Advanced x86:
BIOS and System Management Mode Internals
Chipset Architecture

Xeno Kovah && Corey Kallenberg

LegbaCore, LLC

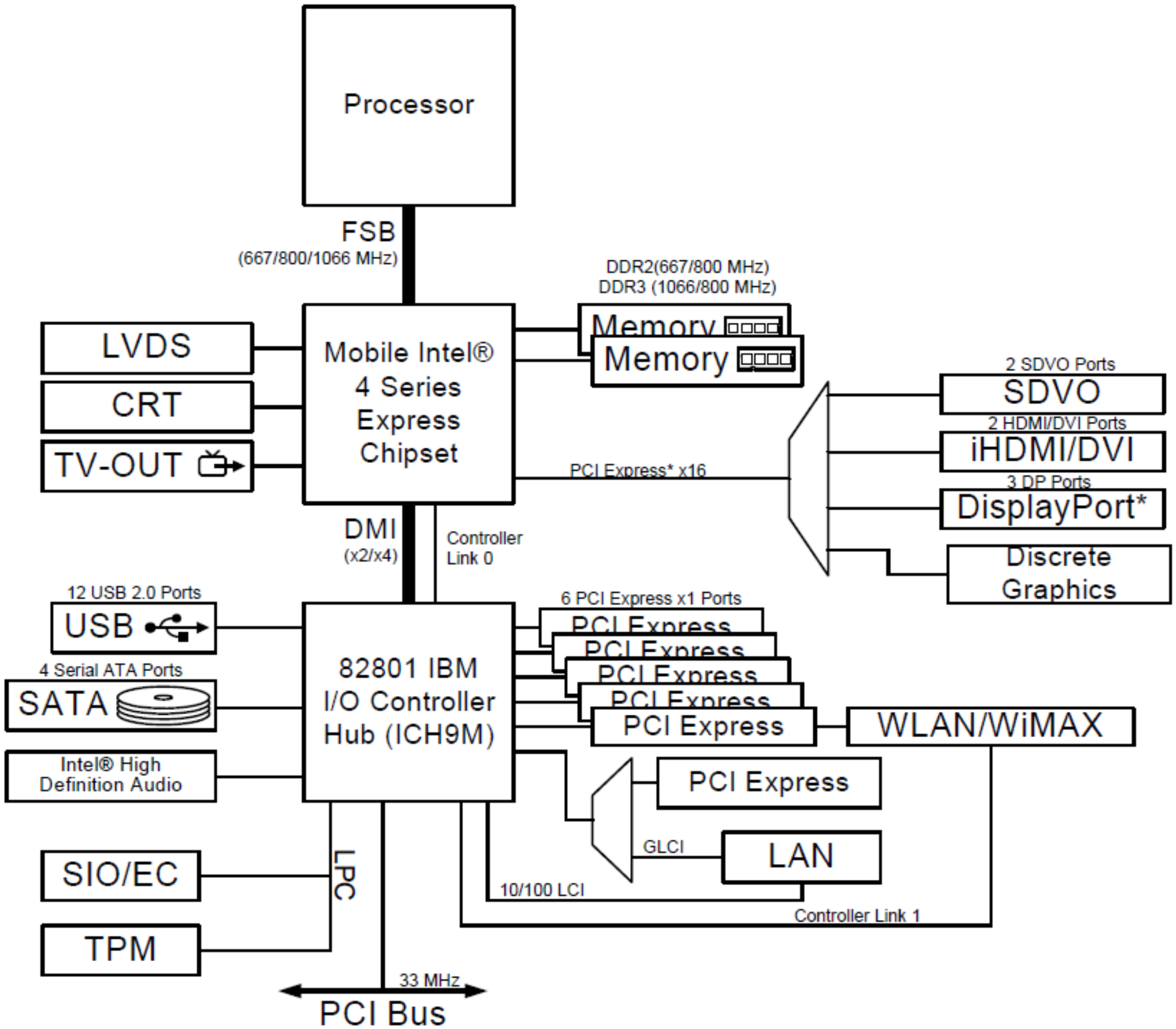
LEGBACORE

WE DO DIGITAL VOODOO

(Basic) Chipset Architecture

Since I always lose the link, CPU datasheets are here:
http://www.intel.com/content/www/us/en/processors/core/core-technical-resources.html

