AudioZ magazin ▸▸▸▸▸ CUSTOM TOOL

#2/ 2-2025

NI-JWTDECRYPTER v1b

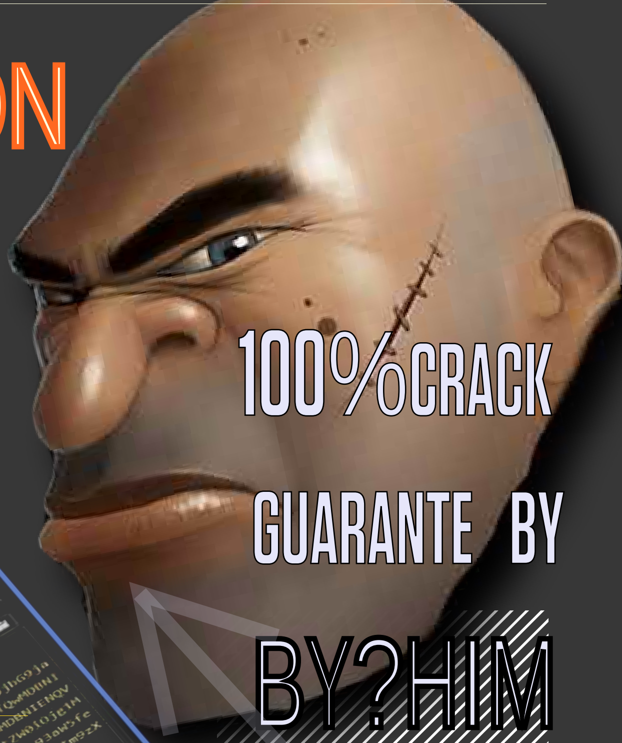
THE
NERD ADD-ON

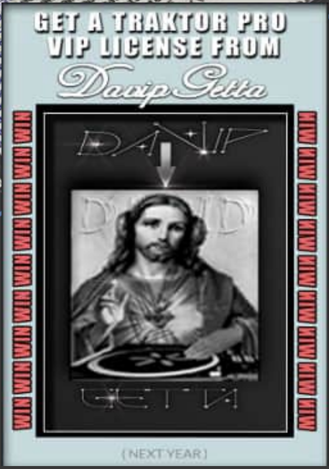
JWT-GENERATOR &
PATCH - TUTORIAL

"For "Reverse Engineering Headz
with at least
Basic Experience,
like me! (Rank aka Tracer)"

Inclusiv
Keygen'n'Patch
EXAMPLE
4N00BZ

100%CRACK
GUARANTE BY
BY?HIM
OR
MAYBE
BY





RANK DMC

Infotainment
100%ILLEGAL CONTENT

SHITS-TORM: feinstaubdieter@gmail.com | tr4c3r@gmx.net ANYTHING ELSE: PM @AudioZ |Or Not ...

D 0,00€ AT 0,00€ CH 00,00CHF LUX 0,00€ IT 0,00€ USD,00

NERDADDON

TABLEOFCONTENTS

GENERATE JWT-FILE's PATCHFILE's MAKE YOUR OWN KEYGEN'N'PATCH

DON'T DISTURB CAPTAIN RANK
HIS EXPRESSION IS JUST SO DIGNIFIED
MIXED BY RANK-AKA-TRACER
CAPTAIN RANK
MUSIC
HOUSE
MOOG
RANK DMC

IF YOU SEE NO SENSE IN THIS PICTURE, THAN YOU'RE RIGHT! THE RE-ASON WHY I ADD THIS:

THERE WAS SO MANY EMPTY SPACE HERE B EFORE THAT I DECIDE TO DROP A PLACE HO LDER HERE, BUT I WA S TO LAZY MADE A N EWONE. SO I ADD SIM PLY A CD-COVER FRO M ME & WRITE THIS ;P

JwtExplaination 1\2 FOREWORD

First of all, I have to mention that my English is not the best (understatement *g*) Because of this, there are also Video-Tutorial available, for Peep'z who cannot follow this Text-Instructions (BUT! also usefull, if you allready have good skills, because the whole procedure of this Explaination is VERY quick, but the text is very long and heavy compared to that!) So long to this. In "Part 1" i try explain short how a Basic JWT-FILE is usually structured and how to generate a JWT-Content in such a Way that it is ultimately accepted as a Full-Version by the related Native-Instruments Product. Finally, "Part 2" revolves all around the topic of Patching. Because in order to generate such an "Ultimate JWT-FILE" (as mentioned above) we can't avoid patching! (The Good thing, we just have to patch at least ONE and Max. TWO Bytes)

In addition, I promise in my NFO that at the End of this Tutorial (incl. provided Software) EVERYONE with Basic Reverse Engineering Skills, is able to create a same NI-Keygen'n'Patch as we all already know (from other Group) Well, i would even say, that ours can do even more at the End! As an Example i have included a finished NI-Keygen+Patch inside this Release. First of all, it doesn't do much different, but it is Universal or so called Generic, furthermore it processes also all IZOTOPE Products with the same scheme and in the end this Patcher has a lot of more or less important Additional Features on Board! YOU SEE, The Main Thing here is that anyone who like can code his own individual \ Experimental KeyKen-Patch with the features he want or not! (" in my case, i just use pure Byte-patched Files that always worx, with or without any NativeAccess\JWT Whatever things or if you have a Internet Connection or not... yes OLDSCHOOL, as long this is possible")

LET's BEGIN: If you open a JWT-FILE with a Text Editor, it begins allways with **"ey"** (BTW. Often also used in cookies, i.e. if you decrypt your cookies you will often find exactly that in there and often it is interesting what you read there, but that's another annoying topic !) **AS EXAMPLE I USE THE FOLLOWING, COMPLETE JWT-CONTENT :**

```
eyJhbGciOiJSUzI1NiIsImtpZCI6ImRmZDRhMGQ3YmI0ZTJmMzUwOWUzZTFhY2NlZTMzNzE2ZmI2NjEwNjg0NDEwYmUwZTNiMTY2OWRkZDg3ZDQwZjgiLCJ0eXAiOiJuaS1
yYXMzIn0.eyJzdWIiOiJhY3RpdmF0aW9uIiwiaGFyZHdhcmVfcHJvZmlsZSI6ImV5SmpiM0psYzE5c2IyY2lPalFzSW1OdmNtVnpYM0JvZVhNaU9qSXNJbU53ZFY5amJHOW
pheUk2TWpRd01Dd2lZM0IxWDJsa0lqb2lRWFYwYUdWdWRHbGpRVTFFSWl3aVkzQjFYMjVoYldVaU9pSkJUVVFnUVhSb2JHOXVJRWR2YkdRZ016RTFNRlVnZDJsMGFDQlNZV
1JsYjI0Z1IzSmhjR2hwWTNNZ0lDQWdJQ0lzSW1Od2RWOXdZV05yY3lJNk1Td2lhR1JmY0hKcElqb2lNelU1TkRBNU5UWTBPQ0lzSW0xbGJTSTZOak0xTWpZd09USTRNQ3dp
Ym1WMFgzQnlhU0k2SWpSRk9qUXhPalUwT2pRNU9qVTJPalExSWl3aWIzTmZkSGx3WlNJNkltOXpYM2RwYmw5NE5qUWlMQ0p2YzE5MWRXbGtJam9pTnpRMllUSTFaRFF0TTJ
JeU15MDBaVFkyTFdKaE16QXRNV1EzWVdJeU5tWTFaVFZpSWl3aWIzTmZkbVZ5WDIxaGFpSTZNVEFzSW05elgzWmxjbDl0YVc0aU9qQjkiLCJzdWJzY3JpcHRpb24iOm51bG
wsImlhdCI6MTcyNDE3MTM0Mywic2VyaWFsIjoiWFhYWFgtWFhYWFgtWFhYWFgtWFhYWFgiLCJuYXRpdmUtaWQiOiIwMDAwMDAwMC0wMDAwLTAwMDAtMDAwMDAwM
DAwMDAwIiwiZXhwIjo5OTk5OTk5OTk5fQ.P6YmqyUUyYJJjx9W4r-K4AZS-
vRBpF_mOvo67aN1_86IDV5EaPJG0qyjuKJUrhRg0p66GuoCeVAOIOnAqqNFoLmrbw_qzrKMPknZhM0xTcLJ52_scFelgi5es3prVTQZqdwnHAYOprHv69qjCOlAoycoKpWR
8opai6YnzobXmynSvyEAZnM71BPm-55znUlTCP3BEpw29zBiSbjQ-SOd1Bs9QTP4vQ-f5zu3QHjcxz19nUFgMNQfQtIjQmGkr4QxS0ZWAWm0klhUS-
3ecoIslnoThRvgu8BKBJbxD1EDW-3F3uLUcPiHF2ecsmy8LNFwHJGUuPe7xUi97ylDs0_Glw
```

