SecuriNets Quals CTF 2023 Submission

Fits under Misc, Codenamed Couch Potato

adm, @adlahbib

Contents

1 Introduction

This is a writeup for the Securinets Quals CTF 2023 possible challenge, which fits under the Misc category with a touch of OSINT. The challenge could be named Couch Potato by adm.

1.1 Description

It's past one, I was probably sleeping in front of my screen, I'm not even sure if I was awake for a bit or not, I'm not even sure if I'm dreaming or not… All I know is that I left the device on my favorite channel and that piece of crap failed me. Agh I need to fix it now. It is no longer responding to the commands I give it, and it is no longer showing my favorite channel! I hate my life, can you help me fix it?

I am looking for three stuff: - *What nonsense was I watching the night the device failed me? - I might need the Up and Down key codes? - The expiration date of my IPTV subscription.*

The flag should be: **Securinets{show_name_upkeycode_downkeycode_YYYYMMDD}** Thanks!

Score: 500 points I guess. Solves: TBA.

1.2 Attachment

A file called `dump.bin` was provided in a zip. Weighing 8 MB. Dating back to February the 1st, 2020. 1:07 AM.

Another file is what seems to be an updated firmware for the device, `Firmware.bin` weighing 4 MB. And dating back to August the 25th, 2020.

2 Analysis

A Couch potato is a lazy guy that sits in front of the TV screen, indicating that we are dealing with a console, set-top-box STB or Digital Video Recorder DVR and not a PCI card satellite/Tuner card or a computer. The user mentioned that he was watching his favorite channel when he fall asleep which make it more likely an STB, or a receiver for simplicity. This also means that the show name we are looking for was broadcasted in his favorite channel.

The user also mentioned that the device failed him, which means that the device is not responding to the commands he is sending to it. Kind of talking about a control unit, or that's clearly a remote control that has some keys malfunctioning, specifically the UP and DOWN arrow keys as we know.

On other hand, the user is suspecting that the IPTV subscription was the thing behind the interruption of his channel. This means that the IPTV subscription was a service provided by the device itself or maybe a third party service. This also means that the STB we're dealing with is a hybrid device, meaning that it can receive satellite signals and also IPTV, making it a 2nd generation STB and there are plenty in the market today, for third world countries.

However, the user could be mistaken as the channels that you can shortlist in the favorites are more likely to be satellite channels, hence the IPTV subscription is not the reason behind the interruption of his favorite channel rather than the satellite signal itself or the cardsharing service he is using.

Note for the readers: I can switch the last part of the flag to cardsharing expiration date instead of IPTV subscription expiration date.

With all that in mind, we can start our information gathering phase.

2.1 Information Gathering

TL;DR.

The thing is devices like this are hard to find in UK, Europe and the US. Unlike Africa and Asia. That's because in European countries and the US, they are mostly banned due to the fact that they are used for cardsharing and IPTV piracy. However, in Africa and Asia, they are still widely used and sold.

So where to look? These devices are not open source nor they have some kind of documentation is to where to look in their ROMs. Satellite forums, subreddits, and Facebook groups are good resources and some deep search would yield some useful tools and details to deal with dump. We kind of need to know how the memory is splitted. The file is indeed a ROM/EEPROM snapshot, so it has a mapping of the memory. We just need to know where the information part is, channel list is, and applications or services are.

The mapping generally includes the following:

- Bootloader
- Kernel or maincode
- User data
- Menu
- …

Each at specific offsets and specific lengths. The user data is the most important part as it contains the channel list.

Keep in mind that if the IPTV subscription was provided by the device itself, then the expiration date could be stored in the device itself or their renewal website. If the IPTV subscription was provided by a third party service, then the expiration date is stored in the third party service database or user panel. In both cases, we need to find the device serial number or MAC address to be able to identify the device and the user. I believe that how they are likely to be stored in the memory dump rather than a plain expiration date.

2.2 Resources

- https://www.satellites.co.uk/forums/
- https://www.reddit.com/r/satellite/
- https://www.tunisia-sat.com/forums/
- https://sat-universe.com/

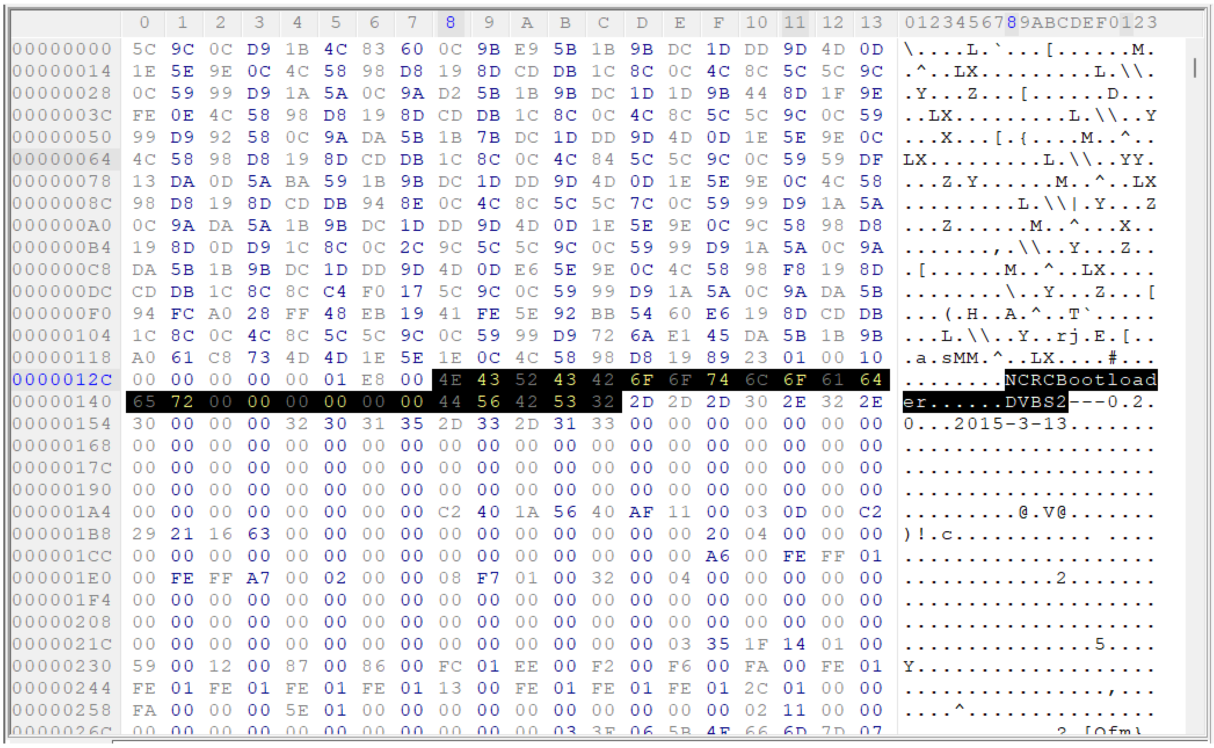
2.3 Tools

HexWorkshop / HxD Editor is a good tool to start with. It is a hex editor that can be used to view and edit files in hexadecimal and binary formats. It is a good tool to start with as it can be used to view the memory dump and search for strings. It can also be used to search for patterns and hex values.

2.4 Writeup

First, let’s investigate the dump file.

`NCRCBootloader` is the start point, which is the bootloader used for these chipsets as indicated in the Hex Editor screen: - ALI3329 - ALI3606 - ALI3601 - ALI3511 - ALI3510 - ALI3516 - ALI3618 - ALI3821



```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10 11 12 13  0123456789ABCDEF0123
00000000  5C 9C 0C D9 1B 4C 83 60 0C 9B E9 5B 1B 9B DC 1D DD 9D 4D 0D  \....L.`...[......M.
00000014  1E 5E 9E 0C 4C 58 98 D8 19 8D CD DB 1C 8C 0C 4C 8C 5C 5C 9C  .^..LX.........L.\\.
00000028  0C 59 99 D9 1A 5A 0C 9A D2 5B 1B 9B DC 1D 1D 9B 44 8D 1F 9E  .Y...Z...[......D...
0000003C  FE 0E 4C 58 98 D8 19 8D CD DB 1C 8C 0C 4C 8C 5C 5C 9C 0C 59  ..LX.........L.\\..Y
00000050  99 D9 92 58 0C 9A DA 5B 1B 7B DC 1D DD 9D 4D 0D 1E 5E 9E 0C  ...X...[.{....M..^..
00000064  4C 58 98 D8 19 8D CD DB 1C 8C 0C 4C 84 5C 5C 9C 0C 59 59 DF  LX.........L.\\..YY.
00000078  13 DA 0D 5A BA 59 1B 9B DC 1D DD 9D 4D 0D 1E 5E 9E 0C 4C 58  ...Z.Y......M..^..LX
0000008C  98 D8 19 8D CD DB 94 8E 0C 4C 8C 5C 5C 7C 0C 59 99 D9 1A 5A  .........L.\\|.Y...Z
000000A0  0C 9A DA 5A 1B 9B DC 1D DD 9D 4D 0D 1E 5E 9E 0C 9C 58 98 D8  ...Z......M..^...X..
000000B4  19 8D 0D D9 1C 8C 0C 2C 9C 5C 5C 9C 0C 59 99 D9 1A 5A 0C 9A  .......,.\\..Y...Z..
000000C8  DA 5B 1B 9B DC 1D DD 9D 4D 0D E6 5E 9E 0C 4C 58 98 F8 19 8D  .[......M..^..LX....
000000DC  CD DB 1C 8C 8C C4 F0 17 5C 9C 0C 59 99 D9 1A 5A 0C 9A DA 5B  ........\..Y...Z...[
000000F0  94 FC A0 28 FF 48 EB 19 41 FE 5E 92 BB 54 60 E6 19 8D CD DB  ...(.H..A.^..T`.....
00000104  1C 8C 0C 4C 8C 5C 5C 9C 0C 59 99 D9 72 6A E1 45 DA 5B 1B 9B  ...L.\\..Y..rj.E.[..
00000118  A0 61 C8 73 4D 4D 1E 5E 1E 0C 4C 58 98 D8 19 89 23 01 00 10  .a.sMM.^..LX....#...
0000012C  00 00 00 00 00 01 E8 00 4E 43 52 43 42 6F 6F 74 6C 6F 61 64  ........NCRCBootload
00000140  65 72 00 00 00 00 00 00 44 56 42 53 32 2D 2D 2D 30 2E 32 2E  er......DVBS2---0.2.
00000154  30 00 00 00 32 30 31 35 2D 33 2D 31 33 00 00 00 00 00 00 00  0...2015-3-13.......
00000168  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....................
0000017C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....................
00000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....................
000001A4  00 00 00 00 00 00 00 00 C2 40 1A 56 40 AF 11 00 03 0D 00 C2  .........@.V@.......
000001B8  29 21 16 63 00 00 00 00 00 00 00 00 00 00 00 20 04 00 00 00  )!.c........... ....
000001CC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A6 00 FE FF 01  ....................
000001E0  00 FE FF A7 00 02 00 00 08 F7 01 00 32 00 04 00 00 00 00 00  ............2.......
000001F4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....................
00000208  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....................
0000021C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 35 1F 14 01 00  ...............5....
00000230  59 00 12 00 87 00 86 00 FC 01 EE 00 F2 00 F6 00 FA 00 FE 01  Y...................
00000244  FE 01 FE 01 FE 01 FE 01 13 00 FE 01 FE 01 FE 01 2C 01 00 00  ................,...
00000258  FA 00 00 00 5E 01 00 00 00 00 00 00 00 00 00 00 02 11 00 00  ....^...............
0000026C  00 00 00 00 00 00 00 00 00 00 00 03 3F 06 5B 4F 66 6D 7D 07  ...........?.[Ofm}.
```

