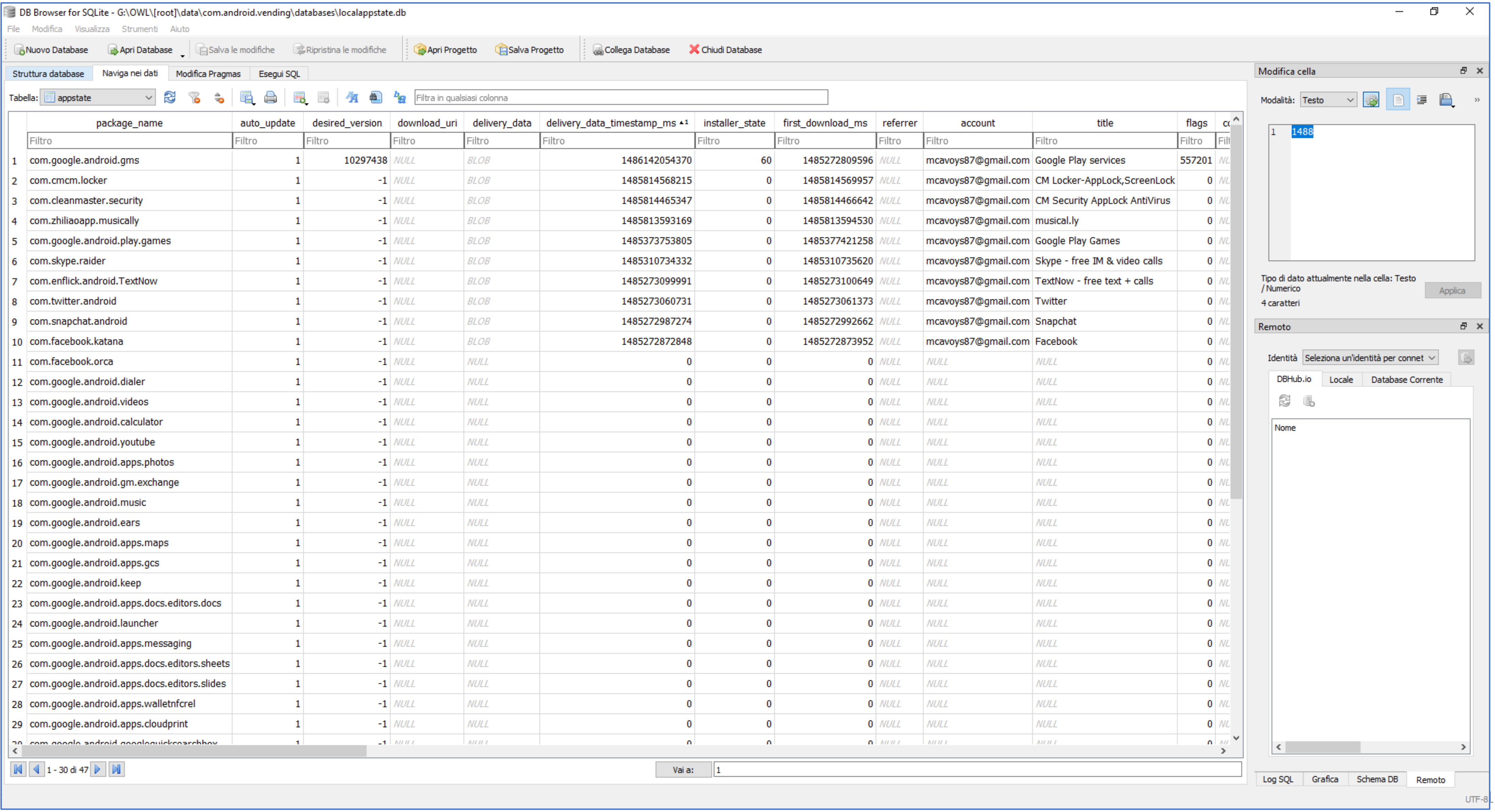


- cache
- code_cache
- dropbox
- heapdump
- ifw
- inputmethod
- install_sessions
- job
- netstats
- procstats
- recent_images
- recent_tasks
- sensors
- shared_prefs
- sync
- time
- usagestats
  - 0
    - daily
    - monthly
    - weekly
    - yearly

Name	Size	Type	Date Modified
daily	4	Directory	06/02/2017 21:29:10
monthly	4	Directory	06/02/2017 21:29:10
weekly	4	Directory	06/02/2017 21:29:10
yearly	4	Directory	06/02/2017 21:29:10
screen_on_time	1	Regular File	06/02/2017 20:53:40
version	1	Regular File	03/01/1970 21:40:46

```
3
6.0.1;REL;3437181
```

Installed Apps (\data\com.android.vending\databases\localappstate.db)



DB Browser for SQLite - G:\OWL\[root]\data\com.android.vending\databases\localappstate.db

Tabella: appstate

	package_name	auto_update	desired_version	download_uri	delivery_data	delivery_data_timestamp_ms ▲1	installer_state	first_download_ms	referrer	account	title	flags	co
	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filt
1	com.google.android.gms	1	10297438	NULL	BLOB	1486142054370	60	1485272809596	NULL	mcavoys87@gmail.com	Google Play services	557201	NU
2	com.cmcm.locker	1	-1	NULL	BLOB	1485814568215	0	1485814569957	NULL	mcavoys87@gmail.com	CM Locker-AppLock,ScreenLock	0	NU
3	com.cleanmaster.security	1	-1	NULL	BLOB	1485814465347	0	1485814466642	NULL	mcavoys87@gmail.com	CM Security AppLock AntiVirus	0	NU
4	com.zhiliaoapp.musically	1	-1	NULL	BLOB	1485813593169	0	1485813594530	NULL	mcavoys87@gmail.com	musical.ly	0	NU
5	com.google.android.play.games	1	-1	NULL	BLOB	1485373753805	0	1485377421258	NULL	mcavoys87@gmail.com	Google Play Games	0	NU
6	com.skype.raider	1	-1	NULL	BLOB	1485310734332	0	1485310735620	NULL	mcavoys87@gmail.com	Skype - free IM & video calls	0	NU
7	com.enflick.android.TextNow	1	-1	NULL	BLOB	1485273099991	0	1485273100649	NULL	mcavoys87@gmail.com	TextNow - free text + calls	0	NU
8	com.twitter.android	1	-1	NULL	BLOB	1485273060731	0	1485273061373	NULL	mcavoys87@gmail.com	Twitter	0	NU
9	com.snapchat.android	1	-1	NULL	BLOB	1485272987274	0	1485272992662	NULL	mcavoys87@gmail.com	Snapchat	0	NU
10	com.facebook.katana	1	-1	NULL	BLOB	1485272872848	0	1485272873952	NULL	mcavoys87@gmail.com	Facebook	0	NU
11	com.facebook.orca	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
12	com.google.android.dialer	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
13	com.google.android.videos	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
14	com.google.android.calculator	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
15	com.google.android.youtube	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
16	com.google.android.apps.photos	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
17	com.google.android.gm.exchange	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
18	com.google.android.music	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
19	com.google.android.ears	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
20	com.google.android.apps.maps	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
21	com.google.android.apps.gcs	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
22	com.google.android.keep	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
23	com.google.android.apps.docs.editors.docs	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
24	com.google.android.launcher	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
25	com.google.android.apps.messaging	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
26	com.google.android.apps.docs.editors.sheets	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
27	com.google.android.apps.docs.editors.slides	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
28	com.google.android.apps.walletnfcrel	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
29	com.google.android.apps.cloudprint	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU
30	com.google.android.googlequicksearchbox	1	-1	NULL	NULL	0	0	0	NULL	NULL	NULL	0	NU

1 - 30 di 47

Vai a: 1

Modifica cella

Modalità: Testo

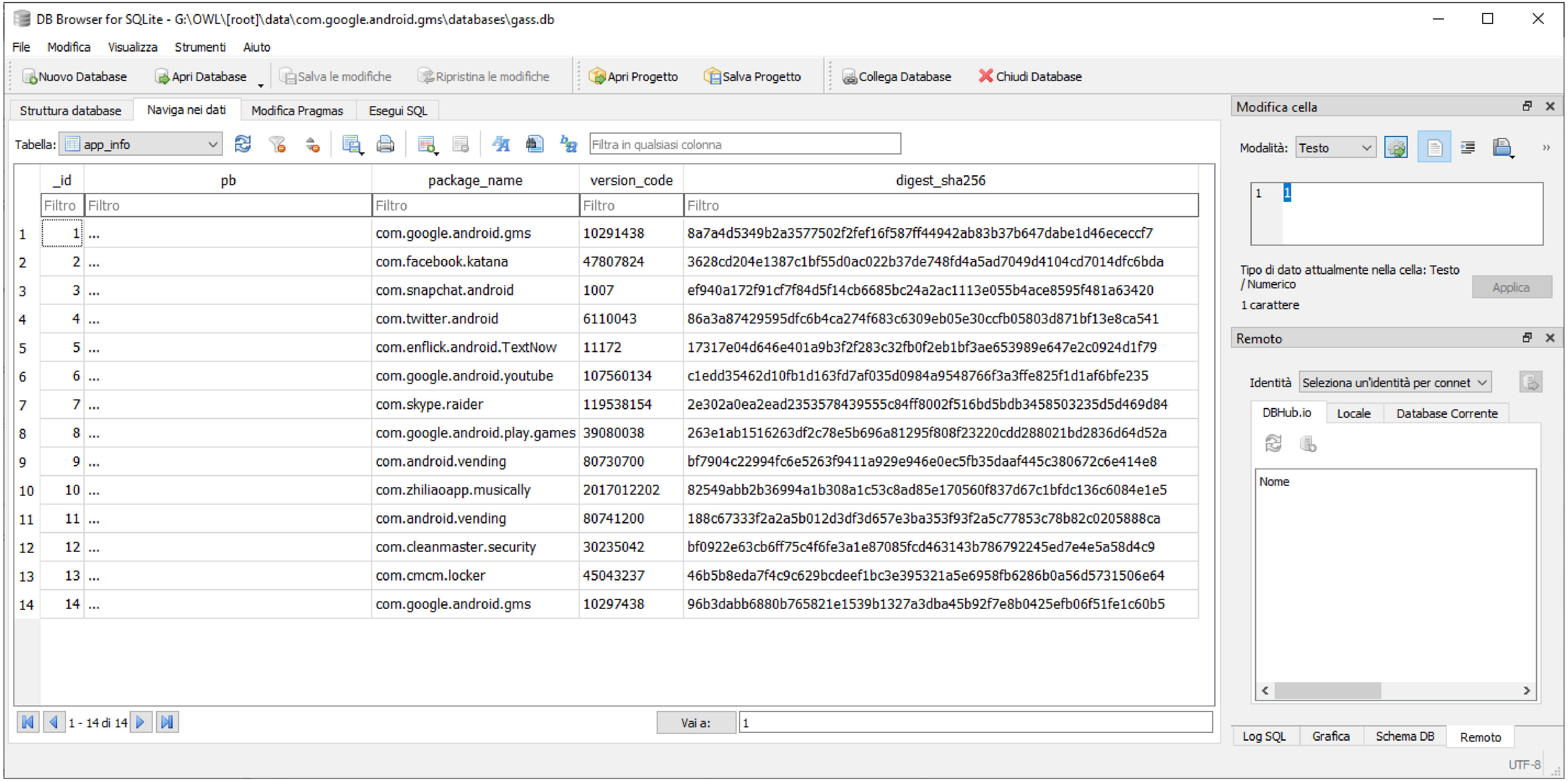
1 1488

Tipo di dato attualmente nella cella: Testo / Numerico

4 caratteri

Identità: Seleziona un'identità per connet

Installed Apps (\data\com.google.android.gms\databases\gass.db)



