Extending Physical Analyzer using Python and .NET

Dex-EU online

November 9, 2021

Sieger Veenhoven

github.com/sieger82

linkedin.com/in/sieger-v

Agenda

- Why extending Physical Analyzer
- Working environment
- SQLite databases
  - Recovery of deleted items
- JSON
- Plists
  - Embedded Plists
- Protobuf
- .NET

Why extending Physical Analyzer

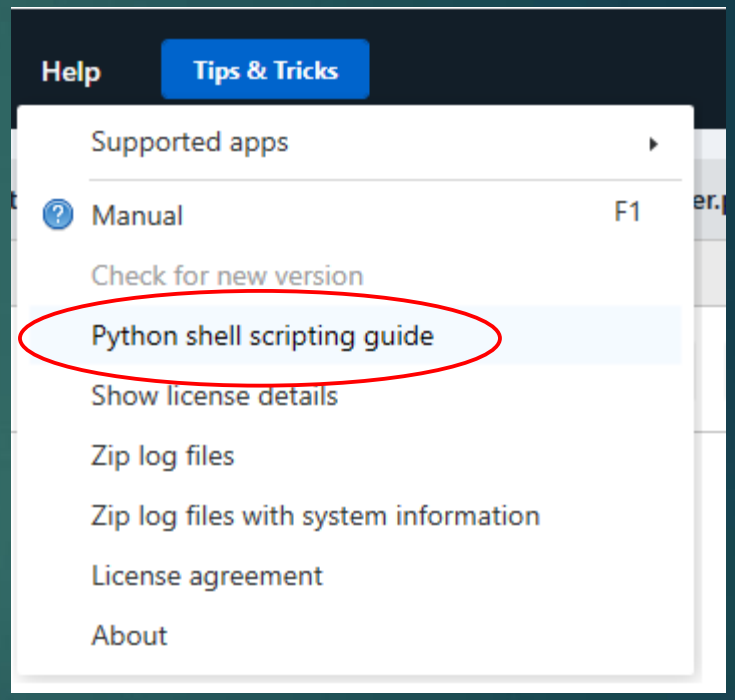
- No Forensic tool can parse <u>everything</u>
- Presenting evidence in familiar environment
- Easy workflow:
  - Extract
  - Parse
  - Run custom scripts

Working environment

- IronPython 2.6 with customizations by Cellebrite
  - Old
  - Some standard libs missing
  - No `pip install`, no wheel, no setup.py
  - Modules on the Internet (e.g. pypi.org)
    - Usually no 2.6 version available
    - Dependencies which are missing in IronPython 2.6
    - A lot of module only work in Cpython (and not IronPython)
  - On the upside:
    - IronPython is .NET based
    - Possibility to use custom .NET DLLs using latest .NET framework

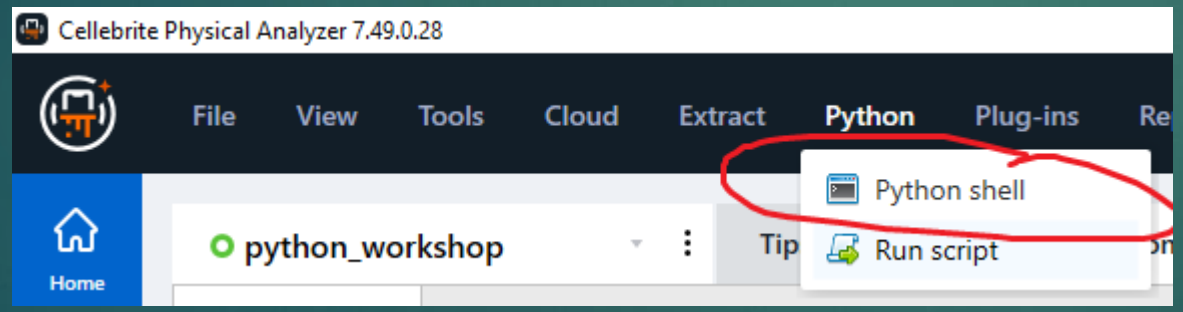
Documentation

- In Physical Analyzer -> Help -> Python shell Scripting Guide
  - Not fully up-to-date !
- Contains information about:
  - SQLite Parser (incl. deleted items)
  - Description of (most) available Content Models
  - 2 example scripts in: `C:\Program Files\Cellebrite Mobile Synchronization\UFED Physical Analyzer\PythonSamples`



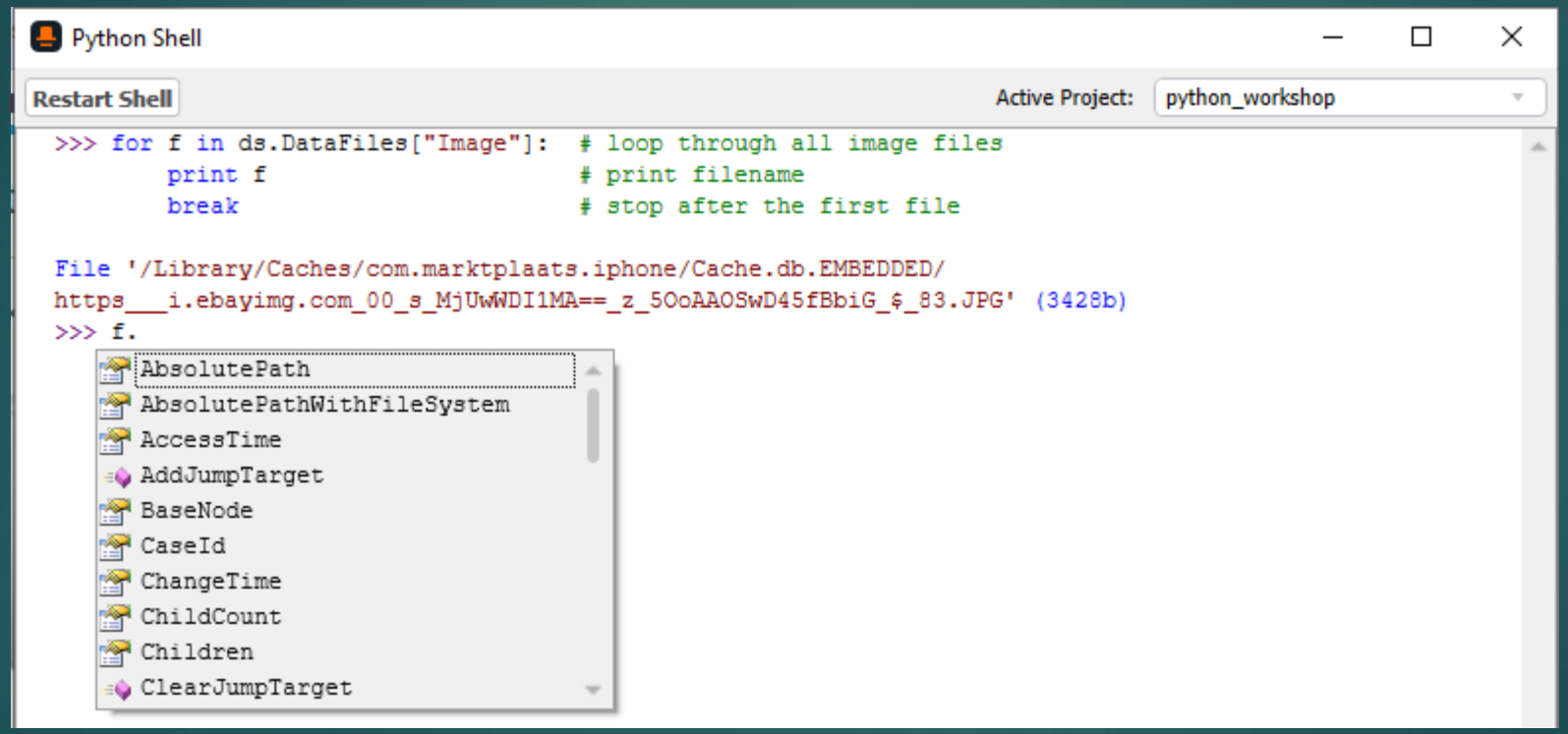
Interactive Python Shell

- Interactive
  - Very useful to test or debug short pieces of code
- Code completion
  - Allows you to find out 'undocumented' functions, methods and properties.

