

Intel ME Cleaner

Using me_cleaner

Needless to say, there is a certain amount of risk of bricking your system when it comes to this procedure. Proceed with caution!

Make sure that any kind of battery is unplugged from the computer

- This includes your laptop battery as well as your RTC (coin cell) battery!

Clip an SPI reader that is compatible with flashrom onto your motherboard's bios chip

- Supported programmers
- Make sure to consult the datasheet for the specific EEPROM that your motherboard uses when wiring the pins to the programmer. For example, on a

3. PIN CONFIGURATION SOIC 150 / 208-MIL

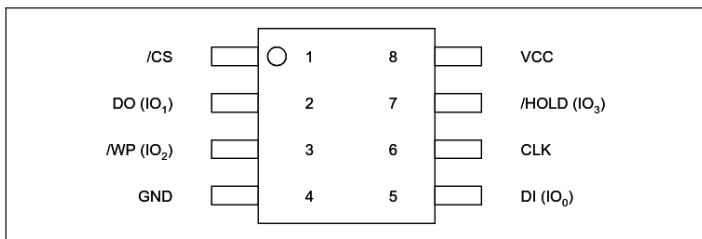


Figure 1a. W25Q16BV Pin Assignments, 8-pin SOIC 150 / 208-mil (Package Code SN & SS)

On a separate computer, interface with the SPI programmer and try reading off of the EEPROM

```
flashrom -p linux_spi:dev=/dev/spidev0.0,spispeed=1000 -r original_dump.bin
```

- May need to mess around with SPI speed
 - If you are using a Raspberry Pi, make sure to enable SPI using `raspi-config`!
- Dump the firmware multiple times and store them safely.

Use me_cleaner to modify the original firmware dump

Consult the project's wiki. Essentially, you can do one of two things:

```
# Set HAP bit as well as attempt to remove portions of the ME firmware
```

```
python me_cleaner.py -S -O modified_image.bin original_dump.bin
```

```
# Only sets HAP bit. Used if the above command fails
```

```
python me_cleaner.py -s -O modified_image.bin original_dump.bin
```

Write to the EEPROM

```
flashrom -p linux_spi:dev=/dev/spidev0.0,spispeed=1000 -w modified_image.bin
```

You may also want to, after writing to the EEPROM, *read the firmware again* and use me_cleaner to verify that the firmware has been cleaned properly.

```
python me_cleaner.py -c firmware_to_check.bin
```

```
# You can also use intelmetool
```

```
sudo intelmetool -m
```

```
# Output:
```

```
# Can't find ME PCI device
```

You can also check in your bios. On my T480 and L390, the ME Firmware Version is blanked out.

Cheers!

Other Notes

Updating the BIOS

For whatever reason, my T480 *really* does not want to update its own bios after using me_cleaner. In contrast, my L390 does not have this issue. Anyways, if you choose to update the bios, make sure that me_cleaner is still active afterwards using the aforementioned methods. My L390 for example keeps its HAP bit set even after a bios upgrade.

Revision #5

Created 26 July 2024 17:17:14 by GT

Updated 26 July 2024 18:20:40 by GT