Above, we see typicall JWT-Content, En-Code with "Base64" Algorithm" JWT-FILES usually consist of **3 PARTS** with Information. **1. The "HEADER" 2. "PAYLOAD-DATA"** *(Including Hardware-Profile, again crypted with BASE64 Algo.)* and **3. A KEY-PAIR** [OF PRIVATE+PUBLIC KEY] (Crypted with **RSA** Algorithm, in this Case: **"RS256"**) **So Let's try De-Code and separate ANY Info-Part (Of total 3) from the JWT-Content Example, above!**

THE FIRST PART: HEADER (From "ey" till the First Dot)**:**

eyJhbGciOiJSUzI1NiIsImtpZCI6ImRmZDRhMGQ3YmI0ZTJmMzUwOWUzZTFhY2NlZTMzNzE2ZmI2NjEwNjg0NDEwYmUwZTNiMTY2OWRkZDg3ZDQwZjgiLCJ0eXAiOiJuaS1yYXMzIn0.

*If you want to follow along, you can use the BASE64 De-Encrypter if you like. (You can find it here: " **\THE NERD-ADDON\SOFTWARE\Base64-Decrypt\BASE64 EN-DECRYPTER.exe**") I recom mend running it and following the steps below to better understand it.*

To De-Crypt that String with **Base64**, we have to replace the "." with "=" (at the End) IF DONE: We get as Result the **HEADER** De-Coded, with the Main-Infos: **ALG , KID, TYPE**. (This is FIXED by Native Instruments, except the RAS Version, but today "ni-ras3" is Default):

```
{
 "alg": "RS256",
 "kid": "dfd4a0d7bb4e2f3509e3e1accee33716fb6610684410be0e3b1669ddd87d40f8",
 "typ": "ni-ras3"
 }
```

JwtExplaination 2\2

THE SECOND PART: PAYLOAD DATA (Again from "ey" till the First Dot):

eyJzdWIiOiJhY3RpdmF0aW9uIiwiaGFyZHdhcmVfcHJvZmlsZSI6ImV5SmpiM0psYzE5c2IyY2lPalFzSW1OdmNtVnpYM0JvZVhNaU9qSXNJbU53ZFY5amJHOWpheUk2T
WpRd01Dd2lZM0IxWDJsa0lqb2lRWFYwYUdWdWRHbGpRVTFFSWl3aVkzQjFYMjVoYldVaU9pSkJUVVFnUVhSb2JHOXVJRWR2YkdRZ016RTFNRlVnZDJsMGFDQlNZ
V1JsYjI0Z1IzSmhjR2hwWTNNZ0lDQWdJQ0lzSW1Od2RWOXdZV05yY3lJNk1Td2lhR1JmY0hKcElqb2lNelU1TkRBNU5UWTBPQ0lzSW0xbGJTSTZOak0xTWpZd09UST
RNQ3dpYm1WMFgzQnlhU0k2SWpSRk9qUXhPalUwT2pRNU9qVTJPalExSWl3aWIzTmZkSGx3WlNJNklt OXpYM2RwYmw5NE5qUWlMQ0p2YzE5MWRXbGtJam9pTnp
RMllUSTFaRFF0TTJJeU15MDBaVFkyTFdKaE16QXRNV1EzWVdJeU5tWTFaVFZpSWl3aWIzTmZkbVZ5WDIxaGFpSTZNVEFzSW05elgzWmxjbDl0YVc0aU9qQjkiLCJzd
WJzY3JpcHRpb24iOm51bGwsImlhdCI6MTcyNDE3MTM0Mywic2VyaWFsIjoiWFhYWFgtWFhYWFgtWFhYWFgtWFhYWFgtWFhYWFgiLCJuYXRpdmUtaWQiOiIwMDAw
MDAwMC0wMDAwLTAwMDAtMDAwMDAwMDAwMDAwIiwiZXhwIjo5OTk5OTk5OTk5fQ.

Here we have to replace the "." at the End with "==" To make it BASE64-Conform. After Decrypt we see:

```
"sub":"activation",
"hardware_profile":
 "eyJjb3Jlc19sb2ciOjQsImNvcmVzX3BoeXMiOjIsImNwdV9jbG9jayI6MjQwMCwiY3B1X2lkIjoiQXV0aGVudGljQU1EIiwiY3B1X25hbWUiOiJBTUQg
 QXRobG9uIEdvbGQgMzE1MFUgd2l0aCBSYWRlb24gR3JhcGhpY3MgICAgICIsImNwdV9wYWNrcyI6MSwiaGRfcHJpIjoiMzU5NDA5NTY0OCIsI
 m1lbSI6NjM1MjYwOTI4MCwibmV0X3ByaSI6IjRFOjQxOjU0OjQ5OjU2OjQ1Iiwib3NfdHlwZSI6Im9zX3dpbl94NjQiLCJvc191dWlkIjoiNzQ2YTI1ZD
 QtM2IyMy00ZTY2LWJhMzAtMWQ3YWIyNmY1ZTViIiwib3NfdmVyX21haiI6MTAsIm9zX3Zlcl9taW4iOjB9",
"subscription":null,
"iat":1724171343,
"serial":"XXXXX-XXXXX-XXXXX-XXXXX-XXXXX",
"native-id":"00000000-0000-0000-000000000000",
"exp":9999999999
```

("The Hardware-Profile is again Embedded and Base64 En-coded, After De-Coding we see this") :

```
{"cores_log":4,"cores_phys":2,"cpu_clock":2400,"cpu_id":"AuthenticAMD","cpu_name":"AMD Athlon Gold 3150U with Radeon Graphics
","cpu_packs":1,"hd_pri":"3594095648","mem":6352609280,"net_pri":"4E:41:54:49:56:45","os_type":"os_win_x64","os_uuid":"746a25d4-
3b23-4e66-ba30-1d7ab26f5e5b","os_ver_maj":10,"os_ver_min":0}
```

THE THIRD AND LAST PART: KEYPAIR (From "P6" till "Glw") :

P6YmqyUUyYJJjx9W4r-K4AZS-
vRBpF_mOvo67aN1_86IDV5EaPJG0qyjuKJUrhRg0p66GuoCeVAOIOnAqqNFoLmrbw_qzrKMPknZhM0xTcLJ52_scFelgi5es3prVTQZqdwnHAYOprHv69qjCOlAoycoKpWR8o
pai6YnzobXmynSvyEAZnM71BPm-55znUlTCP3BEpw29zBiSbjQ-SOd1Bs9QTP4vQ-f5zu3QHjcxz19nUFgMNQfQtIjQmGkr4QxS0ZWAWm0klhUS-
3ecoIslnoThRvgu8BKBJbxD1EDW-3F3uLUcPiHF2ecsmy8LNFwHJGUuPe7xUi97ylDs0_Glw

IS THE Final "PRIVAT\PUBLIC Key-Pair" Part, who use "RSA-Algorithm" *(In NI's case always: "RS256")* **So the one from our JWT-Example look's before En-Code** (String above)**exact this :**