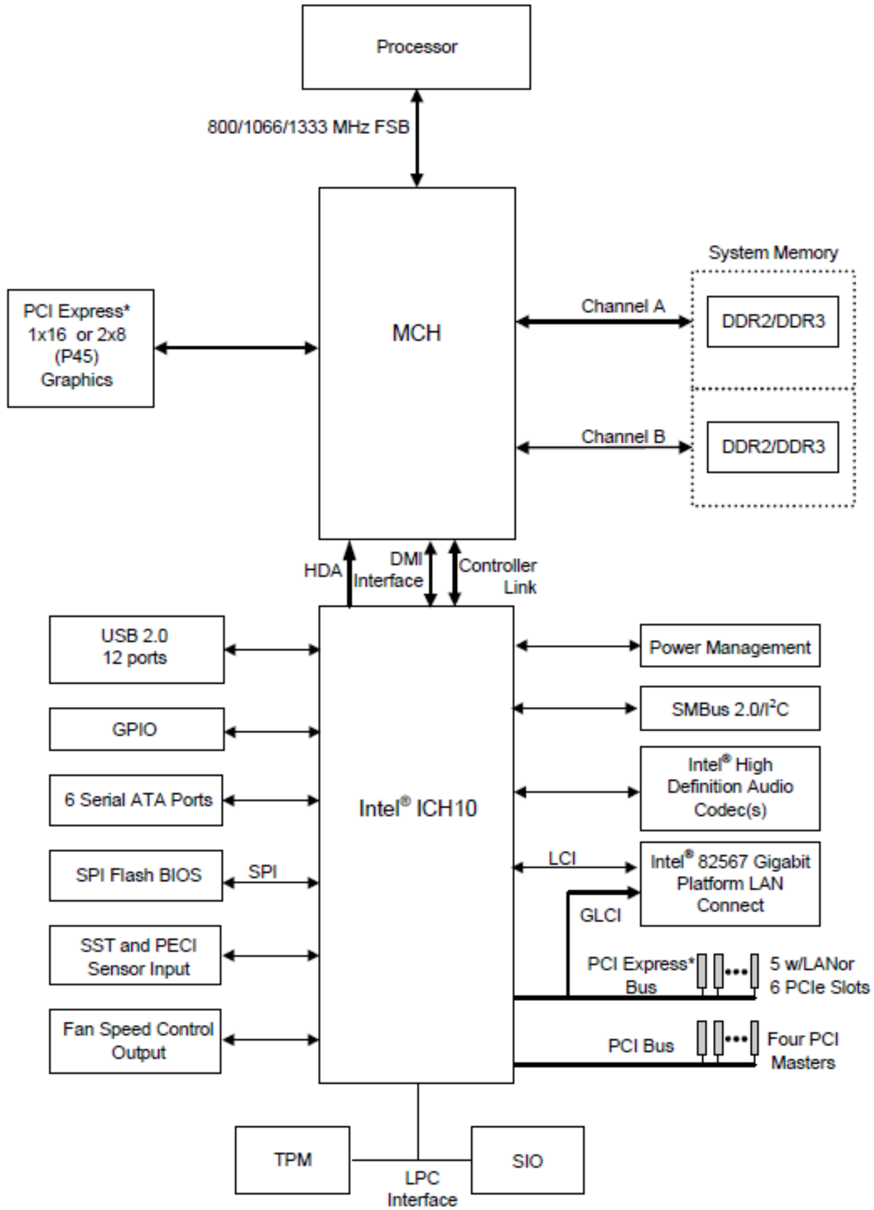
Mobile 4-Series Chipset Block Diagram



- This is a hardware model the Mobile 4-Series chipset and its logical relation to the CPU
- Specialized chips integrated onto the motherboard that interface the processor to system components.
- Two components make up the chipset: the Memory Controller Hub (MCH) and the I/O Controller Hub (ICH)
- These components must be configured to be able to sustain an Operating System.
- BIOS performs this configuration during boot
- I prefer the diagram from the Desktop 4-Series Chipset, which explicitly labels the MCH

