Researching a multiprotocol usb modem

or why “S” in “IoT” still stands for “Security”

Ivan Zorin

Independent Researcher

Who am I? // https://ia.github.io

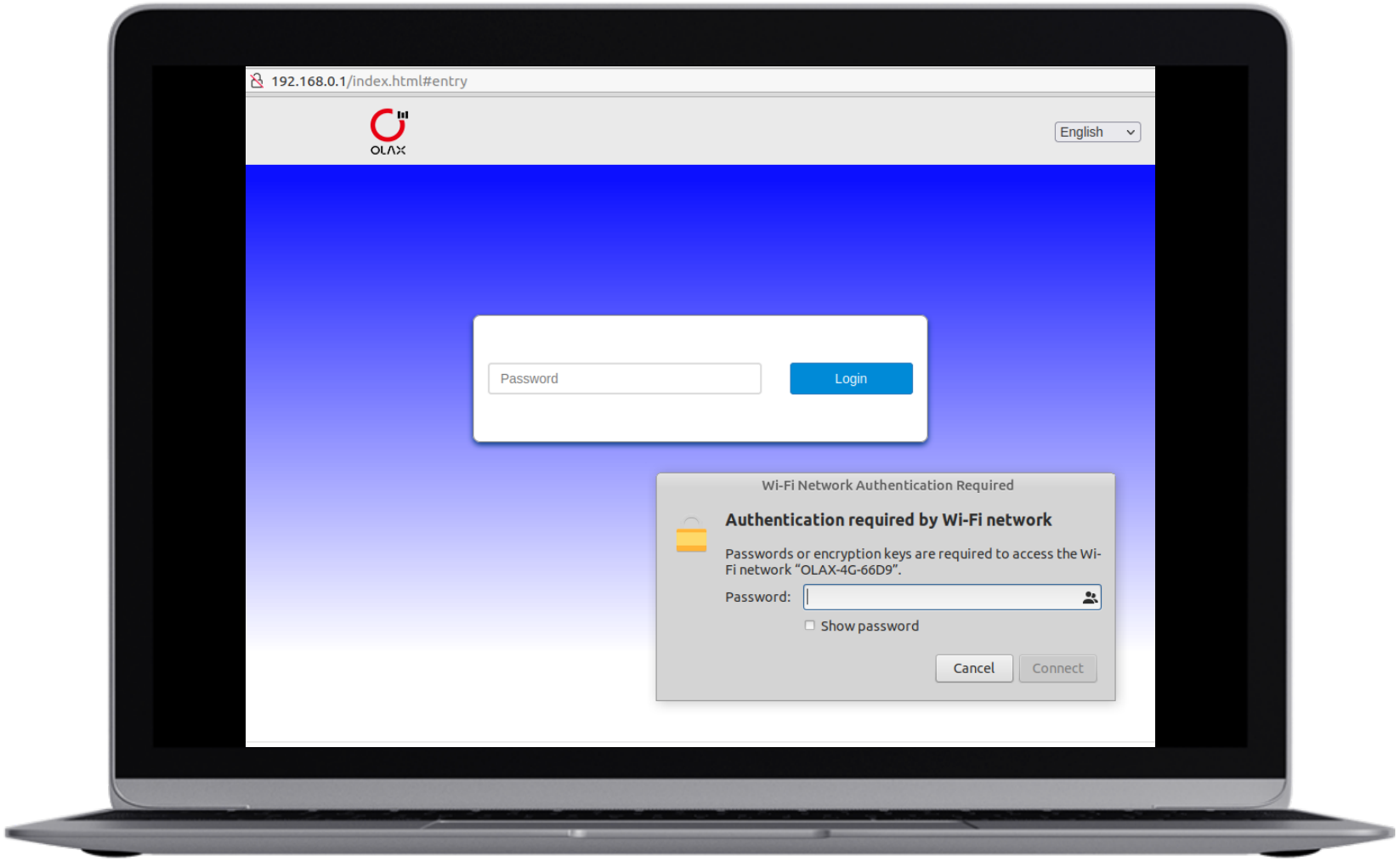
- System Engineer
- Open Source Developer:
  - official IronOS maintainer
  - HydraFW contributor
  - patches, pull requests, bug reports, docs updates, …
- Independent Researcher
- I ❤ Community!
  - Free Software Ideology
  - Right to Repair Movement
  - Hackerspace Culture

Intro

A friend of mine:

- bought multiprotocol usb modem
- but lost & forgot credentials for WiFi AP & WebAdmin
- and did ask me to help…

SadTrombone.ogg



Device *INT

01 OSINT

- fccid.io
- mac.lc
- specifications
- datasheets / schematics

02 PHYINT

- repair kit with screw drivers
- multimeter
- (de)soldering equipment
- *scope

03 SIGINT

- logic analyzer, logic level shifter
- radio sniffers / SDRs (ubertooth, bladerf/hackrf, CC2531), wire sniffers (QC/PD)
- PirateBus / HydraBus, BlackMagicProbe, FlipperZero
- board view software
- nmap, curl, tcpdump / wireshark

