# Anti-VM with ACPI tables

@gsuberland

# whois

- Graham Sutherland
- Twitter: @gsuberland (partyhat)
- IRC: gsuberland on freenode
- Email: contact@fisting.horse

# disclaimer

This talk does not reflect, refract, absorb, ionise, engage in quantum superposition with, or otherwise associate with the views of my employer, their clients, or their clients' clients.

I like where I work. Please don't fire me.

Research done in 3 hours. Slides written in an hour.

I borrowed this laptop from @dominicgs, don't judge me for any donkey porn popups or other sketchy business.

This may or may not be original research. Who knows. The internet is a pretty big place.

# how this came about

- Looking into WPBT at lunch today
- Discovered ACPI tables are A Thing(TM)
- A thought occurs (a rarity, I know)
- Looked into it, vague mentions from places
- I now know that AV knows about this trick

# dafuq is an ACPI table?

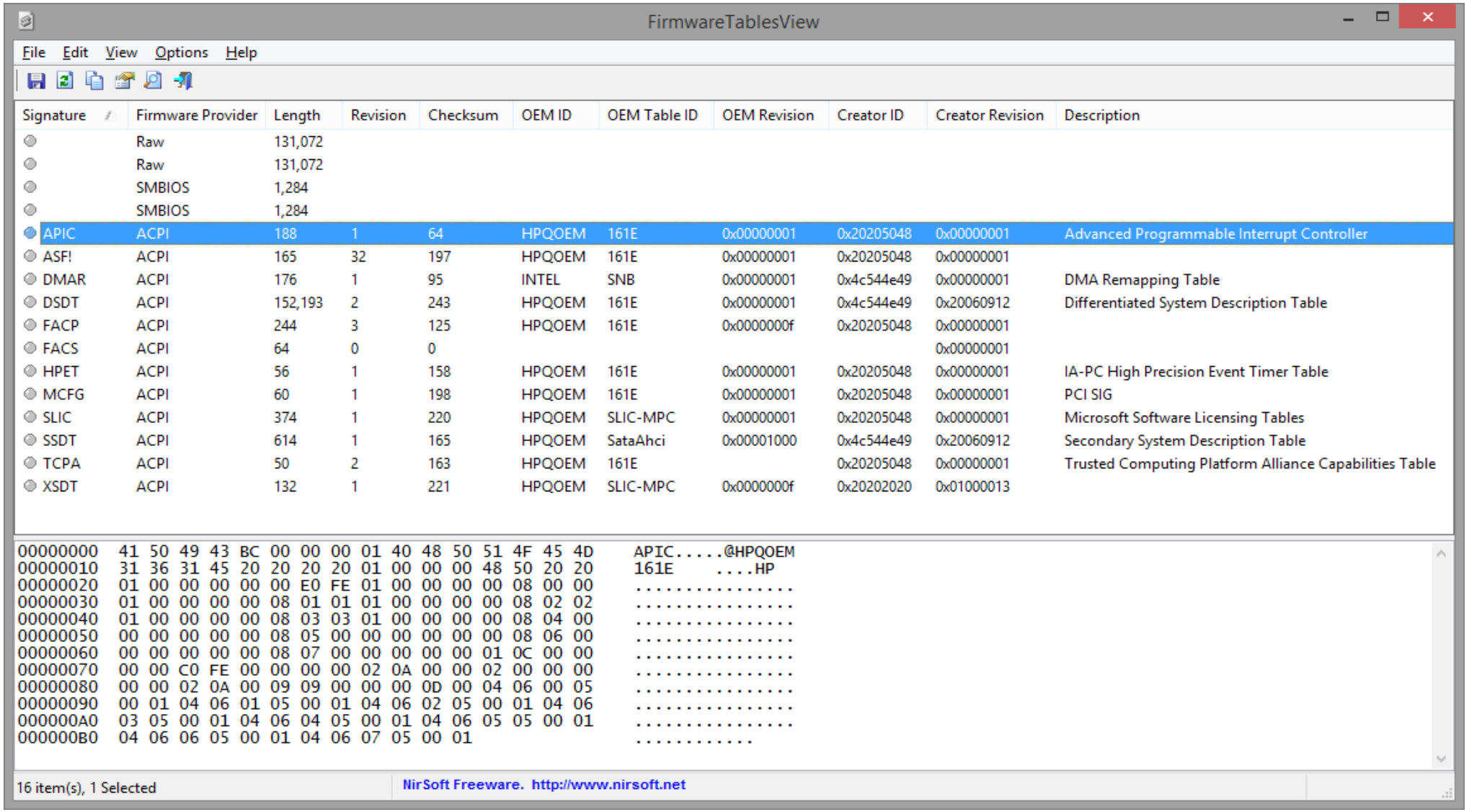
- Bunch of data tables from hardware
- Used to expose hardware config to OS
- Contains stuff like:
  - SMBIOS data
  - APIC data
  - PCI data
  - HPET data
  - SLIC licenses
  - Trusted Computing evil
  - WPBT evil