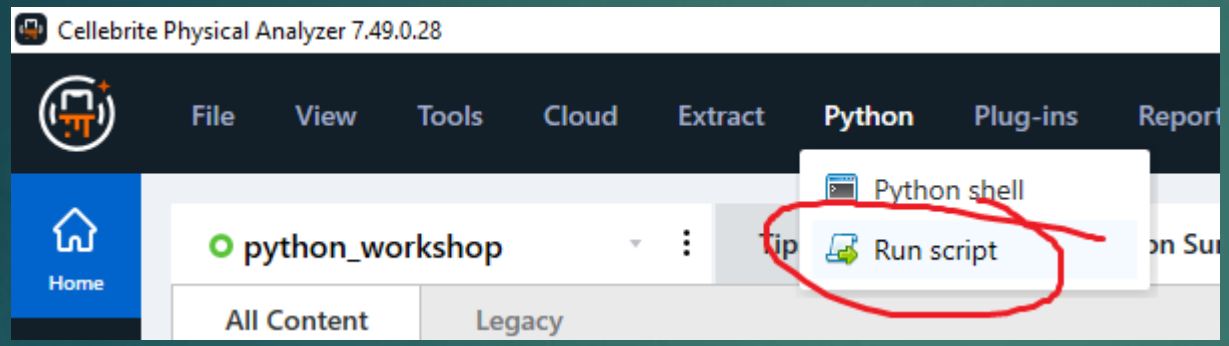


Interactive Python Shell

- Using code completion to find properties of an object:



How to run script files



- Always start your script with:
  - `from physical import *`

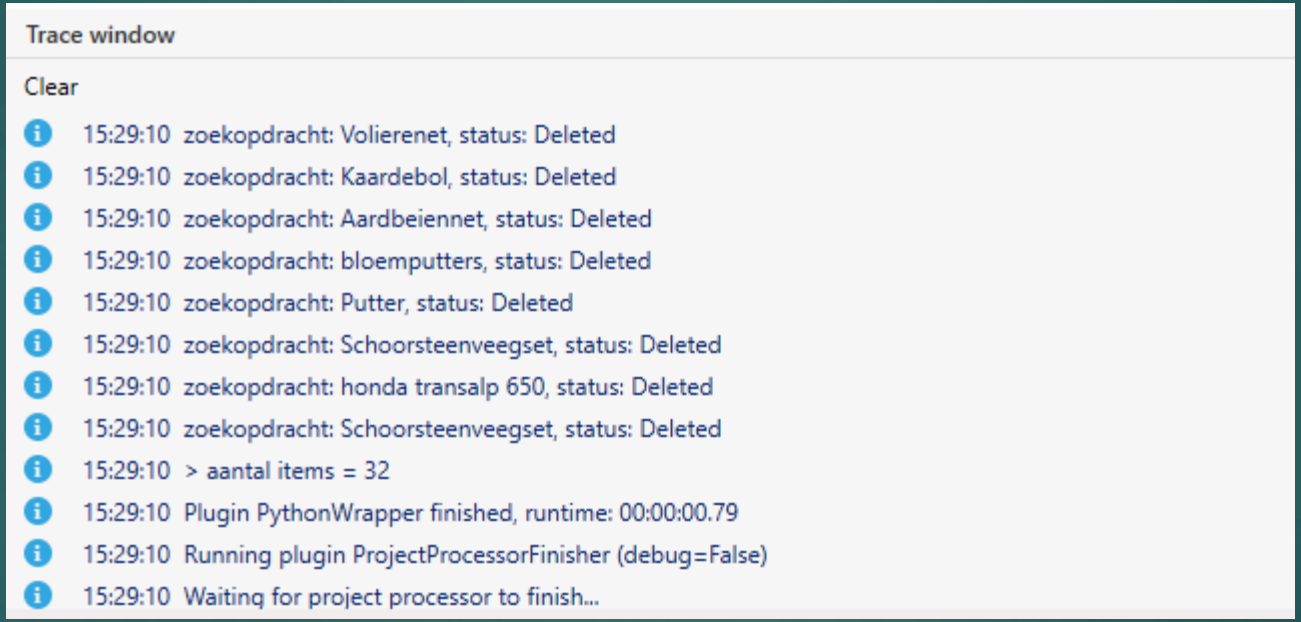
Use Trace window: to spot errors and exceptions

Trace window

Clear

15:27:38 Adding project processor...
15:27:38 Plugin PreProject finished, runtime: 00:00:00.35
15:27:38 Running plugin PythonWrapper (debug=False)
15:27:39 Traceback (most recent call last): File "C:\Users\232466\Documents\git-repos\physical-analyzer-python-.net\uitwerking_1.py", line 4, in C:\Users\23
15:27:39 Failed to execute: PythonWrapper
15:27:39 No module named myCustomModule
15:27:39 Plugin PythonWrapper finished, runtime: 00:00:00.16
15:27:39 Running plugin ProjectProcessorFinisher (debug=False)
15:27:39 Waiting for project processor to finish...
15:27:39 PP: Starting last stage for project: 45899441-e884-4604-b1ba-4664e7ab95c2 (0 items)
15:27:39 Finishing extraction info...
15:27:39 PP: Last stage completed: 00:00:00.03, ProjectId: 45899441-e884-4604-b1ba-4664e7ab95c2, CaseId: a9cc99c9-6e4c-4baf-80e1-130f7ee9decd

Use Trace window: for printing information from script



Loading Python modules

- Modules stored in same directory as script file

```
import os, sys
parent = os.path.dirname(__file__)  # detect the path of current script
sys.path.append(parent)             # append that to python search path
import yourmodule                   # import whatever your module is named
```

- In the interactive shell
  - Don't use '`from physical import *`'!
  - Use absolute paths to load modules

```
import sys
sys.path.append(<absolute path to library>)     # append that to python search path
import yourmodule                               # import whatever your module is named
```

Available standard libs

- simplejson (JSON parser)
- zlib (for gzipped data)
- sctruct, io, binascii, StringIO, codecs (for working with binary data)
- base64
- re (regular expressions)
- hashlib (some standard hash functions)
- time, datetime

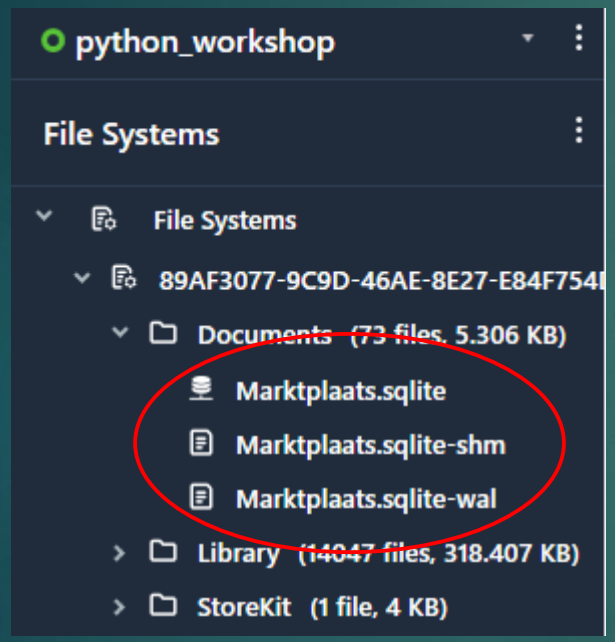
Boilerplate script

- https://github.com/sieger82/physical-analyzer-python-dotnet
- Includes:
  - ccl_bplist -> for parsing of binary .plist files (iOS)
  - pbparser -> for parsing of protobuf data
  - SQLiteParser -> default Cellebrite SQLite parser
  - … add any module from previous slide yourself
- Also in this repo all examples from this presentation

Finding and opening files

- ds
  - Stands for ‘DataStore’
  - Contains all data of active UFED extraction
- ds.FileSystems
  - Contains all parsed Filesystems in current active extraction (can be more than 1!)
- Searching for files uses Regular Expressions

Finding and opening a database




```
>>> for fs in ds.FileSystems:
        for file in fs.Search("Marktplaats.sqlite$"):          # Note the regular expression
                db = SQLiteParser.Database.FromNode(file)
                if db != None:
                        print("> db %s found" % file.Name)
                        print("> using %s WAL node" % db.DBWalNode.Name)
                        db.Tables
                                                               # Note that the corresponding
                                                               # .wal file is detected
> db Marktplaats.sqlite found                                  # and used
> using Marktplaats.sqlite-wal WAL node
Array[str](('ZACTIVESYIAD', 'ZALERT', 'ZALERT_ZCONFIG_INDEX', 'ZCARSEARCHPARAM',
'ZCARSEARCHPARAM_ZRECENTSEARCH_INDEX', 'ZFAVORITE', 'ZFEATURETYPE', 'ZFEATURETYPE_ZAD_INDEX',
'ZMPASYSCONFIGFEATURESWITCH', 'ZMPASYSCONFIGFEATURESWITCH_ZCONFIG_INDEX', 'ZMPAUPCALLCONFIG',
'ZMPAUPCALLCONFIG_ZCONFIG_INDEX', 'ZMYBID', 'Z_METADATA', 'Z_MODELCACHE', 'ZFEATURESWITCH',
'ZLABSCONFIG', 'ZEXPERIMENTGROUPS', 'ZGROUPVALUE', 'ZABSWITCH', 'ZSAVEDPICTURE', 'ZSYSCONFIG',
'ZSHIPPINGPOSTMODEL', 'ZSWIPECONFIG', 'ZGROUPVALUE_ZGROUP_INDEX', 'ZSAVEDPICTURE_ZSYIAD_INDEX',
'ZSWIPECONFIG_ZCONFIG_INDEX', 'ZSYSCONFIG_ZSWIPECONFIG_INDEX', 'ZSYSCONFIG_ZUPCALLCONFIGS_INDEX',
'ZRECENTLYVIEWEDAD', 'ZSELECTEDSYIATTRIBUTEVALUE', 'ZCATEGORY', 'ZCATEGORY_ZCATEGORYID_INDEX',
'ZCATEGORY_ZPARENTCATEGORY_INDEX', 'ZSELECTEDSYIATTRIBUTEVALUE_ZDRAFTAD_INDEX', 'ZRECENTSEARCH',
'ZRECENTSEARCH_ZCARSEARCHPARAM_INDEX', 'ZUNFINISHEDSYIAD', 'ZUNFINISHEDSYIAD_ZSHIPPING_INDEX',
'Z_PRIMARYKEY'))
>>>
```

SQLite databases

- Can't use standard SQLite engine
  - Standard SQLite engines use read/write connection to database (would not be forensically sound)
  - No use in recovering deleted records
  - So you can't do:
    - `import sqlite3`
    - `conn = sqlite3.connect(db_file)`
    - Etc.