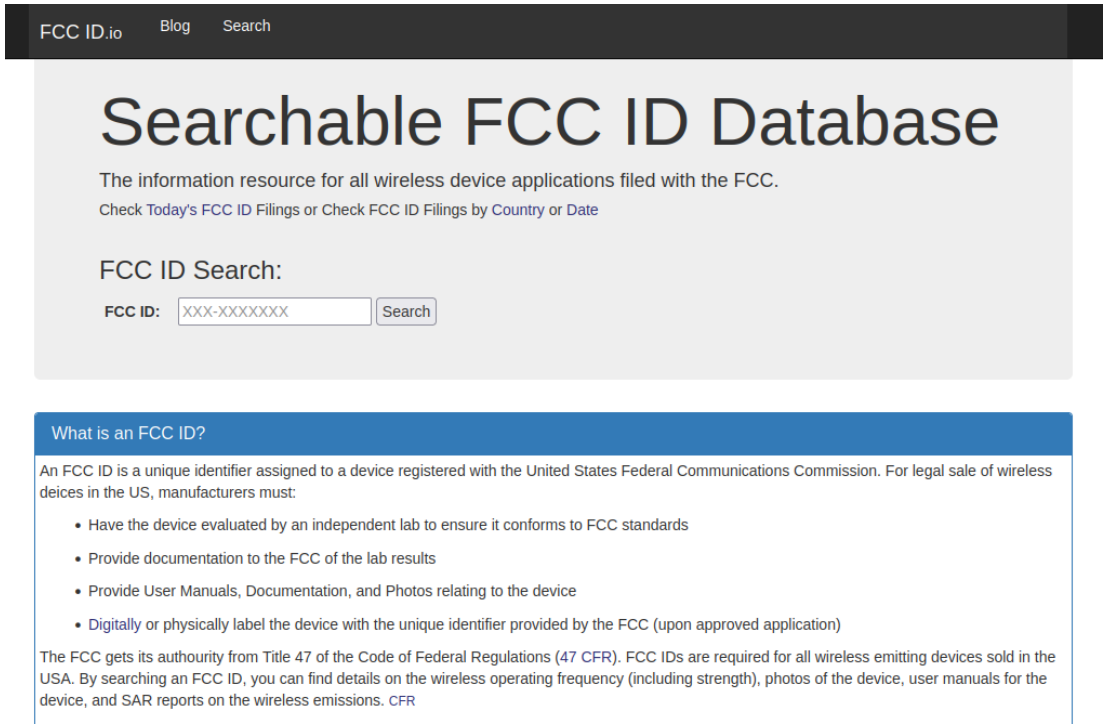
04 BININT

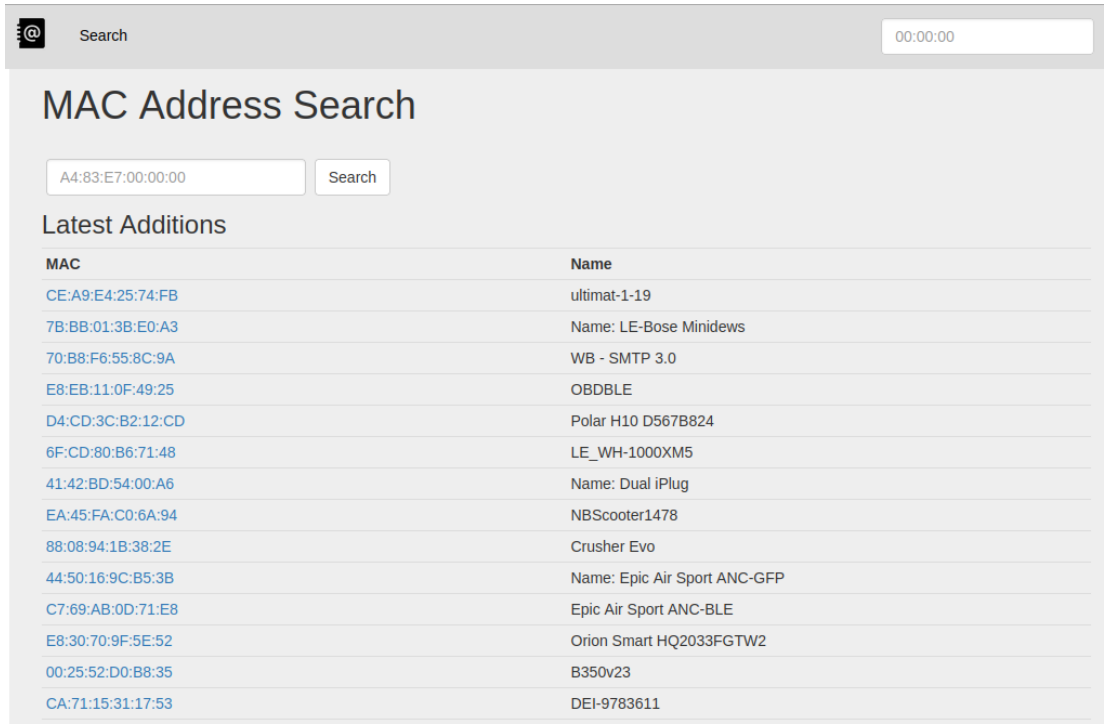
- coreutils { file, hexdump, dd }
- binutils { objdump/objcopy, readelf, strings }
- binwalk, unblob
- gdb / IDA / Ghidra
- mount firmware.fs && cp qemu-ARCH-static firmware.fs/bin/; chroot firmware.fs

05 EVILINT

~~DO NOT~~ BE EVIL TO THE MAX!