DB Browser for SQLite - G:\OWL\[root]\data\com.google.android.gms\databases\gass.db

Tabella: app_info

	_id	pb	package_name	version_code	digest_sha256
1	1	...	com.google.android.gms	10291438	8a7a4d5349b2a3577502f2fef16f587ff44942ab83b37b647dabe1d46ececcf7
2	2	...	com.facebook.katana	47807824	3628cd204e1387c1bf55d0ac022b37de748fd4a5ad7049d4104cd7014dfc6bda
3	3	...	com.snapchat.android	1007	ef940a172f91cf7f84d5f14cb6685bc24a2ac1113e055b4ace8595f481a63420
4	4	...	com.twitter.android	6110043	86a3a87429595dfc6b4ca274f683c6309eb05e30ccfb05803d871bf13e8ca541
5	5	...	com.enflick.android.TextNow	11172	17317e04d646e401a9b3f2f283c32fb0f2eb1bf3ae653989e647e2c0924d1f79
6	6	...	com.google.android.youtube	107560134	c1edd35462d10fb1d163fd7af035d0984a9548766f3a3ffe825f1d1af6bfe235
7	7	...	com.skype.raider	119538154	2e302a0ea2ead2353578439555c84ff8002f516bd5bdb3458503235d5d469d84
8	8	...	com.google.android.play.games	39080038	263e1ab1516263df2c78e5b696a81295f808f23220cdd288021bd2836d64d52a
9	9	...	com.android.vending	80730700	bf7904c22994fc6e5263f9411a929e946e0ec5fb35daaf445c380672c6e414e8
10	10	...	com.zhiliaoapp.musically	2017012202	82549abb2b36994a1b308a1c53c8ad85e170560f837d67c1bfdc136c6084e1e5
11	11	...	com.android.vending	80741200	188c67333f2a2a5b012d3df3d657e3ba353f93f2a5c77853c78b82c0205888ca
12	12	...	com.cleanmaster.security	30235042	bf0922e63cb6ff75c4f6fe3a1e87085fcd463143b786792245ed7e4e5a58d4c9
13	13	...	com.cmcm.locker	45043237	46b5b8eda7f4c9c629bcdeef1bc3e395321a5e6958fb6286b0a56d5731506e64
14	14	...	com.google.android.gms	10297438	96b3dabb6880b765821e1539b1327a3dba45b92f7e8b0425efb06f51fe1c60b5

