

0x01624280 [0,0]

Contents: [Dobrica PavlinuÄjiÄ 's random unstructured stuff]

- Dobrica PavlinuÄjiÄ 's random unstructured stuff (meanIT tablet Q70)
  - ◆ Dobrica PavlinuÄjiÄ 's random unstructured stuff (adb shell)
  - ◆ Dobrica PavlinuÄjiÄ 's random unstructured stuff (board)
- Dobrica PavlinuÄjiÄ 's random unstructured stuff (USB FEL)
  - ◆ Dobrica PavlinuÄjiÄ 's random unstructured stuff (device info)
  - ◆ Dobrica PavlinuÄjiÄ 's random unstructured stuff (extract data from device)
  - ◆ Dobrica PavlinuÄjiÄ 's random unstructured stuff (u-boot)
- Dobrica PavlinuÄjiÄ 's random unstructured stuff (malware pre-installed)

## meanIT tablet Q70

7" IPS Quad Core

recovery: extdroid4.4.2\_r2-a33-v2.0

### adb shell

```
dpavlin@siobhan:~$ adb shell
root@astar-ococci:/ #
```

```
root@astar-ococci:/ # cat /proc/cmdline
console=ttyS0,115200 root=/dev/nandd init=/init loglevel=4 specialstr= partitions=bootloader@nand
```

```
root@astar-ococci:/ # cat /proc/cpuinfo
Processor      : ARMv7 Processor rev 5 (v7l)
processor      : 0
BogoMIPS      : 5714.28
```

```
processor      : 1
BogoMIPS      : 4800.00
```

```
processor      : 3
BogoMIPS      : 4800.00
```

```
Features      : swp half thumb fastmult vfp edsp thumbee neon vfpv3 tls vfpv4 idiva idivt
CPU implementer : 0x41
CPU architecture: 7
CPU variant   : 0x0
CPU part      : 0xc07
CPU revision  : 5
```

```
Hardware      : sun8i
Revision     : 0000
Serial       : 1a884915
```

# board

AL-AX3-751B-V1.0  
2015.03.26

[http://linux-sunxi.org/Aoson\\_M751s](http://linux-sunxi.org/Aoson_M751s)

<https://github.com/lcenowy/linux-kernel-lichee-a33/tree/aoson-m751s>

## USB FEL

Vol+ to enter FEL mode

```
Bus 003 Device 004: ID 1f3a:efe8 Onda (unverified) V972 tablet in flashing mode
```

```
root@x230:~# sunxi-fel ver
AWUSBFEX soc=00001667(A33) 00000001 ver=0001 44 08 scratchpad=00007e00 00000000 00000000

# read SID
root@x230:~# sunxi-fel readl 0x01c23800
0x0461872a

root@x230:~# sunxi-fel sid
0461872a:033c50c3:1a884915:00000000
```

## device info

- [http://linux-sunxi.org/Retrieving\\_device\\_information](http://linux-sunxi.org/Retrieving_device_information)

```
dpavlin@x230:~/a33$ sudo sunxi-fel read 0x42400000 0x82d0 boot1.header

# blocks and version doesn't work any more

root@x230:~# sunxi-fel -v read 0x43000000 0x20000 script.bin

# also doesn't transfer anything and hangs
```

## extract data from device

```
dpavlin@klin:/klin/armbian/sunxi-tools$ make CROSS_COMPILE=arm-linux-gnueabihf- sunxi-meminfo
arm-linux-gnueabihf-gcc -std=c99 -Wall -Wextra -Wno-unused-result -D_POSIX_C_SOURCE=200112L -D_BS
dpavlin@klin:/klin/armbian/sunxi-tools$ make CROSS_COMPILE=arm-linux-gnueabihf- sunxi-script_extractor
arm-linux-gnueabihf-gcc -std=c99 -Wall -Wextra -Wno-unused-result -D_POSIX_C_SOURCE=200112L -D_BS

# put files in /cache/ instead of /sdcard/ since /sdcard/ doesn't have executable permission
dpavlin@x230:/mnt/klin/klin/armbian/sunxi-tools$ adb push sunxi-script_extractor /cache/
[100%] /cache/sunxi-script_extractor
dpavlin@x230:/mnt/klin/klin/armbian/sunxi-tools$ adb push sunxi-meminfo /cache/
[100%] /cache/sunxi-meminfo

root@astar-ococci:/cache # ./sunxi-meminfo
```

```
Error: unknown or unhandled Soc: 0x1667
```

```
255|
```

```
# urgh!
```

```
svroot@astar-ococci:/cache # ./sunxi-script_extractor > a33.bin
```

```
root@astar-ococci:/cache # ls -al a33.bin
```

```
-rw-rw-rw- root      root      131072 2017-10-18 17:57 a33.bin
```

## u-boot

```
dpavlin@klin:/klin/u-boot$ git remote -v
```

```
sunxi  git://git.denx.de/u-boot-sunxi.git (fetch)
```

```
sunxi  git://git.denx.de/u-boot-sunxi.git (push)
```

```
dpavlin@klin:/klin/u-boot$ git checkout -b sunxi/next sunxi/next
```

```
Branch 'sunxi/next' set up to track remote branch 'next' from 'sunxi'.
```

```
Switched to a new branch 'sunxi/next'
```

```
dpavlin@klin:/klin/u-boot$ make CROSS_COMPILE=arm-linux-gnueabihf- q8_a33_tablet_1024x600_defconf
```

```
dpavlin@klin:/klin/u-boot$ make CROSS_COMPILE=arm-linux-gnueabihf- -j4
```

- <http://linux-sunxi.org/FEL/USBBoot>

## malware pre-installed

- com.adups.fota