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCvyZBp11AZXSSX
Lqa7VBO58NTI3+skVWSs6Xpw57WrLzw4/rSeIOXKJfDdIzfrbA4AXE4i+PdxvY1S
HXKKMhiPHhIJvToNW/7pj5IT6T9aQ+QV236uA1CouybpynvcCKwOGeq6S2gAtyzT
3o2ad8T8s5+NDtP0Awgv2x/w4GJNT0G96CfkPDNDPMEjanyyU6MEpLxLkCBDJMnU
Oy6C2cYULZs0bNhzEAgOXvCaDyGHuheqJ2zTYAxOyByiURbWqIqIMmwYo70TE8uw
/SbPTmmXsH6eHrzfb+fwF+L7aqW6z6slSMKLYWPLcROB4kLYjXQhZMZG2UguybIn
jg7uGUgjAgMBAAECggEANNFX+m1O7GgPo/tI7rVa/f4OOVMKeI7N4qR+fSkp7UcS
jb9+LpsM4FnZDuDTnwGHDXWuppRu6PZ+3WLqtPpLZckvu0xngncXVz8jsabeObV3
dVfPruJhHGmrTgjggWL7q3r/C723gKuJJRnUK0r8Xb9s27nOVp2ImrR42uvYrYh4
xjRqv/o8btmHUYxOIYWjPMPad4QfcWRRyC3mtSNHNcaw4LFdczlYvbX5LlfUCwu9
1kBTJcellIP+wixlRuu4UFhmabc1IRFdE3ddkOIk1V1rsEAdcgpYDUFYCXAe/MBS
llhCSkkaFFYwJwDUGpk2cD64P5O4NrtFVtpgx+7BDQKBgQDeTP4ts4k/uj/XXnep
4uZOEFYSAW0hugVvrD2e+PvMGB9jsF5FdoZ6Wy3JYCrE3fLB2oWfo4KTbeTpMmYK
QcH6AxuhpDvjIS5U618OSwThqNUwgAtaWH/riW7B8t8/pP7wzfoQgOE+zH6gu1Ez
ZbfAxKrNICCEAYt6Q070N0dNLwKBgQDKb3zo8Jzy9kOxP561K9nTDeQixGl70/03
jijGpAs6Eex401ZoIQn5JgyGj7paKzH8kamzXdZyfJFij9oahUYnhtdgm/9KQmpN
MSOksRdBTrnNVPxsYs/LoNOPGUYvVcseyZja8lV/fk9PsPQY1f4CIGHmtm/CDutk
GSmPi7+/TQKBgQDOjT+He1BFtGrpVE9fvQI8+pTeuhCKy+uNLb873SEpLCjOWeve
Ixkky1+pwv86WPfdA4wxHp6PGgceXsPNN/his0yTTqSOkCAaq3BxOWdZvaQJIpBp
691AHzyYXXDuFAMGAH0fpICl9yCZfDMgzJyGMrZ5TiaoQT815SCRbmOD5QKBgFLJ
uXnCPU2XrSNl81AAePq5aZ1WWhVMIvh/aOmj2PuMrPrU4zd+m4eLKgA1825A0BaM
s6wpKjR0ATkfv4CtFH3BxX87DPKfqr2a5QrLaclJmu8AXKMu3fBW+25AVdWx7nnO
1HZmONUFIQZkRc+KZHEWMTObVKU2WMn9CGQuMOLZAoGAEg/RBRNhfRnuOetXMszj
/jRBRVhreWGNajzZQCiFNSfivu5bqI6RvKbjlWsP2k1efCTD9V8mbcjKXOjJLEty
M3nnd8TpdXFYy2lEcnrZd5lDLZzHnKEakeCheQ0Ra/Np8MwnNRikZBQ6kAlxkDKP
Rt7OsYUswR1G69pqTjYquq0=
-----END PRIVATE KEY-----
```

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr8mQaddQGV0kly6mu1QT
ufDUyN/rJFVkrOl6cOe1qy88OP60niDlyiXw3SM362wOAFxOIvj3cb2NUh1yijIY
jx4SCb06DVv+6Y+SE+k/WkPkFdt+rgNQqLsm6cp73AisDhnquktoALcs096NmnfE
/LOfjQ7T9AMIL9sf8OBiTU9Bvegn5DwzQzzBI2p8slOjBKS8S5AgQyTJ1DsugtnG
FC2bNGzYcxAIDl7wmg8hh7oXqids02AMTsgcolEW1qiKiDJsGKO9ExPLsP0mz05p
l7B+nh6832/n8Bfi+2qlus+rJUjCi2Fjy3ETgeJC2I10IWTGRtlILsmyJ44O7hlI
    IwIDAQAB
    -----END PUBLIC KEY-----
```

SO LONG TO THE STRUCTURE! Some of the content is not relevant for us as a comparison of copy protection. As an example, "**native-id**" **- "IAT" - "EXP"**. So the Native-ID can always be as eg: **"00000000-0000-0000-000000000000"** 100% Relevant, however, is definitely the (**SNPID**) Serial Number (the first 3 digits) and the **UPID** (**Filename of the JWT FILE**) to correctly identify the respective program. Then your **Hardware-Profile** is relevant, which is individual for Everyone. Its a compilation of various Hard and OS information of your system that gets compared (i.e. assuming you have a legally purchased program from NI, but now use it on your brother's PC, there is probably the first stress, cause he may has a slightly different system than you) The most important or hardest Part of the Copy-Protection is clearly the RSA-KEYPAIR in the Form of PRIVATE and PUBLIC KEY! Because what i have created, myself as an Example above is YES a "**SIGNED-JWT** (Means: Signature of the KeyPaiir must be valid) BUT i created the PUB\PRIVATE Key my self. In real case, this would be an ENCRYPTED-JWT, which means that we **COULDN'T SEE** the **PAYLOAD-DATA** Part De-Crypted at all ! Because we would be missing the **REAL PRIVATE KEY**, and this you can't Decrypt with Basic-Skill (as the Lamer we are) I think even not with Pro-skills. Maybe with "**Master Mind-Genious-Solitaire-Higher state of Passion-Skills**" that excists far as i know in one Land only! (and that*s **not:** ___ *you fill g*) as we Audiowarez-Lovers maybe know :) *By the way: The third Part here was the only way to interact\communicate in the 90ties with the Audiowarez Group "**Radium**" - Never in Raw-Text at IRC or Elsewhere, without exception! May some remember that! ...Old Grand-Fathers *g* (As i am also: School: 70ties | 1st System : ZX-81 "A HELL OF A MASCHINE FOR THAT TIME (SERIOUS!)* ***BACK2 THE THREAD***

LET'S PATCH...

PATCHING TUTORIAL 1\2

PATCHING 2 PARTS OF THE JWT - GENERATED \ RELATED NI-FILE !

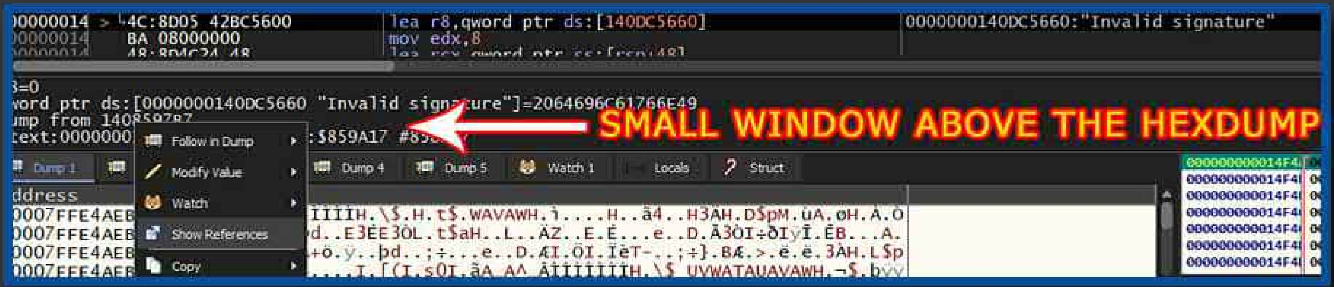
First the question: Why do we still need to patch? And if so, what exactly needs to be patched?

"As already mentioned, the main part (**PATCH 1**) is the PUB\PRIVATE KEY part, which is not valid for us because we created our own. If we now load FM8, it starts as a DEMO and does not show a serial. So we need to patch at least 1 Part-> IF we have previously inserted our valid Hardware-Profile into the JWT, we only need to patch one \ this part (as quoted above, I call it "Bypass Invalid Signature Patch"). The second part that I personally want to patch is the part if we do **NOT** have a valid Hardware-Profile, so that we can use everything as it is and everywhere without constantly generating new JWT-Files for another system. (This is **PATCH 2**) SO LETS start patching, without deeper explaination about Breakpoints or why i patch what i pat-ched here. (There are a lot alternate Ways\Methods, but i think for this here, it is the most easy Way to go for US now!)"