1 - 14 di 14

Vai a: 1

Modifica cella

Modalità: Testo

1 1

Tipo di dato attualmente nella cella: Testo / Numerico

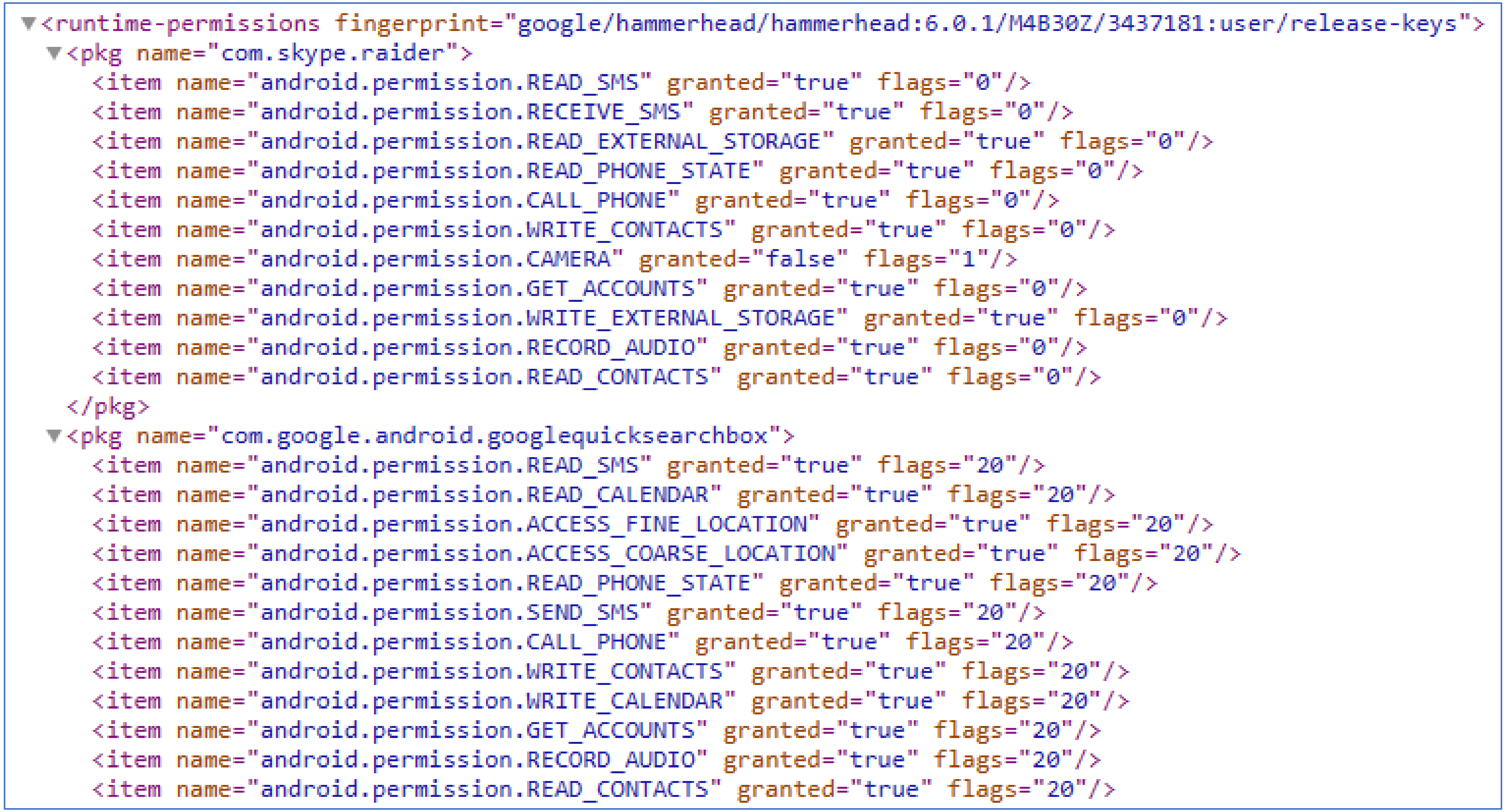
1 carattere

Remoto

Identità Seleziona un'identità per connet

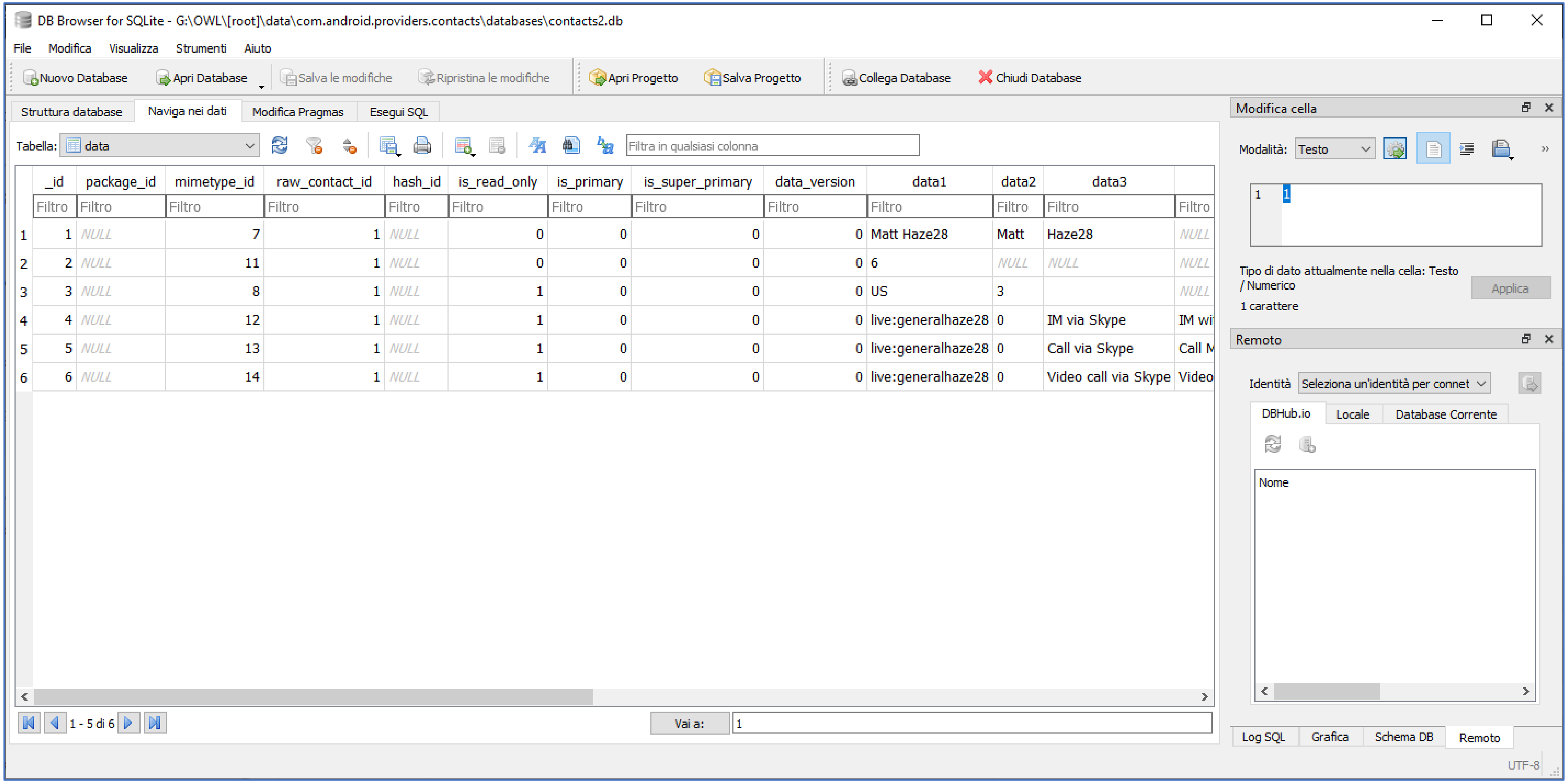
UTF-8

Permissions (\system\users\0\runtime-permissions.xml)



```
▼<runtime-permissions fingerprint="google/hammerhead/hammerhead:6.0.1/M4B30Z/3437181:user/release-keys">
  ▼<pkg name="com.skype.raider">
      <item name="android.permission.READ_SMS" granted="true" flags="0"/>
      <item name="android.permission.RECEIVE_SMS" granted="true" flags="0"/>
      <item name="android.permission.READ_EXTERNAL_STORAGE" granted="true" flags="0"/>
      <item name="android.permission.READ_PHONE_STATE" granted="true" flags="0"/>
      <item name="android.permission.CALL_PHONE" granted="true" flags="0"/>
      <item name="android.permission.WRITE_CONTACTS" granted="true" flags="0"/>
      <item name="android.permission.CAMERA" granted="false" flags="1"/>
      <item name="android.permission.GET_ACCOUNTS" granted="true" flags="0"/>
      <item name="android.permission.WRITE_EXTERNAL_STORAGE" granted="true" flags="0"/>
      <item name="android.permission.RECORD_AUDIO" granted="true" flags="0"/>
      <item name="android.permission.READ_CONTACTS" granted="true" flags="0"/>
    </pkg>
  ▼<pkg name="com.google.android.googlequicksearchbox">
      <item name="android.permission.READ_SMS" granted="true" flags="20"/>
      <item name="android.permission.READ_CALENDAR" granted="true" flags="20"/>
      <item name="android.permission.ACCESS_FINE_LOCATION" granted="true" flags="20"/>
      <item name="android.permission.ACCESS_COARSE_LOCATION" granted="true" flags="20"/>
      <item name="android.permission.READ_PHONE_STATE" granted="true" flags="20"/>
      <item name="android.permission.SEND_SMS" granted="true" flags="20"/>
      <item name="android.permission.CALL_PHONE" granted="true" flags="20"/>
      <item name="android.permission.WRITE_CONTACTS" granted="true" flags="20"/>
      <item name="android.permission.WRITE_CALENDAR" granted="true" flags="20"/>
      <item name="android.permission.GET_ACCOUNTS" granted="true" flags="20"/>
      <item name="android.permission.RECORD_AUDIO" granted="true" flags="20"/>
      <item name="android.permission.READ_CONTACTS" granted="true" flags="20"/>
```

Contacts (\data\com.android.providers.contacts\databases\contacts2.db)



DB Browser for SQLite - G:\OWL\[root]\data\com.android.providers.contacts\databases\contacts2.db

Tabella: data

	_id	package_id	mimetype_id	raw_contact_id	hash_id	is_read_only	is_primary	is_super_primary	data_version	data1	data2	data3	
	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro
1	1	NULL	7	1	NULL	0	0	0	0	Matt Haze28	Matt	Haze28	NULL
2	2	NULL	11	1	NULL	0	0	0	0	6	NULL	NULL	NULL
3	3	NULL	8	1	NULL	1	0	0	0	US	3		NULL
4	4	NULL	12	1	NULL	1	0	0	0	live:generalhaze28	0	IM via Skype	IM wi
5	5	NULL	13	1	NULL	1	0	0	0	live:generalhaze28	0	Call via Skype	Call M
6	6	NULL	14	1	NULL	1	0	0	0	live:generalhaze28	0	Video call via Skype	Video

1 - 5 di 6

Vai a: 1

Modifica cella

Modalità: Testo

1 1

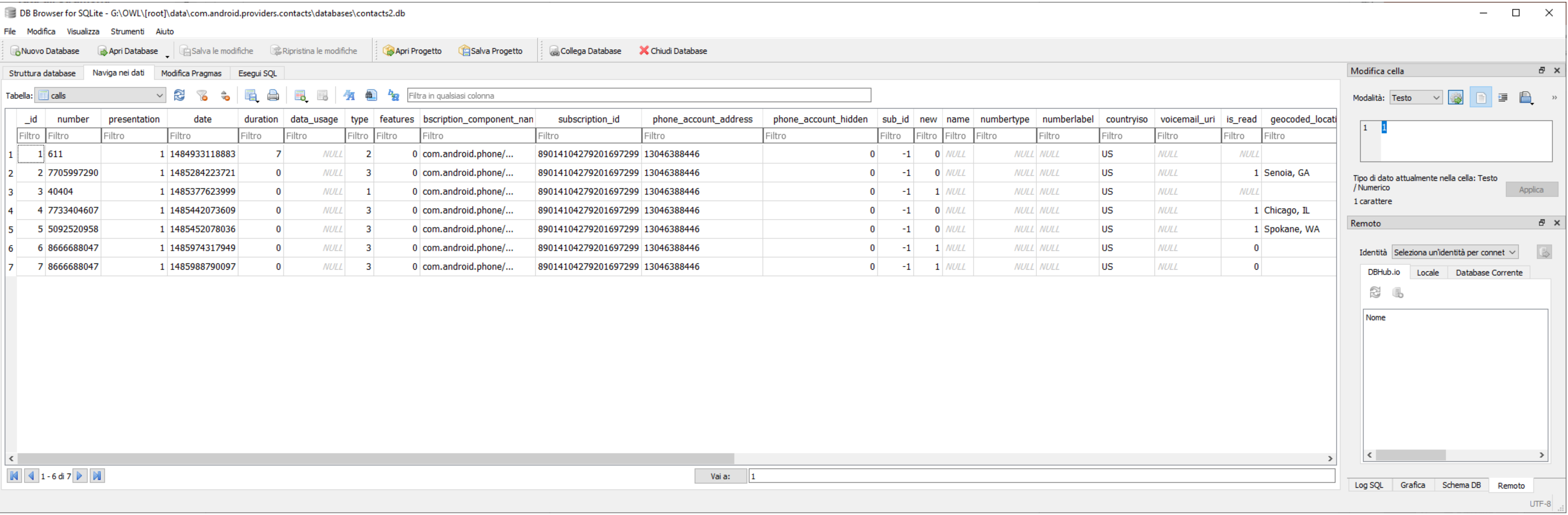
Tipo di dato attualmente nella cella: Testo / Numerico

1 carattere

Remoto

Identità: Seleziona un'identità per connet

Call Log (\data\com.android.providers.contacts\databases\contacts2.db)



DB Browser for SQLite - G:\OWL\[root]\data\com.android.providers.contacts\databases\contacts2.db

Tabella: calls

	_id	number	presentation	date	duration	data_usage	type	features	bscription_component_nan	subscription_id	phone_account_address	phone_account_hidden	sub_id	new	name	numbertype	numberlabel	countryiso	voicemail_uri	is_read	geocoded_locati
	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro
1	1	611	1	1484933118883	7	NULL	2	0	com.android.phone/...	89014104279201697299	13046388446	0	-1	0	NULL	NULL	NULL	US	NULL	NULL	
2	2	7705997290	1	1485284223721	0	NULL	3	0	com.android.phone/...	89014104279201697299	13046388446	0	-1	0	NULL	NULL	NULL	US	NULL	1	Senoia, GA
3	3	40404	1	1485377623999	0	NULL	1	0	com.android.phone/...	89014104279201697299	13046388446	0	-1	1	NULL	NULL	NULL	US	NULL	NULL	
4	4	7733404607	1	1485442073609	0	NULL	3	0	com.android.phone/...	89014104279201697299	13046388446	0	-1	0	NULL	NULL	NULL	US	NULL	1	Chicago, IL
5	5	5092520958	1	1485452078036	0	NULL	3	0	com.android.phone/...	89014104279201697299	13046388446	0	-1	0	NULL	NULL	NULL	US	NULL	1	Spokane, WA
6	6	8666688047	1	1485974317949	0	NULL	3	0	com.android.phone/...	89014104279201697299	13046388446	0	-1	1	NULL	NULL	NULL	US	NULL	0	
7	7	8666688047	1	1485988790097	0	NULL	3	0	com.android.phone/...	89014104279201697299	13046388446	0	-1	1	NULL	NULL	NULL	US	NULL	0	

1 - 6 di 7

Vai a: 1

Modalità: Testo

1 1

Tipo di dato attualmente nella cella: Testo / Numerico

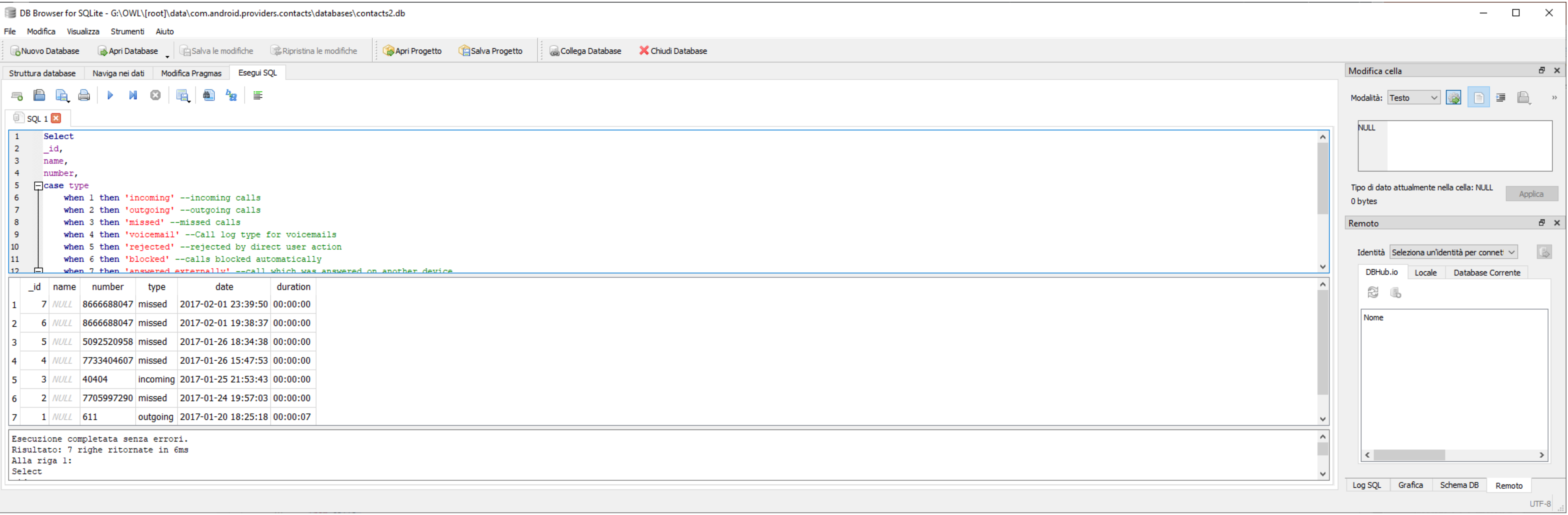
1 carattere

Identità

Call Log Query

```
Select
_id,
name,
number,
case type
        when 1 then 'incoming' --incoming calls
        when 2 then 'outgoing' --outgoing calls
        when 3 then 'missed' --missed calls
        when 4 then 'voicemail' --Call log type for voicemails
        when 5 then 'rejected' --rejected by direct user action
        when 6 then 'blocked' --calls blocked automatically
        when 7 then 'answered externally' --call which was answered on another device
        else type
end as 'type',
datetime(date/1000,'unixepoch','localtime') as 'date',
time(duration,'unixepoch') as 'duration'
from calls
order by _id desc
```