Devices with those chipset have these brands *Starsat, Sunplus, Tiger, StarMax, Geant, Mediastar, QMAX, AzAmerica, Samsat and many more…*

And all of their built-in subscriptions are part of **Gosat**.

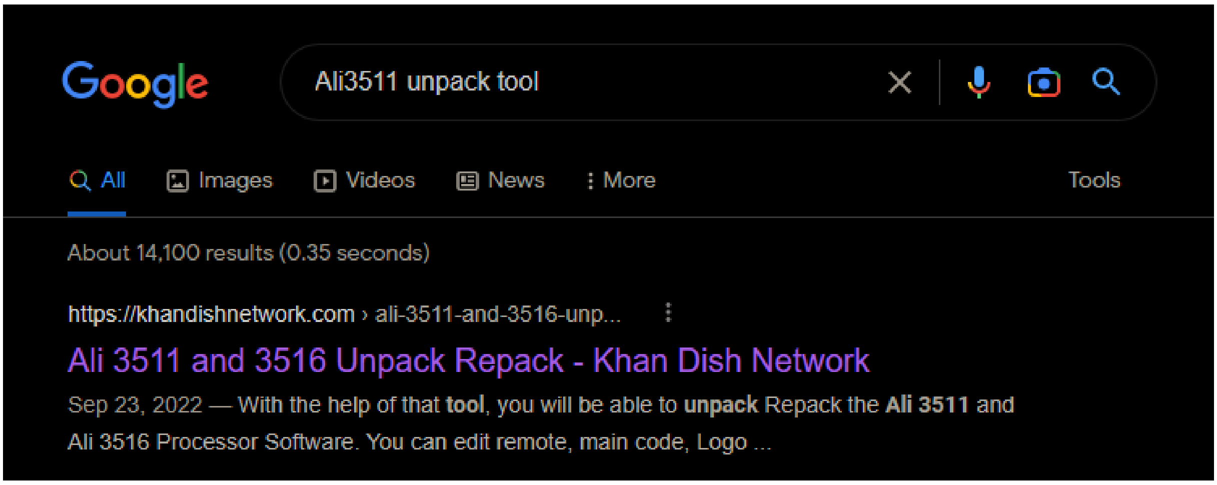
Now, to actually find the specific brand and model, we need to inspect the firmware update file.

To clear things up, the memory dump serves for user data mainly the channels and services as I said while the firmware update file will indicate the remote control being used.

The memory dump is a mapping and can be splitted manually and further investigated. However the firmware is encrypted, you can tell by a first glance, no strings or something in there, and can’t help us much to delve into the remote control unit in use.

Time to google for a way to decrypt such chipset firmware. Let’s use the keyword `ALI3329` or `ALI3511` as they are the most common chipset used in these devices and combine the search with decrypt or unpack tool.

For example:



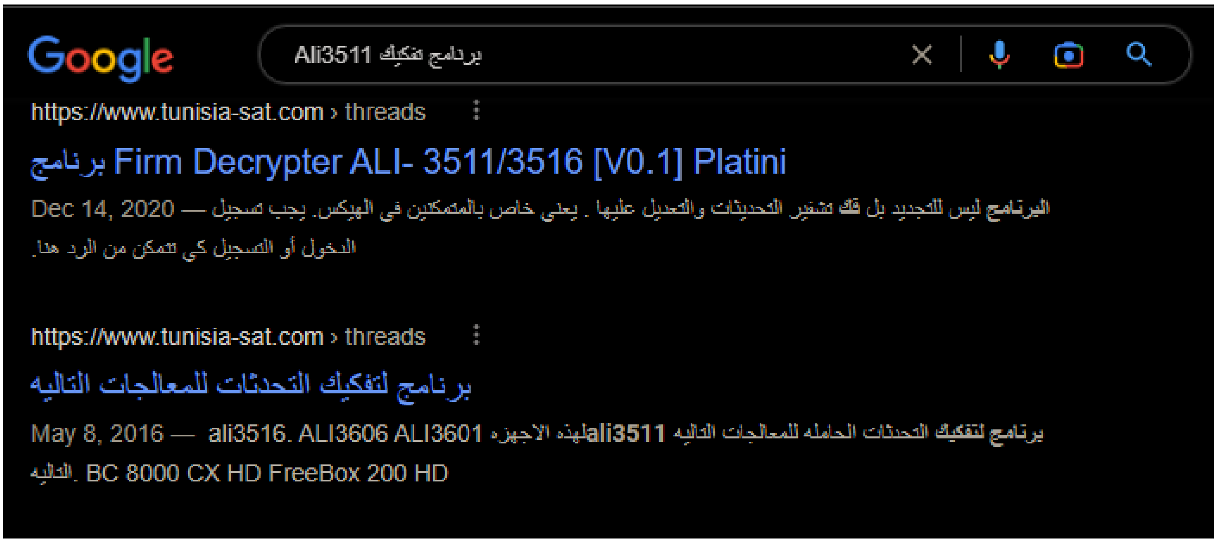
About 14,100 results (0.35 seconds)

https://khandishnetwork.com › ali-3511-and-3516-unp...

Ali 3511 and 3516 Unpack Repack - Khan Dish Network

Sep 23, 2022 — With the help of that **tool**, you will be able to **unpack** Repack the **Ali 3511** and Ali 3516 Processor Software. You can edit remote, main code, Logo ...

And in Arabic:



https://www.tunisia-sat.com › threads

برنامج Firm Decrypter ALI- 3511/3516 [V0.1] Platini

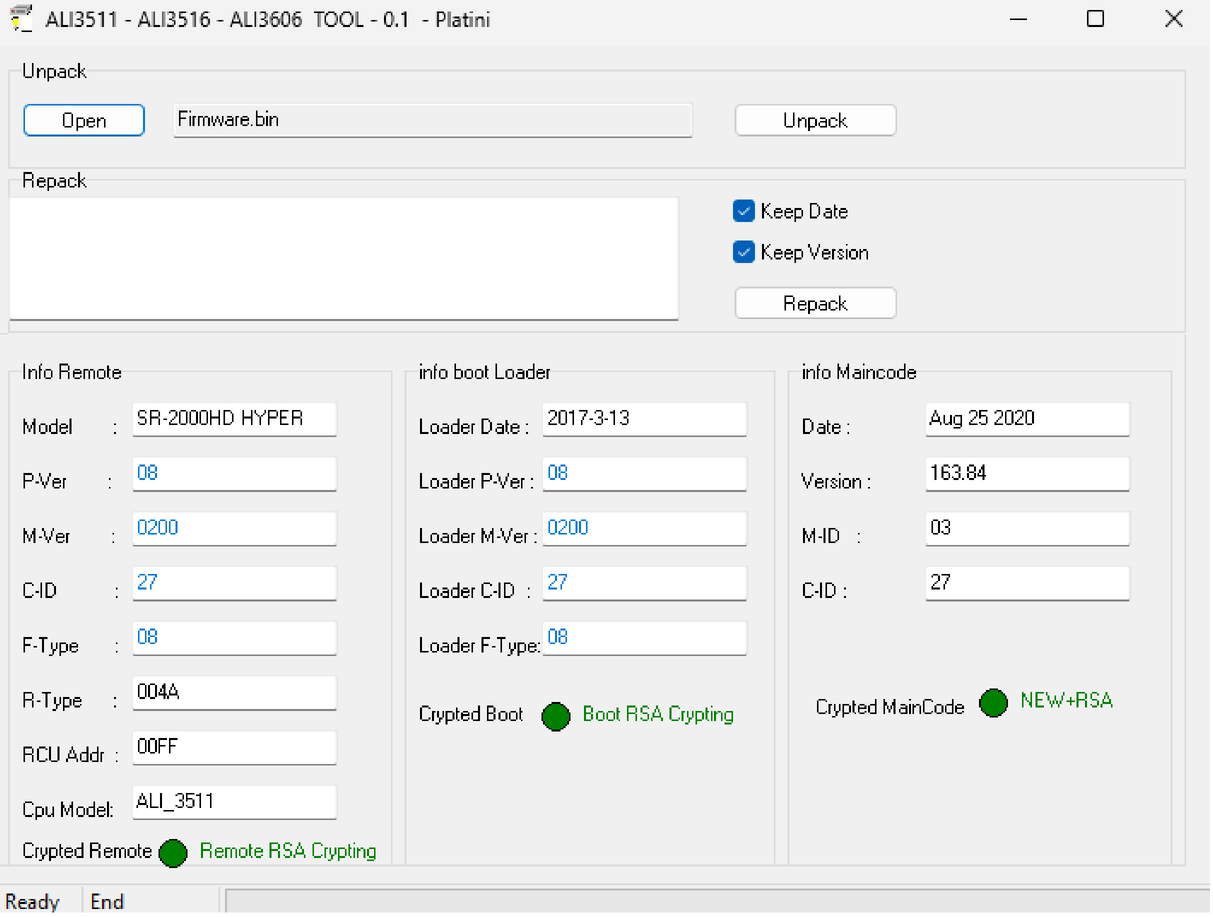
Dec 14, 2020 — البرنامج ليس للتجديد بل فك تشفير التحديثات والتعديل عليها . يعني خاص بالمتمكنين في الهيكس. يجب تسجيل الدخول أو التسجيل كي تتمكن من الرد هنا.

https://www.tunisia-sat.com › threads

برنامج لتفكيك التحدثات للمعالجات التاليه

May 8, 2016 — برنامج لتفكيك التحدثات الحامله للمعالجات التاليه **ali3511** لهذه الاجهزه ALI3601 ALI3606 ali3516. BC 8000 CX HD FreeBox 200 HD التاليه.