Start the Debugger of your Taste, in my case usually IDA-PRO but for this i decide using "X64DBG" Now Load **FM8** inside, if done: "ANALYZE MODULE" with Shortkey: CTRL+A then "SEARCH FOR STRING REFERENCES IN CURRENT MO-DULE" with Shortkey: SHIFT+D - NOW SEARCH: "invalid signature" (FOUND TWO TIMES, CHOOSE THE SECOND AND STEP IN) **THEN:**

```
lea r8,qword ptr ds:[140DC5660]                     | "Invalid signature" <-YOU LAND HERE!
mov edx,8                                           |
lea rcx,qword ptr ss:[rsp+48]                       |
call <fm8.sub_140851970>                            |
lea rdx,qword ptr ds:[140FF38B8]                    |
lea rcx,qword ptr ss:[rsp+48]                       |
call <JMP.&_CxxThrowException>                      |
int3                                                |
lea r8,qword ptr ds:[140DC5648]                     | "Unsupported signing key"
mov edx,7                                           |
lea rcx,qword ptr ss:[rsp+48]                       |
```

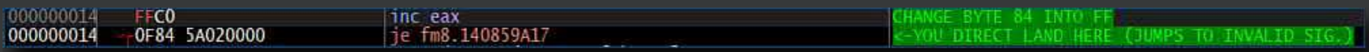
WHERE YOU LANDED : "Show References" (**RightClick** in the small Window above the HexDump *see pic*)



```
)0000014 > └4C:8D05 42BC5600     lea r8,qword ptr ds:[140DC5660]     0000000140DC5660:"Invalid signature"
)0000014    BA 08000000          mov edx,8
3=0
vord ptr ds:[0000000140DC5660 "Invalid signature"]=2064696C61766E49
text:0000000 :$859A17
```

AFTER CLICK "Show References" :

```
test al,al                                           |<-PATCH 1 (I PATCH from 84 into FF )
je fm8.140859A17                                     |<-YOU DIRECT LAND HERE (JUMPS TO INVALID SIG.)
mov rdx,qword ptr ss:[rbp+10]                        |
cmp rdx,10                                           |
jb fm8.1408597FB                                     |
inc rdx                                              |
mov rcx,qword ptr ss:[rbp-8]                         |
mov rax,rcx                                          |
cmp rdx,1000                                         |
jb fm8.1408597F6                                     |
add rdx,27                                           |
```



```
000000014    FFC0            inc eax                CHANGE BYTE 84 INTO FF
000000014   ┬0F84 5A020000   je fm8.140859A17       <-YOU DIRECT LAND HERE (JUMPS TO INVALID SIG.)
```

As you see, we patch one Offset above, where you **LANDED!** For this use Shortkey STRG+E and then change the byte 84 in to FF ("`test al,al`" changes now into "`inc eax`")

! PATCH 1 of 2 DONE !

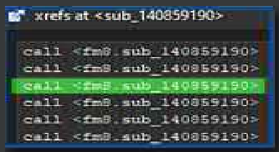
PATCHING TUTORIAL 2\2

PATCHING 2 PARTS OF THE JWT - GENERATED \ RELATED NI-FILE !

Search in **String References** "Your activation is invalid" and step into, **THEN:**

```
mov rax,rsp                                               | <----- SHOW REFERENCES HERE
push rbp                                                  |
push r14                                                  |
push r15                                                  |
lea rbp,qword ptr ds:[rax-5F]                             |
sub rsp,A0                                                |
mov qword ptr ss:[rbp-11],FFFFFFFFFFFFFFFE                |
mov qword ptr ds:[rax+8],rbx                              |
mov qword ptr ds:[rax+18],rsi                             |
mov qword ptr ds:[rax+20],rdi                             |
mov rax,qword ptr ds:[1410FCCF8]                          |
xor rax,rsp                                               |
mov qword ptr ss:[rbp+3F],rax                             |
movzx r14d,r9b                                            |
mov esi,r8d                                               |
mov rbx,rdx                                               |
mov qword ptr ss:[rbp-19],rdx                             |
mov ecx,r8d                                               |
sub ecx,2                                                 |
movdqa xmm0,xmmword ptr ds:[140A81F20]                    |
mov byte ptr ss:[rbp+1F],0                                |
movdqu xmmword ptr ss:[rbp+2F],xmm0                       |
je fm8.140859226                                          |
sub ecx,1                                                 |
je fm8.140859217                                          |
sub ecx,1                                                 |
je fm8.140859208                                          |
cmp ecx,1                                                 |
jne fm8.14085923D                                         |
lea r8d,qword ptr ds:[rcx+1F]                             |
lea rdx,qword ptr ds:[140DC5848]                          | "Your serial number is incorrect."
jmp fm8.140859233                                         |
mov r8d,19                                                |
lea rdx,qword ptr ds:[140DC5828]                          | "Your licence has expired."
jmp fm8.140859233                                         |
mov r8d,44                                                |
lea rdx,qword ptr ds:[140DC57E0]                          | "Your h...open Native Access to re-activate."
jmp fm8.140859233                                         |
mov r8d,1B                                                |
lea rdx,qword ptr ds:[140DC57C0]                          | "Your activation is invalid." <-YOU LAND HERE !
```

...**THEN**, SEE MY NOTE "**<-YOU LAND HERE**", FROM THERE TRACE UP TILL THIS CALL STARTS AND APPLY **"SHOW REFERENCES"** by **RightClick** **inside the small Window above the Hexdump** (As we allready have Done at PATCH 1, if you forgot, go back and check the 1st Picture) ThisTime it shows us all available CALLS From related to this CALL, in this case **TOTALLY 6 CALLS** *see picture* (**Choose the third one,** **step in to by DoubleClick**)



```
xrefs at <sub_140859190>

call <fm8.sub_140859190>
call <fm8.sub_140859190>
call <fm8.sub_140859190>
call <fm8.sub_140859190>
call <fm8.sub_140859190>
call <fm8.sub_140859190>
```

THAN :

```
call <fm8.sub_140859190>                                  |<------------ YOU LAND HERE
nop                                                       |
lea rcx,qword ptr ss:[rsp+F8]                             |
call <fm8.sub_140852110>                                  |
mov rdx,qword ptr ss:[rsp+E8]                             |
cmp rdx,10                                                |
jb fm8.14085603E                                          |
inc rdx                                                   |
mov rcx,qword ptr ss:[rsp+D0]                             |
mov rax,rcx                                               |
cmp rdx,1000                                              |
jb fm8.140856039                                          |
add rdx,27                                                |
mov rcx,qword ptr ds:[rcx-8]                              |
sub rax,rcx                                               |
add rax,FFFFFFFFFFFFFFF8                                  |
cmp rax,1F                                                |
jbe fm8.140856039                                         |
call qword ptr ds:[<_invalid_parameter_noinfo_nor         |
nop                                                       |
mov rcx,qword ptr ds:[r15+88]                             |
test rcx,rcx                                              |
je fm8.140856267                                          |
mov rax,qword ptr ds:[rcx]                                |
lea rdx,qword ptr ss:[rsp+200]                            |
call qword ptr ds:[rax+10]                                |
mov dword ptr ss:[rsp+20],1E                              |
lea rdx,qword ptr ss:[rsp+200]                            |
lea rcx,qword ptr ss:[rsp+F8]                             |
call <fm8.sub_140854640>                                  |
test al,al                                                |  <------- AND PATCH THIS (OUR PATCH 2 OF 2) FROM 84 INTO FF
```

*FINALLY: SEE ^NOTE^ "OUR PATCH 2 of 2" use Shortkey **STRG+E** and change from 84 into FF ("`test al,al`" changes to "`inc eax`")*

! PATCH 2 of 2 DONE !

PATCHING DONE ! ADDITIONAL:

"I WILL GIVE YOU A ALTERNATE METHOD OF THOSE 2 PATCHES - IF THEY WANT WORK FOR YOU OR YOU SIMPLY "LOST" \ DONT ABLE TO FIND THE RIGHT PLACES ..."

If you ask your self if it's EXACT ALWAYS as this Example above, i have to say: 98% - So Usually YES (There are many more ways but RARE Times it's a TINY bit different comparedto here!) I decide use the one as explained here to keep it simple as it could be. SURE! As Example take PATCH 2 here, we stepped in to the third CALL of SIX total to see the target "test al,al" but this depends naturally on the Application we debug\Patch, its clear that this target is sometimes direct inside the first CALL that we get listet and with another more far away. HINT: i suggest just to click andy CALL quick and watch out for "test al,al", then you got it in seconds (my eyes, as example stops automatic if they catch a XOR, MOV, ADD, CMP... lol) HOW EVER :If you think that this method CANT be used as explained with NI-APP "XYZ" or because you just not found this OFFSETS as explained or you simply TOTALLY LOST: Here i give you 2 Alternates to the PATCH 1 and 2 EXAMPLE HERE!

PATCH 2 - ALTERNATE (Works 100% with all):

Inside "X64DBG" Use Shortkey: "CTRL+SHIFT+B" - Here you be able find Byte Pattern-Ranges, just paste following Byte-Range inside: 32 C0 4C 8B 74 24 48 48 8B 5C 24 - If done, "xor al,al" is found at Offset XYZ, STEP IN TO:

```
jmp fm8.14085479D                |
xor al,al                        |<--- YOU LAND HERE (PATCH: 32 C0 to B0 01)
mov r14,qword ptr ss:[rsp+48]    |
```

Patch this as you see in my Note at the Offset (Results in: from "xor al,al" in to "mov al,1"
(btw. a CLASSIC to Patch-Offset Since ever) How ever, this makes the same !