Call Log (\data\com.android.providers.contacts\databases\contacts2.db)

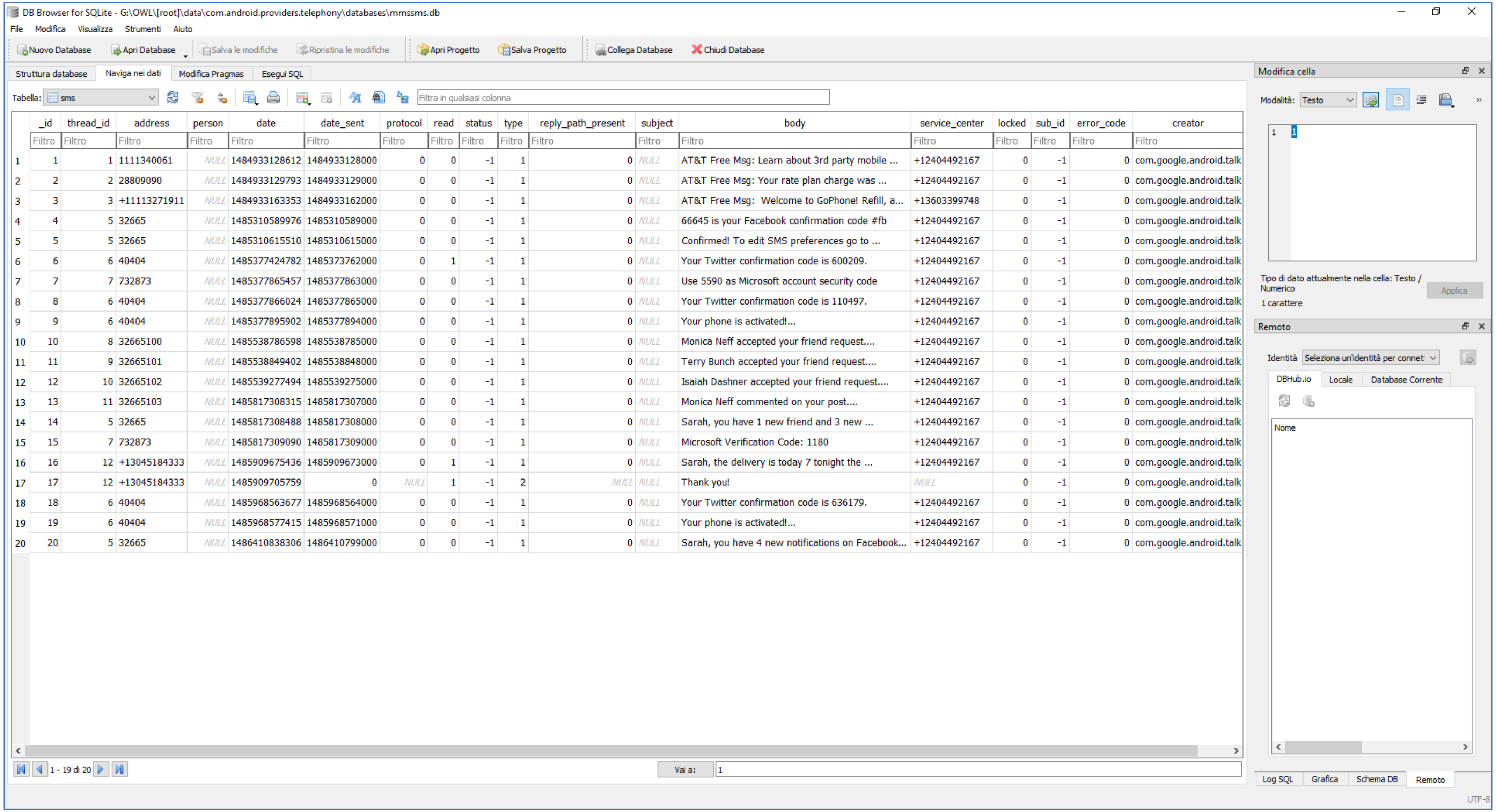


```sql
Select
_id,
name,
number,
case type
    when 1 then 'incoming' --incoming calls
    when 2 then 'outgoing' --outgoing calls
    when 3 then 'missed' --missed calls
    when 4 then 'voicemail' --Call log type for voicemails
    when 5 then 'rejected' --rejected by direct user action
    when 6 then 'blocked' --calls blocked automatically
    when 7 then 'answered externally' --call which was answered on another device
```

	_id	name	number	type	date	duration
1	7	NULL	8666688047	missed	2017-02-01 23:39:50	00:00:00
2	6	NULL	8666688047	missed	2017-02-01 19:38:37	00:00:00
3	5	NULL	5092520958	missed	2017-01-26 18:34:38	00:00:00
4	4	NULL	7733404607	missed	2017-01-26 15:47:53	00:00:00
5	3	NULL	40404	incoming	2017-01-25 21:53:43	00:00:00
6	2	NULL	7705997290	missed	2017-01-24 19:57:03	00:00:00
7	1	NULL	611	outgoing	2017-01-20 18:25:18	00:00:07

```
Esecuzione completata senza errori.
Risultato: 7 righe ritornate in 6ms
Alla riga 1:
Select
```

SMS/MMS (\data\com.android.providers.telephony\databases\mmssms.db)



DB Browser for SQLite - G:\OWL\[root]\data\com.android.providers.telephony\databases\mmssms.db

Tabella: sms

Filtra in qualsiasi colonna

	_id	thread_id	address	person	date	date_sent	protocol	read	status	type	reply_path_present	subject	body	service_center	locked	sub_id	error_code	creator
	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro
1	1	1	1111340061	NULL	1484933128612	1484933128000	0	0	-1	1	0	NULL	AT&T Free Msg: Learn about 3rd party mobile ...	+12404492167	0	-1	0	com.google.android.talk
2	2	2	28809090	NULL	1484933129793	1484933129000	0	0	-1	1	0	NULL	AT&T Free Msg: Your rate plan charge was ...	+12404492167	0	-1	0	com.google.android.talk
3	3	3	+11113271911	NULL	1484933163353	1484933162000	0	0	-1	1	0	NULL	AT&T Free Msg: Welcome to GoPhone! Refill, a...	+13603399748	0	-1	0	com.google.android.talk
4	4	5	32665	NULL	1485310589976	1485310589000	0	0	-1	1	0	NULL	66645 is your Facebook confirmation code #fb	+12404492167	0	-1	0	com.google.android.talk
5	5	5	32665	NULL	1485310615510	1485310615000	0	0	-1	1	0	NULL	Confirmed! To edit SMS preferences go to ...	+12404492167	0	-1	0	com.google.android.talk
6	6	6	40404	NULL	1485377424782	1485373762000	0	1	-1	1	0	NULL	Your Twitter confirmation code is 600209.	+12404492167	0	-1	0	com.google.android.talk
7	7	7	732873	NULL	1485377865457	1485377863000	0	0	-1	1	0	NULL	Use 5590 as Microsoft account security code	+12404492167	0	-1	0	com.google.android.talk
8	8	6	40404	NULL	1485377866024	1485377865000	0	0	-1	1	0	NULL	Your Twitter confirmation code is 110497.	+12404492167	0	-1	0	com.google.android.talk
9	9	6	40404	NULL	1485377895902	1485377894000	0	0	-1	1	0	NULL	Your phone is activated!...	+12404492167	0	-1	0	com.google.android.talk
10	10	8	32665100	NULL	1485538786598	1485538785000	0	0	-1	1	0	NULL	Monica Neff accepted your friend request....	+12404492167	0	-1	0	com.google.android.talk
11	11	9	32665101	NULL	1485538849402	1485538848000	0	0	-1	1	0	NULL	Terry Bunch accepted your friend request....	+12404492167	0	-1	0	com.google.android.talk
12	12	10	32665102	NULL	1485539277494	1485539275000	0	0	-1	1	0	NULL	Isaiah Dashner accepted your friend request....	+12404492167	0	-1	0	com.google.android.talk
13	13	11	32665103	NULL	1485817308315	1485817307000	0	0	-1	1	0	NULL	Monica Neff commented on your post....	+12404492167	0	-1	0	com.google.android.talk
14	14	5	32665	NULL	1485817308488	1485817308000	0	0	-1	1	0	NULL	Sarah, you have 1 new friend and 3 new ...	+12404492167	0	-1	0	com.google.android.talk
15	15	7	732873	NULL	1485817309090	1485817309000	0	0	-1	1	0	NULL	Microsoft Verification Code: 1180	+12404492167	0	-1	0	com.google.android.talk
16	16	12	+13045184333	NULL	1485909675436	1485909673000	0	1	-1	1	0	NULL	Sarah, the delivery is today 7 tonight the ...	+12404492167	0	-1	0	com.google.android.talk
17	17	12	+13045184333	NULL	1485909705759	0	NULL	1	-1	2	NULL	NULL	Thank you!	NULL	0	-1	0	com.google.android.talk
18	18	6	40404	NULL	1485968563677	1485968564000	0	0	-1	1	0	NULL	Your Twitter confirmation code is 636179.	+12404492167	0	-1	0	com.google.android.talk
19	19	6	40404	NULL	1485968577415	1485968571000	0	0	-1	1	0	NULL	Your phone is activated!...	+12404492167	0	-1	0	com.google.android.talk
20	20	5	32665	NULL	1486410838306	1486410799000	0	0	-1	1	0	NULL	Sarah, you have 4 new notifications on Facebook...	+12404492167	0	-1	0	com.google.android.talk

