Given hint- the following info belongs to one person:

first name: ***Cary ,****last name:* ***Thompson,*** *phone:* ***0467674021,*** *time:* ***2013-06-11 15:57:19***

We are given an **encrypted log file** [probably similar to one extracted from a cell-phone database / calls history]

------------------------------- Let's inspect the first line (First names): ---

*86B7***5A3F00004**olga**DD4C00005**FelixB3F9**00007**JuanitaE66E00005JuanaD1A900007Timothy**5BBE**00
004CaryA6E900006Minnie316800004MarcA71A**00007**Rudolph5159**00016**Mickael Barrie Linwood1E
27**00003**Lee538F**00005**WilmaBF49**00005**JamieBB7C**00018**Jephtha Veronika KristenC1A2**00005**Corey
941B**00006**ElviraB4D4**00005**Andre5511**00008**Winifred6444**00006**Jessie56F2**00006**Eloise9F99**00006**
Miguel36AF**00005**Elias3081**00005**LyndaD7AB**00010**Virgil Rut HefinDA5B**00003**Don

Before each first name we have **9 hex** characters, **the last 5** seems to contain digits only of perhaps a sequential series (Un-orderd, not full, with repetitions = non unique e.g **00005**Andre & **00005**Wilma) But it is **actually** a **hex** representation of a decimal value which equals to the **length of the first name string** [**00018**Jephtha Veronika Kristen, len(name)=24= 0x18h].

The first 4 seems like a **unique**-for-each-name 2 bytes value encoded in **hex**. *We will try to figure out what's their meaning later but for now we will assume it's the a* ***'contact id'*** *(max_val = 65,535=FFFF).*

The line **header** (as for each other line in the file) contains a unique 2-bytes field type id [*86B7*].

------------------------------- Let's inspect the second line (Last names): -------------------------------------

*9E60**316800007**Delgado5A3F00004SimsB3F900004SotoFBC500004UllaDA5B00004HallD1A900005Hi
nes515900006HolmesBB7C00007Tirrell56F200007Jenkins**5BBE00008**Thompson551100004TranD7AB
00005WelchDD4C00004WestA71A00005BanksC1A200008Griffith941B00006Powell644400005Payne
BF4900005GreerB4D400006SteeleA6E900006Chavez1E2700006Austin538F00008GonzalezE66E0000
5Bates308100008Chambers36AF00008Alvarado9F9900007Alvarez*

Here same fact about the string length info holds true for the last name. we also see here ***5BBE*** *which is the same id as for Cary first name 'contact id'*

---*What about line #3?* ---

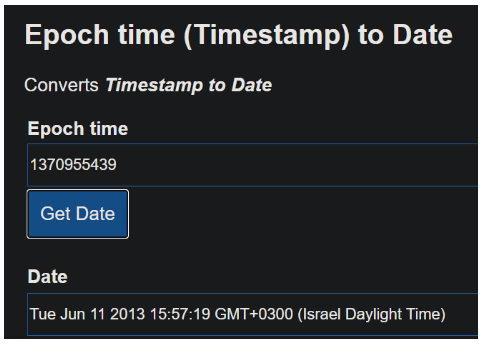
51595A3F0000A08937625719F99**00013**+54 (569) 9547(whitespace)
17405BBE**0000A**0467674021B3F90000A03527538315511000A0188577963BF490000A0674542791
FBC50000A06932067275159000B03-
4612955956F20000A0354203289B3F90000A0633434984D7AB0000A0695304544DA5B0000A05503
……

Same thing goes here – We can see Cary's contact-id 5BBE , **0000A** =10= phone# string len(0467674021). We can also see that a phone number can be given in a different format: **00013**+54 (569) 9547 1740 (len(phone_number_str) = 19 =0x13h)

--_What about line #4?_ --

D812E66E**0000A**13297539619F99**0000A**1326011227538F0000A1341144162316800000A1333737336
D7AB0000A1367834926D1A90000A1340522218B4D40000A1339938392DD4C0000A1346574058C1
A20000A134475357330810000A136293851756F20000A1329934748A71A0000A1383377560B3F900
00A13460667155BBE**0000A**1370955439BF490000A1336724039A6E90000A132550239864440000A
13827086085A3F0000A1353692293BB7C0000A136799576755110000A1327676142DA5B0000A135
36535381E270000A1332164993941B0000A133802356236AF0000A1345444250FBC50000A1345448
25251590000A1355240920