PATCH 1 of 2 - ALTERNATE (WORKS with Various)

There are more than one alternates that work with all - but a interessting one is : If a external *.dll File gets imported in to the Main-Module to do the Job we want to patch!As Example we choose "Guitar Rig 7". After load in to "X64DBG"
and Analyzing all, we go to the Tab "Symbols" and choose the Module "Guitar Rig 7.exe", now show at the right Tab, there are, so called "SYMBOLS" that get's IM or EX-ported. Sort that and scroll till you see "Bcrypt:Bcrypt-VerifySignature". If found, make a right-click and choose "FOLLOW IN DISASSEMBLER", If done apply "SHOW REFERENCES" than you Land from that, inside the "Guitar Rig 7" Main-Code which look's like this:

```
00000001 | FF25 1A95C506          | jmp qword ptr ds:[<BCryptVerifySignature>]
```

AGAIN APPLY "SHOW REFERENCES", THAN:

```
call <JMP.&BCryptVerifySignature> |<--- OU LAND HERE !
                mov edi,eax       |
```

So Finally make any possible that this Verify get by-passed by eg. NOP out the whole CALL or channge the CALL to "MOV EAX,1" or by set a Return (C3) at the first Reference we saw (FF25 1A95C506) or WHAT EVER WORX for you. !!! BUT IMPORTAND !!! is NOT going to deep inside, cause we want (in this Case) patch "Guitar Rig 7.exe" and NOT "Bcrypt.dll" from inside our "System32" Folder, so be awake saving the patched Executable. This makes the same as our Patch 1 here and is a fast explaination how to find the right Place of this alternate IF our PATCH 1 Method is why ever not available!

LEFT TO SAY: Now everybody must be able to realise this with any other NI-App\vst\vsti :) and if you a bit Experianced, breakpoints here also should help: "decodeBase64 failed" \ "No public key" \ "00000-00000-00000-00000-00000"

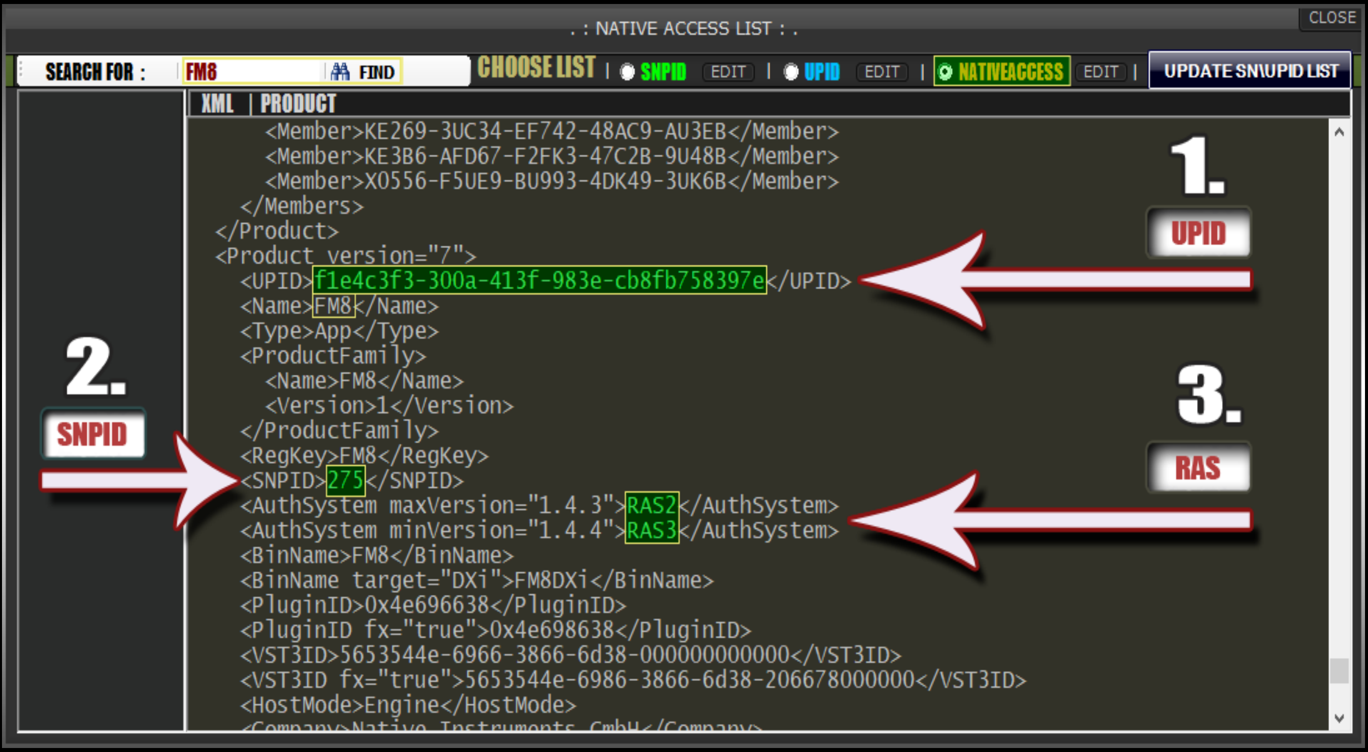
FM8 IS PATCHED - LET'S GENERATE THE JWT FILE TO FINALY GET IT WORK

GENERATE JWT 1\2

LET's START GENERATE A JWT-FILE. In a way NI accepts the JWT-CONTENT after patch the File as purchased. As an Example, we are of course also using **FM8**, which we have already patched and which now **requires** a JWT-File to start as a **FULL** Version! To do this, we need First to **check out three relevant and importand Infos** from FM8 before we can begin generate the JWT! *(The Same in any other you plan to Crack, in other Words:* ***do any other, also "Izotope" stuff, the same as with this FM8 Example****) Now to the 3 Importand Things to found:*

1. UPID 2. SNPID 3. RAS

To find this Infos click inside JWT De-crypter at the Top Menue "More" and then "UPID-SNPID LIST" THEN choose as "LIST" : "NATIVEACCESS" IF DONE "search for: FM8" *(Sometimes you-have to click FIND a few times till the correct place, in this case till the Name is just "FM8")*
Well then you found those 3 importand Infos. See the Picture:



```
      <Member>KE269-3UC34-EF742-48AC9-AU3EB</Member>
      <Member>KE3B6-AFD67-F2FK3-47C2B-9U48B</Member>
      <Member>X0556-F5UE9-BU993-4DK49-3UK6B</Member>
    </Members>
  </Product>
  <Product version="7">
    <UPID>f1e4c3f3-300a-413f-983e-cb8fb758397e</UPID>
    <Name>FM8</Name>
    <Type>App</Type>
    <ProductFamily>
      <Name>FM8</Name>
      <Version>1</Version>
    </ProductFamily>
    <RegKey>FM8</RegKey>
    <SNPID>275</SNPID>
    <AuthSystem maxVersion="1.4.3">RAS2</AuthSystem>
    <AuthSystem minVersion="1.4.4">RAS3</AuthSystem>
    <BinName>FM8</BinName>
    <BinName target="DXi">FM8DXi</BinName>
    <PluginID>0x4e696638</PluginID>
    <PluginID fx="true">0x4e698638</PluginID>
    <VST3ID>5653544e-6966-3866-6d38-000000000000</VST3ID>
    <VST3ID fx="true">5653544e-6986-3866-6d38-206678000000</VST3ID>
    <HostMode>Engine</HostMode>
    <Company>Native Instruments GmbH</Company>
```