SQLite databases

- UFED SQLiteParser
  - SQLiteParser makes the entire database available as iterator with a dict for each record:

Python Shell

Restart Shell Active Project: python_workshop

```
>>> import SQLiteParser
>>> from System.Convert import IsDBNull
>>> for fs in ds.FileSystems:
        for file in fs.Search("Marktplaats.sqlite$"):
                db = SQLiteParser.Database.FromNode(file)
                if db != None:
                        print("> db %s found" % file.Name)


> db Marktplaats.sqlite found
>>> db.Tables
Array[str](('ZACTIVESYIAD', 'ZALERT', 'ZALERT_ZCONFIG_INDEX', 'ZCARSEARCHPARAM', 'ZCARSEARCHPARAM_ZRECENTSEARCH_INDEX',
'ZFAVORITE', 'ZFEATURETYPE', 'ZFEATURETYPE_ZAD_INDEX', 'ZMPASYSCONFIGFEATURESWITCH', 'ZMPASYSCONFIGFEATURESWITCH_ZCONFIG_INDEX',
'ZMPAUPCALLCONFIG', 'ZMPAUPCALLCONFIG_ZCONFIG_INDEX', 'ZMYBID', 'Z_METADATA', 'Z_MODELCACHE', 'ZFEATURESWITCH', 'ZLABSCONFIG',
'ZEXPERIMENTGROUPS', 'ZGROUPVALUE', 'ZABSWITCH', 'ZSAVEDPICTURE', 'ZSYSCONFIG', 'ZSHIPPINGPOSTMODEL', 'ZSWIPECONFIG',
'ZGROUPVALUE_ZGROUP_INDEX', 'ZSAVEDPICTURE_ZSYIAD_INDEX', 'ZSWIPECONFIG_ZCONFIG_INDEX', 'ZSYSCONFIG_ZSWIPECONFIG_INDEX',
'ZSYSCONFIG_ZUPCALLCONFIGS_INDEX', 'ZRECENTLYVIEWEDAD', 'ZSELECTEDSYIATTRIBUTEVALUE', 'ZCATEGORY', 'ZCATEGORY_ZCATEGORYID_INDEX',
'ZCATEGORY_ZPARENTCATEGORY_INDEX', 'ZSELECTEDSYIATTRIBUTEVALUE_ZDRAFTAD_INDEX', 'ZRECENTSEARCH',
'ZRECENTSEARCH_ZCARSEARCHPARAM_INDEX', 'ZUNFINISHEDSYIAD', 'ZUNFINISHEDSYIAD_ZSHIPPING_INDEX', 'Z_PRIMARYKEY'))
```

SQLite databases

Python Shell

Restart Shell Active Project: python_workshop

```
>>> for record in db["ZRECENTSEARCH"]:
        print record

{Z_PK: 131, Z_ENT: 16, Z_OPT: 3, ZCATEGORYID: 0, ZDISTANCE: 0, ZISSOISEARCH: 0, ZPARENTCATEGORYID: 0, ZSEARCHTITLEANDDESCRIPTION:
0, ZSELLERUSERID: 0, ZSORTORDER: 1, ZCARSEARCHPARAM: , ZLIVESINCE: , ZMAXPRICE: , ZMINPRICE: , ZTIMESTAMP: 637271822,774489,
ZSAVEDSEARCHID: , ZSEARCHTERM: Bloemputter, ZSELLERUSERNAME: , ZZIPCODE: , ZATTRIBUTES: , ZLANGUAGES: System.Byte[]}
{Z_PK: 132, Z_ENT: 16, Z_OPT: 10, ZCATEGORYID: 0, ZDISTANCE: 0, ZISSOISEARCH: 0, ZPARENTCATEGORYID: 0, ZSEARCHTITLEANDDESCRIPTION:
0, ZSELLERUSERID: 0, ZSORTORDER: 1, ZCARSEARCHPARAM: , ZLIVESINCE: , ZMAXPRICE: , ZMINPRICE: , ZTIMESTAMP: 637528312,952673,
ZSAVEDSEARCHID: , ZSEARCHTERM: bloemputters, ZSELLERUSERNAME: , ZZIPCODE: , ZATTRIBUTES: , ZLANGUAGES: System.Byte[]}
{Z_PK: 133, Z_ENT: 16, Z_OPT: 2, ZCATEGORYID: 0, ZDISTANCE: 0, ZISSOISEARCH: 0, ZPARENTCATEGORYID: 0, ZSEARCHTITLEANDDESCRIPTION:
0, ZSELLERUSERID: 0, ZSORTORDER: 1, ZCARSEARCHPARAM: , ZLIVESINCE: , ZMAXPRICE: , ZMINPRICE: , ZTIMESTAMP: 626907847,866034,
ZSAVEDSEARCHID: , ZSEARCHTERM: Goudvinken, ZSELLERUSERNAME: , ZZIPCODE: , ZATTRIBUTES: , ZLANGUAGES: }
{Z_PK: 139, Z_ENT: 16, Z_OPT: 2, ZCATEGORYID: 0, ZDISTANCE: 0, ZISSOISEARCH: 0, ZPARENTCATEGORYID: 0, ZSEARCHTITLEANDDESCRIPTION:
0, ZSELLERUSERID: 0, ZSORTORDER: 1, ZCARSEARCHPARAM: , ZLIVESINCE: , ZMAXPRICE: , ZMINPRICE: , ZTIMESTAMP: 628363332,233083,
ZSAVEDSEARCHID: , ZSEARCHTERM: golden retriever, ZSELLERUSERNAME: , ZZIPCODE: , ZATTRIBUTES: , ZLANGUAGES: System.Byte[]}
{Z_PK: 140, Z_ENT: 16, Z_OPT: 1, ZCATEGORYID: 0, ZDISTANCE: 0, ZISSOISEARCH: 0, ZPARENTCATEGORYID: 0, ZSEARCHTITLEANDDESCRIPTION:
0, ZSELLERUSERID: 0, ZSORTORDER: 1, ZCARSEARCHPARAM: , ZLIVESINCE: , ZMAXPRICE: , ZMINPRICE: , ZTIMESTAMP: 626994046,84202,
ZSAVEDSEARCHID: , ZSEARCHTERM: Geyser, ZSELLERUSERNAME: , ZZIPCODE: , ZATTRIBUTES: , ZLANGUAGES: }
{Z_PK: 141, Z_ENT: 16, Z_OPT: 2, ZCATEGORYID: 0, ZDISTANCE: 0, ZISSOISEARCH: 0, ZPARENTCATEGORYID: 0, ZSEARCHTITLEANDDESCRIPTION:
0, ZSELLERUSERID: 0, ZSORTORDER: 1, ZCARSEARCHPARAM: , ZLIVESINCE: , ZMAXPRICE: , ZMINPRICE: , ZTIMESTAMP: 637530837,155243,
ZSAVEDSEARCHID: , ZSEARCHTERM: Europese sijs, ZSELLERUSERNAME: , ZZIPCODE: , ZATTRIBUTES: , ZLANGUAGES: }
{Z_PK: 142, Z_ENT: 16, Z_OPT: 1, ZCATEGORYID: 0, ZDISTANCE: 0, ZISSOISEARCH: 0, ZPARENTCATEGORYID: 0, ZSEARCHTITLEANDDESCRIPTION:
0, ZSELLERUSERID: 0, ZSORTORDER: 1, ZCARSEARCHPARAM: , ZLIVESINCE: , ZMAXPRICE: , ZMINPRICE: , ZTIMESTAMP: 628363453,299656,
ZSAVEDSEARCHID: , ZSEARCHTERM: Sijs, ZSELLERUSERNAME: , ZZIPCODE: , ZATTRIBUTES: , ZLANGUAGES: }
{Z_PK: 143, Z_ENT: 16, Z_OPT: 1, ZCATEGORYID: 1218, ZDISTANCE: 0, ZISSOISEARCH: 0, ZPARENTCATEGORYID: 1098,
ZSEARCHTITLEANDDESCRIPTION: 0, ZSELLERUSERID: 0, ZSORTORDER: 1, ZCARSEARCHPARAM: , ZLIVESINCE: , ZMAXPRICE: , ZMINPRICE: ,
ZTIMESTAMP: 635804681,831097, ZSAVEDSEARCHID: , ZSEARCHTERM: , ZSELLERUSERNAME: , ZZIPCODE: , ZATTRIBUTES: , ZLANGUAGES: }
{Z_PK: 144, Z_ENT: 16, Z_OPT: 2, ZCATEGORYID: 0, ZDISTANCE: 0, ZISSOISEARCH: 0, ZPARENTCATEGORYID: 0, ZSEARCHTITLEANDDESCRIPTION:
0, ZSELLERUSERID: 0, ZSORTORDER: 1, ZCARSEARCHPARAM: , ZLIVESINCE: , ZMAXPRICE: , ZMINPRICE: , ZTIMESTAMP: 637279032,035011,
ZSAVEDSEARCHID: , ZSEARCHTERM: crossmotor, ZSELLERUSERNAME: , ZZIPCODE: , ZATTRIBUTES: , ZLANGUAGES: System.Byte[]}
{Z_PK: 145, Z_ENT: 16, Z_OPT: 1, ZCATEGORYID: 0, ZDISTANCE: 0, ZISSOISEARCH: 0, ZPARENTCATEGORYID: 0, ZSEARCHTITLEANDDESCRIPTION:
```