Intel Mobile 4-Series Chipset Datasheet, pg. 13

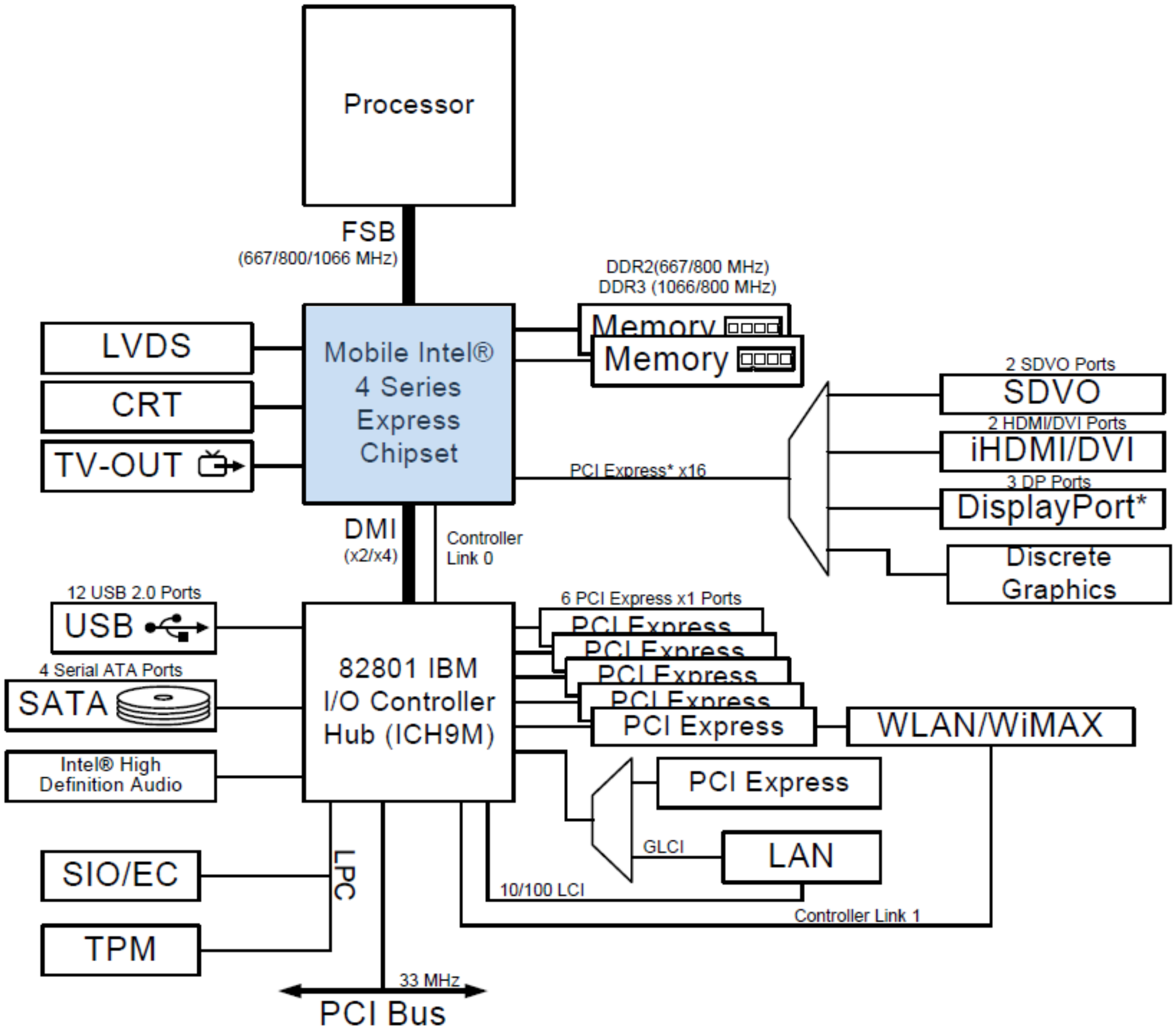
Alternative Block Diagram



- For reference, this is the diagram layout I personally (strongly) prefer
- But it explicitly labels the MCH
- Also lists the SPI device, unlike it’s Mobile counterpart
- However, the MCH on the 4-Series chipset connects to an ICH rev. 10 rather than an ICH rev. 9, which is not what's present on this example E6400 system

