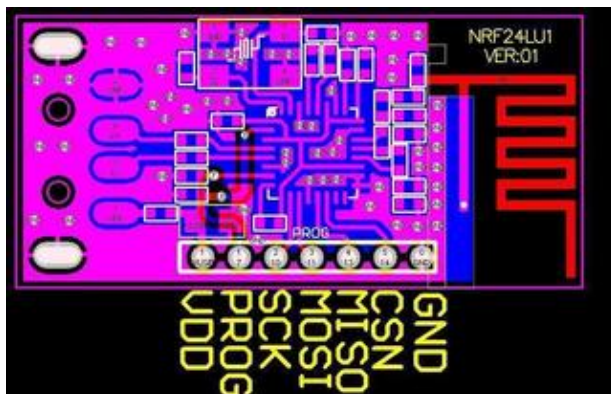


0x00000000 [0, 0]

Contents: [Dobrica PavlinuÄjÄ 's random unstructured stuff]

- Dobrica PavlinuÄjÄ 's random unstructured stuff (pinout)
- Dobrica PavlinuÄjÄ 's random unstructured stuff (original firmware output)
- Dobrica PavlinuÄjÄ 's random unstructured stuff (mouse jack tools)
 - ◆ Dobrica PavlinuÄjÄ 's random unstructured stuff (find device address)
 - ◆ Dobrica PavlinuÄjÄ 's random unstructured stuff (sniff)
- Dobrica PavlinuÄjÄ 's random unstructured stuff (flashing)
 - ◆ Dobrica PavlinuÄjÄ 's random unstructured stuff (bus pirate)
- Dobrica PavlinuÄjÄ 's random unstructured stuff (bootloader)
 - ◆ Dobrica PavlinuÄjÄ 's random unstructured stuff (512 byte replacement)
 - ◆ Dobrica PavlinuÄjÄ 's random unstructured stuff (original bootloader)
- Dobrica PavlinuÄjÄ 's random unstructured stuff (Logitech C-U0007)

pinout



It seems that v2.0 devies are 32k while Internet wants us to beleve that they are 16k (v1.0 maybe?)

original firmware output

```
[11985.181504] usb 2-2.1: new full-speed USB device number 7 using xhci_hcd
[11985.285687] usb 2-2.1: New USB device found, idVendor=1915, idProduct=002b
[11985.285690] usb 2-2.1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[11985.285692] usb 2-2.1: Product: Nordic Semiconductor nRFready Basic Remote Dongle
[11985.285694] usb 2-2.1: Manufacturer: Nordic Semiconductor
[11985.285695] usb 2-2.1: SerialNumber: \xffffffff\xffffffbf\xffffffbf\xffffffef\xffffffbf\xffff
[11985.301719] input: Nordic Semiconductor Nordic Semiconductor nRFready Basic Remote Dongle as /
[11985.361937] hid-generic 0003:1915:002B.0005: input,hiddev0,hidraw2: USB HID v1.11 Keyboard [No
```

mouse jack tools

<https://github.com/BastilleResearch/mousejack>

find device address

```
dpavlin@nuc:/nuc/nRF24L01/mousejack/nrf-research-firmware/tools$ ./nrf24-scanner.py
[2017-01-07 13:50:59.174] 12 0 65:6F:91:A9:07
[2017-01-07 13:51:07.012] 8 10 65:6F:91:A9:07 00:C2:00:00:F8:FF:FE:00:00:49
[2017-01-07 13:51:15.216] 8 10 65:6F:91:A9:07 00:C2:00:00:17:D0:FF:00:00:58
[2017-01-07 13:51:15.231] 8 0 65:6F:91:A9:07
[2017-01-07 13:51:15.698] 12 0 65:6F:91:A9:07
[2017-01-07 13:51:23.456] 8 10 65:6F:91:A9:07 00:C2:00:00:EB:BF:FF:00:00:95
[2017-01-07 13:51:23.503] 8 10 65:6F:91:A9:07 00:C2:00:00:FF:0F:FF:00:00:31
[2017-01-07 13:51:23.509] 8 0 65:6F:91:A9:07
[2017-01-07 13:51:23.840] 12 0 65:6F:91:A9:07
```