Well, we are looking for **Cary's** *time info :* ***2013-06-11 15:57:19'.*** *As I know from previous experiments with Linux kernel scheduler, in many systems – datetime(date+time) is encoded in a special manner:*


Epoch time (Timestamp) to Date

Converts *Timestamp to Date*

Epoch time

1370955439

Get Date

Date

Tue Jun 11 2013 15:57:19 GMT+0300 (Israel Daylight Time)

Unix time (also known as **POSIX** time or epoch time) is a system for describing instants in time, defined as the **number of seconds that have elapsed since 00:00:00 Coordinated Universal Time (UTC), Thursday, 1 January 1970,**[1][note 1] not counting leap seconds.[1][2][note 2] It is used widely in **Unix-like and many other operating systems and file formats**. Because it does not handle leap seconds, it is neither a linear representation of time nor a true representation of UTC.[note 3] Unix time may be checked on most Unix systems by typing date +%s on the command line. Source: Wikipedia.

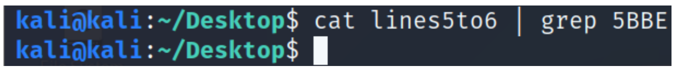
It probably won't change until 2038 (variable type size is large enough to store values) - https://en.wikipedia.org/wiki/Year_2038_problem

-- What about lines #5 & #6 ? --

Both lines start with the same header 6704 (Same data type), and ends with = or == (possible hint for base64 encoding of the field data itself).

Together, they contains more than 100k chars so we won't paste them all here but paste snippets:

Unfortunately , The id string '5BBE' isn't visible within these lines + just trying to apply base64decode on each of the lines (while skipping/removing the header 6704) won't help and we won't find in the output the '5BBE' string.

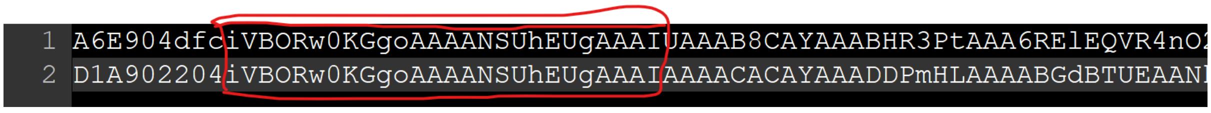

```
kali@kali:~/Desktop$ cat lines5to6 | grep 5BBE
kali@kali:~/Desktop$ 
```

BUT an id like **5A3F** as seen previously does appear in the search. [not all contacts has this piece of data saved, they might be missing other data types which others has]

So the input format still holds true:
<id(2bytes)><string_len(5bytes)><data>….<id><string_len><data>

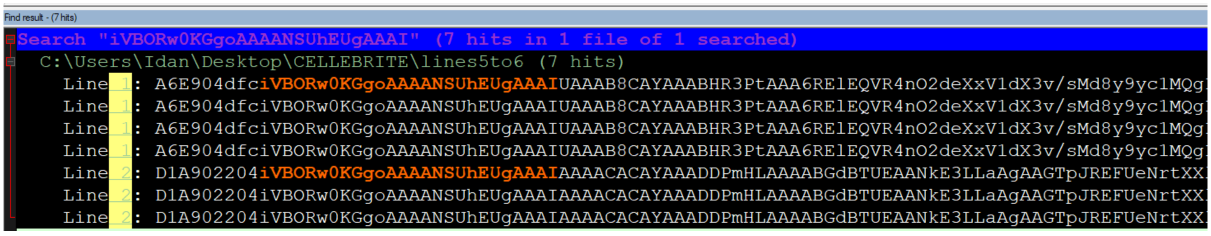
A sample for data length : 0x04dfc = = 19,964 bytes/chars, that's a lot and probably we are dealing with raw bytes/raw binary data of a non-text file (exactly 19KB (dividing by 1024), perhaps an icon/image).