Intel 4-Series Chipset Datasheet, pg. 25

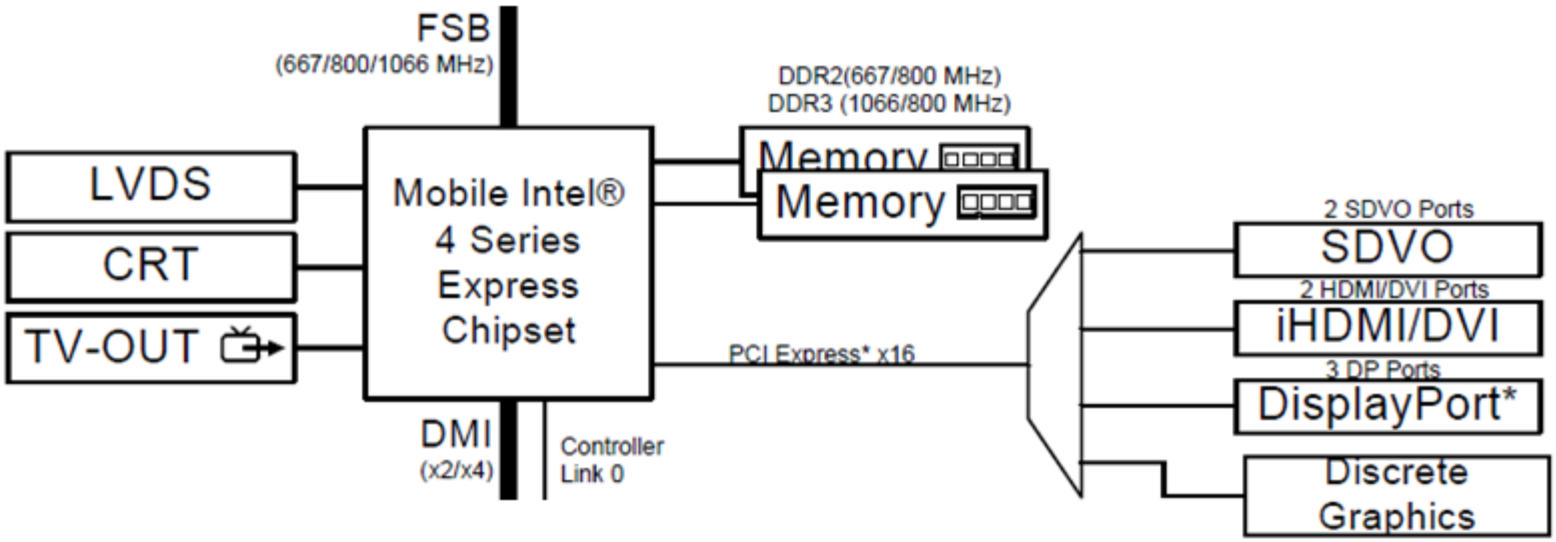
Mobile 4-Series Chipset Block Diagram



- Memory Controller Hub (MCH)
- Interfaces the processor with the rest of the system
- Connected via a fast bridge/bus (originally FSB, became HyperTransport (AMD) and QuickPath (Intel), the latter which became DMI (or DMI 2.0)
  - From a logical perspective it's invisible to us for our purposes
- Sometimes called the Northbridge
- Contains a Memory Controller and an interface for PCI Express graphics
- A 'G' in front of MCH indicates it has on-board graphics