# so what?

- Tables have names
- Tables have OEM IDs
- Tables have OEM Table IDs
- Tables have Creator IDs
- Tables contain system-specific data
- This stuff isn't (usually) faked by VMs
- It's accessible from ring3, non-admin!
  - (on Windows)

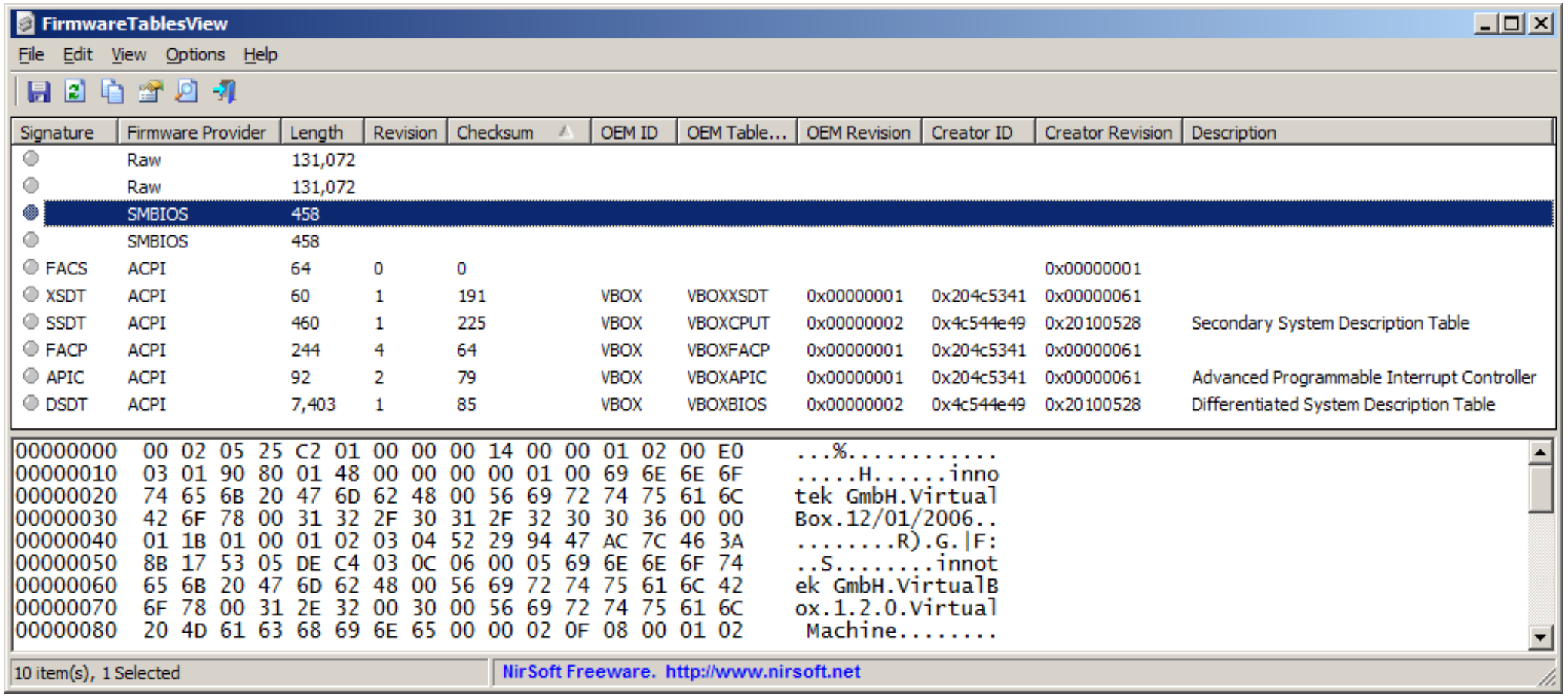
# what you talkin bout willis?