Using the tool, we determine that the model is SR-2000HD HYPER and the remote control is SR-2000HD HYPER. Hence the brand is Starsat.



ALI3511 - ALI3516 - ALI3606 TOOL - 0.1 - Platini

Unpack

Open Firmware.bin Unpack

Repack

☑ Keep Date
☑ Keep Version

Repack

Info Remote

Model : SR-2000HD HYPER
P-Ver : 08
M-Ver : 0200
C-ID : 27
F-Type : 08
R-Type : 004A
RCU Addr : 00FF
Cpu Model: ALI_3511
Crypted Remote ● Remote RSA Crypting

info boot Loader

Loader Date : 2017-3-13
Loader P-Ver : 08
Loader M-Ver : 0200
Loader C-ID : 27
Loader F-Type: 08
Crypted Boot ● Boot RSA Crypting

info Maincode

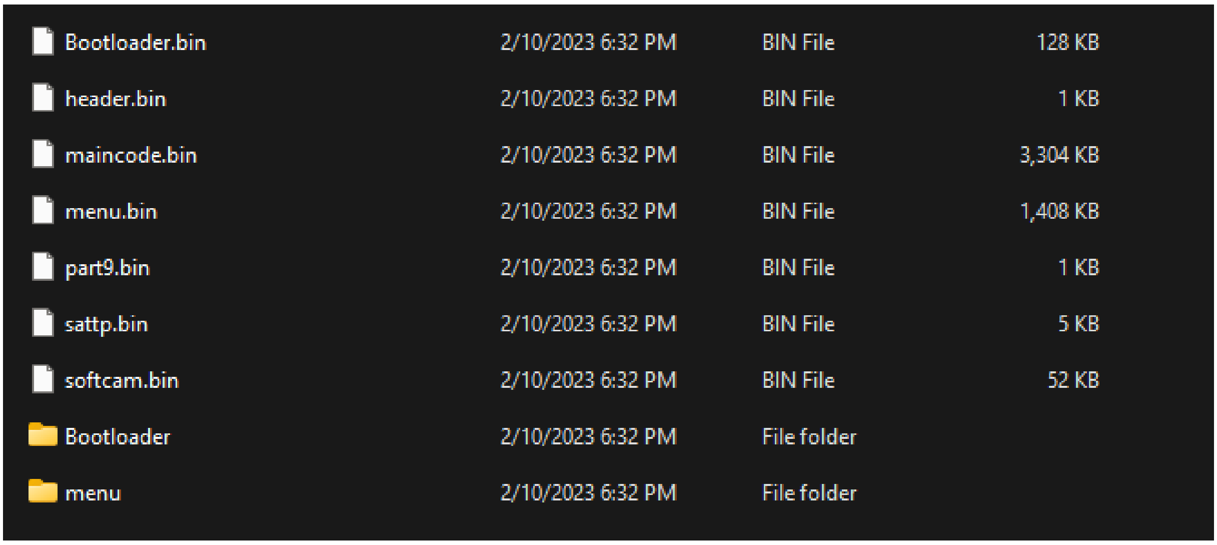
Date : Aug 25 2020
Version : 163.84
M-ID : 03
C-ID : 27
Crypted MainCode ● NEW+RSA

Ready End

The unpack and repack features are used to decrypt and extract parts of the firmware like the bootloader, maincode, user data if any was supplied by the manufacturer, the menu, the remote, and sometimes a softcam (that's out of our scope today, maybe in another challenge!). And the repack to insert modified parts and RSA encrypt the whole thing again. Like for instance, we can insert the main menu (including themes and applications) or the remote control unit of a different model or brand and repack it to be used with the device we have, as long as they are using the very same chipset. Well this time, rest assured it is the Hyper remote control and when we talk about key code we mean the IR Infrared key code.

So the whole memory dump thing and the firmware kind of contain similar stuff at least, one being encrypted and the other not.

See here, the content of the folder when unpacked.

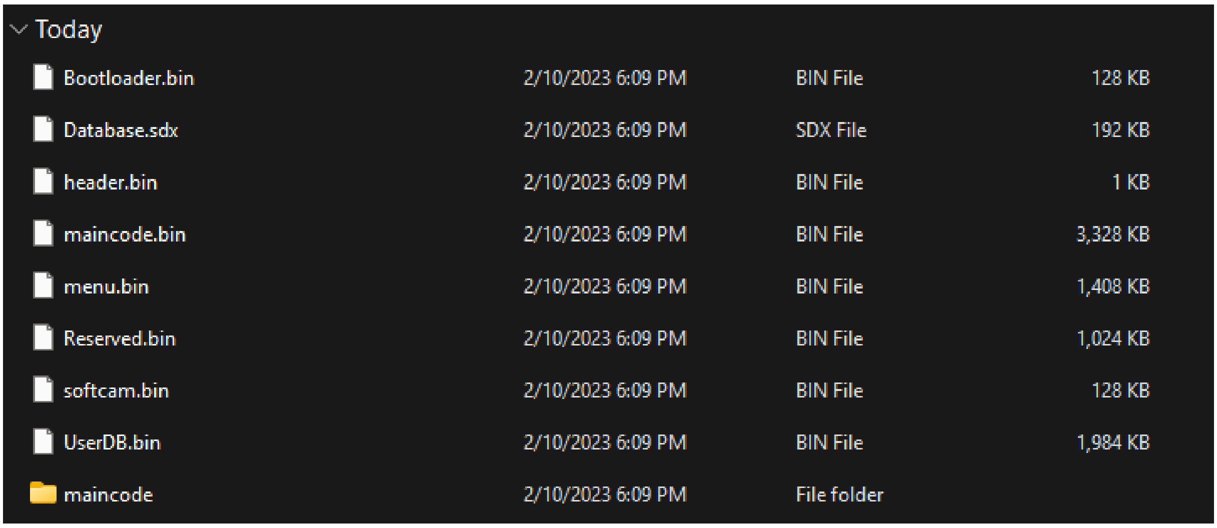


Bootloader.bin	2/10/2023 6:32 PM	BIN File	128 KB
header.bin	2/10/2023 6:32 PM	BIN File	1 KB
maincode.bin	2/10/2023 6:32 PM	BIN File	3,304 KB
menu.bin	2/10/2023 6:32 PM	BIN File	1,408 KB
part9.bin	2/10/2023 6:32 PM	BIN File	1 KB
sattp.bin	2/10/2023 6:32 PM	BIN File	5 KB
softcam.bin	2/10/2023 6:32 PM	BIN File	52 KB
Bootloader	2/10/2023 6:32 PM	File folder	
menu	2/10/2023 6:32 PM	File folder	

So why not, giving the dump a try and unpack it as well, we are chasing the user data part anyway. And the tool might very much help. Otherwise I will show how to proceed manually knowing the offsets and lengths found on a forum.

2.4.1 Finding the show

As I said before, we can deal with this part either using the tool or manually. Well, the tool was able to yield this:



Today

Bootloader.bin	2/10/2023 6:09 PM	BIN File	128 KB
Database.sdx	2/10/2023 6:09 PM	SDX File	192 KB
header.bin	2/10/2023 6:09 PM	BIN File	1 KB
maincode.bin	2/10/2023 6:09 PM	BIN File	3,328 KB
menu.bin	2/10/2023 6:09 PM	BIN File	1,408 KB
Reserved.bin	2/10/2023 6:09 PM	BIN File	1,024 KB
softcam.bin	2/10/2023 6:09 PM	BIN File	128 KB
UserDB.bin	2/10/2023 6:09 PM	BIN File	1,984 KB
maincode	2/10/2023 6:09 PM	File folder	

Very nice, I can see `database.sdx` file there!

Well, to proceed manullay you need to know the offsets and lengths beforehand. This is what I meant:

```
++++++++++++++++++++++++++++++++++++++
Name : Bootloader.bin
SIZE : 128,00 KB
CRC : 0x00AF7F6C
offset : 0x00000128
++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++
Name : maincode.bin
SIZE : 3,25 MB
CRC : 0x19E8C348
offset : 0x00020128
++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++
Name : menu.bin
SIZE : 1,38 MB
CRC : 0x10934143
offset : 0x00360128
++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++
Name : Database.sdx
SIZE : 9,80 KB
CRC : 0x00146C71
offset : 0x004C0128
++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++
Name : softcam.bin
SIZE : 42,38 KB
CRC : 0x008D5F15
offset : 0x004C2860
++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++
Name : sattp.bin
SIZE : 12,54 KB
CRC : 0x00097FDA
offset : 0x004CD1E8
++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++
Name : Padding.bin
SIZE : 522,06 KB
```

```
CRC : 0x040E1F6B
offset : 0x004D040C
++++++++++++++++++++++++++++++++++++++
```