1 - 19 di 20

Vai a: 1

Modalità: Testo

1 1

Tipo di dato attualmente nella cella: Testo / Numerico

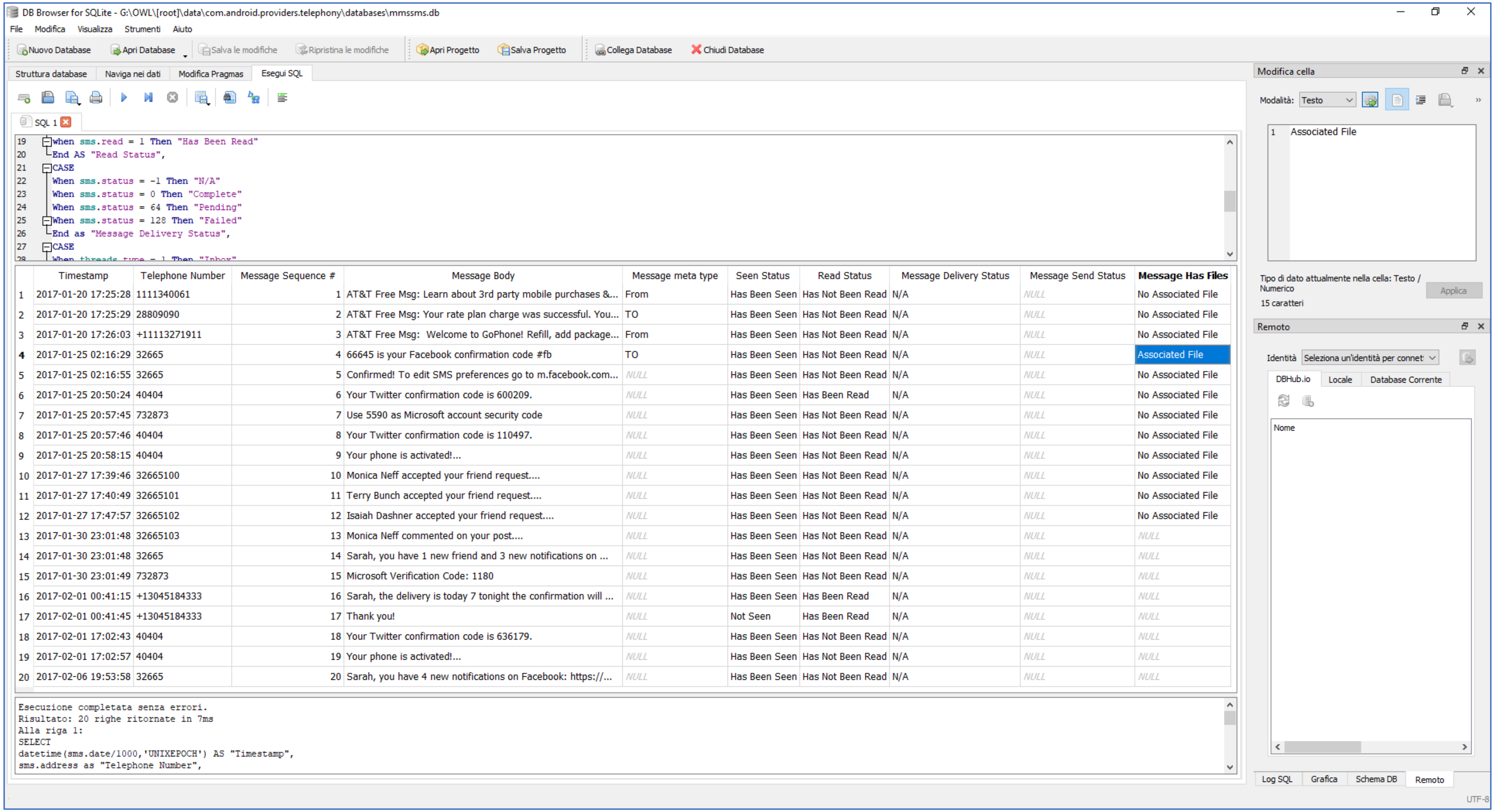
1 carattere

Identità: Seleziona un'identità per connet

SMS/MMS Query

```
SELECT
datetime(sms.date/1000,'UNIXEPOCH') AS "Timestamp",
sms.address as "Telephone Number",
sms._id as "Message Sequence #",
sms.body As "Message Body",
CASE
WHEN addr.type = 151 Then "TO"
WHEN addr.type = 150 Then "Subject"
When addr.type = 137 then "From"
When addr.type = 130 then "CC"
WHEN addr.type = 129 then "BCC"
End as "Message meta type",
CASE
When sms.seen = 0 Then "Not Seen"
When sms.seen = 1 Then "Has Been Seen"
End as "Seen Status ",
CASE
When sms.read = 0 Then "Has Not Been Read"
when sms.read = 1 Then "Has Been Read"
End AS "Read Status",
CASE
When sms.status = -1 Then "N/A"
When sms.status = 0 Then "Complete"
When sms.status = 64 Then "Pending"
When sms.status = 128 Then "Failed"
End as "Message Delivery Status",
CASE
When threads.type = 1 Then "Inbox"
When threads.type = 2 then "Sent"
When threads.type = 3 Then "Draft"
When threads.type = 4 then "Outbox"
When threads.type = 5 then "Failed"
When threads.type = 6 then "Queued"
End As "Message Send Status",
CASE
When threads.has_attachment = 0 Then "No Associated File"
When threads.has_attachment = 1 Then "Associated File"
End as "Message Has Files"
FROM sms
left join threads on threads._id = sms._id
left join addr on addr._id = sms._id
order by sms.date
```

SMS/MMS (\data\com.android.providers.telephony\databases\mmssms.db)



```
when sms.read = 1 Then "Has Been Read"
End AS "Read Status",
CASE
When sms.status = -1 Then "N/A"
When sms.status = 0 Then "Complete"
When sms.status = 64 Then "Pending"
When sms.status = 128 Then "Failed"
End as "Message Delivery Status",
CASE
When threads.type = 1 Then "Inbox"
```

	Timestamp	Telephone Number	Message Sequence #	Message Body	Message meta type	Seen Status	Read Status	Message Delivery Status	Message Send Status	Message Has Files
1	2017-01-20 17:25:28	1111340061	1	AT&T Free Msg: Learn about 3rd party mobile purchases &...	From	Has Been Seen	Has Not Been Read	N/A	NULL	No Associated File
2	2017-01-20 17:25:29	28809090	2	AT&T Free Msg: Your rate plan charge was successful. You...	TO	Has Been Seen	Has Not Been Read	N/A	NULL	No Associated File
3	2017-01-20 17:26:03	+11113271911	3	AT&T Free Msg: Welcome to GoPhone! Refill, add package...	From	Has Been Seen	Has Not Been Read	N/A	NULL	No Associated File
4	2017-01-25 02:16:29	32665	4	66645 is your Facebook confirmation code #fb	TO	Has Been Seen	Has Not Been Read	N/A	NULL	Associated File
5	2017-01-25 02:16:55	32665	5	Confirmed! To edit SMS preferences go to m.facebook.com...	NULL	Has Been Seen	Has Not Been Read	N/A	NULL	No Associated File
6	2017-01-25 20:50:24	40404	6	Your Twitter confirmation code is 600209.	NULL	Has Been Seen	Has Been Read	N/A	NULL	No Associated File
7	2017-01-25 20:57:45	732873	7	Use 5590 as Microsoft account security code	NULL	Has Been Seen	Has Not Been Read	N/A	NULL	No Associated File
8	2017-01-25 20:57:46	40404	8	Your Twitter confirmation code is 110497.	NULL	Has Been Seen	Has Not Been Read	N/A	NULL	No Associated File
9	2017-01-25 20:58:15	40404	9	Your phone is activated!...	NULL	Has Been Seen	Has Not Been Read	N/A	NULL	No Associated File
10	2017-01-27 17:39:46	32665100	10	Monica Neff accepted your friend request....	NULL	Has Been Seen	Has Not Been Read	N/A	NULL	No Associated File
11	2017-01-27 17:40:49	32665101	11	Terry Bunch accepted your friend request....	NULL	Has Been Seen	Has Not Been Read	N/A	NULL	No Associated File
12	2017-01-27 17:47:57	32665102	12	Isaiah Dashner accepted your friend request....	NULL	Has Been Seen	Has Not Been Read	N/A	NULL	No Associated File
13	2017-01-30 23:01:48	32665103	13	Monica Neff commented on your post....	NULL	Has Been Seen	Has Not Been Read	N/A	NULL	NULL
14	2017-01-30 23:01:48	32665	14	Sarah, you have 1 new friend and 3 new notifications on ...	NULL	Has Been Seen	Has Not Been Read	N/A	NULL	NULL
15	2017-01-30 23:01:49	732873	15	Microsoft Verification Code: 1180	NULL	Has Been Seen	Has Not Been Read	N/A	NULL	NULL
16	2017-02-01 00:41:15	+13045184333	16	Sarah, the delivery is today 7 tonight the confirmation will ...	NULL	Has Been Seen	Has Been Read	N/A	NULL	NULL
17	2017-02-01 00:41:45	+13045184333	17	Thank you!	NULL	Not Seen	Has Been Read	N/A	NULL	NULL
18	2017-02-01 17:02:43	40404	18	Your Twitter confirmation code is 636179.	NULL	Has Been Seen	Has Not Been Read	N/A	NULL	NULL
19	2017-02-01 17:02:57	40404	19	Your phone is activated!...	NULL	Has Been Seen	Has Not Been Read	N/A	NULL	NULL
20	2017-02-06 19:53:58	32665	20	Sarah, you have 4 new notifications on Facebook: https://...	NULL	Has Been Seen	Has Not Been Read	N/A	NULL	NULL

```
Esecuzione completata senza errori.
Risultato: 20 righe ritornate in 7ms
Alla riga 1:
SELECT
datetime(sms.date/1000,'UNIXEPOCH') AS "Timestamp",
sms.address as "Telephone Number",
```