OSINT


FCC ID.io
Blog
Search
Searchable FCC ID Database
The information resource for all wireless device applications filed with the FCC.
Check Today's FCC ID Filings or Check FCC ID Filings by Country or Date
FCC ID Search:
FCC ID:
XXX-XXXXXXX
Search
What is an FCC ID?
An FCC ID is a unique identifier assigned to a device registered with the United States Federal Communications Commission. For legal sale of wireless deices in the US, manufacturers must:
Have the device evaluated by an independent lab to ensure it conforms to FCC standards
Provide documentation to the FCC of the lab results
Provide User Manuals, Documentation, and Photos relating to the device
Digitally or physically label the device with the unique identifier provided by the FCC (upon approved application)
The FCC gets its authourity from Title 47 of the Code of Federal Regulations (47 CFR). FCC IDs are required for all wireless emitting devices sold in the USA. By searching an FCC ID, you can find details on the wireless operating frequency (including strength), photos of the device, user manuals for the device, and SAR reports on the wireless emissions. CFR


Search
00:00:00
MAC Address Search
A4:83:E7:00:00:00
Search
Latest Additions
MAC
Name
CE:A9:E4:25:74:FB
ultimat-1-19
7B:BB:01:3B:E0:A3
Name: LE-Bose Minidews
70:B8:F6:55:8C:9A
WB - SMTP 3.0
E8:EB:11:0F:49:25
OBDBLE
D4:CD:3C:B2:12:CD
Polar H10 D567B824
6F:CD:80:B6:71:48
LE_WH-1000XM5
41:42:BD:54:00:A6
Name: Dual iPlug
EA:45:FA:C0:6A:94
NBScooter1478
88:08:94:1B:38:2E
Crusher Evo
44:50:16:9C:B5:3B
Name: Epic Air Sport ANC-GFP
C7:69:AB:0D:71:E8
Epic Air Sport ANC-BLE
E8:30:70:9F:5E:52
Orion Smart HQ2033FGTW2
00:25:52:D0:B8:35
B350v23
CA:71:15:31:17:53
DEI-9783611

PHYINT

SIGINT: what is «signal»?

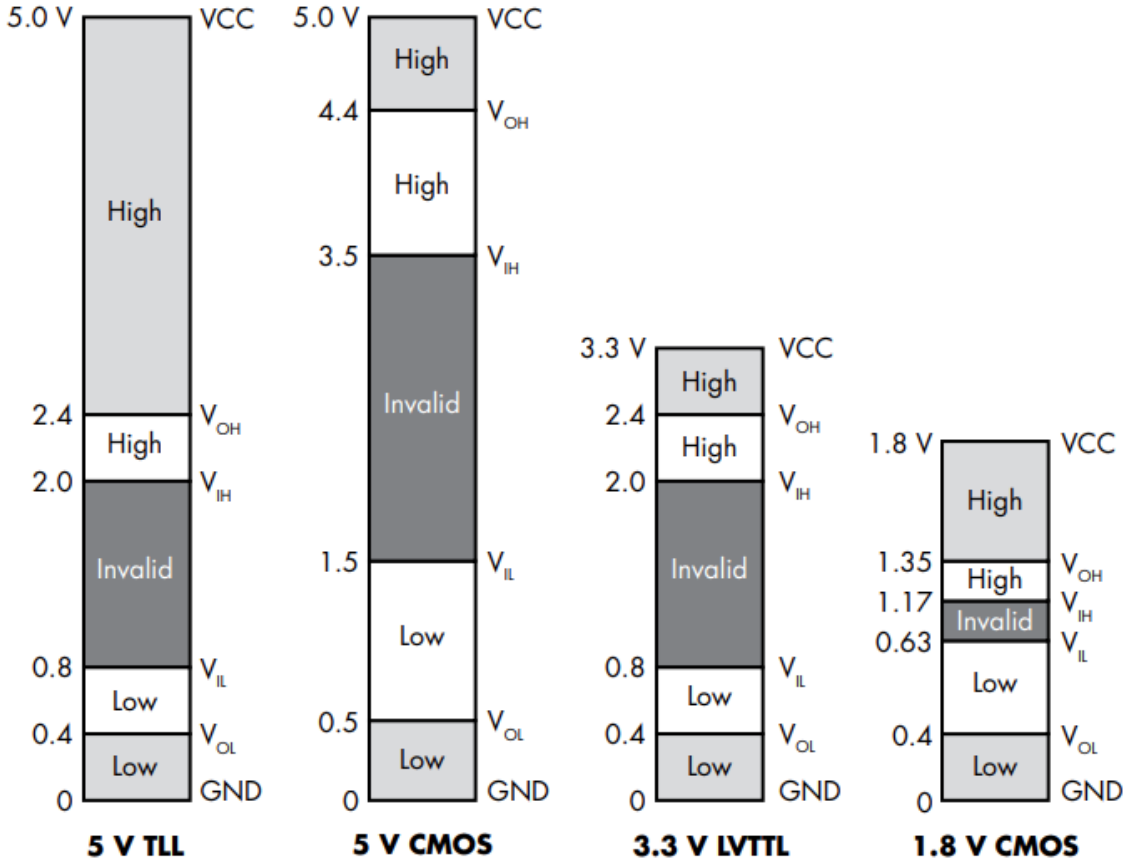
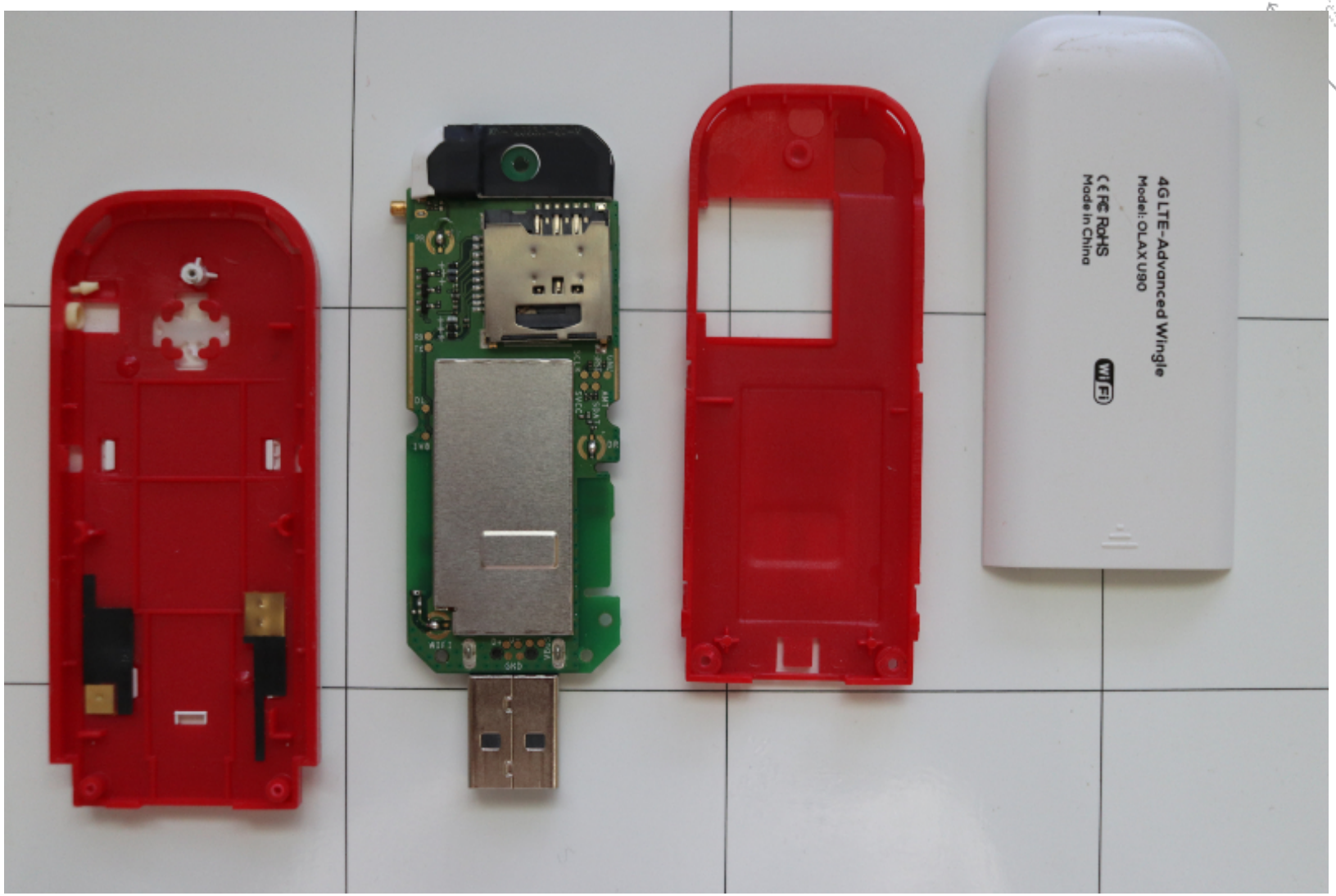