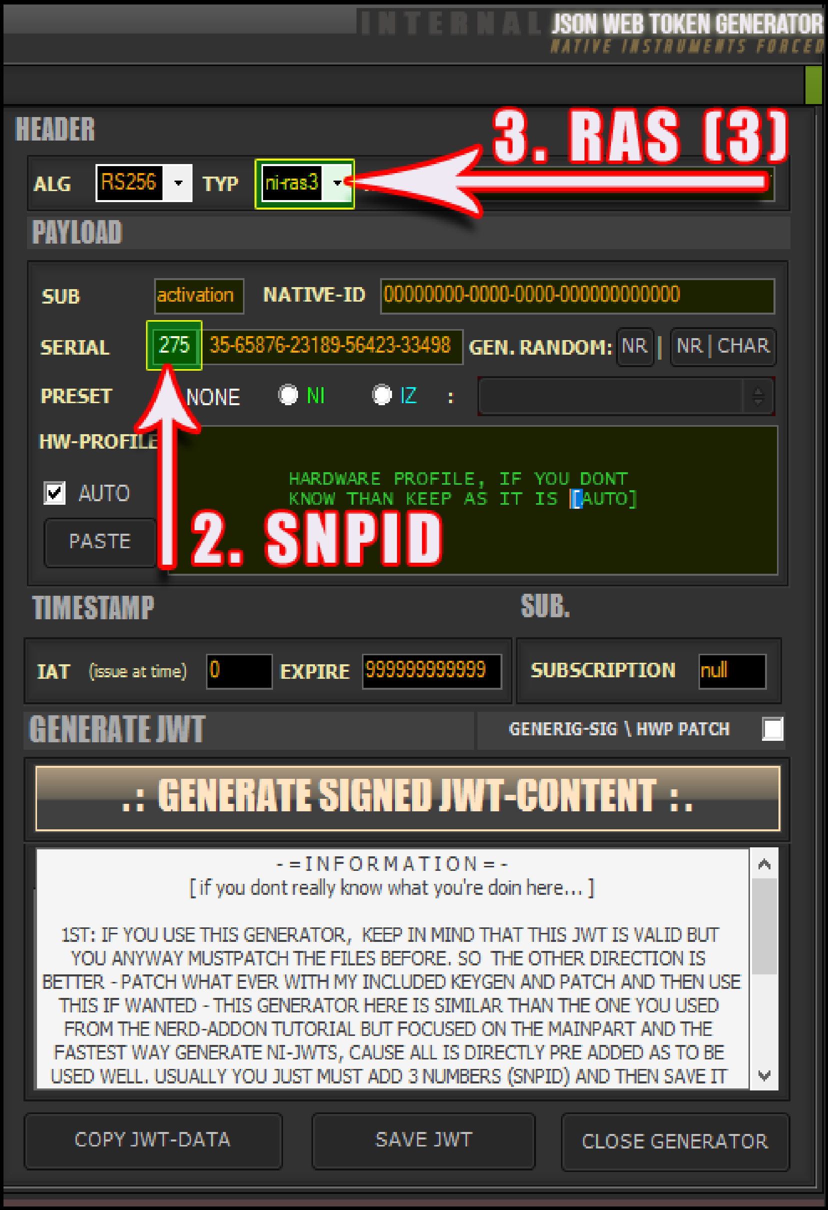
1. **UPID = f1e4c3f3-300a-413f-983e-cb8fb758397e**
   (UPID MEANS: The ***Filename*** **and unique Product Number* from a Product (here FM8)*
2. **SNPID = 275**
   (SNPID MEANS The ***first 3 Digits*** *of the Serial (****RELEVANT****) that FM8 uses. The rest of the Serial is* ***NOT RELEVANT****, just any Numbers eg :27535-65876-23189-56432-33498)*
3. **RAS VERSION = 3**
   (All before Version FM8 v.1.4.4 is RAS2, and because of: We Patch no old Bananas ! ***Version 3 is RELEVANT*** *for us here now (but It's mostley RAS3)*

So open a Text-Editor, for this NOTEPAD is OK and copy\paste the related Info's:

UPID:
f1e4c3f3-300a-413f-983e-cb8fb758397e
SNPID:
275
RAS (Version):
3

GENERATE JWT 2\2

Now you can close the "UPID - SNPID LIST" Window and Open the internal JWT-GENERATOR from the Top Menue "More" and then: "INTERNAL JWT GENERATOR" - IF DONE you see This:



ALG RS256 TYP ni-ras3

SUB activation NATIVE-ID 00000000-0000-0000-000000000000

SERIAL 275 35-65876-23189-56423-33498 GEN. RANDOM: NR | NR | CHAR

PRESET NONE ● NI ● IZ :

HW-PROFILE ✓ AUTO

HARDWARE PROFILE, IF YOU DONT KNOW THAN KEEP AS IT IS [AUTO]

IAT (issue at time) 0 EXPIRE 999999999999 SUBSCRIPTION null

- = I N F O R M A T I O N = -
[if you dont really know what you're doin here...]

1ST: IF YOU USE THIS GENERATOR, KEEP IN MIND THAT THIS JWT IS VALID BUT YOU ANYWAY MUSTPATCH THE FILES BEFORE. SO THE OTHER DIRECTION IS BETTER - PATCH WHAT EVER WITH MY INCLUDED KEYGEN AND PATCH AND THEN USE THIS IF WANTED - THIS GENERATOR HERE IS SIMILAR THAN THE ONE YOU USED FROM THE NERD-ADDON TUTORIAL BUT FOCUSED ON THE MAINPART AND THE FASTEST WAY GENERATE NI-JWTS, CAUSE ALL IS DIRECTLY PRE ADDED AS TO BE USED WELL. USUALLY YOU JUST MUST ADD 3 NUMBERS (SNPID) AND THEN SAVE IT

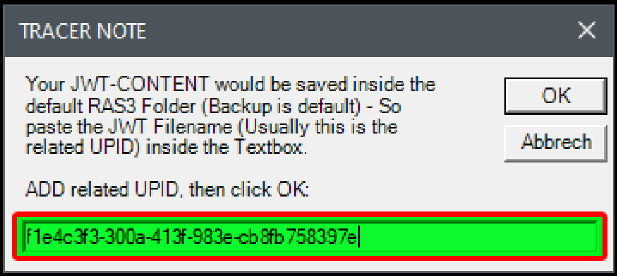
NOW ADD THE 3 IMPORTAND THINGS (SEE YOUR NOTEPAD, THE PREVIOUS PASTED STUFF) INSIDE RELATED JWT-GENERATOR FIELDS! WE BEGIN WITH:

2. THE SNPID
WHO WAS "275" FOR FM8 SO PASTE THIS INSIDE THE SERIAL TAB, IF DONE CLICK "GEN.RANDOM" AND "NR" TO AUTO-GENERATE THE REST NUMBERS AFTER OUR SNPID AS SERIAL! THEN CONTINIOU WITH:

3. RAS
AS WE ADD INSIDE NOTEPAD, WE KNOW THAT-IT WAS RAS3 SO SET THE TYP INSIDE JWT - GENERATOR TO: "ni-ras3"

IF DONE CLICK:
.: GENERATE SIGNED JWT-CONTENT :.

THEN YOU SEE THE GENERATED JWT-CONTENT (That you not yet see here. It's Inside the HW-PROFILE and INFORMATIONS Window that you see here at the left Picture, after click ".: GENERATE... ") FINALLY CLICK "SAVE JWT" THEN A TEXT-BOX POP UP, HERE YOU HAVE TO PASTE: THE UPID:



Your JWT-CONTENT would be saved inside the default RAS3 Folder (Backup is default) - So paste the JWT Filename (Usually this is the related UPID) inside the Textbox.

ADD related UPID, then click OK:

f1e4c3f3-300a-413f-983e-cb8fb758397e

Now this GENERATED JWT get saved inside our Systems RAS3 Folder: ***[c:\Users\Public\Documents\Native Instruments\Native Access\ ras3\]*** As "f1e4c3f3-300a-413f-983e-cb8fb758397e.jwt" File! If you allready have stored this FM8 Jwt-File then yours get Backuped as default before our's from here get saved! *(By the Way if you ask your self...: The Public\Privat Key is always Auto-Generated by this internal JWT-Generator)*

YOU'RE DONE!

Now, as our FM8 JWT is generated and inside the right Place it is Time to start our Previous Patched FM8. As you see, FM8 starts as **FULL VERSION** and also shows our SERIAL-NR. **ALL WORKS AS PURCHASED**! *I Say this cause some ones out there think that Release-Groups (ANY) uses special Full Versions inside theire Releases... **NO** mostley they use also the TRIAL Versions and then sometimes they made a Installer of all. WHY? Cause the Trials are 100% the same as the one you purchased in a Shop with the exception that the TRIALS are cracked by WHO EVER, maybe YOU since now :)* [And if someone asks what is the Difference by using the Presets inside JWT-GENERATOR with this what we have made here now: Usually nothing except that the Presets are allready correct Pre-filled with eg. SNPID etc. and they doesnt need that you add the UPID after save! SHORT: After select a Preset just click "**.:GENERATE SIGNED JWT CONTENT :.**" followed by "**SAVEJWT**" and also Done!

