WiNX

Uploading Firmware

www.HackerArsenal.com

PENTESTER
ACADEMY

HACKER
ARSENAL
ARTILLERY FOR CYBER WARRIORS

Uploading Firmware

The device comes with the Scanner firmware installed by default. However, other compatible firmware can be download from www.HackerArsenal.com. We will be using the Deceptacon firmware for this demo but the exact same process applies to other firmware downloaded from our website.

Uploading Firmware using Windows/Linux/Mac

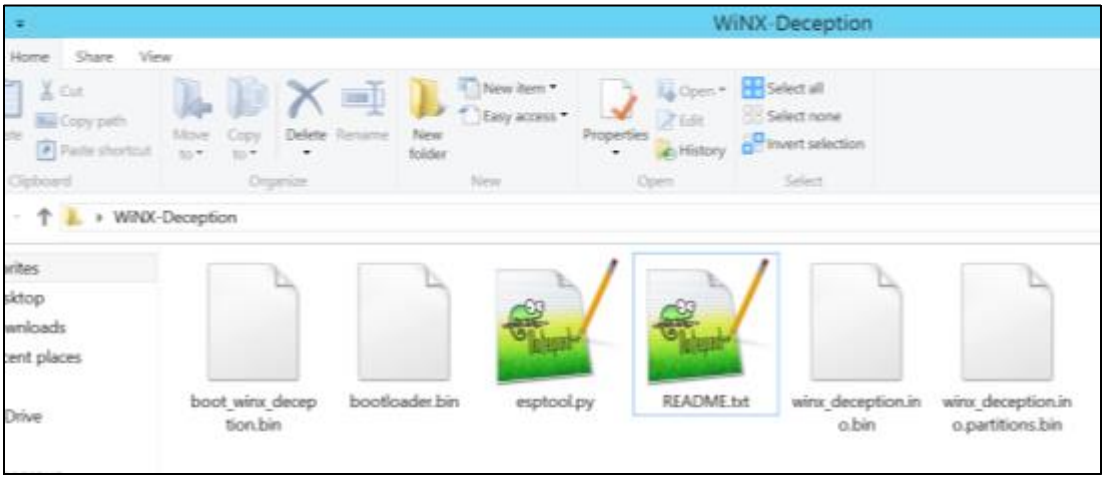
Most operating systems should have the drivers to communicate with our device. However, if this is not the case then you can download the drivers from here:

https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers

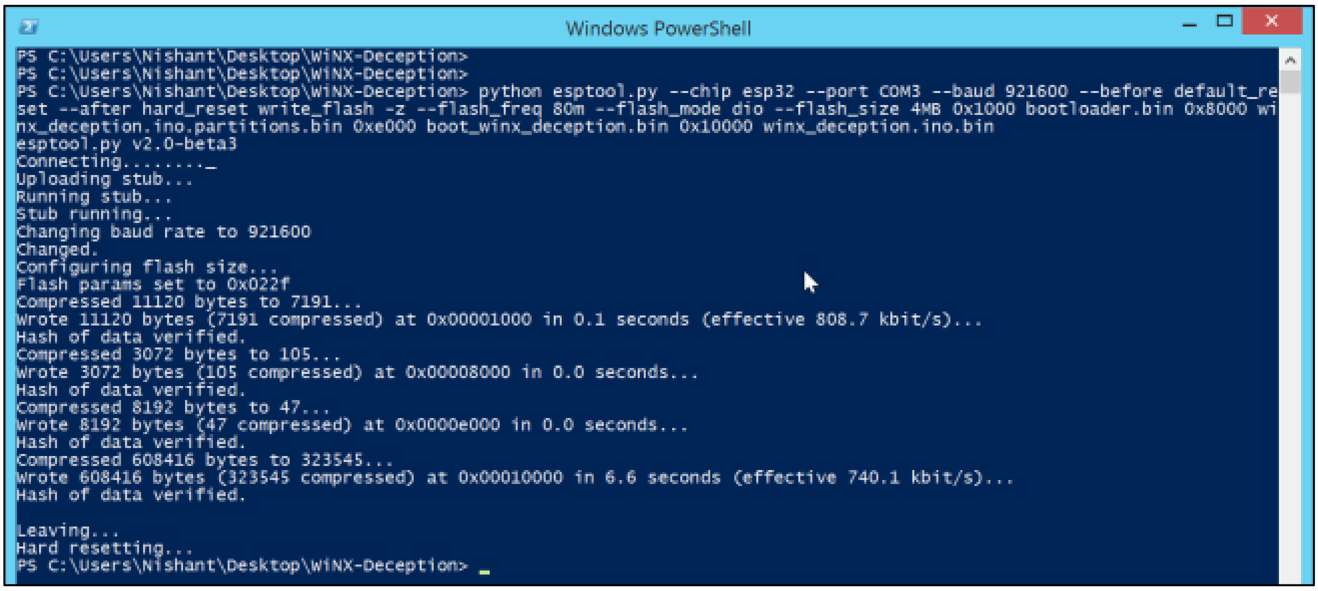
We will be communicating with the device using its serial port which is available over USB. We are going to flash the firmware using a python script called **esptool.py**. The same script will be used on all operating systems. *It is important to note that you will have to run as root / administrator depending on the privileges needed to access the device on your system.*