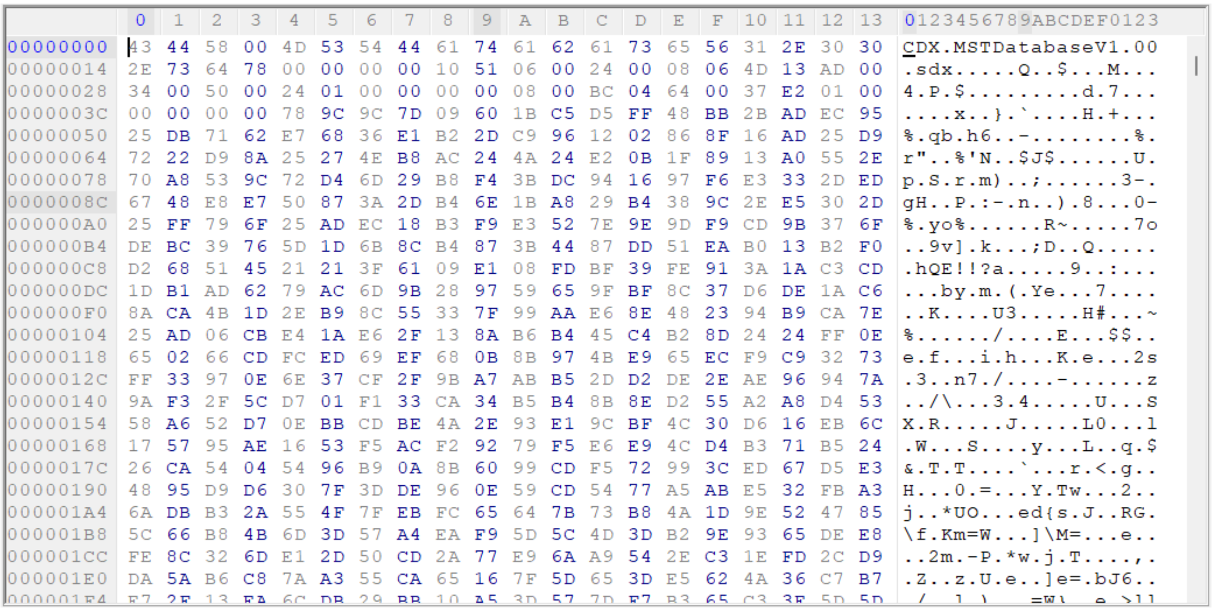
Found here: https://www.tunisia-sat.com/forums/threads/3242761/page-47

We know `database.sdx` holds the user data meaning the channels. sattp is another file that holds the different satellites and their frequencies aka transponders.

When we open the file in a hex editor, We can't read any useful information out of it. This means that there should be a tool in place to view and edit the channels for the specific chipset family we are dealing with as the file seems highly compressed.

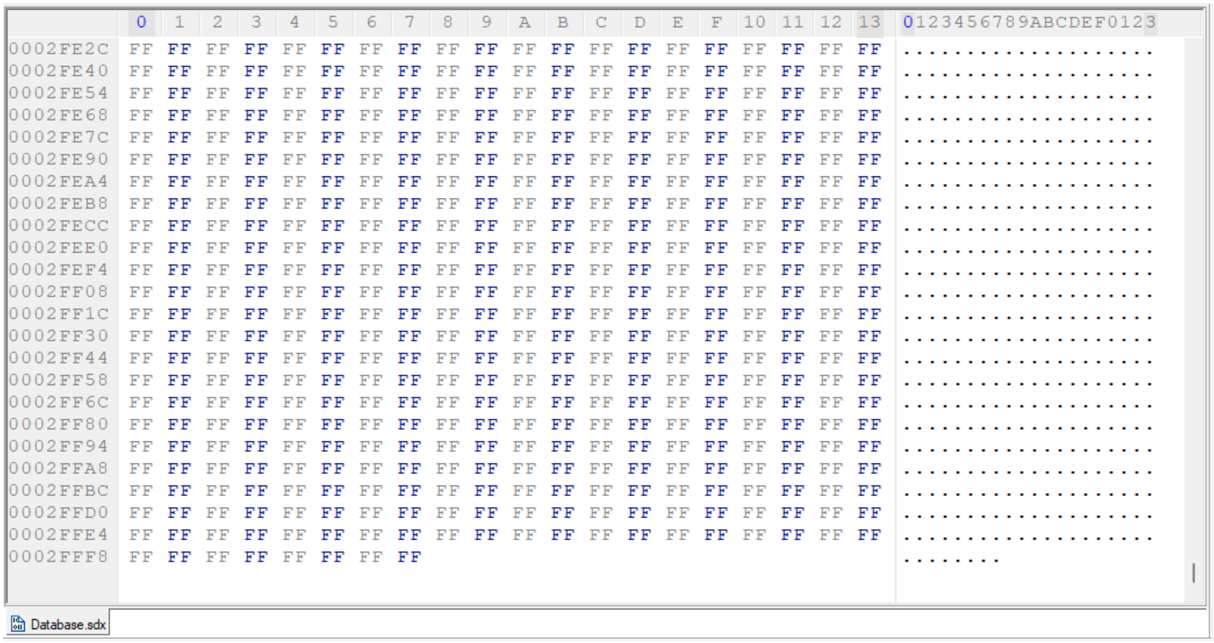
Here's a view from hex editor first.

Starts off like this



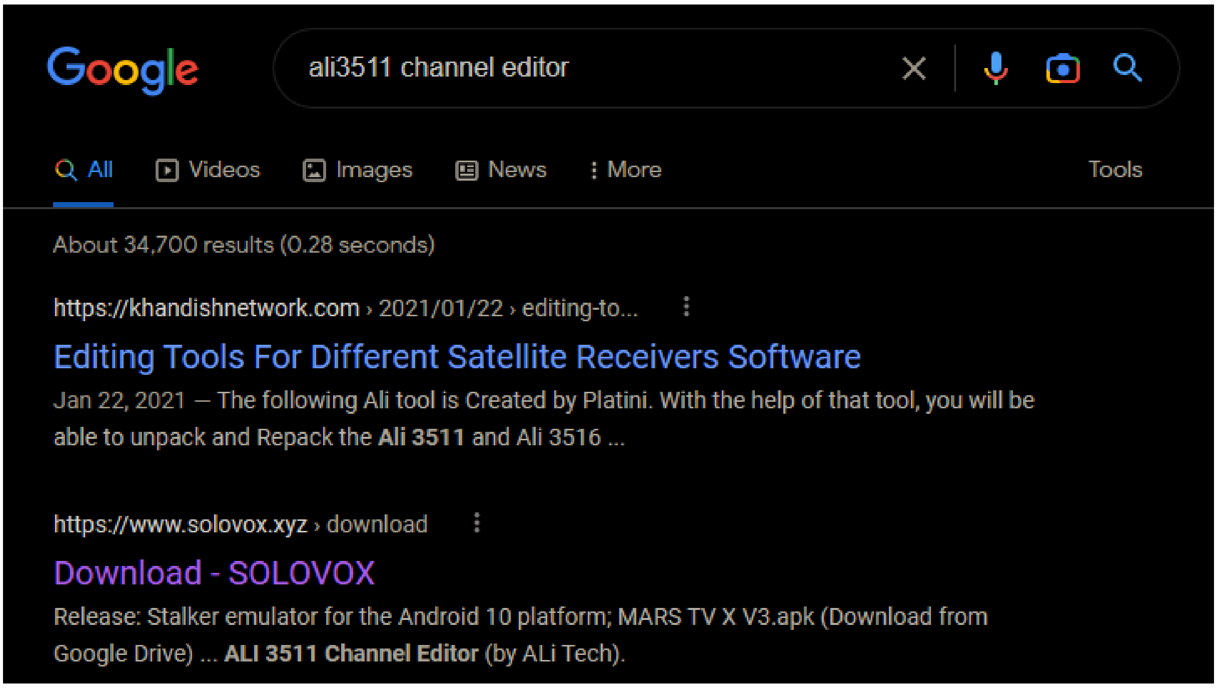
```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10 11 12 13  0123456789ABCDEF0123
00000000  43 44 58 00 4D 53 54 44 61 74 61 62 61 73 65 56 31 2E 30 30  CDX.MSTDatabaseV1.00
00000014  2E 73 64 78 00 00 00 00 10 51 06 00 24 00 08 06 4D 13 AD 00  .sdx.....Q..$...M...
00000028  34 00 50 00 24 01 00 00 00 00 08 00 BC 04 64 00 37 E2 01 00  4.P.$.........d.7...
0000003C  00 00 00 00 78 9C 9C 7D 09 60 1B C5 D5 FF 48 BB 2B AD EC 95  ....x..}.`....H.+...
00000050  25 DB 71 62 E7 68 36 E1 B2 2D C9 96 12 02 86 8F 16 AD 25 D9  %.qb.h6..-........%.
00000064  72 22 D9 8A 25 27 4E B8 AC 24 4A 24 E2 0B 1F 89 13 A0 55 2E  r"..%'N..$J$......U.
00000078  70 A8 53 9C 72 D4 6D 29 B8 F4 3B DC 94 16 97 F6 E3 33 2D ED  p.S.r.m)..;......3-.
0000008C  67 48 E8 E7 50 87 3A 2D B4 6E 1B A8 29 B4 38 9C 2E E5 30 2D  gH..P.:-.n..).8...0-
000000A0  25 FF 79 6F 25 AD EC 18 B3 F9 E3 52 7E 9E 9D F9 CD 9B 37 6F  %.yo%......R~.....7o
000000B4  DE BC 39 76 5D 1D 6B 8C B4 87 3B 44 87 DD 51 EA B0 13 B2 F0  ..9v].k...;D..Q.....
000000C8  D2 68 51 45 21 21 3F 61 09 E1 08 FD BF 39 FE 91 3A 1A C3 CD  .hQE!!?a.....9..:...
000000DC  1D B1 AD 62 79 AC 6D 9B 28 97 59 65 9F BF 8C 37 D6 DE 1A C6  ...by.m.(.Ye...7....
000000F0  8A CA 4B 1D 2E B9 8C 55 33 7F 99 AA E6 8E 48 23 94 B9 CA 7E  ..K....U3.....H#...~
00000104  25 AD 06 CB E4 1A E6 2F 13 8A B6 B4 45 C4 B2 8D 24 24 FF 0E  %....../....E...$$..
00000118  65 02 66 CD FC ED 69 EF 68 0B 8B 97 4B E9 65 EC F9 C9 32 73  e.f...i.h...K.e...2s
0000012C  FF 33 97 0E 6E 37 CF 2F 9B A7 AB B5 2D D2 DE 2E AE 96 94 7A  .3..n7./....-......z
00000140  9A F3 2F 5C D7 01 F1 33 CA 34 B5 B4 8B 8E D2 55 A2 A8 D4 53  ../\...3.4.....U...S
00000154  58 A6 52 D7 0E BB CD BE 4A 2E 93 E1 9C BF 4C 30 D6 16 EB 6C  X.R.....J.....L0...l
00000168  17 57 95 AE 16 53 F5 AC F2 92 79 F5 E6 E9 4C D4 B3 71 B5 24  .W...S....y...L..q.$
0000017C  26 CA 54 04 54 96 B9 0A 8B 60 99 CD F5 72 99 3C ED 67 D5 E3  &.T.T....`...r.<.g..
00000190  48 95 D9 D6 30 7F 3D DE 96 0E 59 CD 54 77 A5 AB E5 32 FB A3  H...0.=...Y.Tw...2..
000001A4  6A DB B3 2A 55 4F 7F EB FC 65 64 7B 73 B8 4A 1D 9E 52 47 85  j..*UO...ed{s.J..RG.
000001B8  5C 66 B8 4B 6D 3D 57 A4 EA F9 5D 5C 4D 3D B2 9E 93 65 DE E8  \f.Km=W...]\M=...e..
000001CC  FE 8C 32 6D E1 2D 50 CD 2A 77 E9 6A A9 54 2E C3 1E FD 2C D9  ..2m.-P.*w.j.T....,.
000001E0  DA 5A B6 C8 7A A3 55 CA 65 16 7F 5D 65 3D E5 62 4A 36 C7 B7  .Z..z.U.e..]e=.bJ6..
000001F4  E7 2F 13 FA 6C DB 29 BB 10 A5 3D 57 7D F7 B3 65 C3 3F 5D 5D  ./..l.)....=W}..e.?]]
```