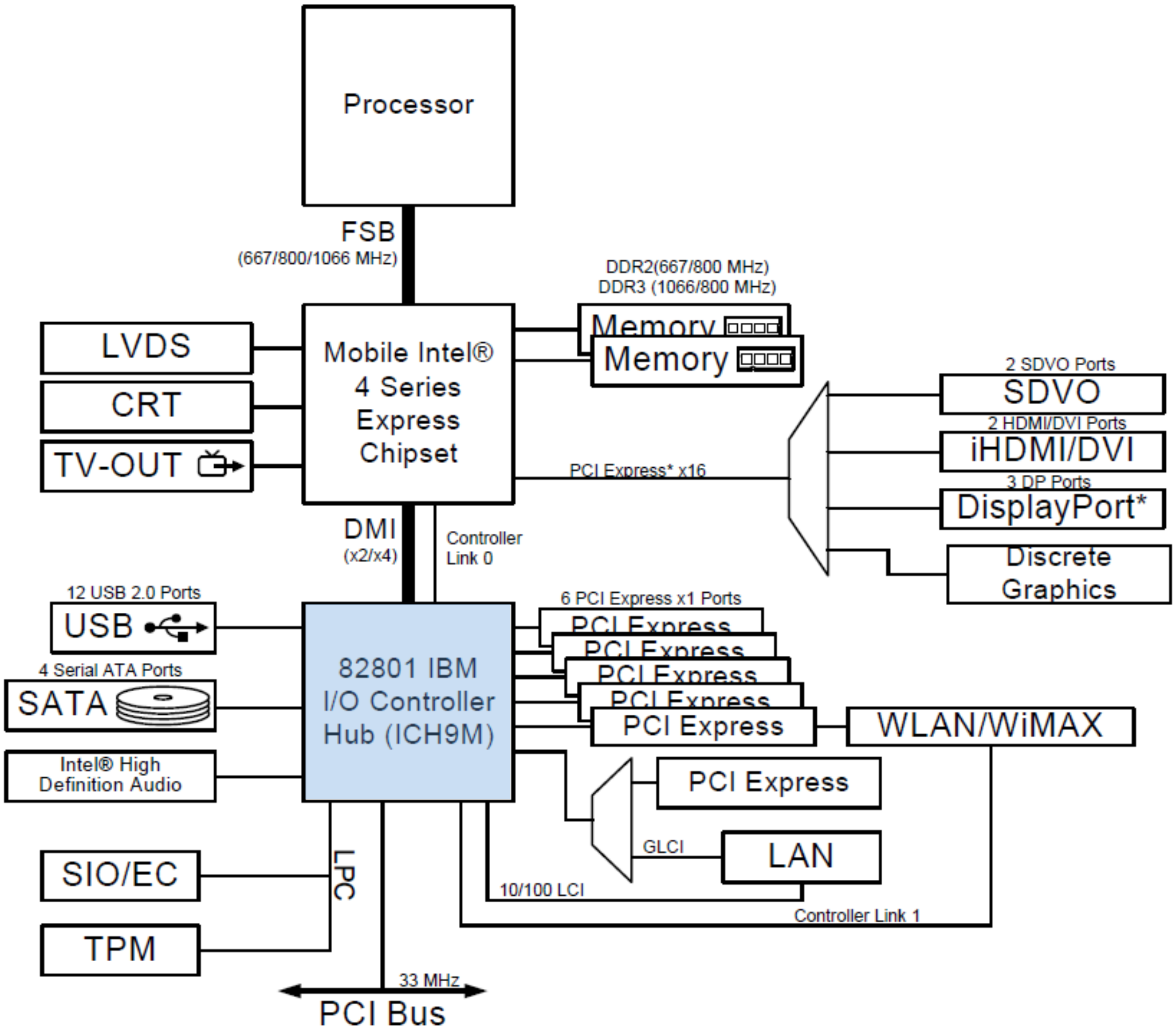
Intel Mobile 4-Series Chipset Datasheet

Memory Controller Hub (MCH)



- For this course on BIOS/UEFI security, the aspects of the MCH (or Platform Controller Hub (PCH) as it has evolved to) we care about most are:
  1. Chipset Configuration registers
  2. DRAM Controller Registers
- In PCH systems the DRAM Controller Registers move into the CPU (we will talk about this in a bit)

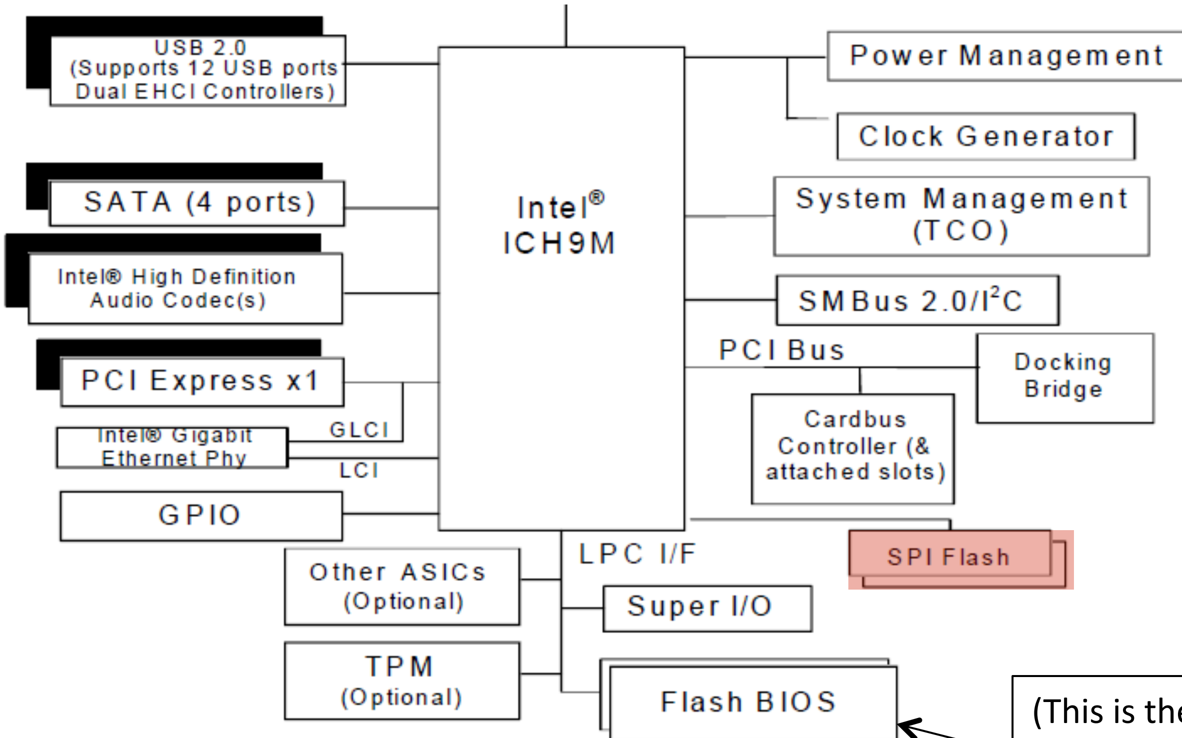
Intel Mobile 4-Series Chipset Datasheet, pg. 13



- I/O Controller Hub
- Interfaces the MCH (and thus the processor) to system devices

Intel Mobile 4-Series Chipset Datasheet

Serial-Peripheral Interface (SPI)