Windows:

Step 1: Download the firmware you would like to install. This should typically be a ZIP file from our website. Extract the contents of the ZIP file. The folder structure should look like the one below:



Step 2: The *README.txt* in the extracted directory contains the operating system specific command to run to upload the firmware. Please ensure that your device is connected to your laptop. On Windows, open a PowerShell terminal and change to the extracted directory. Now, paste the command and execute it. This should upload and flash the firmware on the device.



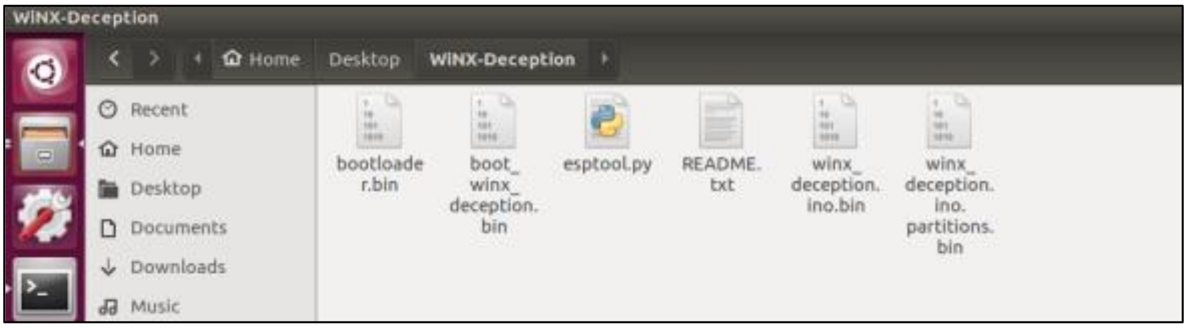
```
PS C:\Users\Nishant\Desktop\WiNX-Deception>
PS C:\Users\Nishant\Desktop\WiNX-Deception>
PS C:\Users\Nishant\Desktop\WiNX-Deception> python esptool.py --chip esp32 --port COM3 --baud 921600 --before default_re
set --after hard_reset write_flash -z --flash_freq 80m --flash_mode dio --flash_size 4MB 0x1000 bootloader.bin 0x8000 wi
nx_deception.ino.partitions.bin 0xe000 boot_winx_deception.bin 0x10000 winx_deception.ino.bin
esptool.py v2.0-beta3
Connecting........_
Uploading stub...
Running stub...
Stub running...
Changing baud rate to 921600
Changed.
Configuring flash size...
Flash params set to 0x022f
Compressed 11120 bytes to 7191...
Wrote 11120 bytes (7191 compressed) at 0x00001000 in 0.1 seconds (effective 808.7 kbit/s)...
Hash of data verified.
Compressed 3072 bytes to 105...
Wrote 3072 bytes (105 compressed) at 0x00008000 in 0.0 seconds...
Hash of data verified.
Compressed 8192 bytes to 47...
Wrote 8192 bytes (47 compressed) at 0x0000e000 in 0.0 seconds...
Hash of data verified.
Compressed 608416 bytes to 323545...
Wrote 608416 bytes (323545 compressed) at 0x00010000 in 6.6 seconds (effective 740.1 kbit/s)...
Hash of data verified.

Leaving...
Hard resetting...
PS C:\Users\Nishant\Desktop\WiNX-Deception> _
```

Your device is now ready to use!