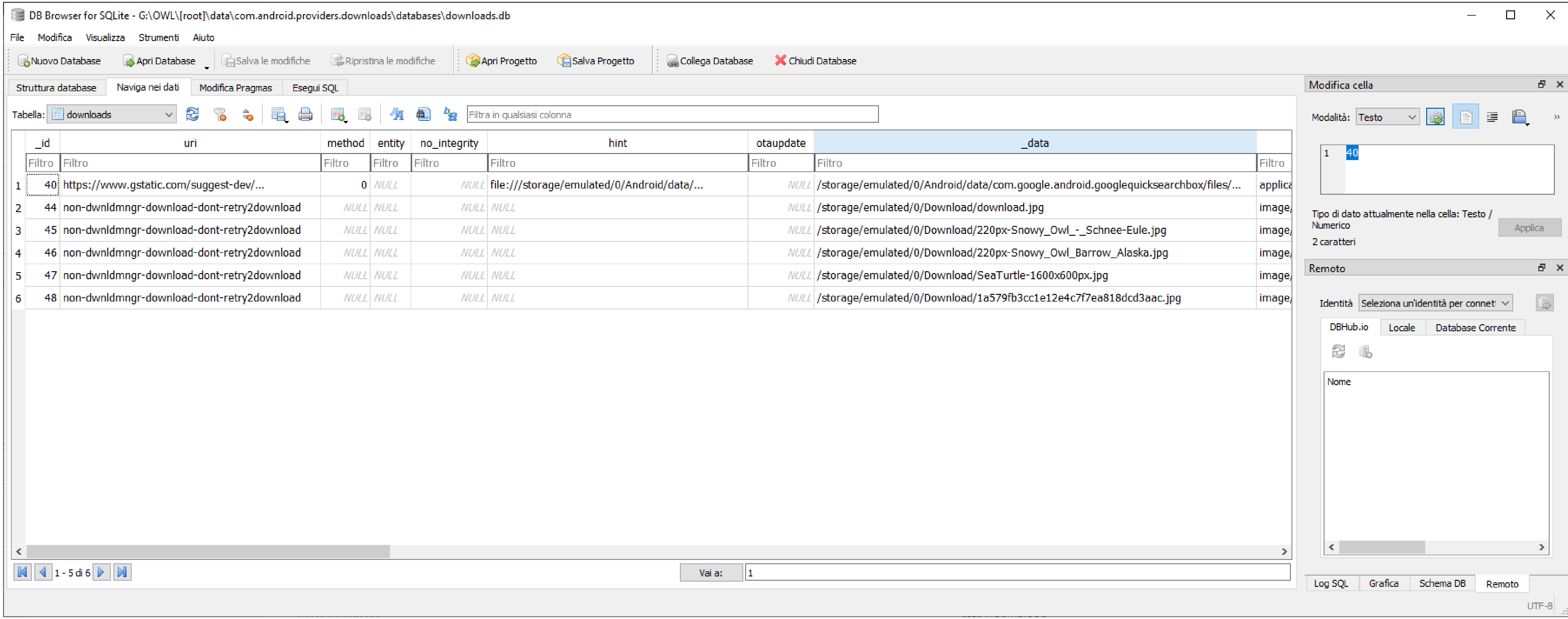
Modalità: Testo

1 Associated File

Tipo di dato attualmente nella cella: Testo / Numerico
15 caratteri

Identità Seleziona un'identità per connet

Downloads (\data\com.android.providers.downloads\databases\downloads.db)



DB Browser for SQLite - G:\OWL\[root]\data\com.android.providers.downloads\databases\downloads.db

Tabella: downloads

	_id	uri	method	entity	no_integrity	hint	otaupdate	_data	
	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro
1	40	https://www.gstatic.com/suggest-dev/...	0	NULL	NULL	file:///storage/emulated/0/Android/data/...	NULL	/storage/emulated/0/Android/data/com.google.android.googlequicksearchbox/files/...	applica
2	44	non-dwnldmngr-download-dont-retry2download	NULL	NULL	NULL	NULL	NULL	/storage/emulated/0/Download/download.jpg	image/
3	45	non-dwnldmngr-download-dont-retry2download	NULL	NULL	NULL	NULL	NULL	/storage/emulated/0/Download/220px-Snowy_Owl_-_Schnee-Eule.jpg	image/
4	46	non-dwnldmngr-download-dont-retry2download	NULL	NULL	NULL	NULL	NULL	/storage/emulated/0/Download/220px-Snowy_Owl_Barrow_Alaska.jpg	image/
5	47	non-dwnldmngr-download-dont-retry2download	NULL	NULL	NULL	NULL	NULL	/storage/emulated/0/Download/SeaTurtle-1600x600px.jpg	image/
6	48	non-dwnldmngr-download-dont-retry2download	NULL	NULL	NULL	NULL	NULL	/storage/emulated/0/Download/1a579fb3cc1e12e4c7f7ea818dcd3aac.jpg	image/

1 - 5 di 6

Vai a: 1

Modalità: Testo

1 40

Tipo di dato attualmente nella cella: Testo / Numerico

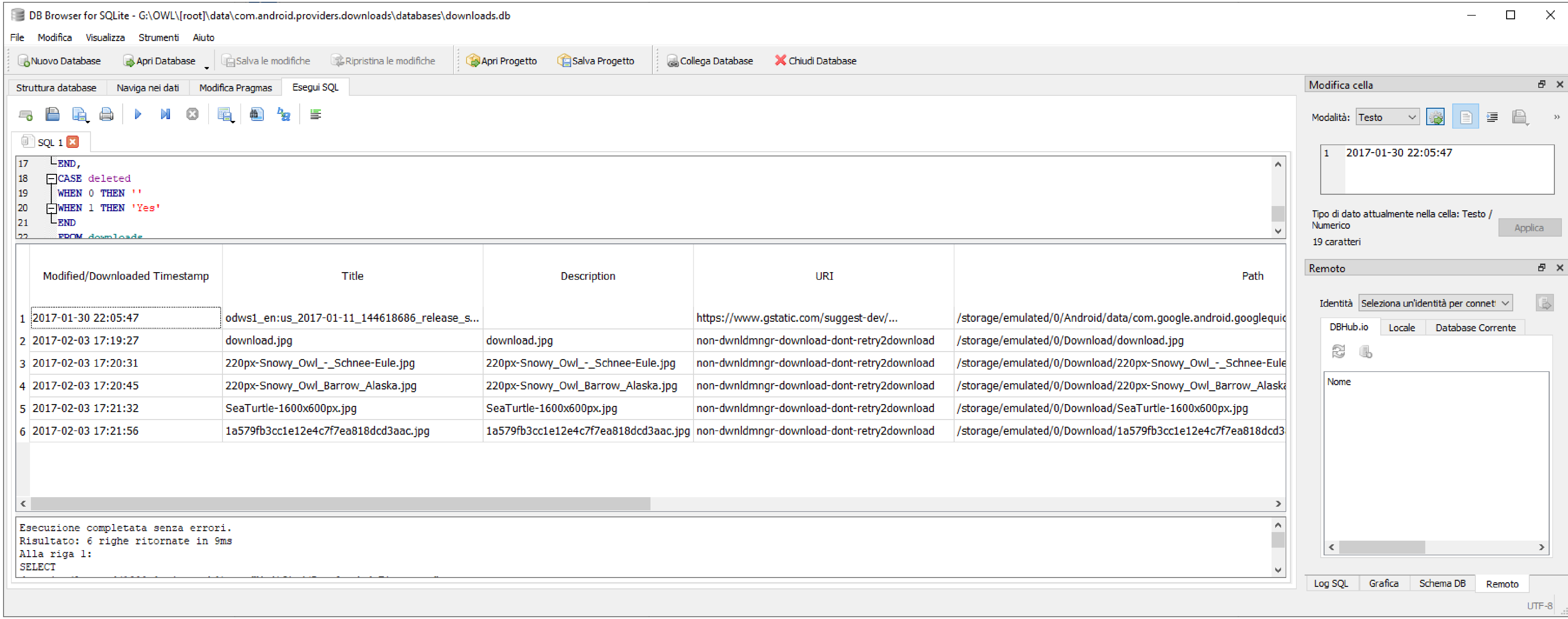
2 caratteri

Identità Seleziona un'identità per connet

Downloads Query

```
SELECT
datetime(lastmod/1000,'unixepoch') as "Modified/Downloaded Timestamp",
title AS "Title",
description AS "Description",
uri AS "URI",
_data AS "Path",
mimetype AS "MIME Type",
notificationpackage AS "Notification Package",
current_bytes AS "Downloaded Bytes",
total_bytes AS "Total bytes",
status AS "Status",
errorMsg AS "Error Message",
etag,
CASE is_visible_in_downloads_ui
WHEN 0 THEN 'No'
WHEN 1 THEN 'Yes'
END,
CASE deleted
WHEN 0 THEN ''
WHEN 1 THEN 'Yes'
END
FROM downloads
```

Downloads (\data\com.android.providers.downloads\databases\downloads.db)



```
  END,
CASE deleted
WHEN 0 THEN ''
WHEN 1 THEN 'Yes'
END
FROM downloads
```

	Modified/Downloaded Timestamp	Title	Description	URI	Path
1	2017-01-30 22:05:47	odws1_en:us_2017-01-11_144618686_release_s...		https://www.gstatic.com/suggest-dev/...	/storage/emulated/0/Android/data/com.google.android.googlequic
2	2017-02-03 17:19:27	download.jpg	download.jpg	non-dwnldmngr-download-dont-retry2download	/storage/emulated/0/Download/download.jpg
3	2017-02-03 17:20:31	220px-Snowy_Owl_-_Schnee-Eule.jpg	220px-Snowy_Owl_-_Schnee-Eule.jpg	non-dwnldmngr-download-dont-retry2download	/storage/emulated/0/Download/220px-Snowy_Owl_-_Schnee-Eule
4	2017-02-03 17:20:45	220px-Snowy_Owl_Barrow_Alaska.jpg	220px-Snowy_Owl_Barrow_Alaska.jpg	non-dwnldmngr-download-dont-retry2download	/storage/emulated/0/Download/220px-Snowy_Owl_Barrow_Alaska
5	2017-02-03 17:21:32	SeaTurtle-1600x600px.jpg	SeaTurtle-1600x600px.jpg	non-dwnldmngr-download-dont-retry2download	/storage/emulated/0/Download/SeaTurtle-1600x600px.jpg
6	2017-02-03 17:21:56	1a579fb3cc1e12e4c7f7ea818dcd3aac.jpg	1a579fb3cc1e12e4c7f7ea818dcd3aac.jpg	non-dwnldmngr-download-dont-retry2download	/storage/emulated/0/Download/1a579fb3cc1e12e4c7f7ea818dcd3