Figure 2-3: Different standard voltage thresholds. Legend: VCC = supply voltage, V_{OH} = required minimum high output voltage, V_{IH} = required minimum high input voltage, V_{IL} = required maximum low input voltage, V_{OL} = required maximum low output voltage, and GND = ground.

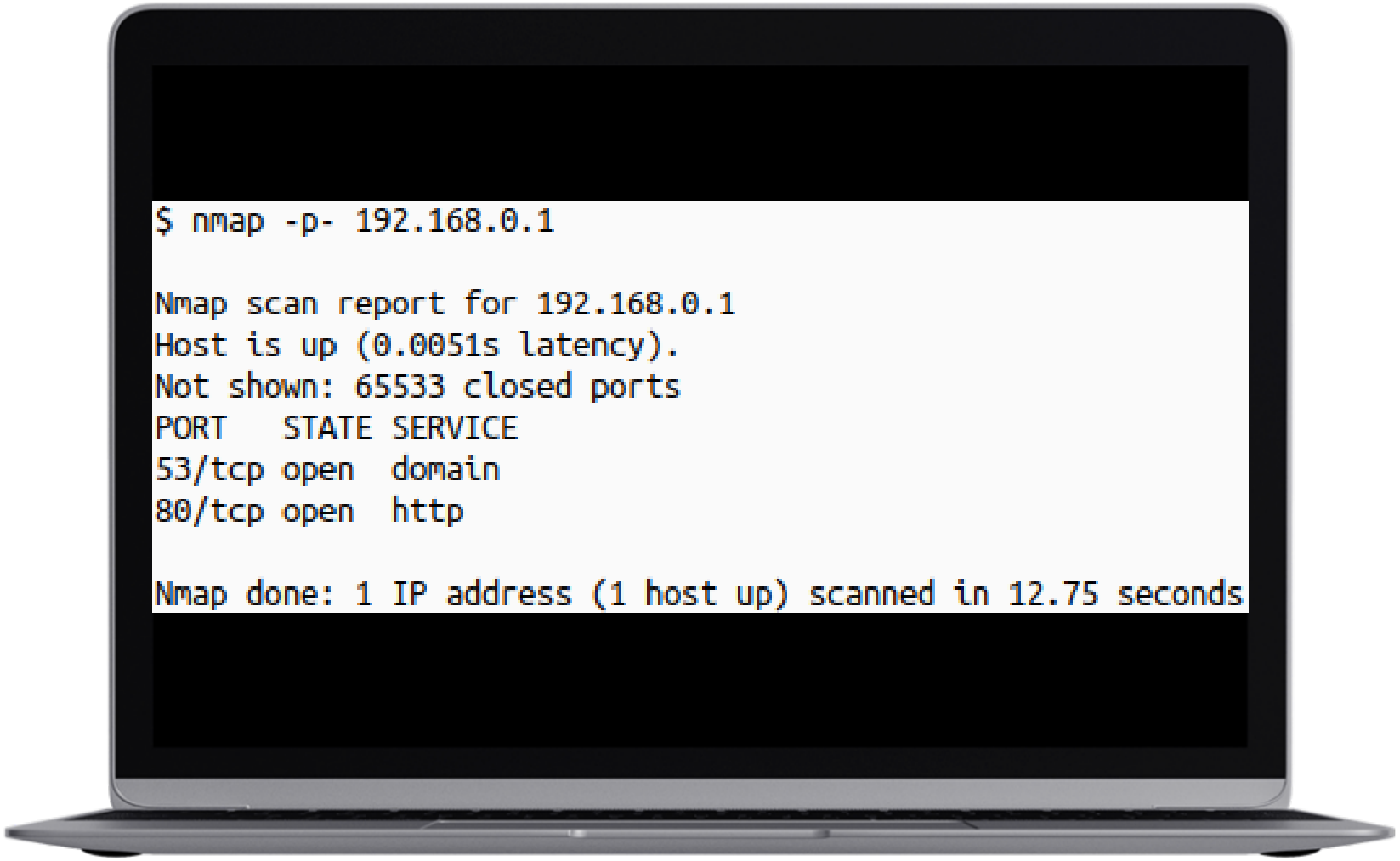
Olax U90


4G LTE-Advanced Wingle
Model: OLAX U90
CE FC RoHS
Made in China
Wi Fi

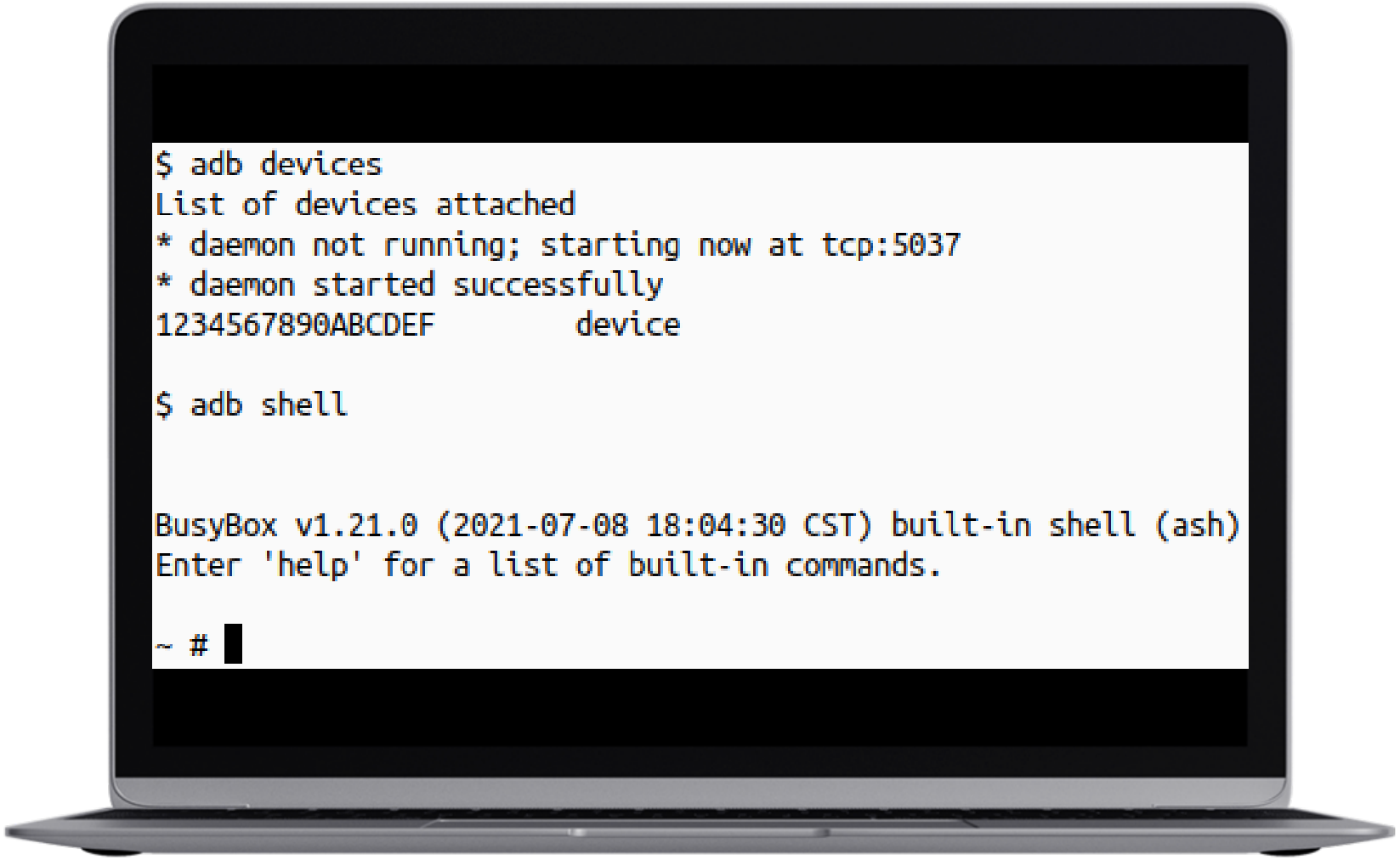
Interfaces

```
[ 3960.206037] usb 2-2: new high-speed USB device number 10 using xhci_hcd
[ 3960.355482] usb 2-2: New USB device found, idVendor=19d2, idProduct=0548
[ 3960.355493] usb 2-2: New USB device strings: Mfr=2, Product=4, SerialNumber=5
[ 3960.355498] usb 2-2: Product: SZXF Mobile Boardband
[ 3960.355502] usb 2-2: Manufacturer: SZXF,Incorporated
[ 3960.355505] usb 2-2: SerialNumber: 1234567890ABCDEF
[ 3960.356773] usb-storage 2-2:1.0: USB Mass Storage device detected
[ 3960.358918] scsi host3: usb-storage 2-2:1.0
[ 3961.362862] scsi 3:0:0:0: CD-ROM            SZXF USB  SCSI CD-ROM 2.3 1    PQ: 0 ANSI: 2
[ 3961.363229] scsi 3:0:0:1: Direct-Access     SZXF MMC  Storage 2.31         PQ: 0 ANSI: 2
[ 3961.364146] sr 3:0:0:0: Power-on or device reset occurred
[ 3961.364653] sr 3:0:0:0: [sr0] scsi-1 drive
[ 3961.364885] sr 3:0:0:0: Attached scsi CD-ROM sr0
[ 3961.365028] sr 3:0:0:0: Attached scsi generic sg3 type 5
[ 3961.365446] sd 3:0:0:1: Attached scsi generic sg4 type 0
[ 3961.365566] sd 3:0:0:1: Power-on or device reset occurred
[ 3961.366346] sd 3:0:0:1: [sdd] Attached SCSI removable disk