Linux:

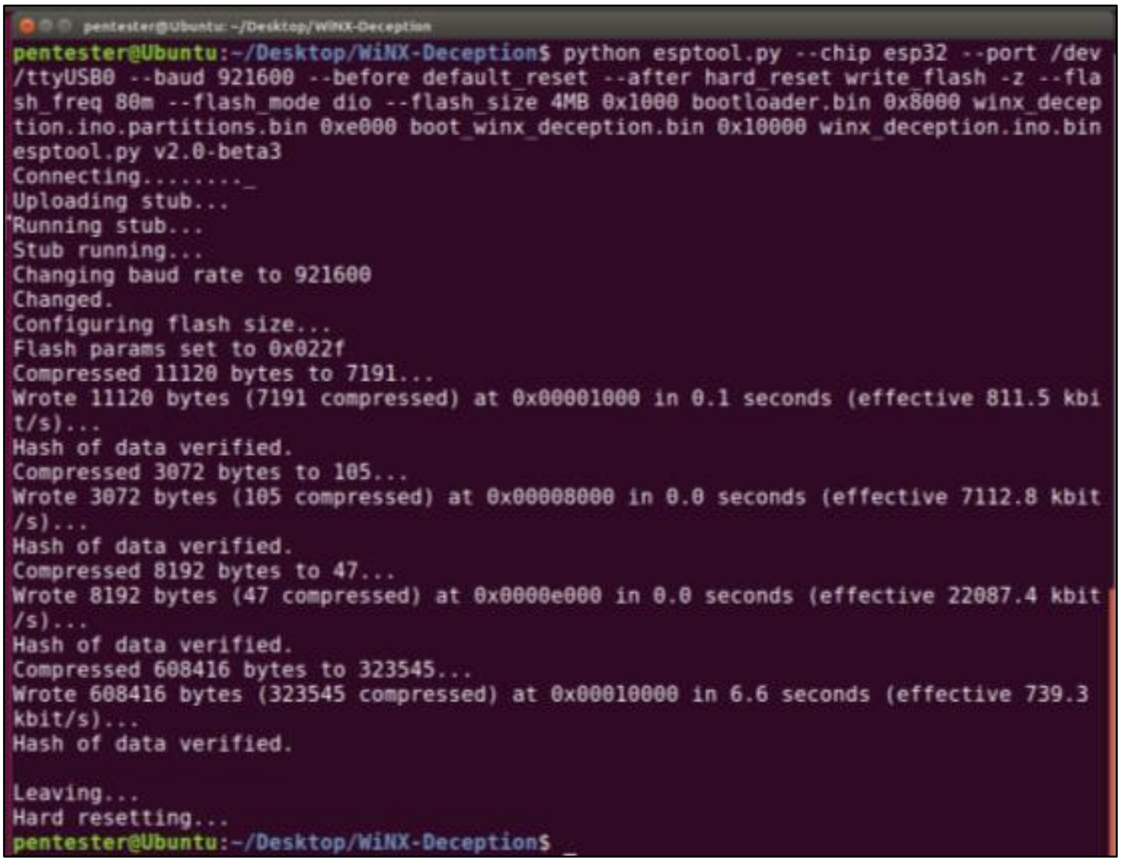
We will be using Ubuntu, but steps would be similar for other Linux distributions.

Step 1: Download and extract the firmware from Hacker Arsenal website. Ensure your device is connected to the laptop.



Copy the command given in the README.txt for Linux. Please make sure the **port** parameter is set correctly.