We can see a repeating pattern in the data [we are looking for something like [“magic bytes/numbers”]



```
A6E904dfciVBORw0KGgoAAAANSUhEUgAAAIUAAAB8CAYAAABHR3PtAAA6RElEQVR4nO2
D1A902204iVBORw0KGgoAAAANSUhEUgAAAIAAAACACAYAAADDPmHLAAAABGdBTUEAAN
```

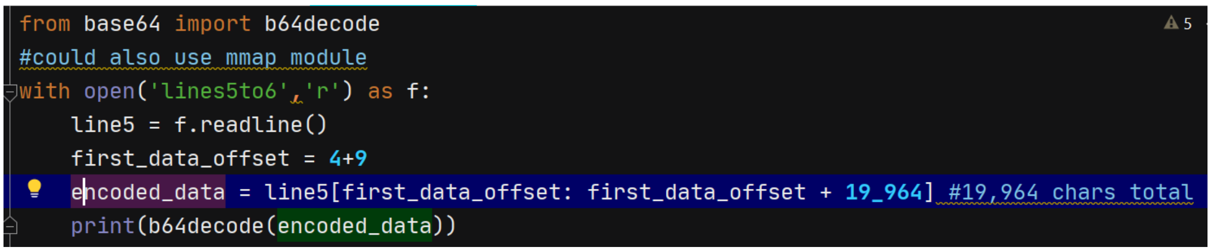
(a string which **occurs 7 times**. We will later see that **actually 9 contacts** has profile image)



```
Find result - (7 hits)
Search "iVBORw0KGgoAAAANSUhEUgAAAI" (7 hits in 1 file of 1 searched)
  C:\Users\Idan\Desktop\CELLEBRITE\lines5to6 (7 hits)
    Line 1: A6E904dfciVBORw0KGgoAAAANSUhEUgAAAIUAAAB8CAYAAABHR3PtAAA6RElEQVR4nO2deXxV1dX3v/sMd8y9yc1MQg
    Line 1: A6E904dfciVBORw0KGgoAAAANSUhEUgAAAIUAAAB8CAYAAABHR3PtAAA6RElEQVR4nO2deXxV1dX3v/sMd8y9yc1MQg
    Line 1: A6E904dfciVBORw0KGgoAAAANSUhEUgAAAIUAAAB8CAYAAABHR3PtAAA6RElEQVR4nO2deXxV1dX3v/sMd8y9yc1MQg
    Line 1: A6E904dfciVBORw0KGgoAAAANSUhEUgAAAIUAAAB8CAYAAABHR3PtAAA6RElEQVR4nO2deXxV1dX3v/sMd8y9yc1MQg
    Line 2: D1A902204iVBORw0KGgoAAAANSUhEUgAAAIAAAACACAYAAADDPmHLAAAABGdBTUEAANkE3LLaAgAAGTpJREFUeNrtXX
    Line 2: D1A902204iVBORw0KGgoAAAANSUhEUgAAAIAAAACACAYAAADDPmHLAAAABGdBTUEAANkE3LLaAgAAGTpJREFUeNrtXX
    Line 2: D1A902204iVBORw0KGgoAAAANSUhEUgAAAIAAAACACAYAAADDPmHLAAAABGdBTUEAANkE3LLaAgAAGTpJREFUeNrtXX
```

We notice something weird – the first data bytes should begin in index 10

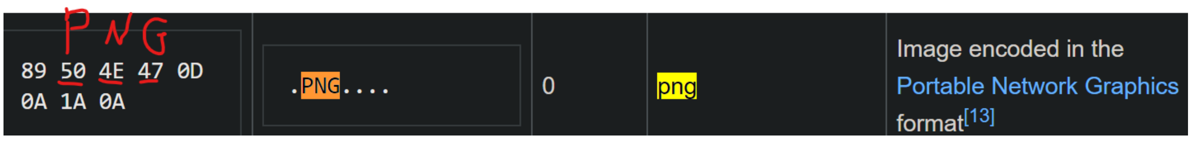
So let's try to base64 decode the first data field (of length 19,964 bytes/chars)



```python
from base64 import b64decode
#could also use mmap module
with open('lines5to6','r') as f:
    line5 = f.readline()
    first_data_offset = 4+9
    encoded_data = line5[first_data_offset: first_data_offset + 19_964] #19,964 chars total
    print(b64decode(encoded_data))
```

And we get:

b'\x89PNG\r\n\x1a\n\x00\x00\x00\rIHDR\x00\x00\x00\x85\x00\x00\x00|\x08\x06\x00\x00\x00GGs\xed\x00\x00:DIDATx\



89 50 4E 47 0D 0A 1A 0A	.PNG....	0	png	Image encoded in the Portable Network Graphics format[13]

Now we 'just' need to write a script/project to handle these tasks.