[ 3964.372858] usb 2-2: USB disconnect, device number 10
[ 3964.761994] usb 2-2: new high-speed USB device number 11 using xhci_hcd
[ 3964.911348] usb 2-2: New USB device found, idVendor=19d2, idProduct=0536
[ 3964.911357] usb 2-2: New USB device strings: Mfr=2, Product=4, SerialNumber=5
[ 3964.911361] usb 2-2: Product: SZXF Mobile Boardband
[ 3964.911365] usb 2-2: Manufacturer: SZXF,Incorporated
[ 3964.911368] usb 2-2: SerialNumber: 1234567890ABCDEF
[ 3964.915470] cdc_ether 2-2:1.0 eth0: register 'cdc_ether' at usb-0000:00:14.0-2, ZTE CDC Ethernet Device, 34:4b:5
[ 3964.917129] usb-storage 2-2:1.6: USB Mass Storage device detected
[ 3964.918175] scsi host3: usb-storage 2-2:1.6
[ 3964.981303] cdc_ether 2-2:1.0 enx344b50000000: renamed from eth0
[ 3965.027950] IPv6: ADDRCONF(NETDEV_UP): enx344b50000000: link is not ready
[ 3965.228215] userif-2: sent link down event.
[ 3965.228227] userif-2: sent link up event.
[ 3965.786710] userif-2: sent link down event.
[ 3965.786722] userif-2: sent link up event.
[ 3965.946549] scsi 3:0:0:0: Direct-Access     SZXF MMC  Storage 2.31         PQ: 0 ANSI: 2
[ 3965.947313] sd 3:0:0:0: Attached scsi generic sg3 type 0
[ 3965.947546] sd 3:0:0:0: Power-on or device reset occurred
[ 3965.949989] sd 3:0:0:0: [sdd] Attached SCSI removable disk
```

Connectivity



adb access


$ adb devices
List of devices attached
* daemon not running; starting now at tcp:5037
* daemon started successfully
1234567890ABCDEF device
$ adb shell
BusyBox v1.21.0 (2021-07-08 18:04:30 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.
~ #