[NOT NEEDED\OPTIONAL: IF INTERESTED, THERE IS A "JWT-GENERATOR ADVANCED" IN THE NERD-ADDON\SOFTWARE FOLDER, MAY CHECK THE "READ ME.txt" INSIDE BEFORE..."]

NOW YOU KNOW ENOUGH TO

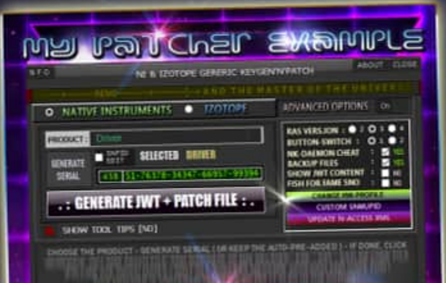
CODE YOUR INDIVIDUAL

NATIVE INSTRUMENTS

GENERIC

X 64 PATCH

AND KEYGEN



RENO ——[-+AND THE MASTER OF THE UNIVERSE

○ NATIVE INSTRUMENTS ● IZOTOPE

ADVANCED OPTIONS On

PRODUCT : Driver

SNPID EDIT

SELECTED DRIVER

GENERATE SERIAL 458 51-76378-34347-66957-99394

. : GENERATE JWT + PATCH FILE : .

SHOW TOOL TIPS [NO]

RAS VERSJON : ● 2 ○ 3 ● 4

BUTTON-SWITCH : ○ 1 ● 2

NK-DAEMON CHEAT : ✓ YES

BACKUP FILES : ✓ YES

SHOW JWT CONTENT : ☐ NO

FISH FOR FAME SNO : ☐ NO

CHANGE HW-PROFILE

CUSTOM SNWUPID

UPDATE N-ACCESS XML

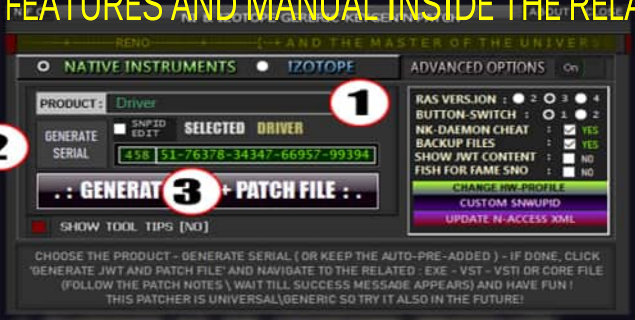
CHOOSE THE PRODUCT - GENERATE SERIAL (OR KEEP THE AUTO-PRE-ADDED) - IF DONE, CLICK

AND HOW TO

MY EXAMPLE

QUICK TUTORIAL

CHECK THE FULL FEATURES AND MANUAL INSIDE THE RELATED FOLDER !



RENO ——[-+AND THE MASTER OF THE UNIVERSE

○ NATIVE INSTRUMENTS ● IZOTOPE

ADVANCED OPTIONS On

PRODUCT : Driver

SNPID EDIT

SELECTED DRIVER

GENERATE SERIAL 458 51-76378-34347-66957-99394

. : GENERAT + PATCH FILE : .

SHOW TOOL TIPS [NO]

RAS VERSJON : ● 2 ○ 3 ● 4

BUTTON-SWITCH : ○ 1 ● 2

NK-DAEMON CHEAT : ✓ YES

BACKUP FILES : ✓ YES

SHOW JWT CONTENT : ☐ NO

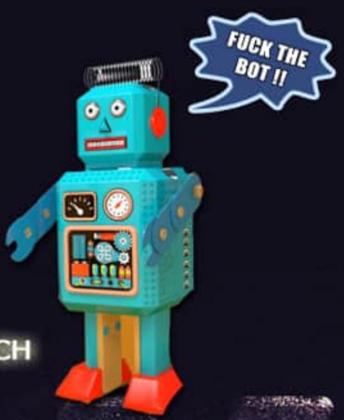
FISH FOR FAME SNO : ☐ NO

CHANGE HW-PROFILE

CUSTOM SNWUPID

UPDATE N-ACCESS XML

CHOOSE THE PRODUCT - GENERATE SERIAL (OR KEEP THE AUTO-PRE-ADDED) - IF DONE, CLICK 'GENERATE JWT AND PATCH FILE' AND NAVIGATE TO THE RELATED : EXE - VST - VSTI OR CORE FILE (FOLLOW THE PATCH NOTES \ WAIT TILL SUCCESS MESSAGE APPEARS) AND HAVE FUN ! THIS PATCHER IS UNIVERSAL\GENERIC SO TRY IT ALSO IN THE FUTURE!



1 CHOOSE NI OR IZOTOPE PRODUCT

2 GENERATE SERIAL OR KEEP AUTOGENERATED

3 CLICK THE GENERATE\PATCH BUTTON, FOLLOW THE PATCH

CRACK

WE CAME TO END...I hope it was pleasant, understandable and you can cope well with this Tutorial (On my side: My humble Family decided to visit me at my Art Gallery yesterday, to give me FEEDBACK on this...(AND: IT WAS COMPLETELY POSITIVE) I MADE A SNAPSHOT, see:

PRESENTS
NERDADDON
FFTNP FMPFS ?!
WTF?!
OUR LIVE IS TOTALLY OUT OF THE FRAME
PLEASE SOME ONE SAVE ME FROM MY HUSBAND
AUDIOZ
I FEEL TOTALLY COMPLETE--- WONDER FULL!
GOOD EVENING HANS SOLO, CHEERS
WTF?!
ALFRED E NEWMAN
ROMAN POLANSKI
NO ONE KNOWS ...I AM BELLE E POC
Elite Romance
Total war
THT FRZZN 2MAIL IM SURE IAM A REPPSBCH
THAT FROZEN SMILE.. IM SURE HE IS A REPLICANT!
THAT FROZEN SMILE.. IM SURE SHE IS A REPLICANT!
HEY YOU'RE ABOVE ME, IM SURE YOU'RE NOT IMMANUEL KANT!
FCK
RUB MA COCK*N*U CAN*T LOOK WTF?!
I FCK BELL'E' POC
IM NOT POC
MILK N TOST N HORNY
HELP
YO

FINAL WORDS

Last but not least, a little **TIP** to absolute beginners: Don't let yourself get discouraged, and if your ego is hurt, believe me: if your stuff doesn't even come close to real Soft or Scene Releases from REALLY elite Guys, THAN: why not, blow everything up a little bit! As a suggestion, insist that you want to be quoted (in a creditz text or patch-scroller at the end) or:

- *Add background Music like a World War Firework, if a "About Window" opens!*
- *A Release Header with the FULL spectrum of Colors, like a "Morning Concert from Wagner"*
- *Fast and hard cuted Scenes with gimmicks, inside a help video.*
- *An "NFO File" that "Nero" would have LOVED to BURN down!*
- *Small manipulations that only Rasputin (and YOU) could do, inside randnoti*

Ah, forget the LAST one. YOU get the idea, everything is allowed - may the force be with you! :)

This really does work, because I often get completely overrated hymns of praise in messages. Or people don't want to believe that I haven't cracked program xyz (which I don't even know) even though I try to answer honestly and seriously that this isn't the case. They think you're flirting by making yourself look smaller than you are. And that's absolutely because of the tips mentioned i think, no im sure today by think back cause i did something at the past because I found it funny and the user might also find it a little §$%&/whtevr. BUT at the end something completely different came out of it... a man-made prodigy by peepz that is not one BECAUSE OF SILLY CRAP! **I ONLY SAY THAT** as FINAL WORDS, in absolute seriousness **becau**...

AH FUCK, SORRY FOLKS, MY GIRLFRIEND want ALSO SAY SOMETHING TO YOU NOW! omg...