And ends padded with 0xFF



```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10 11 12 13  0123456789ABCDEF0123
0002FE2C  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FE40  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FE54  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FE68  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FE7C  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FE90  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FEA4  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FEB8  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FECC  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FEE0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FEF4  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FF08  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FF1C  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FF30  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FF44  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FF58  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FF6C  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FF80  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FF94  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FFA8  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FFBC  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FFD0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FFE4  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....................
0002FFF8  FF FF FF FF FF FF FF FF                                      ........
```

Let's google a bit…



ali3511 channel editor

About 34,700 results (0.28 seconds)

https://khandishnetwork.com › 2021/01/22 › editing-to...

Editing Tools For Different Satellite Receivers Software

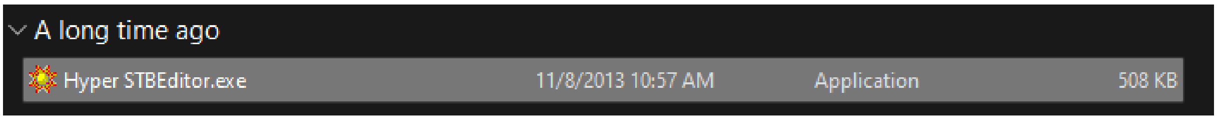
Jan 22, 2021 — The following Ali tool is Created by Platini. With the help of that tool, you will be able to unpack and Repack the **Ali 3511** and Ali 3516 ...

https://www.solovox.xyz › download

Download - SOLOVOX

Release: Stalker emulator for the Android 10 platform; MARS TV X V3.apk (Download from Google Drive) ... **ALI 3511 Channel Editor** (by ALi Tech).

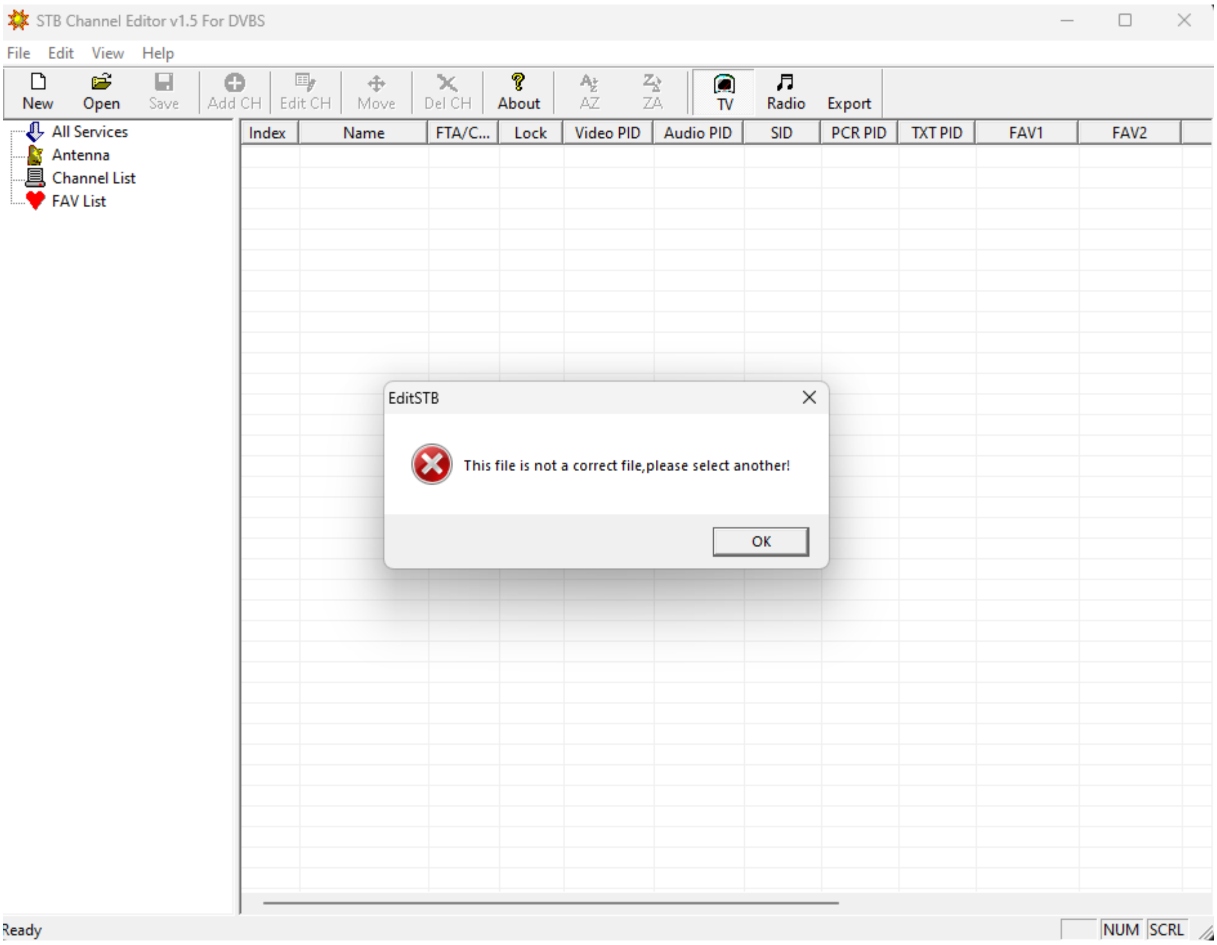
I got this



A long time ago

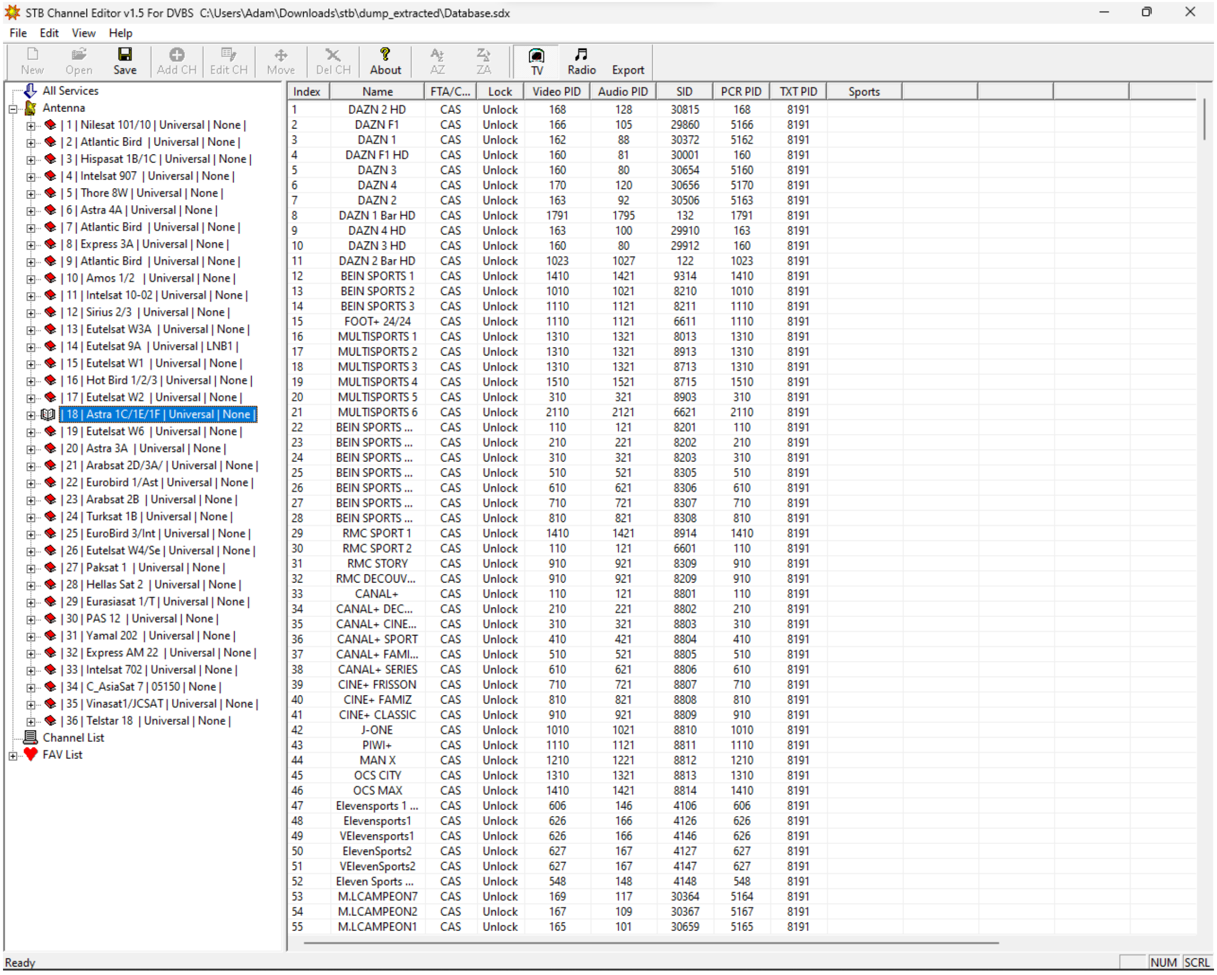
Hyper STBEditor.exe 11/8/2013 10:57 AM Application 508 KB

When trying to first open the database, I got this error message


STB Channel Editor v1.5 For DVBS
File Edit View Help
New Open Save Add CH Edit CH Move Del CH About AZ ZA TV Radio Export
All Services
Antenna
Channel List
FAV List
Index Name FTA/C... Lock Video PID Audio PID SID PCR PID TXT PID FAV1 FAV2
EditSTB
OK
Ready
NUM SCRL

This file is not a correct file,please select another!