Guess OS?

```
BusyBox v1.21.0 (2021-07-08 18:04:30 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

~ # free
             total       used       free     shared    buffers     cached
Mem:         44372      34616       9756          0          0       6140
-/+ buffers/cache:      28476      15896
Swap:        12284          0      12284
~ # cat /proc/cpuinfo
Processor       : ARMv7 Processor rev 4 (v7l)
BogoMIPS        : 620.54
Features        : swp half thumb fastmult edsp tls
CPU implementer : 0x41
CPU architecture: 7
CPU variant     : 0x0
CPU part        : 0xd03
CPU revision    : 4

Hardware        : TSP ZX297520V3
Revision        : 0000
Serial          : 0000000000000000
~ # cat /proc/version
Linux version 3.4.110-rt140 (SCM@ZTE) (gcc version 4.7.2 (Buildroot 2013.02) ) #2 PREEMPT RT Thu Jul 8 17:59:10 CST 2021
~ # cat /proc/cmdline
mem=50M root=ubi0:rootfs ubi.mtd=5 ro rootfstype=ubifs console=ttyS1,921600 no_console_suspend mtdparts=spi-nand:128k@0x0(
zloader),1m@0x20000(uboot),1m@0x120000(uboot-mirr),2m@0x220000(nvrofs),16m@0x420000(imagefs),22m@0x1420000(rootfs),8m@0x2a
20000(resource),75m@0x3220000(userdata) lcd_id=255 lcd_dif=201 battery_idt=0 board_dif=2 boot_reason=0
~ # df -h
Filesystem                Size      Used Available Use% Mounted on
ubi0:rootfs              17.7M     11.7M      6.0M  66% /
mdev                     21.7M         0     21.7M   0% /dev
tmpfs                    21.7M         0     21.7M   0% /tmp
tmpfs                    21.7M         0     21.7M   0% /dev/shm
mtd:imagefs              16.0M      7.6M      8.4M  47% /mnt/imagefs
mtd:resource              8.0M      2.7M      5.3M  33% /mnt/resource
ubi1_0                   64.9M      2.4M     62.5M   4% /mnt/userdata
/dev/mtdblock3            2.0M    464.0K      1.5M  23% /mnt/nvrofs
```

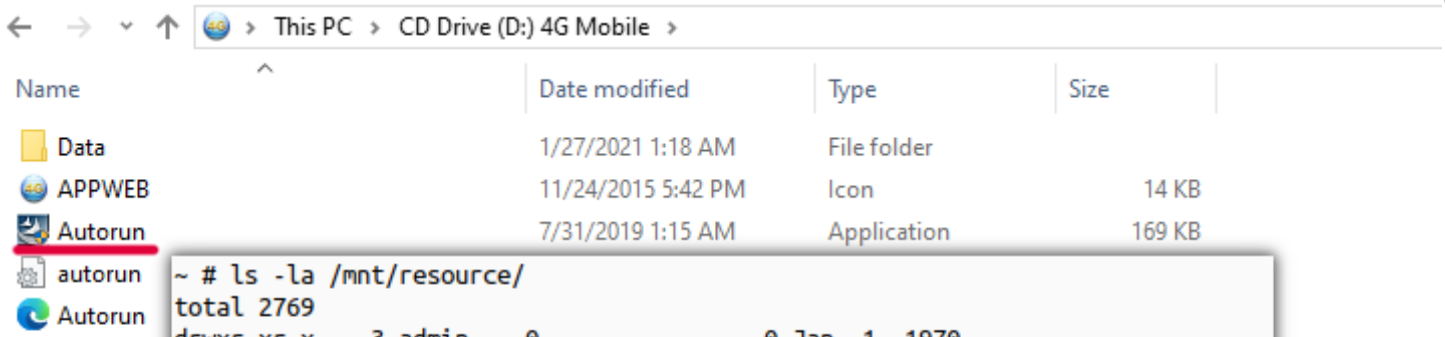
Extract & Locate

53/tcp open

```
~ # netstat -tulnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:53              0.0.0.0:*               LISTEN      1263/dnsmasq
tcp        0      0 127.0.0.1:5037          0.0.0.0:*               LISTEN      1418/adbd
tcp        0      0 :::53                   :::*                    LISTEN      1263/dnsmasq
tcp        0      0 :::80                   :::*                    LISTEN      1414/goahead
udp        0      0 0.0.0.0:53              0.0.0.0:*                           1263/dnsmasq
udp        0      0 0.0.0.0:67              0.0.0.0:*                           1262/udhcpd
udp        0      0 0.0.0.0:1464            0.0.0.0:*                           1263/dnsmasq
udp        0      0 :::53                   :::*                                1263/dnsmasq
~ # cat /mnt/userdata/etc_rw/udhcpd.conf

start 192.168.0.100
end 192.168.0.200
interface br0
option subnet 255.255.255.0
option dns 192.168.0.1
option router 192.168.0.1
option lease 86400
pidfile /etc_rw/udhcpd.pid
lease_file /etc_rw/udhcpd.leases
~ # cat /mnt/userdata/etc_rw/dnsmasq.conf
nameserver 8.8.8.8
nameserver 10.10.32.130
nameserver 10.10.32.131
```