Step 2: Launch a shell and change to the extracted directory. Now, paste the command and execute it.

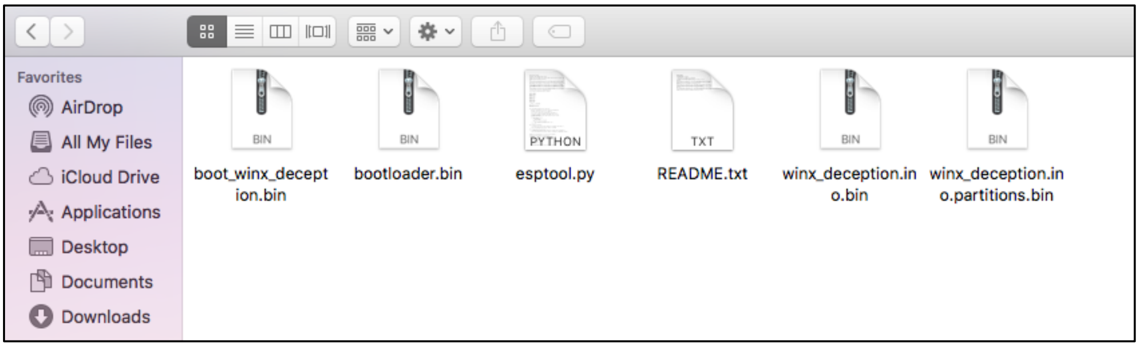


```
pentester@Ubuntu:~/Desktop/WiNX-Deception$ python esptool.py --chip esp32 --port /dev
/ttyUSB0 --baud 921600 --before default_reset --after hard_reset write_flash -z --fla
sh_freq 80m --flash_mode dio --flash_size 4MB 0x1000 bootloader.bin 0x8000 winx_decep
tion.ino.partitions.bin 0xe000 boot_winx_deception.bin 0x10000 winx_deception.ino.bin
esptool.py v2.0-beta3
Connecting........_
Uploading stub...
Running stub...
Stub running...
Changing baud rate to 921600
Changed.
Configuring flash size...
Flash params set to 0x022f
Compressed 11120 bytes to 7191...
Wrote 11120 bytes (7191 compressed) at 0x00001000 in 0.1 seconds (effective 811.5 kbi
t/s)...
Hash of data verified.
Compressed 3072 bytes to 105...
Wrote 3072 bytes (105 compressed) at 0x00008000 in 0.0 seconds (effective 7112.8 kbit
/s)...
Hash of data verified.
Compressed 8192 bytes to 47...
Wrote 8192 bytes (47 compressed) at 0x0000e000 in 0.0 seconds (effective 22087.4 kbit
/s)...
Hash of data verified.
Compressed 608416 bytes to 323545...
Wrote 608416 bytes (323545 compressed) at 0x00010000 in 6.6 seconds (effective 739.3
kbit/s)...
Hash of data verified.

Leaving...
Hard resetting...
pentester@Ubuntu:~/Desktop/WiNX-Deception$ _
```