Getting data from the db

```
for fs in ds.FileSystems:
    for file in fs.Search("Marktplaats.sqlite$"):
        db = SQLiteParser.Database.FromNode(file)
        if db != None:
            print("> db %s found" % file.Name)
            i = 0
            for row in db["ZRECENTSEARCH"]:
                if not IsDBNull(row["ZSEARCHTERM"].Value):  # IsDBNull: check for Null value
                    print row["ZSEARCHTERM"].Value          # Note the ["column name"].Value notation
                    i += 1
            print("> aantal items = %d" % i)
```

Getting data from the db

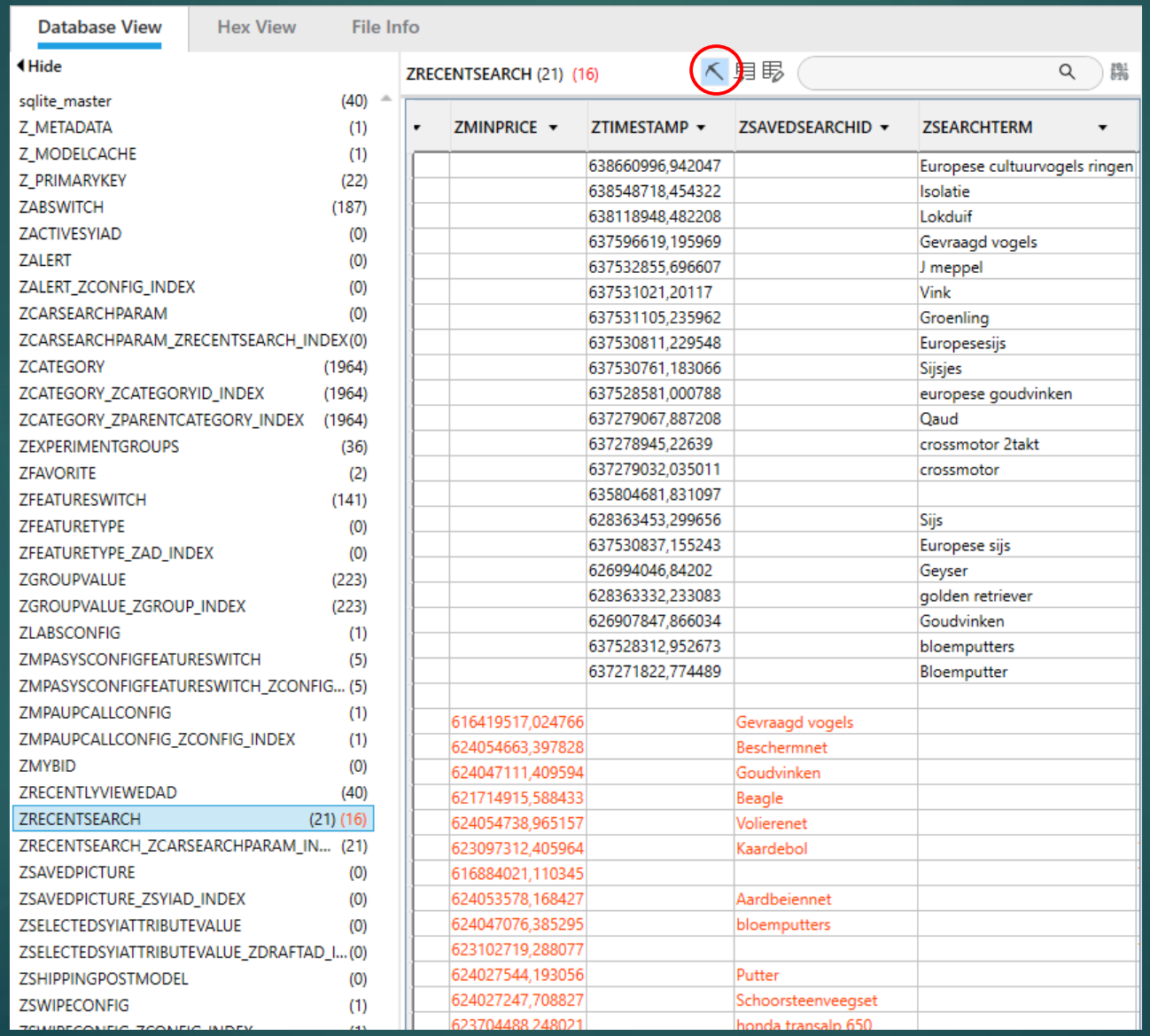
Python Shell

Restart Shell Active Project: python_workshop

```
                if db != None:
                        print("> db %s found" % file.Name)
                        i = 0
                        for row in db["ZRECENTSEARCH"]:
                                if not IsDBNull(row["ZSEARCHTERM"].Value):
                                        print row["ZSEARCHTERM"].Value
                                        i += 1
                        print("> aantal items = %d" % i)


> db Marktplaats.sqlite found                    # IsDBNull: check for Null value
Bloemputter                                      # Note the ["column name"].Value notation
bloemputters
Goudvinken
golden retriever
Geyser
Europese sijs
Sijs
crossmotor
crossmotor 2takt
Qaud
europese goudvinken
Sijsjes
Europesesijs
Groenling
Vink
J meppel
Gevraagd vogels
Lokduif
Isolatie
Europese cultuurvogels ringen
> aantal items = 20
>>>
```

Deleted items



ZMINPRICE	ZTIMESTAMP	ZSAVEDSEARCHID	ZSEARCHTERM
	638660996,942047		Europese cultuurvogels ringen
	638548718,454322		Isolatie
	638118948,482208		Lokduif
	637596619,195969		Gevraagd vogels
	637532855,696607		J meppel
	637531021,20117		Vink
	637531105,235962		Groenling
	637530811,229548		Europesesijs
	637530761,183066		Sijsjes
	637528581,000788		europese goudvinken
	637279067,887208		Qaud
	637278945,22639		crossmotor 2takt
	637279032,035011		crossmotor
	635804681,831097		
	628363453,299656		Sijs
	637530837,155243		Europese sijs
	626994046,84202		Geyser
	628363332,233083		golden retriever
	626907847,866034		Goudvinken
	637528312,952673		bloemputters
	637271822,774489		Bloemputter
616419517,024766		Gevraagd vogels	
624054663,397828		Beschermnet	
624047111,409594		Goudvinken	
621714915,588433		Beagle	
624054738,965157		Volierenet	
623097312,405964		Kaardebol	
616884021,110345			
624053578,168427		Aardbeiennet	
624047076,385295		bloemputters	
623102719,288077			
624027544,193056		Putter	
624027247,708827		Schoorsteenveegset	
623704488,248021		honda transalp 650	

Deleted items

Without table signature

```
for fs in ds.FileSystems:
    for file in fs.Search("Marktplaats.sqlite$"):
        db = SQLiteParser.Database.FromNode(file)
        if db != None:
            print("> db %s found" % file.Name)
            i = 0
            ts = SQLiteParser.TableSignature("ZRECENTSEARCH")   # create empty table signature
            for row in db.ReadTableRecords(ts, True):           # read table using table signature
                if not IsDBNull(row["ZSEARCHTERM"].Value):
                    print str(row["ZSEARCHTERM"].Value)         #  the 'True' means 'use deleted'
                    i += 1
            print("> aantal items = %d" % i)
```

```
> db Marktplaats.sqlite found
Bloemputter
bloemputters
Goudvinken
golden retriever
Geyser
Europese sijs
Sijs
crossmotor
crossmotor 2takt
Qaud
europese goudvinken
Sijsjes
Europesesijs
Groenling
Vink
J meppel
Gevraagd vogels
Lokduif
Isolatie
Europese cultuurvogels ringen
××dd×

x×
××
×<<x×
> aantal items = 23
>>>
```

Deleted items

- We can help Physical Analyser in parsing deleted record by providing a 'table signature'

Serial Type	Content Size	Meaning
0	0	Null.
1	1	8-bit twos-complement integer.
2	2	Big-endian 16-bit twos-complement integer.
3	3	Big-endian 24-bit twos-complement integer.
4	4	Big-endian 32-bit twos-complement integer.
5	6	Big-endian 48-bit twos-complement integer.
6	8	Big-endian 64-bit twos-complement integer.
7	8	Big-endian IEEE 754-2008 64-bit floating point number.
8	0	Integer constant 0. Only available for schema format 4 and higher.
9	0	Integer constant 1. Only available for schema format 4 and higher.
10, 11		Not used. Reserved for expansion.
N>12 and even	(N-12)/2	A BLOB that is (N-12)/2 bytes in length.
N>13 and odd	(N-13)/2	A string in the database encoding and (N-13)/2 bytes in length. The nul terminator is omitted.