Here are the textual – results (first name whitespaces omitted):

```
Total contacts found: 26
---------------------------------------
Full name:
        Juanita Soto
Phone number(s):
        0352753831
        0633434984
        0389927752
Call logs:
        2012-08-27 14:25:15
---------------------------------------
Full name:
        MickaelBarrieLinwood Holmes
Phone number(s):
        03-46129559
Call logs:
        2012-12-11 17:48:40
---------------------------------------
Full name:
        VirgilRutHefin Welch
Phone number(s):
        0695304544
Call logs:
        2013-05-06 13:08:46
```

```
----------------------------------------
Full name:
            Ulla
Phone number(s):
            0693206727
Call logs:
            2012-08-20 10:37:32
----------------------------------------
Full name:
            Miguel Alvarez
Phone number(s):
            +54 (569) 9547 1740
Call logs:
            2012-01-08 10:27:07
----------------------------------------
Full name:
            Corey Griffith
Phone number(s):
            062966368
Call logs:
            2012-08-12 09:39:33
----------------------------------------
Full name:
            Andre Steele
Phone number(s):
            0487621854
Call logs:
            2012-06-17 16:06:32
----------------------------------------
Full name:
            Juana Bates
Phone number(s):
            048865961
Call logs:
            2012-02-20 18:06:01
----------------------------------------
Full name:
            Eloise Jenkins
Phone number(s):
            0354203289
Call logs:
            2012-02-22 20:19:08
----------------------------------------
Full name:
            Rudolph Banks
Phone number(s):
            054-446 3472
Call logs:
            2013-11-02 09:32:40
----------------------------------------
Full name:
            Cary Thompson
Phone number(s):
            0467674021
Call logs:
            2013-06-11 15:57:19
----------------------------------------
Full name:
            Felix West
Phone number(s):
            072-4621547
Call logs:
            2012-09-02 11:20:58
----------------------------------------
Full name:
            Wilma Gonzalez
Phone number(s):
            +54 (5655) 225 8210
Call logs:
            2012-07-01 15:02:42
----------------------------------------
Full name:
            olga Sims
Phone number(s):
            0893762571
Call logs:
            2012-11-23 19:38:13
----------------------------------------
Full name:
            Minnie Chavez
Phone number(s):
            0955772319
Call logs:
            2012-01-02 13:06:38
----------------------------------------
Full name:
            Jamie Greer
Phone number(s):
            0674542791
            078075896
            017041440
Call logs:
            2012-05-11 11:13:59
----------------------------------------
Full name:
            Marc Delgado
Phone number(s):
            0907216170
Call logs:
            2012-04-06 21:35:36
----------------------------------------
Full name:
            Lynda Chambers
Phone number(s):
Call logs:
            2013-03-10 20:01:57
----------------------------------------
Full name:
            Don Hall
Phone number(s):
            0550311777
            0859268458
Call logs:
            2012-11-23 08:52:18
```

```
----------------------------------------
Full name:
        Lee Austin
Phone number(s):
        0223104540
Call logs:
        2012-03-19 15:49:53
----------------------------------------
Full name:
        Elvira Powell
Phone number(s):
        0459735388
        0448806609
Call logs:
        2012-05-26 12:12:42
----------------------------------------
Full name:
        Timothy Hines
Phone number(s):
        0129734311
        059-603163
Call logs:
        2012-06-24 10:16:58
----------------------------------------
Full name:
        Winifred Tran
Phone number(s):
        0188577963
Call logs:
        2012-01-27 16:55:42
----------------------------------------
Full name:
        Elias Alvarado
Phone number(s):
        0891632801
Call logs:
        2012-08-20 09:30:50
----------------------------------------
Full name:
        Jessie Payne
Phone number(s):
        071-5312005
        0226514301
Call logs:
        2013-10-25 16:43:28
----------------------------------------
Full name:
        JephthaVeronikaKristen Tirrell
Phone number(s):
        0245395151
Call logs:
        2013-05-08 09:49:27
```