sniff

```
dpavlin@nuc:/nuc/nRF24L01/mousejack/nrf-research-firmware/tools$ ./nrf24-sniffer.py -c 8 12 -a 65
[2017-01-07 13:53:34.922] 8 5 65:6F:91:A9:07 00:40:00:08:B8
[2017-01-07 13:53:34.930] 8 5 65:6F:91:A9:07 00:40:00:08:B8
[2017-01-07 13:53:34.938] 8 5 65:6F:91:A9:07 00:40:00:08:B8
[2017-01-07 13:53:34.946] 8 5 65:6F:91:A9:07 00:40:00:08:B8
[2017-01-07 13:53:34.962] 8 5 65:6F:91:A9:07 00:40:00:08:B8
[2017-01-07 13:53:34.970] 8 5 65:6F:91:A9:07 00:40:00:08:B8
[2017-01-07 13:53:34.979] 8 22 65:6F:91:A9:07 00:D3:44:0F:5C:E6:CD:54:B5:71:8C:F9:99:33:00:00
[2017-01-07 13:53:34.986] 8 5 65:6F:91:A9:07 00:40:00:08:B8
[2017-01-07 13:53:34.994] 8 10 65:6F:91:A9:07 00:4F:00:01:18:00:00:00:00:98
[2017-01-07 13:53:35.125] 8 5 65:6F:91:A9:07 00:40:01:18:A7
[2017-01-07 13:53:35.278] 8 22 65:6F:91:A9:07 00:D3:B0:F4:B3:27:E3:BE:34:72:8C:F9:99:34:00:00
[2017-01-07 13:53:35.285] 8 5 65:6F:91:A9:07 00:40:00:08:B8
[2017-01-07 13:53:35.301] 8 5 65:6F:91:A9:07 00:40:00:08:B8
```

flashing

<https://github.com/BastilleResearch/mousejack/issues/6>
https://wiki.bitcraze.io/projects:crazyradio:spi_programming

bus pirate

https://github.com/koolatron/buspirate_nrf24lu1p

```
t=0x8e4f8c8, temp=0x14f03, 1[0, 2]
cell=0x8e4f8c8, temp=0x14f03, 1[0, 2]
Bus Pirate nRF24LU1+
cell=0x8e4f8c8, temp=0x14f03, 1[0, 2]
cell=0x8e4f8c8, temp=0x14f03, 1[0, 2]
3V3 -> VDD
cell=0x8e500d8, temp=0x14f03, 1[0, 2]
cell=0x8e500d8, temp=0x14f03, 1[0, 2]
AUX -> PROG
cell=0x8e50318, temp=0x14f03, 1[0, 2]
cell=0x8e50318, temp=0x14f03, 1[0, 2]
SCK -> SCK
cell=0x8e50578, temp=0x14f03, 1[0, 2]
cell=0x8e50578, temp=0x14f03, 1[0, 2]
MOSI -> MOSI
cell=0x8e50838, temp=0x14f03, 1[0, 2]
cell=0x8e50838, temp=0x14f03, 1[0, 2]
MISO -> MISO
```

cell=0x8e501b16,irq=50e50d78,1[6,2]	CS	->	CSN
cell=0x8e50e2e1,irq=50e571058,1[7,2]	GND	->	GND

```
dpavlin@nuc:/nuc/nRF24L01/buspirate_nrf24lu1p$ ./flasher.pl -device /dev/ttyUSB0 -input ../mousej
```

bootloader

512 byte replacement

<https://github.com/ahtn/nrf24lu1p-512-bootloader>

original bootloader

https://github.com/al177/buspirate_nrf24lu1p

Logitech C-U0007

Version with fixed ctrl+c exit bug: <https://github.com/cl0udz/mousejack>

```
dpavlin@x230:/x230/mousejack$ git remote -v
cl0udz https://github.com/cl0udz/mousejack (fetch)
cl0udz https://github.com/cl0udz/mousejack (push)
```

```
dpavlin@x230:/x230/mousejack/nrf-research-firmware$ make logitech_install
```

```
[Fri Apr 27 22:10:16 2018] usb 1-1.2: new full-speed USB device number 23 using ehci-pci
[Fri Apr 27 22:10:16 2018] usb 1-1.2: New USB device found, idVendor=1915, idProduct=0102
[Fri Apr 27 22:10:16 2018] usb 1-1.2: New USB device strings: Mfr=1, Product=2, SerialNumber=0
[Fri Apr 27 22:10:16 2018] usb 1-1.2: Product: Research Firmware
[Fri Apr 27 22:10:16 2018] usb 1-1.2: Manufacturer: RFStorm
```

```
dpavlin@x230:/x230/mousejack/nrf-research-firmware$ ./tools/nrf24-scanner.py
[2018-04-29 14:23:51.370] 5 22 65:6F:91:A9:07 00:D3:D5:D7:4F:76:ED:63:55:70:EC:77:61:0F:00:00
[2018-04-29 14:23:51.786] 9 5 65:6F:91:A9:07 00:40:00:08:B8
```