Serial Type	Content Size
0	SQLiteParser.Tools.SignatureType.Null
1	SQLiteParser.Tools.SignatureType.Byte
2	SQLiteParser.Tools.SignatureType.Short
3	SQLiteParser.Tools.SignatureType.Int24
4	SQLiteParser.Tools.SignatureType.Int
5	SQLiteParser.Tools.SignatureType.Int48
6	SQLiteParser.Tools.SignatureType.Long
7	SQLiteParser.Tools.SignatureType.Float
8	SQLiteParser.Tools.SignatureType.Const0
9	SQLiteParser.Tools.SignatureType.Const1
N>12 and even	SQLiteParser.Tools.SignatureType.Text
N>13 and odd	SQLiteParser.Tools.SignatureType.Blob

Deleted items

With table signature

```
for fs in ds.FileSystems:
    for file in fs.Search("Marktplaats.sqlite$"):
        db = SQLiteParser.Database.FromNode(file)
        if db != None:
            print("> db %s found" % file.Name)
            i = 0
            ts = SQLiteParser.TableSignature("ZRECENTSEARCH")                                    # create empty table signature
            SQLiteParser.Tools.AddSignatureToTable(ts, 'ZTIMESTAMP', SQLiteParser.Tools.SignatureType.Float)    # define timestamp field
            SQLiteParser.Tools.AddSignatureToTable(ts, 'ZSEARCHTERM', SQLiteParser.Tools.SignatureType.Text)    # define searchterm field
            for row in db.ReadTableRecords(ts, True):                                            # read table using table signature
                if not IsDBNull(row["ZSEARCHTERM"].Value):                                       #  the 'True' means 'use deleted'
                    print("zoekopdracht: %s, status: %s" % (row["ZSEARCHTERM"].Value, str(row.Deleted)))
                    i += 1
            print("> aantal items = %d" % i)
```

Deleted items

```
> db Marktplaats.sqlite found
zoekopdracht: Bloemputter, status: Intact
zoekopdracht: bloemputters, status: Intact
zoekopdracht: Goudvinken, status: Intact
zoekopdracht: golden retriever, status: Intact
zoekopdracht: Geyser, status: Intact
zoekopdracht: Europese sijs, status: Intact
zoekopdracht: Sijs, status: Intact
zoekopdracht: crossmotor, status: Intact
zoekopdracht: crossmotor 2takt, status: Intact
zoekopdracht: Qaud, status: Intact
zoekopdracht: europese goudvinken, status: Intact
zoekopdracht: Sijsjes, status: Intact
zoekopdracht: Europesesijs, status: Intact
zoekopdracht: Groenling, status: Intact
zoekopdracht: Vink, status: Intact
zoekopdracht: J meppel, status: Intact
zoekopdracht: Gevraagd vogels, status: Intact
zoekopdracht: Lokduif, status: Intact
zoekopdracht: Isolatie, status: Intact
zoekopdracht: Europese cultuurvogels ringen, status: Intact
zoekopdracht: Gevraagd vogels, status: Deleted
zoekopdracht: Beschermnet, status: Deleted
zoekopdracht: Goudvinken, status: Deleted
zoekopdracht: Beagle, status: Deleted
zoekopdracht: Volierenet, status: Deleted
zoekopdracht: Kaardebol, status: Deleted
zoekopdracht: Aardbeiennet, status: Deleted
zoekopdracht: bloemputters, status: Deleted
zoekopdracht: Putter, status: Deleted
zoekopdracht: Schoorsteenveegset, status: Deleted
zoekopdracht: honda transalp 650, status: Deleted
zoekopdracht: Schoorsteenveegset, status: Deleted
> aantal items = 32
>>>
```

Presenting data in PA

- Content Models
  - Pre-defined (see manual)
  - Generic model
    - 10 multi-use fields
    - 3 timestamp fields
  - Data.Models (in python shell)

```
>>> Data.Models.
    ReplyMessageData
    ReservationStatus
    Ride
    RideStatus
    SampleDataType
    SampleSourceType
    ScrambledMessageData
    SearchedItem
    SearchItemOrigin
    SearchMatch
```

8.1. List of dependent and independent Models

The independent **Models** that are added to the **DataStore** tree:

Contact	UserAccount	VoiceMail
SMS	CalendarEntry	Password
Email	Journey	InstalledApplication
MMS	Cookie	ApplicationUsage
Note	VisitedPage	DictionaryWord
Chat	WebBookmark	SharedFile
Location	BluetoothDevice	Map
SearchedItem	WirelessNetwork	Notification
InstantMessage	CarvedString	PoweringEvent

PhoneNumber	Attachment	UserID
StreetAddress	WebAddress	Party
ContactPhoto	Organization	Coordinate
EmailAddress		

Presenting data in PA

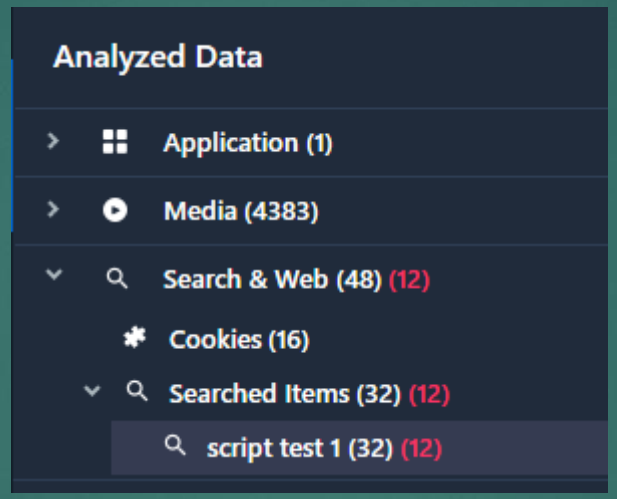
See Github -> sqlite_demo.py

```
from physical import *

import SQLiteParser
from System.Convert import IsDBNull

results = []                                                                                    # prepare empty results array
for fs in ds.FileSystems:
    for file in fs.Search("Marktplaats.sqlite$"):
        db = SQLiteParser.Database.FromNode(file)
        if db != None:
            print("> db %s found" % file.Name)
            i = 0
            ts = SQLiteParser.TableSignature("ZRECENTSEARCH")                                   # create empty table signature
            SQLiteParser.Tools.AddSignatureToTable(ts, 'ZTIMESTAMP', SQLiteParser.Tools.SignatureType.Float)    # define timestamp field
            SQLiteParser.Tools.AddSignatureToTable(ts, 'ZSEARCHTERM', SQLiteParser.Tools.SignatureType.Text)    # define searchterm field
            for row in db.ReadTableRecords(ts, True):                                           # read table using table signature
                if not IsDBNull(row["ZSEARCHTERM"].Value):                                      #  the 'True' means 'use deleted'
                    zk = SearchedItem()                                                         # create a model of type SearchedItem
                    zk.Value.Value = row["ZSEARCHTERM"].Value                                   # add the 'searchterm value'
                    zk.Value.Source = MemoryRange(row["ZSEARCHTERM"].Source)                    # add source indicator
                    zk.TimeStamp.Value = TimeStamp.FromUnixTime(row["ZTIMESTAMP"].Value+978307200)    # add timestamp
                    zk.Deleted = row.Deleted                                                    # add intact / deleted indicator
                    zk.Source.Value = "script test 1"                                           # add source app
                    results.append(zk)                                                          # append to results array
                    print("zoekopdracht: %s, status: %s" % (row["ZSEARCHTERM"].Value, str(row.Deleted)))
                    i += 1
            print("> aantal items = %d" % i)
ds.Models.AddRange(results)                                                                     # add all results to DataStore
```

Presenting data in PA

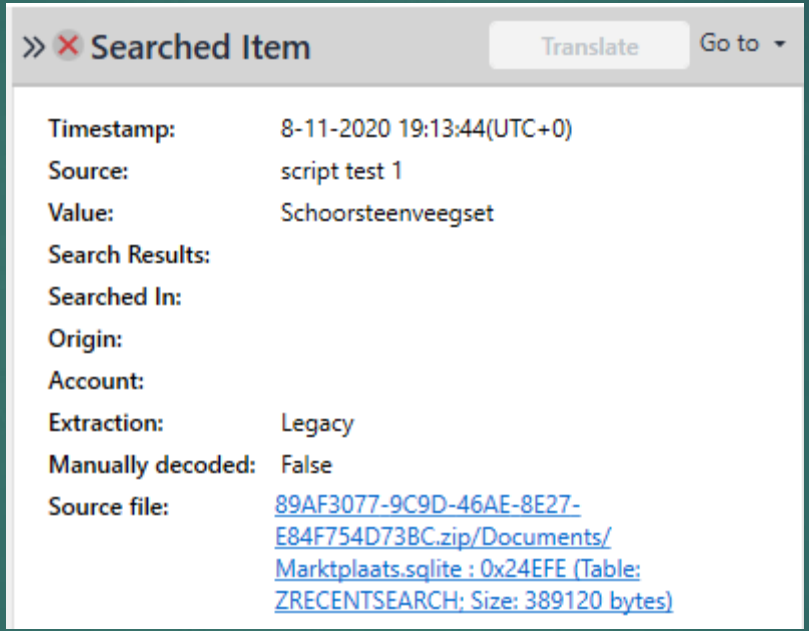


Presenting data in PA

#	Timestamp	Value	Position	Map Address	Source
16	12-3-2021 19:57:02(UTC+0)	Bloemputter			script test 1
17	29-11-2020 17:24:13(UTC+...	Sijs			script test 1
18	29-11-2020 17:22:12(UTC+...	golden retriever			script test 1
19	13-11-2020 21:00:46(UTC+...	Geyser			script test 1
20	12-11-2020 21:04:07(UTC+...	Goudvinken			script test 1
21	8-11-2020 19:13:44(UTC+0)	Schoorsteenveegset			script test 1
22	10-10-2020 20:32:18(UTC+...	Volierenet			script test 1
23	10-10-2020 20:31:03(UTC+...	Beschermnet			script test 1
24	10-10-2020 20:12:58(UTC+...	Aardbeiennet			script test 1
25	10-10-2020 18:25:11(UTC+...	Goudvinken			script test 1
26	10-10-2020 18:24:36(UTC+...	bloemputters			script test 1