## picture > 1000 WORDs



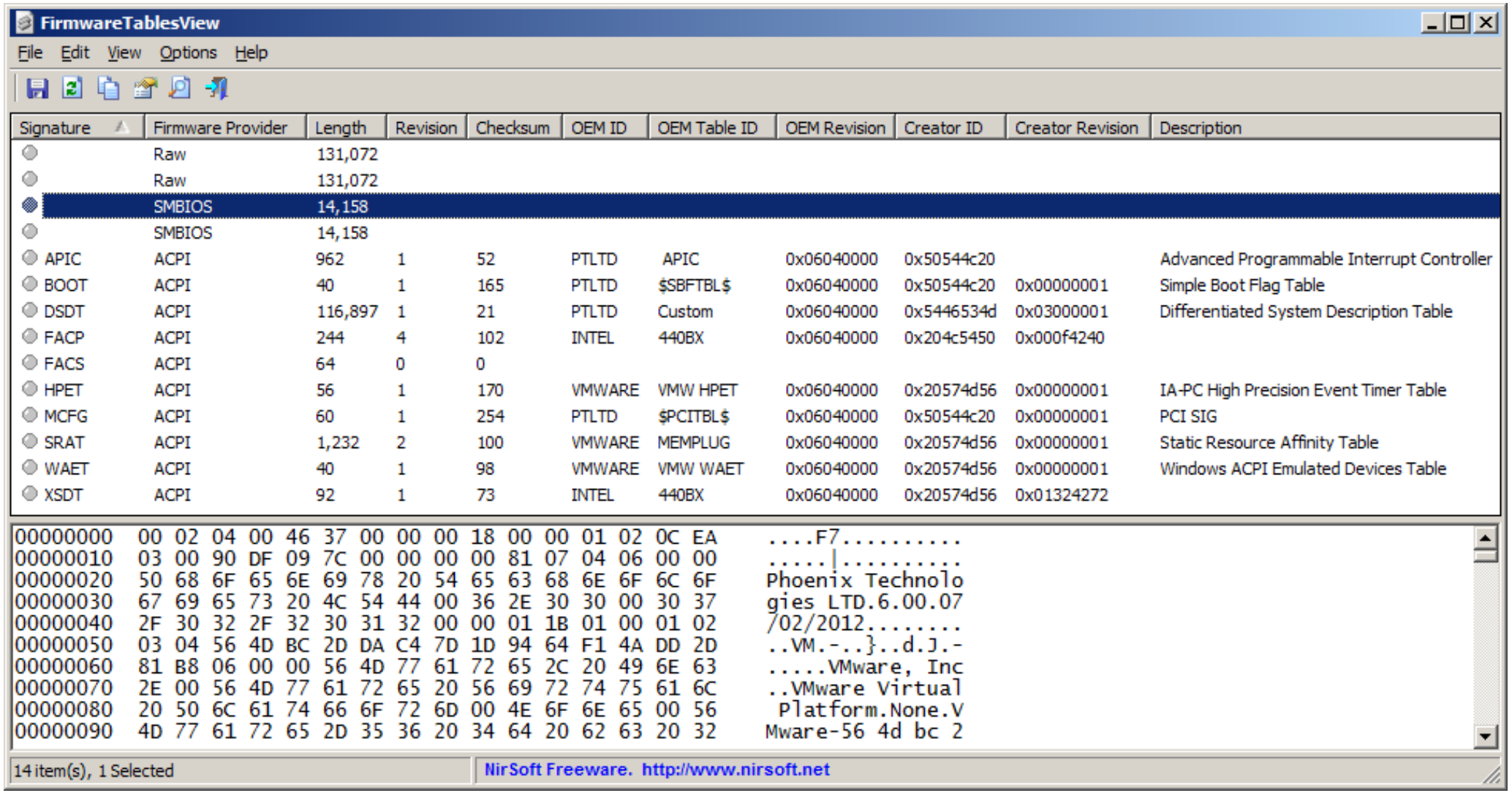
# virtually undetectable differences

## 2008R2 x64, VirtualBox



# and on vmware?

## 2008R2 x64, VMware Workstation



# teh code?

- Kernel32.dll
  - EnumSystemFirmwareTables
  - GetSystemFirmwareTable
- Fully documented on MSDN
- Trivial to use, even a Lemon could do it
- Probably comparable APIs on Linux/BSD
  - (I am a Windows monkey, don't ask me.)

# approach

- Enumerate ACPI, FIRM, RSMB system tables
- Get info & contents for each table
- Check for known VM values
- Exit if found

# countermeasures

- VboxAntiVMDetectHardened (kernelmode.info)
  - Replaces some ACPI tables
  - Fixes lots of hardware descriptors
  - Doesn't fix everything!
  - Only for VirtualBox.
- AV
  - Some AV detects code that enumerates firmware tables, via heuristic magics.
- Only run Windows XP
  - XP doesn't support dumping FIRM and RSMB
  - This is not a solution ever :-\
- ???
  - Anyone know something I don't?

# future research

- Results from ESXi, QEMU, KVM, etc.
- Results from other guest operating systems.
- Deeper analysis of table contents for variances.
- A public PoC that's actually worth a damn.
- ????

# kthxbai

any questions?