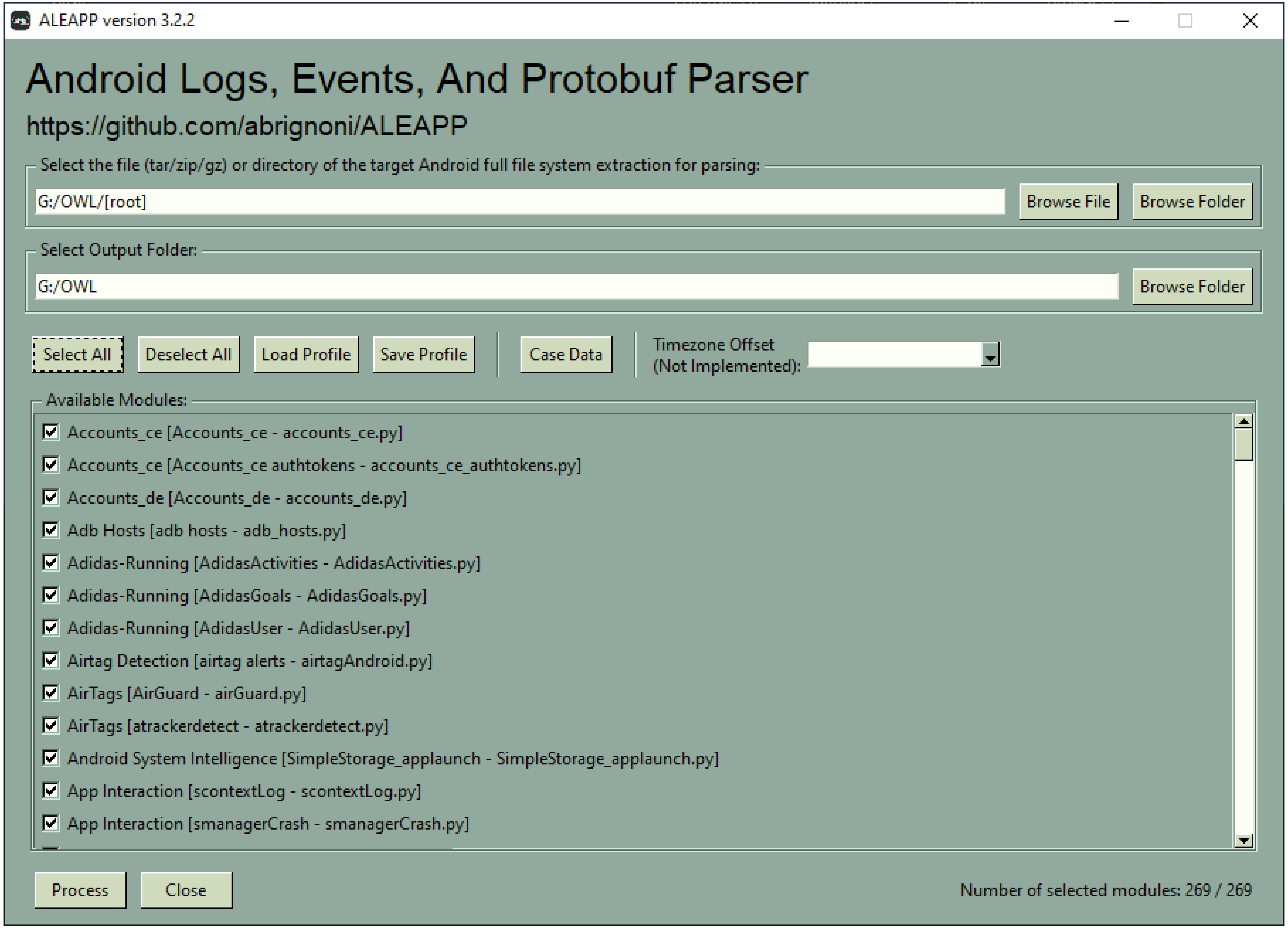
```
Esecuzione completata senza errori.
Risultato: 6 righe ritornate in 9ms
Alla riga 1:
SELECT
```

Modifica cella:

```
1  2017-01-30 22:05:47
```

Tipo di dato attualmente nella cella: Testo / Numerico
19 caratteri

aLEAPP



Android Logs, Events, And Protobuf Parser

https://github.com/abrignoni/ALEAPP

Select the file (tar/zip/gz) or directory of the target Android full file system extraction for parsing:

G:/OWL/[root]

Select Output Folder:

G:/OWL

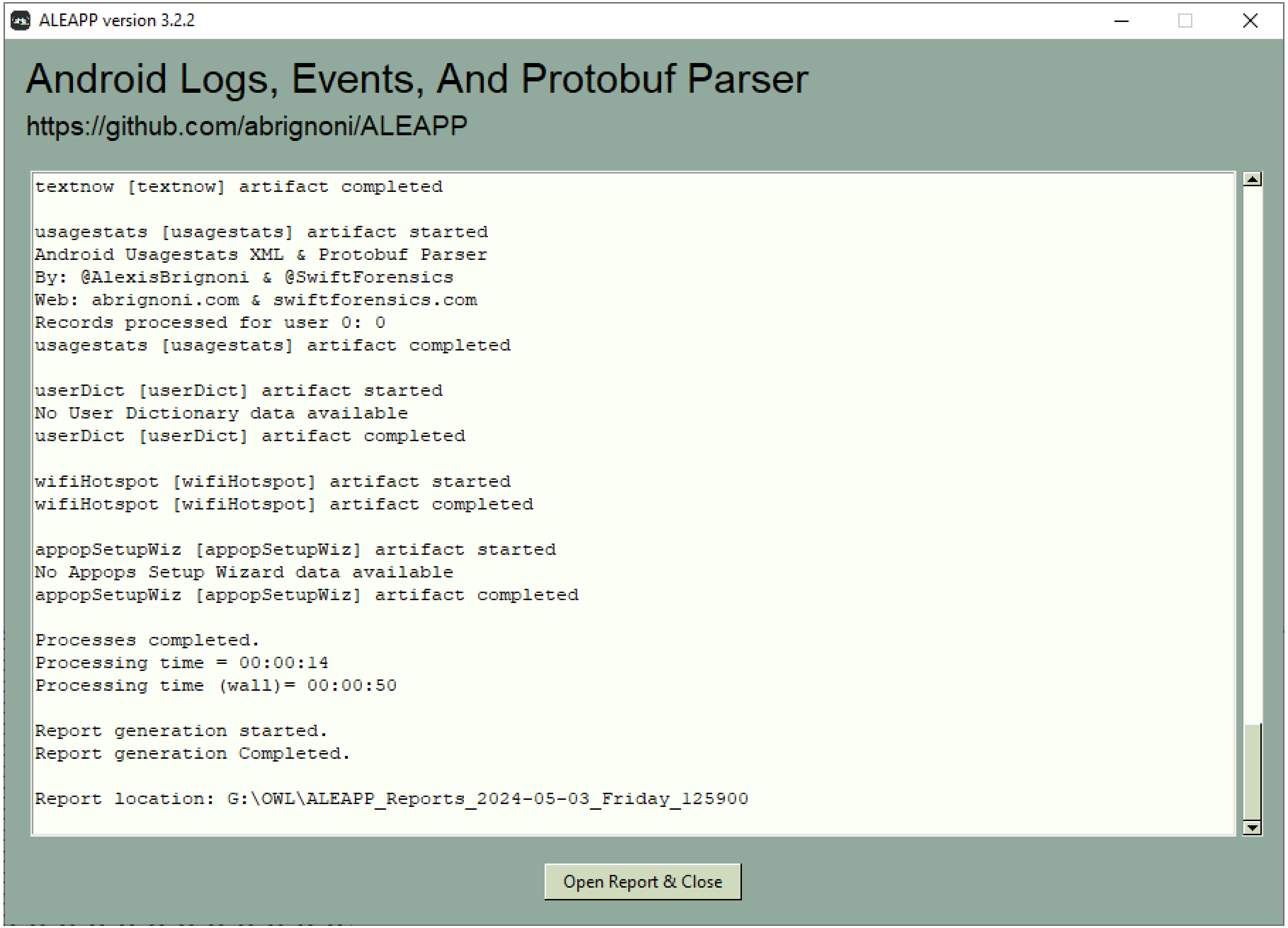
Timezone Offset (Not Implemented):

Available Modules:

- ☑ Accounts_ce [Accounts_ce - accounts_ce.py]
- ☑ Accounts_ce [Accounts_ce authtokens - accounts_ce_authtokens.py]
- ☑ Accounts_de [Accounts_de - accounts_de.py]
- ☑ Adb Hosts [adb hosts - adb_hosts.py]
- ☑ Adidas-Running [AdidasActivities - AdidasActivities.py]
- ☑ Adidas-Running [AdidasGoals - AdidasGoals.py]
- ☑ Adidas-Running [AdidasUser - AdidasUser.py]
- ☑ Airtag Detection [airtag alerts - airtagAndroid.py]
- ☑ AirTags [AirGuard - airGuard.py]
- ☑ AirTags [atrackerdetect - atrackerdetect.py]
- ☑ Android System Intelligence [SimpleStorage_applaunch - SimpleStorage_applaunch.py]
- ☑ App Interaction [scontextLog - scontextLog.py]
- ☑ App Interaction [smanagerCrash - smanagerCrash.py]