Total: 32 Deduplication: 0 Items: 32/32 Selected: 32

Presenting data in PA



JSON data

```
for fs in ds.FileSystems:
    for f in fs.Search(".*"):                                   # search any file (use a smarter regex in your script!)
        if f != None and f.Data != None:                        # check if it's not an empty file
            data = None
            try:
                data = simplejson.loads(f.read(), encoding='utf-8') # try to parse as JSON
            except:
                pass                                            # if not valid json, do nothing
            if data != None:
                if isinstance(data, list):                      # if type = list -> multiple json objects in one file
                    for i in data:
                        parse_mp_json(i)                        # custom function to parse each json object indiviually for content
                else:
                    parse_mp_json(data)                         # otherwise, just parse the json object (function)
```

JSON data


```
{'_embedded': {'mc:conversations': [{'_embedded': {'mc:latest-message': {'id': '0d4a9eb0-76be-11eb-bf5f-1f1eea36a1bb', 'receivedDate':
'2021-02-24T16:33:40Z', 'isRead': True, 'senderId': 20      , 'text': 'Is het mogelijk om per telefoon veder af te spreken mijn nummer is
06        '}}, 'sellerId': 11      , 'unreadMessagesCount': 0, 'title': '2 koppel + 1 losse pop bloemputters', 'itemId': 'm1668      ',
'otherParticipant': {'id': 204     , 'name': 'gb      ', 'isReviewable': False}, '_links': {'describedby': {'href': 'https://api.marktplaats.nl/
messagebox/v1/docs/conversation.html'}, 'mc:messages': {'href': '/messagebox/v1/my-conversations/1rh3%3A45196n4%3A2frm10sp3/messages', 'title': 'The
messages in this conversation.'}, 'mc:other-participant': {'href': '/v1/users/204     ', 'title': 'The other participant of this conversation.'},
```


- Resulting data is a nested dict
  - Write a script that takes exactly the fields you need
  - Then create a ContentModel to present the data in Physical Analyzer

JSON data

See Github -> json_demo.py

```
from physical import *

import simplejson
import time

myMarktplaatsConversations = []                          # empty result array
mySourceValue = 'Marktplaats berichten'                  # source app indicator

def parse_mp_json(data):
    if data.has_key('_embedded'):                            # do some checks, and then just get the fields you need and put them in you Content Model
        if data['_embedded'].has_key('mc:conversations'):
            for _conv in data['_embedded']['mc:conversations']:
                myConv = GenericModel ()
                myConv.Field1.Value = str(_conv['itemId'])
                myConv.Field2.Value = _conv['title'].strip()
                myConv.Field3.Value = str(_conv['sellerId'])
                myConv.Field4.Value = str(_conv['otherParticipant']['id'])
                myConv.Field5.Value = _conv['otherParticipant']['name']
                myConv.Field6.Value = str(_conv['_embedded']['mc:latest-message']['senderId'])
                myConv.Field7.Value = _conv['_embedded']['mc:latest-message']['text']
                myConv.TimeStamp1.Value = TimeStamp.FromUnixTime(time.mktime(time.strptime(_conv['_embedded']['mc:latest-message']['receivedDate'], "%Y-
                myConv.Field1.Source = f.Data
                myConv.Source.Value = mySourceValue
                myMarktplaatsConversations.append(myConv)
```

```
ds.Models.AddRange(myMarktplaatsConversations)              # add the results to the DataStore
```

JSON data

Cellebrite Physical Analyzer 7.49.0.28

File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks

Search Advanced

python_workshop

Search

Analyzed Data

- Application (1)
- Manual Data Collection (462)
  - Generic model (462)
    - Marktplaats berichten (462)
- Media (4383)
- Search & Web (112) (36)
  - Cookies (16)
  - Searched Items (96) (36)
    - script test 1 (96) (36)

Data files

- Configurations (21)
- Databases (21)
- Text (7)
- Uncategorized (9694)

Tips & Tricks | Marktplaats berichten (462)

juli, 2020 | augustus, 2020 | september, 2020 | oktober, 2020 | november, 2020 | december, 2020 | januari, 2021 | februari, 2021 | maart, 2021

Export Filters Actions Search

#	Timestamp 1	Timestamp 2	Timestamp 3	Field 1	Field 2
28	27-3-2021 11:52:16(UTC+0)			m168130	Bloemputters
29	19-3-2021 17:54:28(UTC+0)			m168130	Bloemputters
30	20-3-2021 10:44:24(UTC+0)			m168130	Bloemputters
31	20-3-2021 10:46:59(UTC+0)			m168130	Bloemputters
32	21-3-2021 10:14:57(UTC+0)			m168130	Bloemputters
33	21-3-2021 11:46:02(UTC+0)			m168130	Bloemputters
34	21-3-2021 12:05:47(UTC+0)			m168130	Bloemputters
35	21-3-2021 13:00:01(UTC+0)			m168130	Bloemputters
36	21-3-2021 15:39:11(UTC+0)			m168130	Bloemputter

Total: 462 Deduplication: 0 Items: 462/462 Selected: 462

Generic model — Translate — Go to

Field 1:	m168
Field 2:	Bloemputters
Field 3:	112
Field 4:	2429
Field 5:	Ap
Field 6:	11290
Field 7:	Ik bel straks
Field 8:	
Field 9:	
Field 10:	
Timestamp 1:	20-3-2021 10:46:59(UTC+0)
Timestamp 2:	
Timestamp 3:	
Extraction:	Legacy
Manually decoded:	False
Source:	Marktplaats berichten
Source file:	

Trace window

Clear

09:58:47 Plugin PythonWrapper finished, runtime: 00:00:01.15
09:58:47 Running plugin ProjectProcessorFinisher (debug=False)
09:58:47 Waiting for project processor to finish...
09:58:47 PP: Starting last stage for project: 45899441-e884-4604-b1ba-4664e7ab95c2 (0 items)
09:58:47 Finishing extraction info...
09:58:47 PP: Last stage completed: 00:00:00.06, ProjectId: 45899441-e884-4604-b1ba-4664e7ab95c2, CaseId: a9cc99c9-6e4c-4baf-80e1-130f7ee9decd
09:58:47 Waited for project processor for: 00:00:00.07

bplist

- again the result is a dict (like JSON), by now you should know how to get info from this and present it in Physical Analyzer
- See Github -> plist_demo.py

Python Shell

Restart Shell Active Project: python_workshop

```
============== 'ds' is now set to project: python_workshop ===========
>>> import sys
>>> sys.path.append("C:\\Users\\      \\Documents\\git-repos\\physical-analyzer-python-.net\\ccl-bplist")
>>> import ccl_bplist
>>> ccl_bplist.set_object_converter(ccl_bplist.NSKeyedArchiver_common_objects_convertor)
>>> for fs in ds.FileSystems:
        for f in fs.Search("com\.marktplaats\.iphone\.plist$"):
                plist = ccl_bplist.load(f)


>>> plist
```

add ccl-bplist to path
load ccl-bplist module
set parsing of NSKeyedArchiver format