And the issue is that the Userdata has a static size as indicated before. As the receiver's capacity fits a maximum of 6100 channels. So the database file is padded with 0xFF to reach the maximum size. Let's get rid of the padded data and try again..



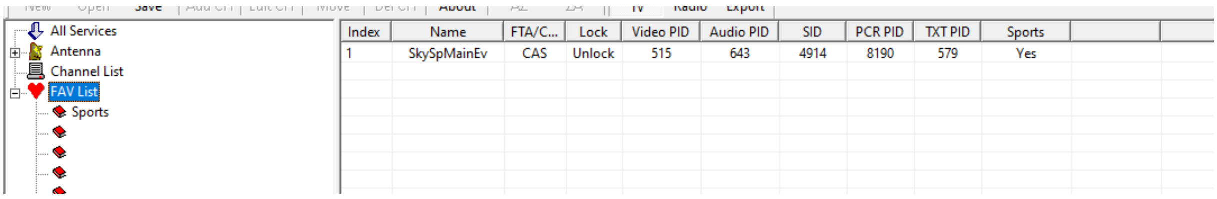
STB Channel Editor v1.5 For DVBS C:\Users\Adam\Downloads\stb\dump_extracted\Database.sdx

All Services
Antenna
1	Nilesat 101/10	Universal	None
2	Atlantic Bird	Universal	None
3	Hispasat 1B/1C	Universal	None
4	Intelsat 907	Universal	None
5	Thore 8W	Universal	None
6	Astra 4A	Universal	None
7	Atlantic Bird	Universal	None
8	Express 3A	Universal	None
9	Atlantic Bird	Universal	None
10	Amos 1/2	Universal	None
11	Intelsat 10-02	Universal	None
12	Sirius 2/3	Universal	None
13	Eutelsat W3A	Universal	None
14	Eutelsat 9A	Universal	LNB1
15	Eutelsat W1	Universal	None
16	Hot Bird 1/2/3	Universal	None
17	Eutelsat W2	Universal	None
18	Astra 1C/1E/1F	Universal	None
19	Eutelsat W6	Universal	None
20	Astra 3A	Universal	None
21	Arabsat 2D/3A/	Universal	None
22	Eurobird 1/Ast	Universal	None
23	Arabsat 2B	Universal	None
24	Turksat 1B	Universal	None
25	EuroBird 3/Int	Universal	None
26	Eutelsat W4/Se	Universal	None
27	Paksat 1	Universal	None
28	Hellas Sat 2	Universal	None
29	Eurasiasat 1/T	Universal	None
30	PAS 12	Universal	None
31	Yamal 202	Universal	None
32	Express AM 22	Universal	None
33	Intelsat 702	Universal	None
34	C_AsiaSat 7	05150	None
35	Vinasat1/JCSAT	Universal	None
36	Telstar 18	Universal	None
Channel List
FAV List

Index	Name	FTA/C...	Lock	Video PID	Audio PID	SID	PCR PID	TXT PID	Sports
1	DAZN 2 HD	CAS	Unlock	168	128	30815	168	8191	
2	DAZN F1	CAS	Unlock	166	105	29860	5166	8191	
3	DAZN 1	CAS	Unlock	162	88	30372	5162	8191	
4	DAZN F1 HD	CAS	Unlock	160	81	30001	160	8191	
5	DAZN 3	CAS	Unlock	160	80	30654	5160	8191	
6	DAZN 4	CAS	Unlock	170	120	30656	5170	8191	
7	DAZN 2	CAS	Unlock	163	92	30506	5163	8191	
8	DAZN 1 Bar HD	CAS	Unlock	1791	1795	132	1791	8191	
9	DAZN 4 HD	CAS	Unlock	163	100	29910	163	8191	
10	DAZN 3 HD	CAS	Unlock	160	80	29912	160	8191	
11	DAZN 2 Bar HD	CAS	Unlock	1023	1027	122	1023	8191	
12	BEIN SPORTS 1	CAS	Unlock	1410	1421	9314	1410	8191	
13	BEIN SPORTS 2	CAS	Unlock	1010	1021	8210	1010	8191	
14	BEIN SPORTS 3	CAS	Unlock	1110	1121	8211	1110	8191	
15	FOOT+ 24/24	CAS	Unlock	1110	1121	6611	1110	8191	
16	MULTISPORTS 1	CAS	Unlock	1310	1321	8013	1310	8191	
17	MULTISPORTS 2	CAS	Unlock	1310	1321	8913	1310	8191	
18	MULTISPORTS 3	CAS	Unlock	1310	1321	8713	1310	8191	
19	MULTISPORTS 4	CAS	Unlock	1510	1521	8715	1510	8191	
20	MULTISPORTS 5	CAS	Unlock	310	321	8903	310	8191	
21	MULTISPORTS 6	CAS	Unlock	2110	2121	6621	2110	8191	
22	BEIN SPORTS ...	CAS	Unlock	110	121	8201	110	8191	
23	BEIN SPORTS ...	CAS	Unlock	210	221	8202	210	8191	
24	BEIN SPORTS ...	CAS	Unlock	310	321	8203	310	8191	
25	BEIN SPORTS ...	CAS	Unlock	510	521	8305	510	8191	
26	BEIN SPORTS ...	CAS	Unlock	610	621	8306	610	8191	
27	BEIN SPORTS ...	CAS	Unlock	710	721	8307	710	8191	
28	BEIN SPORTS ...	CAS	Unlock	810	821	8308	810	8191	
29	RMC SPORT 1	CAS	Unlock	1410	1421	8914	1410	8191	
30	RMC SPORT 2	CAS	Unlock	110	121	6601	110	8191	
31	RMC STORY	CAS	Unlock	910	921	8309	910	8191	
32	RMC DECOUV...	CAS	Unlock	910	921	8209	910	8191	
33	CANAL+	CAS	Unlock	110	121	8801	110	8191	
34	CANAL+ DEC...	CAS	Unlock	210	221	8802	210	8191	
35	CANAL+ CINE...	CAS	Unlock	310	321	8803	310	8191	
36	CANAL+ SPORT	CAS	Unlock	410	421	8804	410	8191	
37	CANAL+ FAMI...	CAS	Unlock	510	521	8805	510	8191	
38	CANAL+ SERIES	CAS	Unlock	610	621	8806	610	8191	
39	CINE+ FRISSON	CAS	Unlock	710	721	8807	710	8191	
40	CINE+ FAMIZ	CAS	Unlock	810	821	8808	810	8191	
41	CINE+ CLASSIC	CAS	Unlock	910	921	8809	910	8191	
42	J-ONE	CAS	Unlock	1010	1021	8810	1010	8191	
43	PIWI+	CAS	Unlock	1110	1121	8811	1110	8191	
44	MAN X	CAS	Unlock	1210	1221	8812	1210	8191	
45	OCS CITY	CAS	Unlock	1310	1321	8813	1310	8191	
46	OCS MAX	CAS	Unlock	1410	1421	8814	1410	8191	
47	Elevensports 1 ...	CAS	Unlock	606	146	4106	606	8191	
48	Elevensports1	CAS	Unlock	626	166	4126	626	8191	
49	VElevensports1	CAS	Unlock	626	166	4146	626	8191	
50	ElevenSports2	CAS	Unlock	627	167	4127	627	8191	
51	VElevenSports2	CAS	Unlock	627	167	4147	627	8191	
52	Eleven Sports ...	CAS	Unlock	548	148	4148	548	8191	
53	M.LCAMPEON7	CAS	Unlock	169	117	30364	5164	8191	
54	M.LCAMPEON2	CAS	Unlock	167	109	30367	5167	8191	
55	M.LCAMPEON1	CAS	Unlock	165	101	30659	5165	8191	

Now, it's working like charm, and I already see some familiar TV channels on Astra 1 (19.2 East).

Let's expand the favorites section



All Services
Antenna
Channel List
FAV List
Sports

Index	Name	FTA/C...	Lock	Video PID	Audio PID	SID	PCR PID	TXT PID	Sports
1	SkySpMainEv	CAS	Unlock	515	643	4914	8190	579	Yes

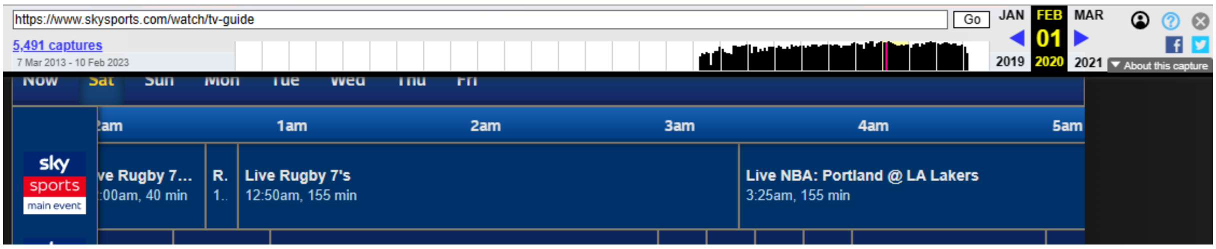
And there is Sky Sports Main Event, UK-based sports channel that is part of BSkyB or Sky Group, pay-television channel and availble for satellite subsribers via Eurobird 1, Astra 2 (28.2 East). Sky Sports Main Event broadcasts the biggest events of sports in the UK.

Now, great work to reach this point, but we are not done yet. We need to find the right show at that past date, meaning at 1:07 AM on February the 1st, 2020.

Well, Sky TV Guide won't keep such data for more than a week or two, so we need to find another way.

I guess you know what I mean, what else than the way back machine!