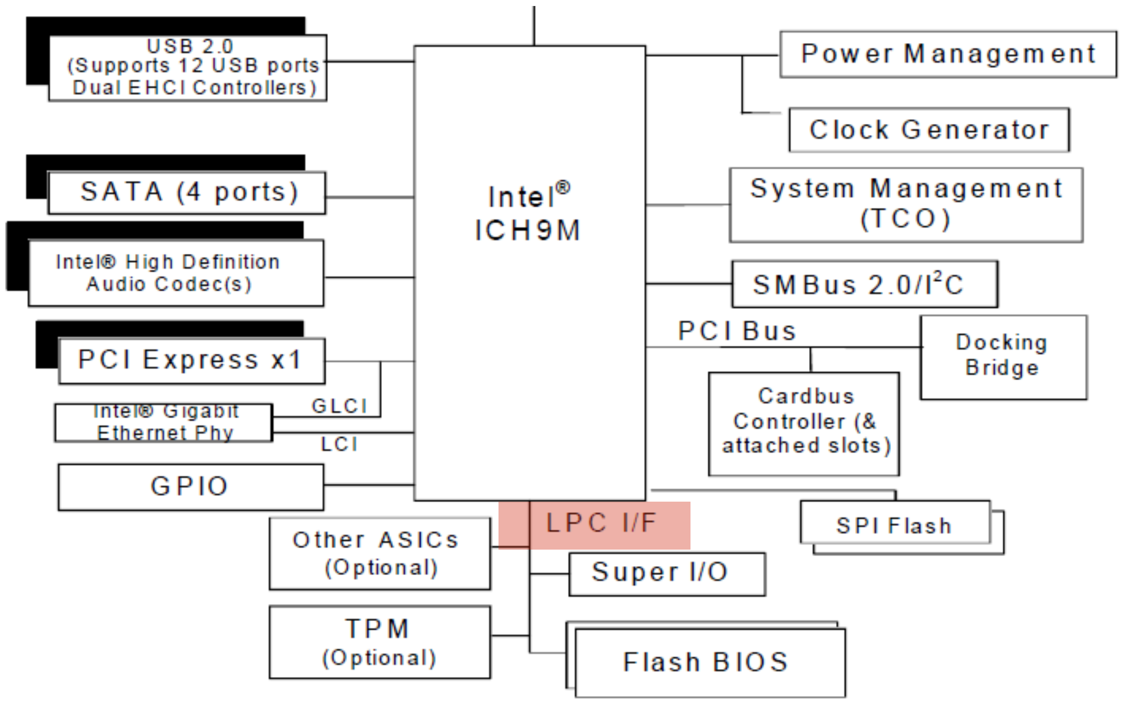


(This is the Firmware Hub (FWH). We'll cover this briefly when we talk about SPI.)

- It's where the BIOS binary resides
- CPU execution starts here upon system startup
- Interface to the device is Memory-Mapped
- We'll cover memory-mapping in the Address Space portion of the course
- From a software development, configuration is still the same when the ICH is consolidated into a PCH

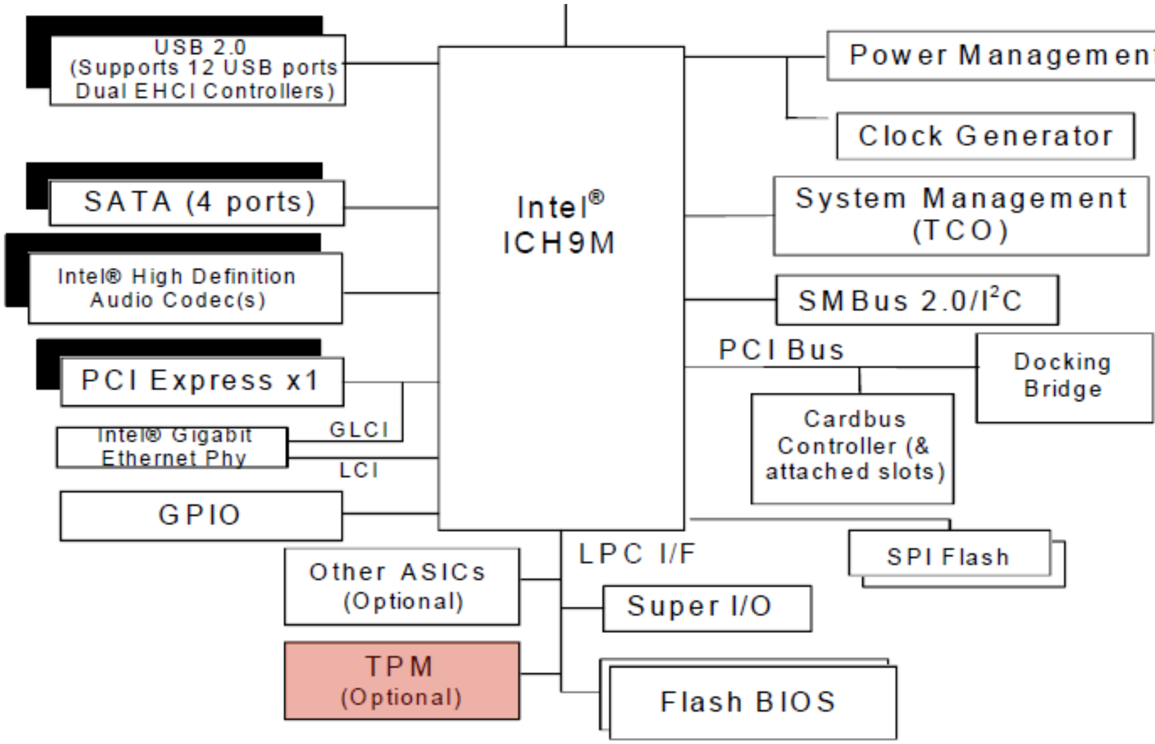
Intel I/O Controller Hub 9 Datasheet, because it includes a more complete block diagram