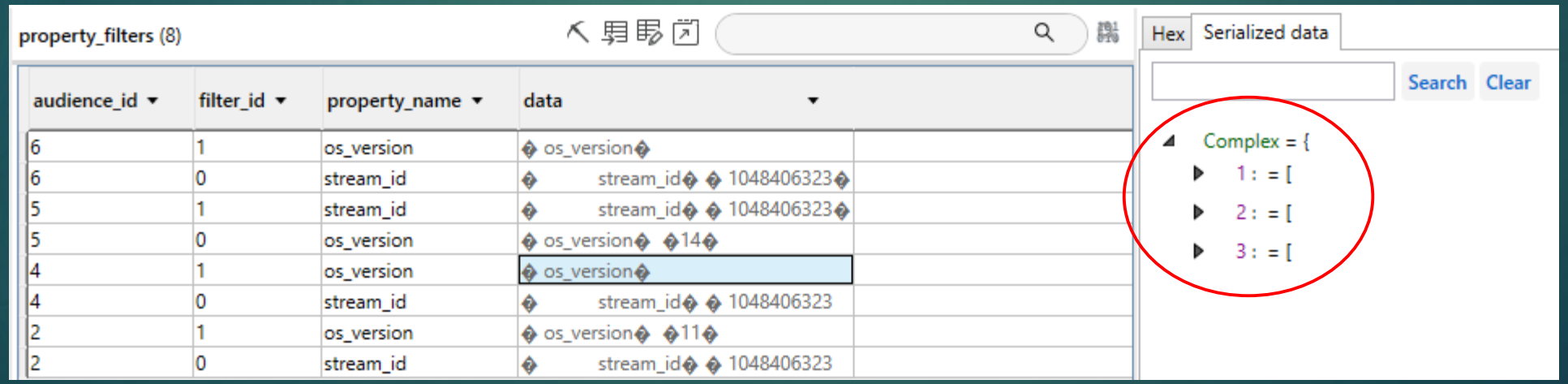
find a plist
and load it

print the parsed plist


```
{'apnsnotificationdevicetoken': u'$\xdaHfB?(@-\x8e\x102oA\x98\xb19\xc3\xba\xeb\x8ajn\xaf\xf8\x9d\x9c\xf7^\x88D\xb3',
'com.firebase.instanceid.user_defaults.locale': 'nl_NL', '/google/ads/wk_initialization_load': '0', '/google/ads/gad:rbv_max_bg_tm_not_dismis_ms': '300000', '/
google/ads/gads:wiggle_debug_gesture:enable': 'false', '/google/ads/banner_prevent_autoplay': 'false', '/google/ads/gads:nativeTestAdLabel:enabled': 'true', '/
google/ads/content_url_fingerprint': 'UmjMw_opxY8gCcovgtNbgKn8bd8qNnEexcJ7IpXigqRN8YWO34zDvQ==', 'ADMS_START': datetime.datetime(2021, 3, 30, 12, 1, 14, 158572),
'ConsecutiveDaysOpenedCount': 0, 'ATEngagementIsUpdateBuildKey': True, '/google/ads/wv_request_poll_interval': '0', 'GDPRvendorListVersion': 159, 'GMSInstanceID-
version': '3.1.1', 'personalisedGoogleAdsValue': True, 'RunThisVersion': 835, '/google/ads/banner_wv_class': 'wk', 'GID_AppHasRunBefore': True,
'escrowOnboarding': True, '/google/ads/gads:sai:interstitial_screen_enabled': '1', '/google/ads/gads:interstitial_ad_pool:schema': ['customTargeting', 'extras',
'u_so'], 'ATDeviceLastUpdatePreferenceKey': datetime.datetime(2018, 4, 1, 15, 20, 6, 548187), 'WebKitMediaPlaybackAllowsAirPlay': True, 'AAMUserId':
'5875652013919398231423349361805462786 2', 'PPOLastShownDate': datetime.datetime(2019, 5, 15, 20, 15, 15, 852519), 'google_timing_/4282/ios/mpnl.565/
babykleding_mutsen_sjaals_en_wanten/vip/t_app_ios_vip_mid1': {'adapter': {'end': 0, 'start': 2651, 'category': 'adapter'}},
'com.facebook.sdk:serverConfiguration1652748041707995': u'bplist00\xd4\x00\x01\x00\x02\x00\x03\x00\x04\x00\x05\x00\x08\x01\x1d\x01\x1eT$topX$objectsX$versionY
$archiver\xd1\x00\x06\x00\x07Troot\x80\x01\xaf\x10?\x00\t\x00\n\x00=\x00>\x00?\x00@\x00F\x00L\x00T\x00U\x00V\x00\\\x00&\x00^\x00f\x00)\x00h\x00l\x00\x80\x00\x81
\x00\x82\x00\x83\x00\x84\x00\x85\x00\x86\x00\x87\x00\x88\x00\x8e\x00\x8f\x00\x99\x00\x9a\x00\x9f\x00\xa0\x00\xa1\x00+\x00\xa5\x00\xa6\x00\xaa\x00\xad\x00\xb3\x00
```

Protobuf

- Binary serialized format van Google
- Can be found in files and database fields
- Does not provide field names, numbered instead



Protobuf

- again the result is a dict you can use
- See Github -> protobuf_demo.py

Python Shell

Restart Shell Active Project: python_workshop

```
>>> import sys
>>> sys.path.append("C:\\Users\\      \\Documents\\git-repos\\physical-analyzer-python-.net")      # add script dir to path
>>> # import protobuf decoder
>>> import protobuf_decoder.parse as pbparser                                                       # load pbparser module
>>> # for SQLite databases
>>> import SQLiteParser
>>> from System.Convert import IsDBNull
>>> for fs in ds.FileSystems:
        for f in fs.Search("google\-app\-measurement\.sql$"):                                       # open the database with protobuf fields
                db = SQLiteParser.Database.FromNode(f)
                for row in db["raw_events"]:
                        print pbparser.Decode(bytes(row["data"].Value))                             # for each record print the decoded protobuf
```

```
{'01:01:embedded message': {'01:00:string': '_et', '03:01:Varint': 3423}, '01:03:embedded message': {'01:00:string': '_o', '02:01:string': 'auto'}, '03:04:Varint':
1617102889780L, '01:00:embedded message': {'01:00:string': '_si', '03:01:Varint': 4779444671064220808L}, '01:02:embedded message': {'01:00:string': '_sc',
'02:01:string': 'NotificationCenterViewController'}}
{'01:01:embedded message': {'01:00:string': '_pc', '02:01:string': 'NotificationCenterViewController'}, '01:03:embedded message': {'01:00:string': '_o',
'02:01:string': 'auto'}, '03:05:Varint': 1617102889781L, '01:00:embedded message': {'01:00:string': '_si', '03:01:Varint': 4779444671064220752L}, '01:02:embedded
message': {'01:00:string': '_sc', '02:01:string': 'MyMarktplaatsViewController'}, '01:04:embedded message': {'01:00:string': '_pi', '03:01:Varint':
4779444671064220808L}}
{'01:01:embedded message': {'01:00:string': '_et', '03:01:Varint': 1238}, '01:03:embedded message': {'01:00:string': '_o', '02:01:string': 'auto'}, '03:04:Varint':
1617102891019L, '01:00:embedded message': {'01:00:string': '_si', '03:01:Varint': 4779444671064220752L}, '01:02:embedded message': {'01:00:string': '_sc',
'02:01:string': 'MyMarktplaatsViewController'}}
{'01:01:embedded message': {'01:00:string': '_pc', '02:01:string': 'MyMarktplaatsViewController'}, '01:03:embedded message': {'01:00:string': '_o', '02:01:string':
'auto'}, '03:05:Varint': 1617102891020L, '01:00:embedded message': {'01:00:string': '_si', '03:01:Varint': 4779444671064220754L}, '01:02:embedded message':
{'01:00:string': '_sc', '02:01:string': 'ChatSplitViewController'}, '01:04:embedded message': {'01:00:string': '_pi', '03:01:Varint': 4779444671064220752L}}
{'01:01:embedded message': {'01:00:string': '_pc', '02:01:string': 'ChatSplitViewController'}, '01:03:embedded message': {'01:00:string': '_o', '02:01:string':
```

When Python is not enough - .NET

- clr: Common Language Runtime
- .NET libraries
- System installed .NET version is used (4.7.2)

Create a new project

library

Clear all

Recent project templates

Library (.NET Framework) F#

C# | All platforms | All project types

Class library
A project for creating a class library that targets .NET Standard or .NET Core
C# Android Linux macOS Windows Library

WPF Class library
A project for creating a class library that targets a .NET Core WPF Application
C# Windows Desktop Library

WPF Custom Control Library
A project for creating a custom control library for .NET Core WPF Applications
C# Desktop Library

WPF User Control Library
A project for creating a user control library for .NET Core WPF Applications
C# Windows Desktop Library

Class Library (.NET Framework)
A project for creating a C# class library (.dll)
C# Windows Library

Back Next

Configure your new project

Class Library (.NET Framework) C# Windows Library

Project name

hello_world

Location

C:\Users\Sieger\source\repos

...

Solution name

hello_world

☑ Place solution and project in the same directory

Framework

.NET Framework 4.7.2

Back Create

File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help Search (Ctrl+Q) hello_world

Debug Any CPU Start Live Share

Class1.cs

hello_world | hello_world.Greeter | Print(string name)

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;

namespace hello_world
{
    0 references
    public class Greeter
    {
        0 references
        public static string Print(string name)
        {
            return "hello " + name + ", from .NET";
        }

    }
}
```

100 % No issues found Ln: 13 Ch: 52 SPC CRLF

Output

Show output from: Build

```
Build started...
1>------ Build started: Project: hello_world, Configuration: Debug Any CPU ------
1>  hello_world -> C:\Users\Sieger\source\repos\hello_world\bin\Debug\hello_world.dll
========== Build: 1 succeeded, 0 failed, 0 up-to-date, 0 skipped ==========
```

Solution Explorer

Search Solution Explorer (Ctrl+;)

Solution 'hello_world' (1 of 1 project)

- hello_world
  - Properties
  - References
  - Class1.cs

Properties

Server Explorer Toolbox

Build succeeded Add to Source Control

.NET

See Github -> dotnet_demo.py and hello_world

Python Shell

Restart Shell

Active Project: python_workshop

```
>>> import clr                                                                                    # load clr module
>>> sys.path.append("C:\\Users\\      \\Documents\\git-repos\\physical-analyzer-python-.net\\hello_world\\bin\\Debug")   # add path to you .NET assembly
>>> clr.AddReference("hello_world")                                                               # add the .NET assembly to clr
>>> import hello_world                                                                            # load the .NET assembly
>>> hello_world.Greeter.Print("Bill")                                                             # use a function from your .NET assembly
'hello Bill, from .NET'
>>>
```

.NET

- Possibilities only limited by what .NET can do:
  - Encryption / decryption
  - SQLCipher
  - GIT interaction
  - …

.NET AES/GCM decryption

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using Org.BouncyCastle.Crypto.Engines;
using Org.BouncyCastle.Crypto.Modes;
using Org.BouncyCastle.Crypto.Parameters;
using Org.BouncyCastle.Security;

namespace FbDecryptBouncyCastle
{
    public class AesGcm
    {
        public static string Decrypt(string encodedCiper, string encodedKey)
        {
            // decode base64 input
            byte[] myCipher = Convert.FromBase64String(encodedCiper);
            byte[] myKey = Convert.FromBase64String(encodedKey);

            // get IV
            var myIV = new byte[12];
            Buffer.BlockCopy(myCipher, 0, myIV, 0, 12);

            // get Tag
            var cipherLength = Buffer.ByteLength(myCipher);
            var myTag = new byte[16];
            Buffer.BlockCopy(myCipher, cipherLength - 16, myTag, 0, 16);

            //leave tag appended to ciphertext
            var newCipher = new byte[cipherLength - 12];
            Buffer.BlockCopy(myCipher, 12, newCipher, 0, cipherLength - 12);
```

```
            var keyParameter = new KeyParameter(myKey);
            var keyParameters = new AeadParameters(keyParameter, 128, myIV);
            var Cipher = CipherUtilities.GetCipher("AES/GCM/NoPadding");
            Cipher.Init(false, keyParameters);
            var decryptedData = Cipher.DoFinal(newCipher);
            return Encoding.UTF8.GetString(decryptedData);
        }
    }
}
```