Number of selected modules: 269 / 269

aLEAPP

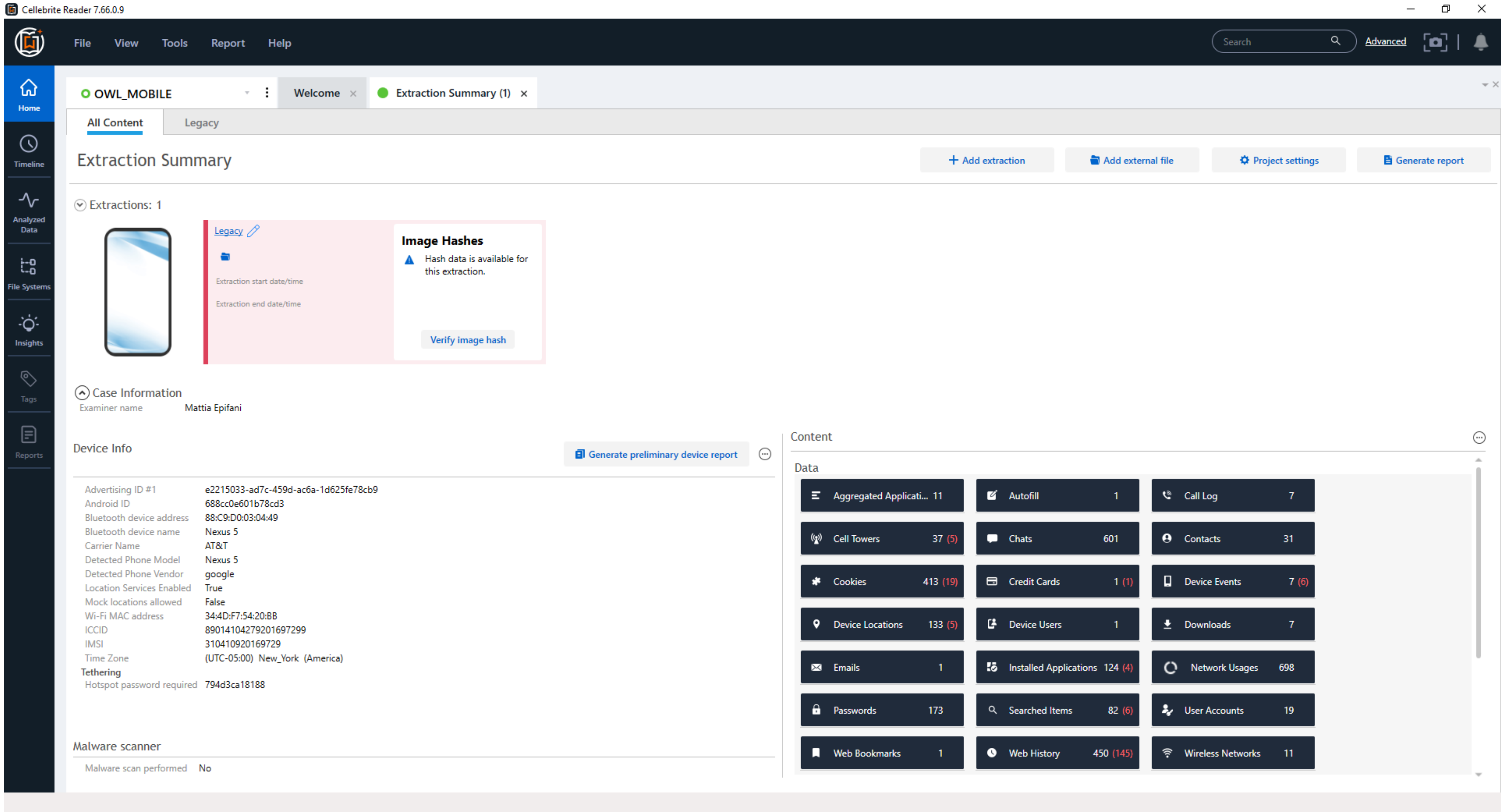


Android Logs, Events, And Protobuf Parser

https://github.com/abrignoni/ALEAPP

```
textnow [textnow] artifact completed

usagestats [usagestats] artifact started
Android Usagestats XML & Protobuf Parser
By: @AlexisBrignoni & @SwiftForensics
Web: abrignoni.com & swiftforensics.com
Records processed for user 0: 0
usagestats [usagestats] artifact completed

userDict [userDict] artifact started
No User Dictionary data available
userDict [userDict] artifact completed

wifiHotspot [wifiHotspot] artifact started
wifiHotspot [wifiHotspot] artifact completed

appopSetupWiz [appopSetupWiz] artifact started
No Appops Setup Wizard data available
appopSetupWiz [appopSetupWiz] artifact completed

Processes completed.
Processing time = 00:00:14
Processing time (wall)= 00:00:50

Report generation started.
Report generation Completed.

Report location: G:\OWL\ALEAPP_Reports_2024-05-03_Friday_125900
```

Cellebrite Reader



Extraction Summary

Extractions: 1

Legacy

Extraction start date/time

Extraction end date/time

Image Hashes

Hash data is available for this extraction.

Case Information

Examiner name Mattia Epifani

Device Info

Advertising ID #1	e2215033-ad7c-459d-ac6a-1d625fe78cb9
Android ID	688cc0e601b78cd3
Bluetooth device address	88:C9:D0:03:04:49
Bluetooth device name	Nexus 5
Carrier Name	AT&T
Detected Phone Model	Nexus 5
Detected Phone Vendor	google
Location Services Enabled	True
Mock locations allowed	False
Wi-Fi MAC address	34:4D:F7:54:20:BB
ICCID	89014104279201697299
IMSI	310410920169729
Time Zone	(UTC-05:00) New_York (America)
Tethering	
Hotspot password required	794d3ca18188

Malware scanner

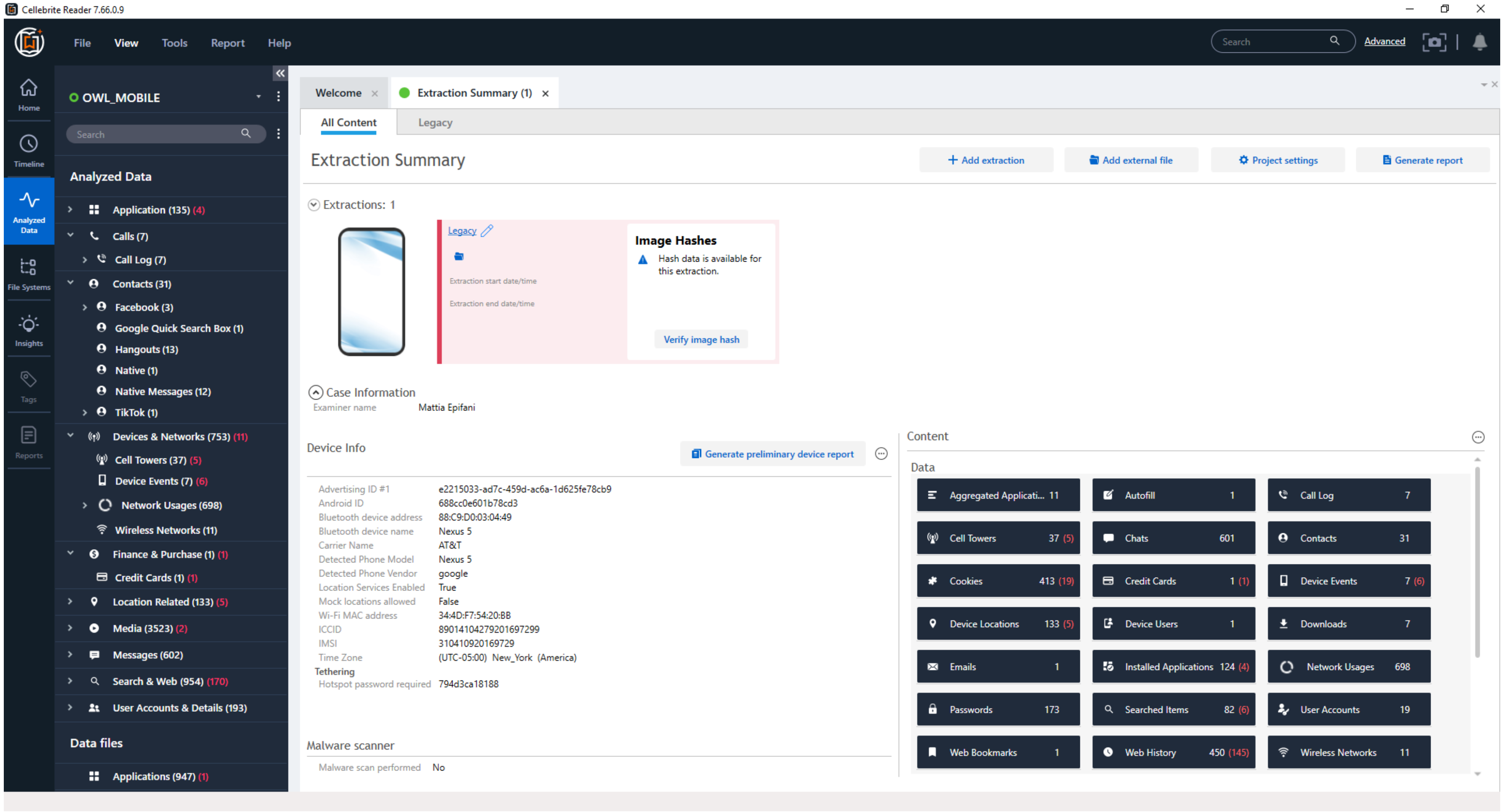
Malware scan performed No

Content

Data

Aggregated Applicati...	11
Autofill	1
Call Log	7
Cell Towers	37 (5)
Chats	601
Contacts	31
Cookies	413 (19)
Credit Cards	1 (1)
Device Events	7 (6)
Device Locations	133 (5)
Device Users	1
Downloads	7
Emails	1
Installed Applications	124 (4)
Network Usages	698
Passwords	173
Searched Items	82 (6)
User Accounts	19
Web Bookmarks	1
Web History	450 (145)
Wireless Networks	11

Cellebrite Reader



OWL_MOBILE

Search

Analyzed Data

- Application (135) (4)
- Calls (7)
  - Call Log (7)
- Contacts (31)
  - Facebook (3)
  - Google Quick Search Box (1)
  - Hangouts (13)
  - Native (1)
  - Native Messages (12)
  - TikTok (1)
- Devices & Networks (753) (11)
  - Cell Towers (37) (5)
  - Device Events (7) (6)
  - Network Usages (698)
  - Wireless Networks (11)
- Finance & Purchase (1) (1)
  - Credit Cards (1) (1)
- Location Related (133) (5)
- Media (3523) (2)
- Messages (602)
- Search & Web (954) (170)
- User Accounts & Details (193)

Data files

- Applications (947) (1)

Extraction Summary

Extractions: 1

Legacy

Extraction start date/time

Extraction end date/time

Image Hashes

Hash data is available for this extraction.

Verify image hash

Case Information

Examiner name	Mattia Epifani

Device Info

Generate preliminary device report

Advertising ID #1	e2215033-ad7c-459d-ac6a-1d625fe78cb9
Android ID	688cc0e601b78cd3
Bluetooth device address	88:C9:D0:03:04:49
Bluetooth device name	Nexus 5
Carrier Name	AT&T
Detected Phone Model	Nexus 5
Detected Phone Vendor	google
Location Services Enabled	True
Mock locations allowed	False
Wi-Fi MAC address	34:4D:F7:54:20:BB
ICCID	89014104279201697299
IMSI	310410920169729
Time Zone	(UTC-05:00) New_York (America)
Tethering	
Hotspot password required	794d3ca18188

Malware scanner

Malware scan performed	No

Content

Data

Aggregated Applicati... 11	Autofill 1	Call Log 7
Cell Towers 37 (5)	Chats 601	Contacts 31
Cookies 413 (19)	Credit Cards 1 (1)	Device Events 7 (6)
Device Locations 133 (5)	Device Users 1	Downloads 7
Emails 1	Installed Applications 124 (4)	Network Usages 698
Passwords 173	Searched Items 82 (6)	User Accounts 19
Web Bookmarks 1	Web History 450 (145)	Wireless Networks 11

Exercise 1

1. What is the SSID and BSSID of the Wi-Fi Network that the device was connected to on 24th January 2017 at 14:28:15 UTC?

2. Which keywords were searched on the Google Play Store?

3. When did the user searched for «snowy owl» on Google Chrome?

4. What is the Twitter Username of the owner of the device?