Head over to archive.org and submit the link for the Sky TV Guide and try to narrow your search to a date that's equal or close to the date in question, as shown below!



https://www.skysports.com/watch/tv-guide

5,491 captures
7 Mar 2013 - 10 Feb 2023

ve Rugby 7… :00am, 40 min

R. 1..

Live Rugby 7's 12:50am, 155 min

Live NBA: Portland @ LA Lakers 3:25am, 155 min

And that is the first part of the flag: `live_rugby_7's` or `live_rugby_7s`

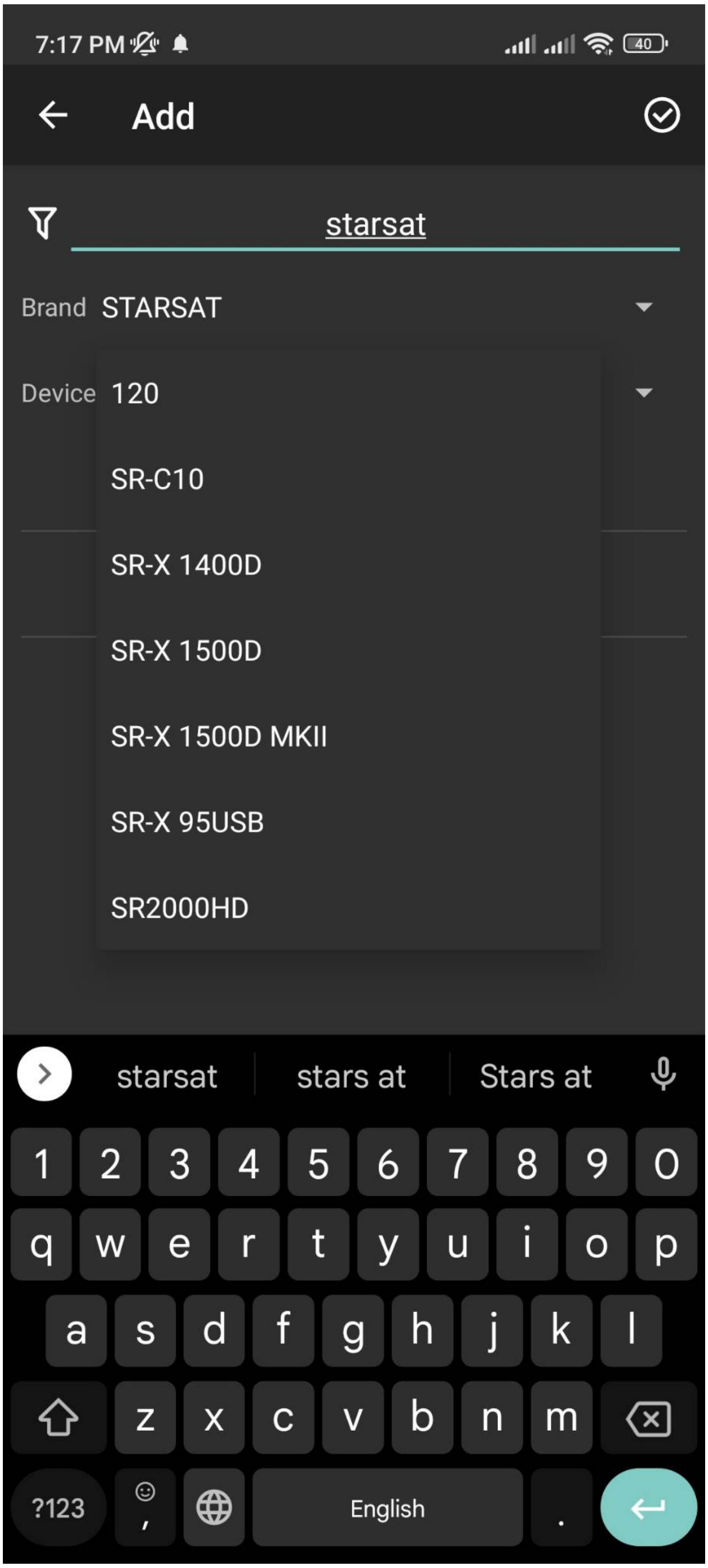
2.4.2 Finding the keycodes

We know it is Starsat SR-2000HD Hyper's remote control, well unless you have the same remote control or probably a remote of the same brand and an Arduino card embedded with an IR receiver, you will need to improvise! Like check online there GitHub repos that keep track of IR key codes for different remotes. Or you can use a forum like https://www.remotecentral.com/ to find the key codes for the remote control.

However for this part, I will use an Android app like IRplus or any alternatives and pick the device in question from the list then head over to check the keys, I will provide screenshots for what I've found.