CD-ROM Image

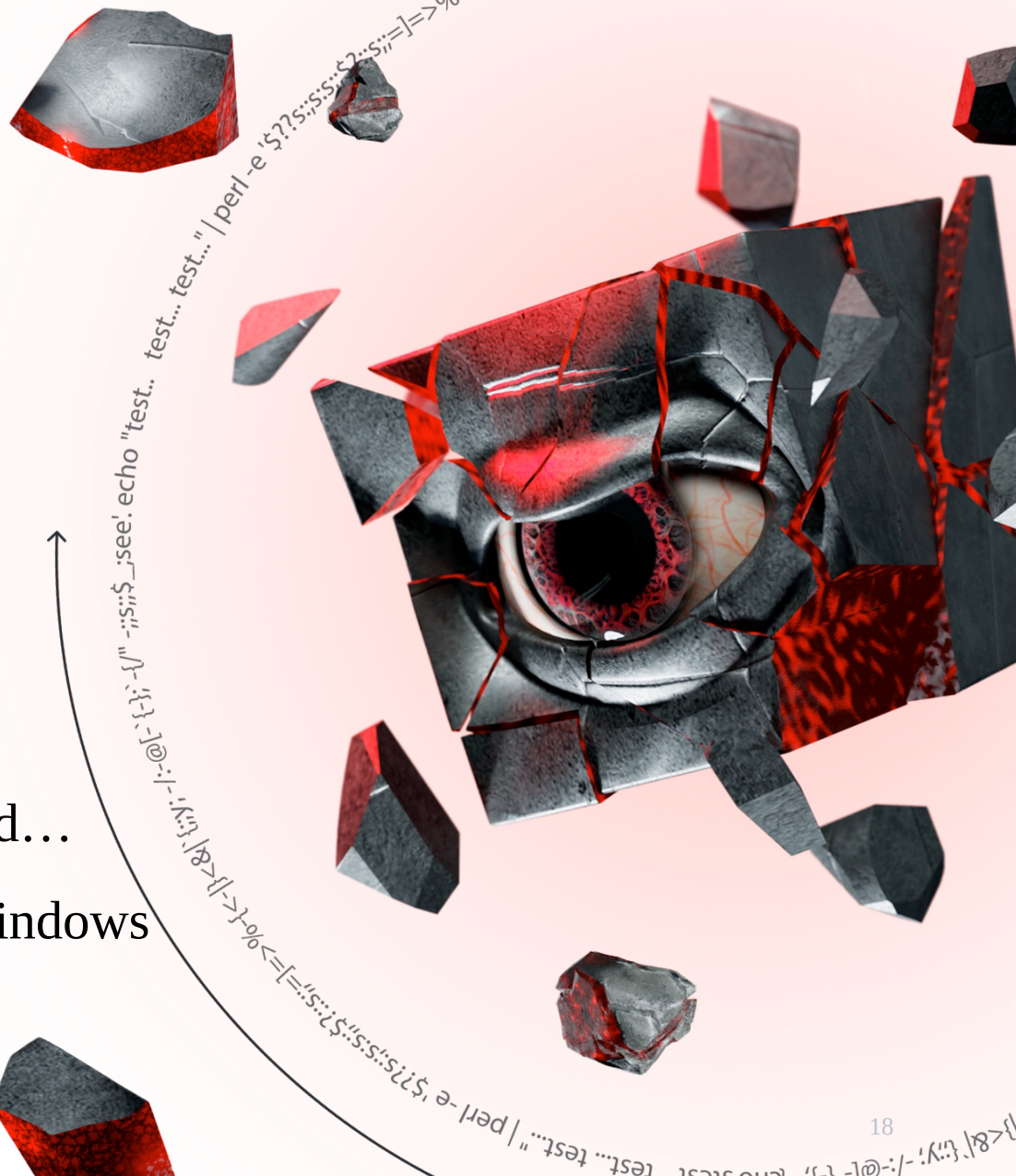



```
~ # ls -la /mnt/resource/
total 2769
drwxr-xr-x    3 admin    0               0 Jan  1  1970 .
drwxrwxr-x    6 1000     1000          432 Jul  8  2021 ..
-rw-r--r--    1 admin    0             32768 Jul  8  2021 CHARGING.bin
-rw-r--r--    1 admin    0                16 Jul  8  2021 LCDINFO.bin
-rw-r--r--    1 admin    0             32768 Jul  8  2021 LOGO.bin
-rw-r--r--    1 admin    0             32768 Jul  8  2021 LOWBAT.bin
-rw-r--r--    1 admin    0             32768 Jul  8  2021 NOBAT.bin
-rw-r--r--    1 admin    0             32768 Jul  8  2021 UPDATING.bin
-rwxr-xr-x    1 admin    0           2670592 Jul  8  2021 ufi_cdrom.iso
~ # exit
$ adb pull /mnt/resource/ufi_cdrom.iso .
/mnt/resource/ufi_cdrom.iso: 1 file pulled. 6.4 MB/s (2670592 bytes in 0.397s)
$ mount -t iso9660 -o loop ./ufi_cdrom.iso /mnt/iso
mount: /mnt/iso: WARNING: device write-protected, mounted read-only.
$ ls -la /mnt/iso
total 189
dr-xr-xr-x 1 root root   2048 Jan 27  2021 .
drwxr-xr-x 1 root root     40 Jun  8  2023 ..
-r-xr-xr-x 1 root root  13942 Nov 25  2015 APPWEB.ico
-r-xr-xr-x 1 root root 173056 Jul 31  2019 Autorun.exe
-r-xr-xr-x 1 root root     46 Jan 22  2015 autorun.inf
-r-xr-xr-x 1 root root    837 Jul 10  2020 Autorun.xml
dr-xr-xr-x 1 root root   2048 Jan 27  2021 Data
```

Covert Channel

Vectors of attack

- BadUSB:
  - CDROM
  - NIC
  - KBD(???)
- (Re)supply chain attack
- Redistribution:
  - infect Windows by a modem with payload…
  - …which infects modems connected to Windows
- Evil WiFi (karma/mana/evil twin/…)



What’s Next?

- u-boot command line
- “populating” test points
- telecom chipset
- …

Mitigations

- factory reset
- hashing of passwords & other credentials
- data encryption (fs/block layer)
- rootfs protection
- secure boot, chain of trust, …

Conclusions

- cheap hardware == cheap security
- a lot of vulnerable devices are out there
- “*insignificant device*” – *DOES NOT MEAN HARMLESS DEVICE*
- (secure) engineering > programming languages, toolchains, buzzwords…

ON FF ONE 2024

Q&A