Low-Pin Count (LPC)



- The devices on the ICH which we care about most are:
- LPC (Low-Pin Count) controller device
- Firmware Hub (legacy)
- Trusted Platform Module (TPM)

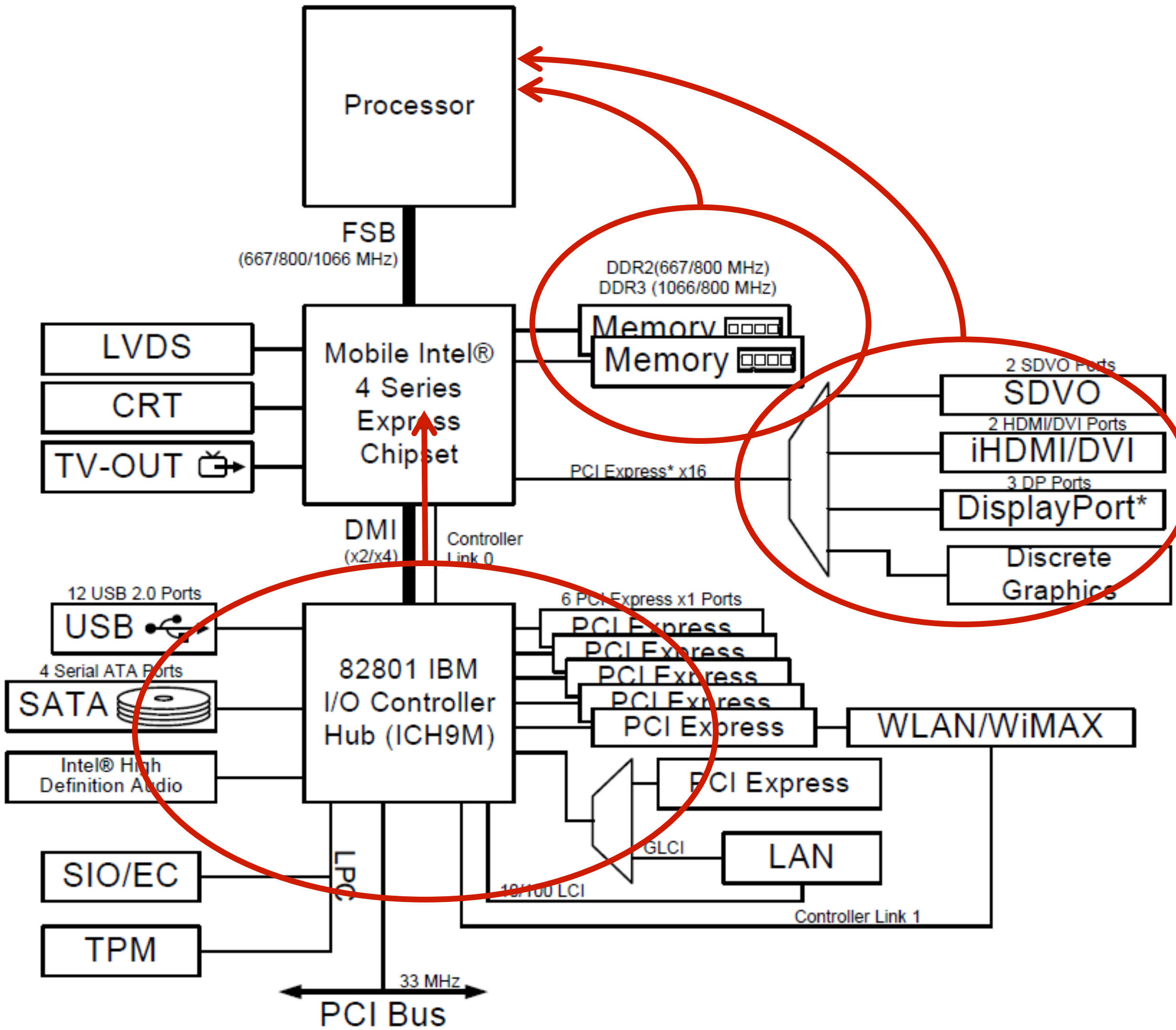
Trusted Platform Module (TPM)