net.binarymode.android.irplus

1. Selecting the remote control from the list:



Brand STARSAT

Device 120

SR-C10

SR-X 1400D

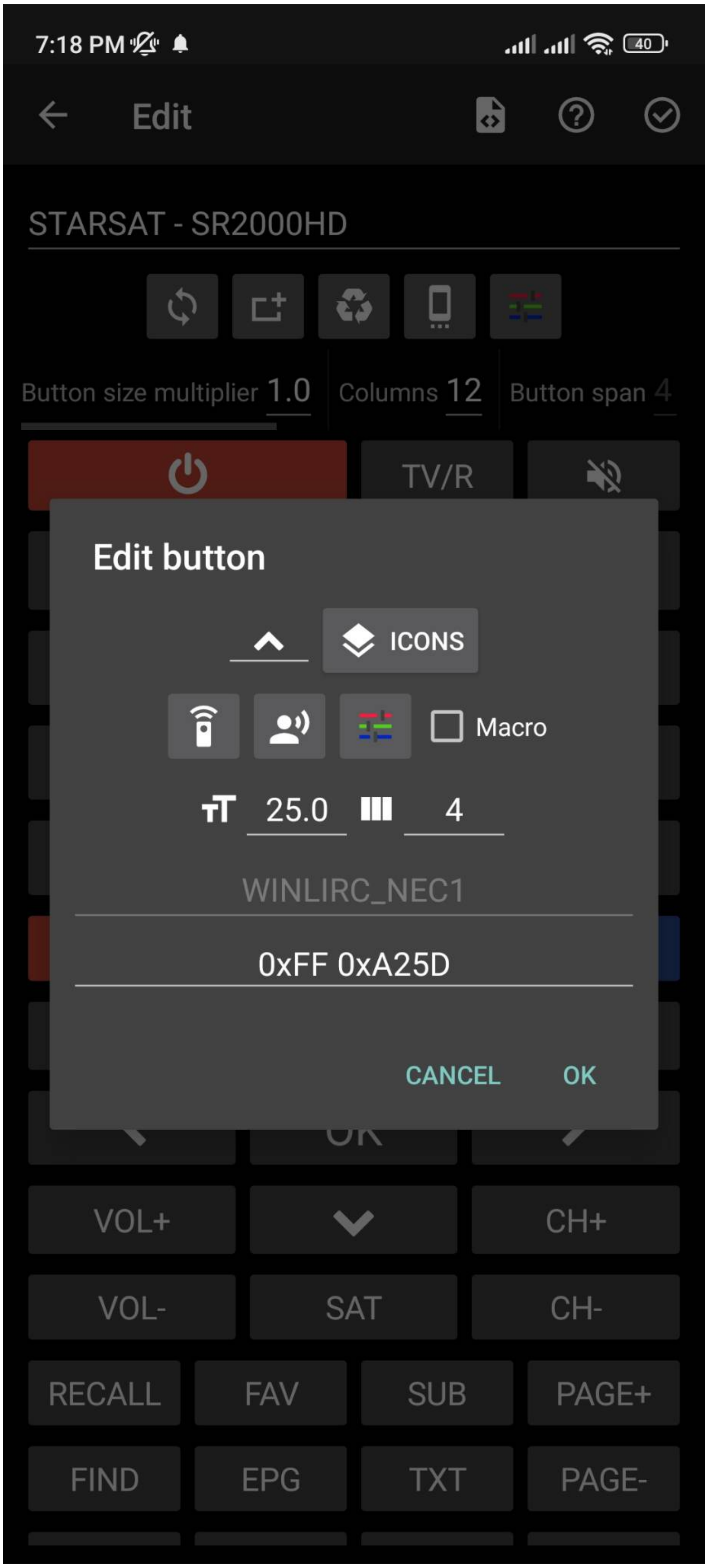
SR-X 1500D

SR-X 1500D MKII

SR-X 95USB

SR2000HD

2. Editing the remote and checking the Up arrow



STARSAT - SR2000HD

Button size multiplier 1.0 Columns 12 Button span 4

Edit button

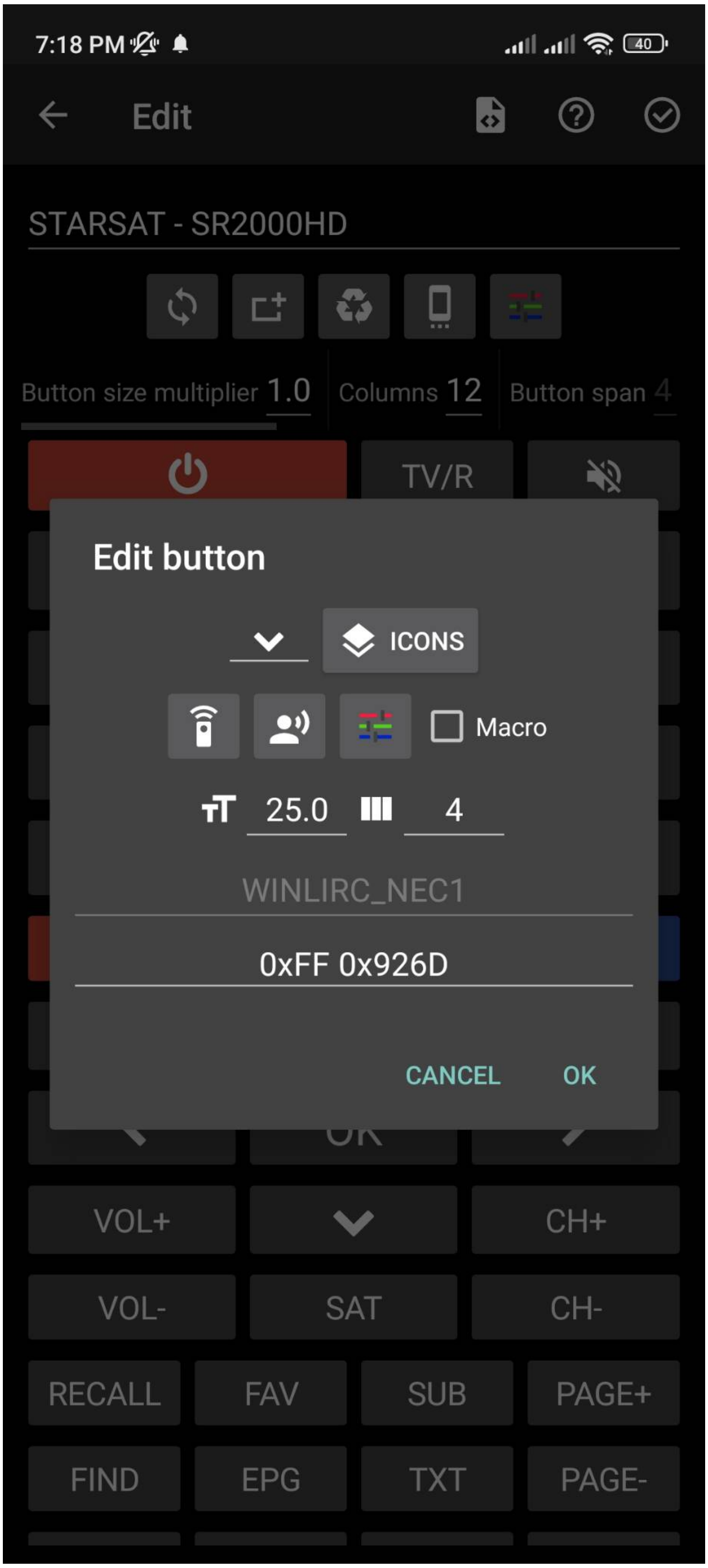
□ Macro

25.0 4

WINLIRC_NEC1

0xFF 0xA25D

3. Checking the Down arrow



STARSAT - SR2000HD

Button size multiplier 1.0 Columns 12 Button span 4

Edit button

□ Macro

25.0 4

WINLIRC_NEC1

0xFF 0x926D

And that is the second part of the flag: `0xffa25d_0xff926d`

2.4.3 Finding the expiration date

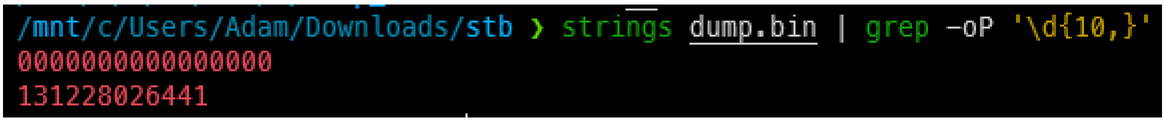
Now for the fun part, if you dig around the web about Starsat 2000 Hyper you will end up with one official built in service, Apollo that offers IPTV as well as VOD Video on Demand.

And there is an online service to renew and check your current subscription by just providing the serial number.

www.renewbox.net

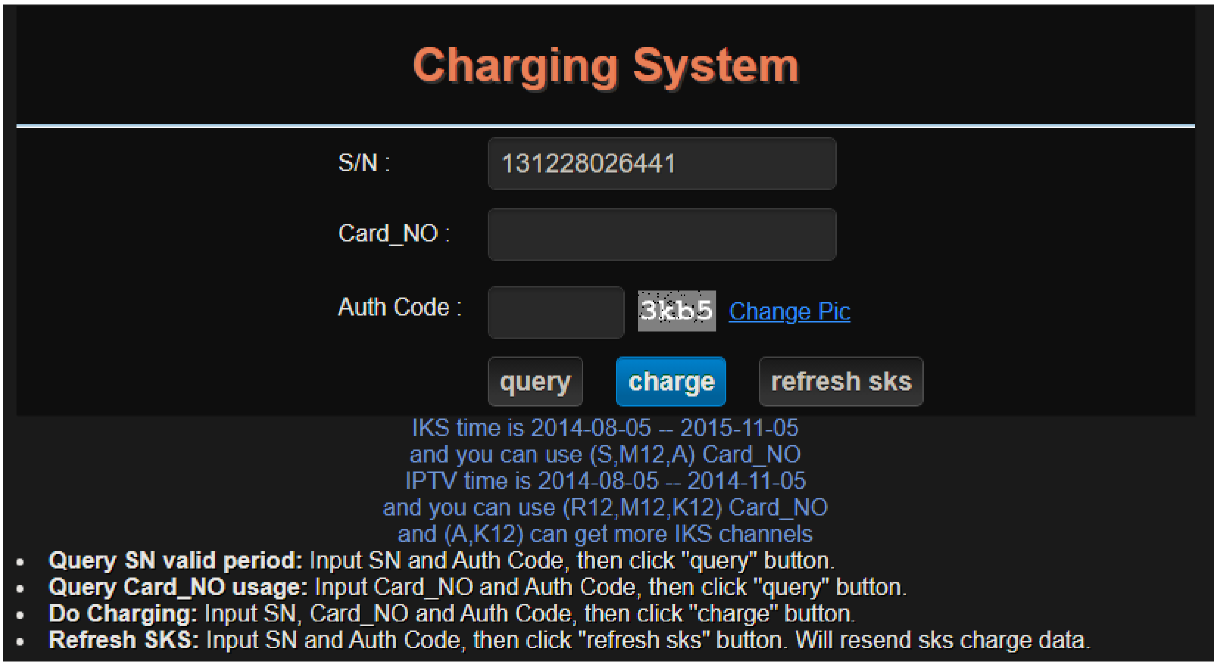
The serial number in most cases is a long number like consists of maybe more than 10 digits. And it can't be in the firmware since it is released to the public to update their devices. So it must be within the memory of the device itself.

Let's grep that easily!



```
/mnt/c/Users/Adam/Downloads/stb ❯ strings dump.bin | grep -oP '\d{10,}'
0000000000000000
131228026441
```

And there it is, the serial number, let's query the IPTV validity.



Charging System

S/N : 131228026441

Card_NO :

Auth Code :

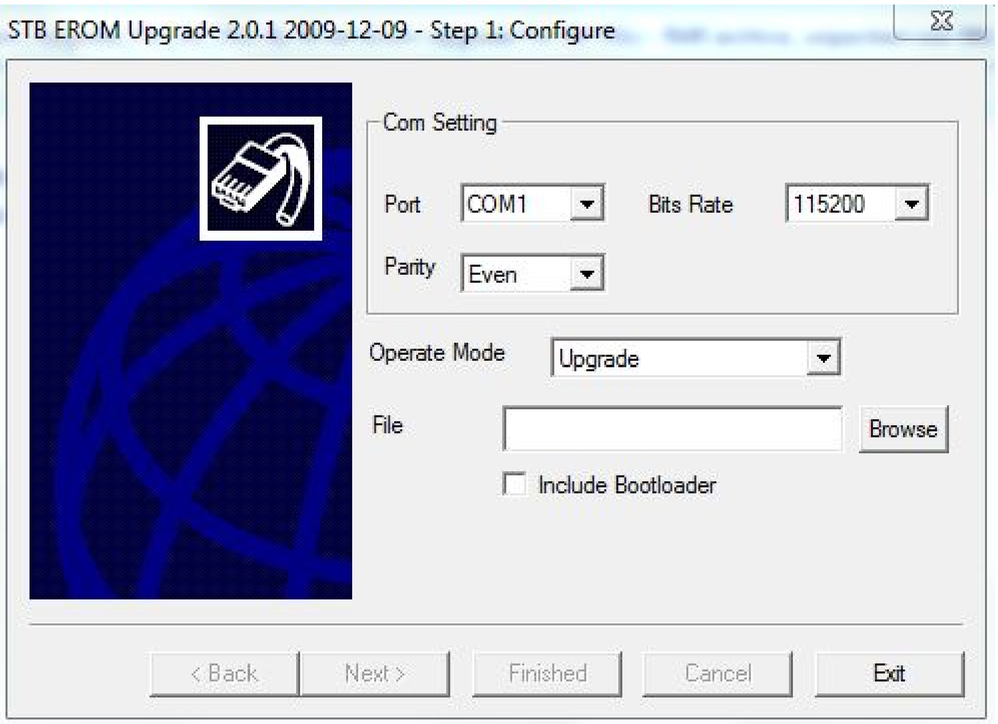
IKS time is 2014-08-05 -- 2015-11-05
and you can use (S,M12,A) Card_NO
IPTV time is 2014-08-05 -- 2014-11-05
and you can use (R12,M12,K12) Card_NO
and (A,K12) can get more IKS channels

- **Query SN valid period:** Input SN and Auth Code, then click "query" button.
- **Query Card_NO usage:** Input Card_NO and Auth Code, then click "query" button.
- **Do Charging:** Input SN, Card_NO and Auth Code, then click "charge" button.
- **Refresh SKS:** Input SN and Auth Code, then click "refresh sks" button. Will resend sks charge data.

And the last part of the flag is `20141105`

3 The Idea

To do such challenge, you need to have the device first, a Serial cable RS232, a USB to RS232 converter if needed, and a loader utility. The loader is used to pull the memory as well as to pass another memory dump or even firmware to the device. The loader itself allows you to select what parts to dump, like just the userdata or the whole memory.



STB EROM Upgrade 2.0.1 2009-12-09 - Step 1: Configure

Com Setting

Port: COM1

Bits Rate: 115200

Parity: Even

Operate Mode: Upgrade

File:

□ Include Bootloader

4 Final Words

First here is the flag: **Securinets{live_rugby_7s_0xffa25d_0xff926d_20141105}**

This is a proposed draft Misc challenge for the Securinets Quals CTF 2023. I must disclouse that I take no responsibility in loading/flashing this whole dump to a similar device to the one in the challenge as it was customized to fit my needs. I also don't publicly support TV shows piracy, cardsharing and IPTVs. I am open to any feedback and suggestions that could help improve this challenge. I hope you enjoyed reading this writeup. Feel free to let me know if you have any questions or comments.

Please keep in mind that this is a draft and that the challenge is not yet released. I will update this writeup if any changes are made to the challenge. Furthermore, it is a proprietary and confidential challenge, so please do not share it with anyone. Thank you for your understanding.

4.1 Acknowledgements

Ahmed T., Rachad A., and Ayoub B.: Highly skilled custom firmware developers and porting specialists. Tunisia-sat forum member.

Nacef: My cousin, for introducing me to such stuff at an early age.

Thanks for reading!