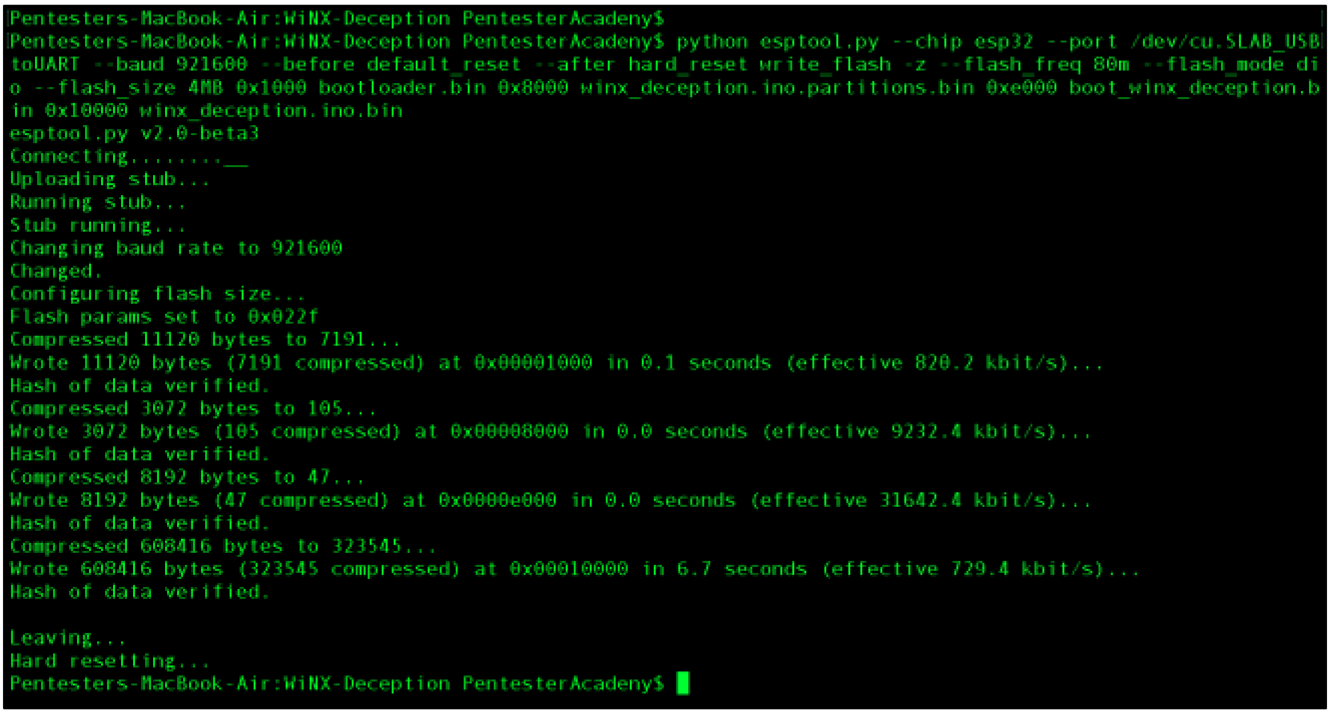
Your device is now ready to use!

Mac:

Step 1: Download and extract the firmware from our website. Ensure your device is connected to your laptop.



Step 2: Copy the command from *README.txt* for the Mac and execute it on a command prompt



```
Pentesters-MacBook-Air:WiNX-Deception PentesterAcadeny$
Pentesters-MacBook-Air:WiNX-Deception PentesterAcadeny$ python esptool.py --chip esp32 --port /dev/cu.SLAB_USB
toUART --baud 921600 --before default_reset --after hard_reset write_flash -z --flash_freq 80m --flash_mode di
o --flash_size 4MB 0x1000 bootloader.bin 0x8000 winx_deception.ino.partitions.bin 0xe000 boot_winx_deception.b
in 0x10000 winx_deception.ino.bin
esptool.py v2.0-beta3
Connecting........__
Uploading stub...
Running stub...
Stub running...
Changing baud rate to 921600
Changed.
Configuring flash size...
Flash params set to 0x022f
Compressed 11120 bytes to 7191...
Wrote 11120 bytes (7191 compressed) at 0x00001000 in 0.1 seconds (effective 820.2 kbit/s)...
Hash of data verified.
Compressed 3072 bytes to 105...
Wrote 3072 bytes (105 compressed) at 0x00008000 in 0.0 seconds (effective 9232.4 kbit/s)...
Hash of data verified.
Compressed 8192 bytes to 47...
Wrote 8192 bytes (47 compressed) at 0x0000e000 in 0.0 seconds (effective 31642.4 kbit/s)...
Hash of data verified.
Compressed 608416 bytes to 323545...
Wrote 608416 bytes (323545 compressed) at 0x00010000 in 6.7 seconds (effective 729.4 kbit/s)...
Hash of data verified.

Leaving...
Hard resetting...
Pentesters-MacBook-Air:WiNX-Deception PentesterAcadeny$ █
```

Your device is now ready to use!

Next Steps:

Depending on the firmware you flashed on the device, please refer to its guide to get started.