.NET AES/GCM decryption

Python Shell

Restart Shell Active Project: python_workshop

```
>>>
>>>
>>> import sys
>>> import clr
>>> sys.path.append("C:\\Users\\      \\Documents\\git-repos\\                          \\dll")
>>> clr.AddReference("FbDecryptBouncyCastle")
>>> import FbDecryptBouncyCastle
>>>
>>> encrypted_data = "qP01w5V25kDv434juAhhDXZQV0IEOTzUQZJuGfs4pDNhLzqarGGUh+7qSQf+/E/WDNzjeVIDvVsMkCRNG9TATvOV1s8JrcLs/XgIgVoC"
>>> key = "FISuBJEVfjNMiBWv7O4ZYIZfRIp/3q84jY4/vPlmN64="
>>>
>>> FbDecryptBouncyCastle.AesGcm.Decrypt(encrypted_data, key)
'just some text to demonstra AES/GCM decryption :-)'
>>>
```

Extra: embedded plists

note the embedded bplist

Python Shell

Restart Shell

Active Project: python_workshop

```
========== 'ds' is now set to project: python_workshop ==========
>>> import sys
>>> sys.path.append("C:\\Users\\      \\Documents\\git-repos\\physical-analyzer-python-.net\\ccl-bplist")
>>> import ccl_bplist
>>> ccl_bplist.set_object_converter(ccl_bplist.NSKeyedArchiver_common_objects_convertor)
>>> for fs in ds.FileSystems:
        for f in fs.Search("com\.marktplaats\.iphone\.plist$"):
                plist = ccl_bplist.load(f)


>>> plist
{'apnsnotificationdevicetoken': u'$\xdaHfB?(@-\x8e\x102oA\x98\xb19\xc3\xba\xeb\x8ajn\xaf\xf8\x9d\x9c\xf7^\x88D\xb3',
'com.firebase.instanceid.user_defaults.locale': 'nl_NL', '/google/ads/wk_initialization_load': '0', '/google/ads/gad:rbv_max_bg_tm_not_dismis_ms': '300000', '/
google/ads/gads:wiggle_debug_gesture:enable': 'false', '/google/ads/banner_prevent_autoplay': 'false', '/google/ads/gads:nativeTestAdLabel:enabled': 'true', '/
google/ads/content_url_fingerprint': 'UmjMw_opxY8gCcovgtNbgKn8bd8qNnEexcJ7IpXigqRN8YWO34zDvQ==', 'ADMS_START': datetime.datetime(2021, 3, 30, 12, 1, 14, 158572),
'ConsecutiveDaysOpenedCount': 0, 'ATEngagementIsUpdateBuildKey': True, '/google/ads/wv_request_poll_interval': '0', 'GDPRvendorListVersion': 159, 'GMSInstanceID-
version': '3.1.1', 'personalisedGoogleAdsValue': True, 'RunThisVersion': 835, '/google/ads/banner_wv_class': 'wk', 'GID_AppHasRunBefore': True,
'escrowOnboarding': True, '/google/ads/gads:sai:interstitial_screen_enabled': '1', '/google/ads/gads:interstitial_ad_pool:schema': ['customTargeting', 'extras',
'u_so'], 'ATDeviceLastUpdatePreferenceKey': datetime.datetime(2018, 4, 1, 15, 20, 6, 548187), 'WebKitMediaPlaybackAllowsAirPlay': True, 'AAMUserId':
'5875652013919398231423349361805462786 2', 'PPOLastShownDate': datetime.datetime(2019, 5, 15, 20, 15, 15, 852519), 'google_timing_/4282/ios/mpnl.565/
babykleding mutsen sjaals en wanten/vip/t app ios vip mid1': {'adapter': {'end': 0, 'start': 2651, 'category': 'adapter'}},
'com.facebook.sdk:serverConfiguration1652748041707995': u'bplist00\xd4\x00\x01\x00\x02\x00\x03\x00\x04\x00\x05\x00\x08\x01\x1d\x01\x1eT$topX$objectsX$versionY
$archiver\xd1\x00\x06\x00\x07Troot\x80\x01\xaf\x10?\x00\t\x00\n\x00=\x00>\x00?\x00@\x00F\x00L\x00T\x00U\x00V\x00\\\x00&\x00^\x00f\x00)\x00h\x00l\x00\x80\x00\x81
\x00\x82\x00\x83\x00\x84\x00\x85\x00\x86\x00\x87\x00\x88\x00\x8e\x00\x8f\x00\x99\x00\x9a\x00\x9f\x00\xa0\x00\xa1\x00+\x00\xa5\x00\xa6\x00\xaa\x00\xad\x00\xb3\x00
\xb9\x00\xbf\x00\xc5\x00\xc6\x00\xca\x00\xcb\x00\xcc\x00\xd2\x00\xd8\x00\xde\x00\xe4\x00\xea\x00\xf0\x00\xf1\x00\xf5\x00\xf6\x00\xfc\x01\x02\x01\x08\x01\x0e\x01
\x12\x01\x16\x01\x19U$null\xdf\x10\x19\x00\x0b\x00\x0c\x00\r\x00\x0e\x00\x0f\x00\x10\x00\x11\x00\x12\x00\x13\x00\x14\x00\x15\x00\x16\x00\x17\x00\x18\x00\x19\x00
\x1a\x00\x1b\x00\x1c\x00\x1d\x00\x1e\x00\x1f\x00 \x00!\x00"\x00#\x00$\x00%\x00&\x00\'\x00(\x00)\x00)\x00+\x00(\x00)\x00.\x00&\x00(\x00&\x00&\x003\x004\x005\x006
```

Extra: embedded plists

- ccl-bplist expects a file
  - So you can't do:
    `embedded_plist = ccl_bplist.load(plist["embedded value"]`
- Instead, use StringIO to emulate a file:

Python Shell

Restart Shell Active Project: python_workshop

```
>>> import StringIO
>>> emulated_file = StringIO.StringIO(plist["com.facebook.sdk:serverConfiguration1652748041707995"])
>>> embedded_plist = ccl_bplist.load(emulated_file)
>>> print embedded_plist
{'$version': 100000, '$objects': ['$null', {'errorConfigs': UID: 16, 'implicitPurchaseLoggingEnabled': True, 'timestamp': UID: 60, 'nativeAuthFlowEnabled': True,
'$class': UID: 62, 'smarstLoginBookmarkMenuURL': UID: 0, 'smarstLoginBookmarkIconURL': UID: 0, 'codelessEventsEnabled': False, 'version': 2,
'sessionTimeoutInterval': 60.0, 'systemAuthenticationEnabled': True, 'dialogFlows': UID: 7, 'SDKUpdateMessage': UID: 0, 'smartLoginEnabled': 0, 'dialogConfigs':
UID: 5, 'appID': UID: 2, 'loggingToken': UID: 0, 'eventBindings': UID: 0, 'defaultShareMode': UID: 4, 'appName': UID: 3, 'loginTooltipEnabled': False,
'trackAppUninstallEnabled': False, 'advertisingIDEnabled': True, 'implicitLoggingEnabled': True, 'loginTooltipText': UID: 0}, '1652748041707995', 'Marktplaats',
'share_sheet', {'NS.objects': [], '$class': UID: 6, 'NS.keys': []}, {'$classes': ['NSDictionary', 'NSObject'], '$classname': 'NSDictionary'}, {'NS.objects': [UID:
10, UID: 13], '$class': UID: 6, 'NS.keys': [UID: 8, UID: 9]}, 'message', 'default', {'NS.objects': [UID: 12], '$class': UID: 6, 'NS.keys': [UID: 11]},
'use_native_flow', True, {'NS.objects': [UID: 15, UID: 12], '$class': UID: 6, 'NS.keys': [UID: 11, UID: 14]}, 'use_safari_vc', False, {'configurationDictionary':
UID: 17, '$class': UID: 59}, {'NS.objects': [UID: 26, UID: 38, UID: 40, UID: 46, UID: 48, UID: 50, UID: 55, UID: 57], '$class': UID: 37, 'NS.keys': [UID: 18, UID:
19, UID: 20, UID: 21, UID: 22, UID: 23, UID: 24, UID: 25]}, '190', '102', '4', '9', '17', '1', '341', '2', {'NS.objects': [UID: 28], '$class': UID: 37, 'NS.keys':
[UID: 27]}, '*', {'options': UID: 30, 'category': UID: 34, 'action': UID: 35, 'description': UID: 29, '$class': UID: 36}, 'Please log into this app again to
reconnect your Facebook account.', {'NS.objects': [UID: 31, UID: 32], '$class': UID: 33}, 'OK', 'Cancel', {'$classes': ['NSArray', 'NSObject'], '$classname':
```