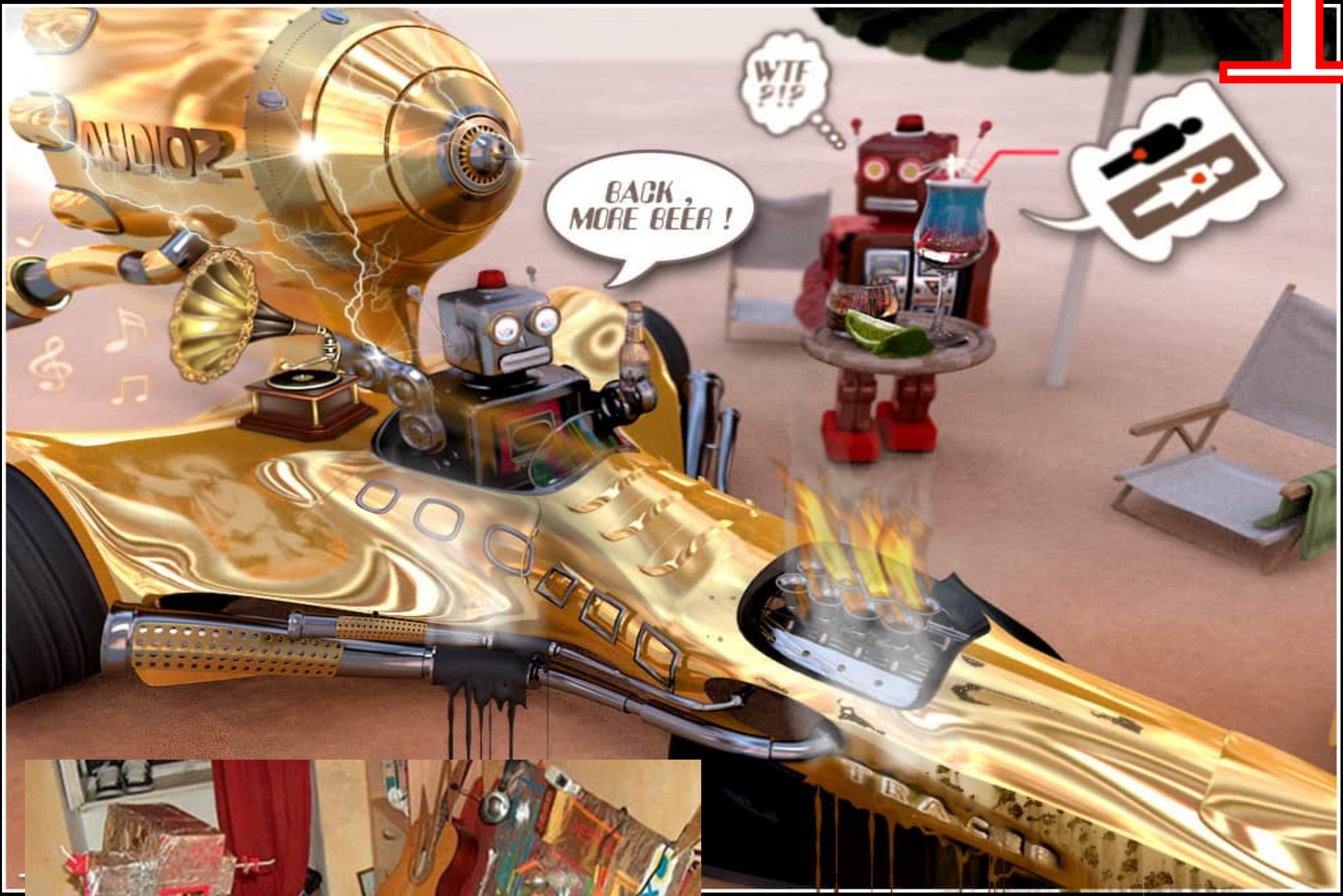
„ hey... psssssssst,
Guys, my boyfriend doesn't know any better, I'm a little embarrassed for him and I want to apologize to you, it must have been torture. Take my present, good Night!“

HERE IS MY GIFT & TUTORIAL TO YOU:

1. Cut out confetti elements along the lines.
2. Paint smileys on both sides of the elements and cover them with crepe paper.
3. Throw them around with **wild laughter!**

ME AGAIN... WTF! YOU'RE STILL THERE ? Get home safely now and drive carefully. Make something nice out of the day, my dears! (or What ever you do) and if do nothing... a little inspiration perhaps:

1. DRIVE HOME 2. GO STUDIO & MAKE GOOD MUSIC
3. SHARE IT WITH LOVE AT PLANET AUDIOZ

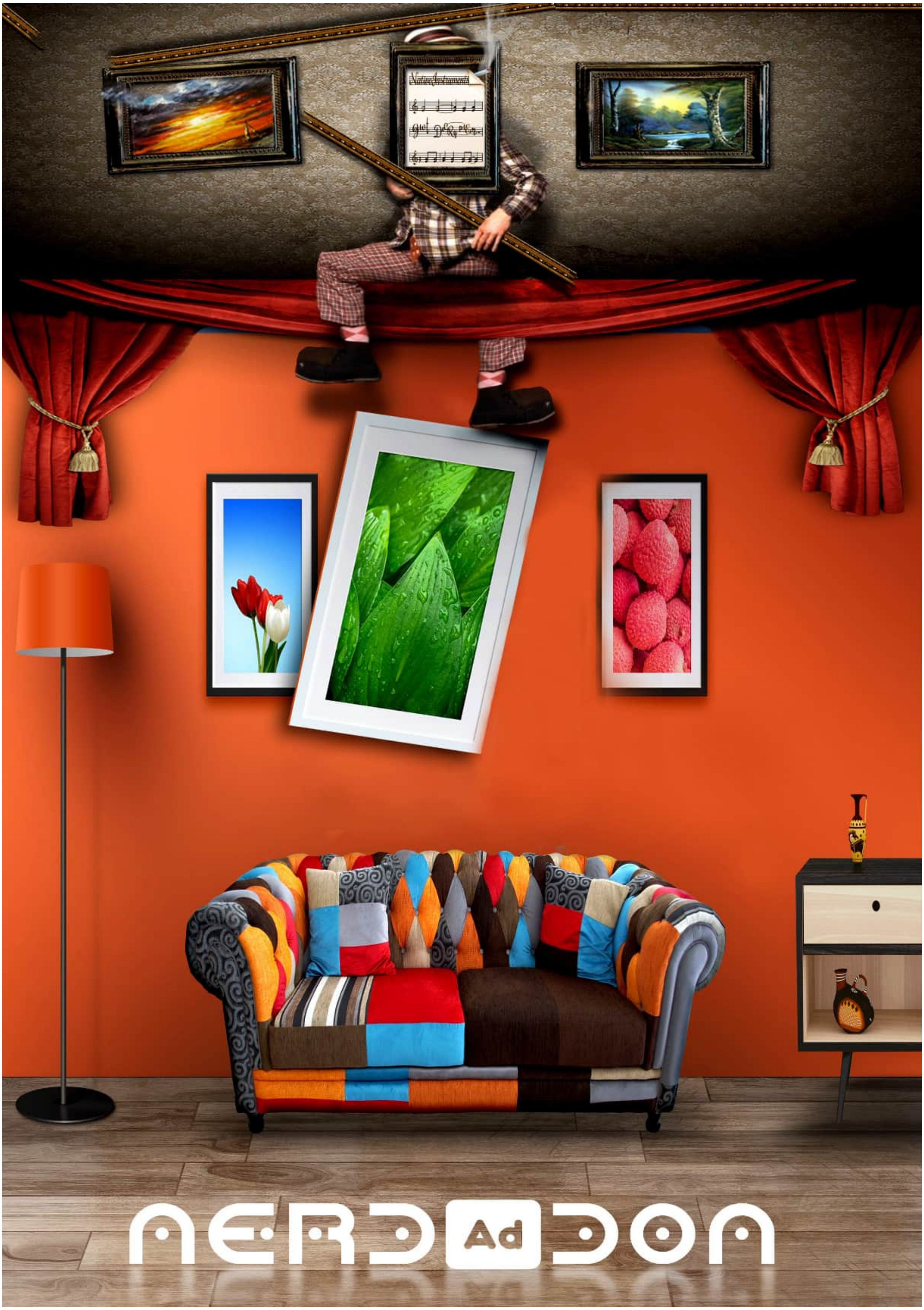


```
Respect & Honour
          [AUDIO-RELEASES-RELATED]

            SANDOR 'n' DEEPZ0NE
  ..: with the whole story that 1997 began :..

      [   AIR    ] ..... [   R2R    ]
      [  Assign  ] ..... [   H2o    ]
      [   Zone   ] ..... [  Oxygen  ]
      [ 0xdBass  ] ..... [ Delirium ]
      [   Beat   ] ..... [ Dynamics ]
      [  Arctic  ] ..... [ Invision ]
      [  Talio   ] ..... [ AudioP2P ]
      [ Digisan  ] ..... [ Embrace  ]
      [   Ind    ] ..... [   Mpt    ]
      [  Union   ] ..... [   Doa    ]
      [  CHAOS   ]  <->  [ HORSEMEN ]
```

PEACE


Native Instruments
NERD Ad DON