- Extends the security functions within the TPM chip to the CPU/ system
- Memory-Mapped (fixed address)
- Software operation is still the same when the ICH is consolidated into a PCH

Intel I/O Controller Hub 9 Datasheet, because it includes a more complete block diagram

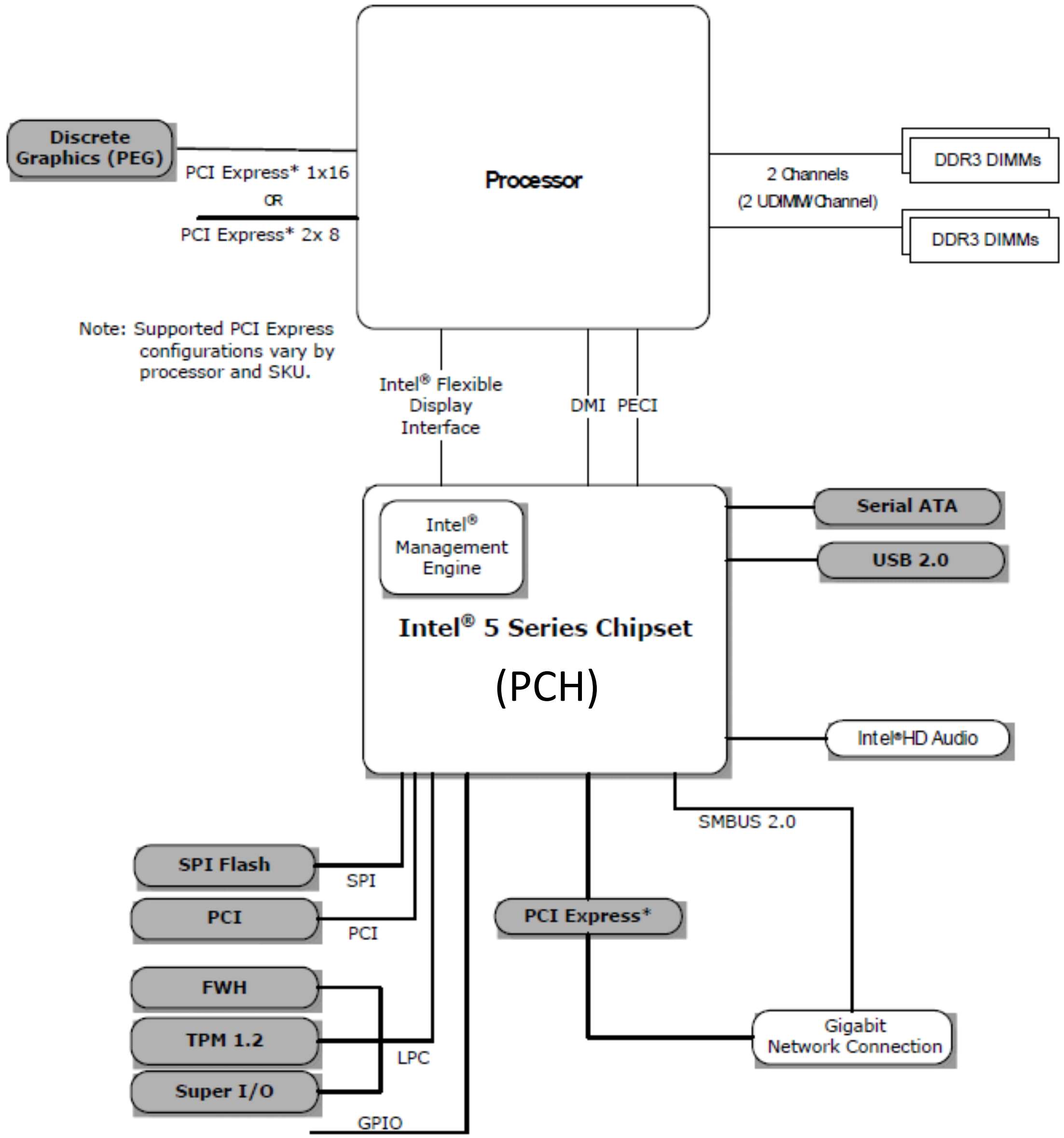
Evolution to Platform Controller Hub (PCH)



- Bottleneck reduction
- Memory Controller moved into the CPU
  - AMD did this in ~2003 with Athlon64
  - Intel ~2008 (Core i-series CPU)
- Graphics processing unit too
- The Northbridge was essentially eliminated to form a single component (PCH)
- Overall trend is to move high-bottleneck areas closer to the CPU which has the fastest clock on the system

Intel 4-Series Chipset Datasheet

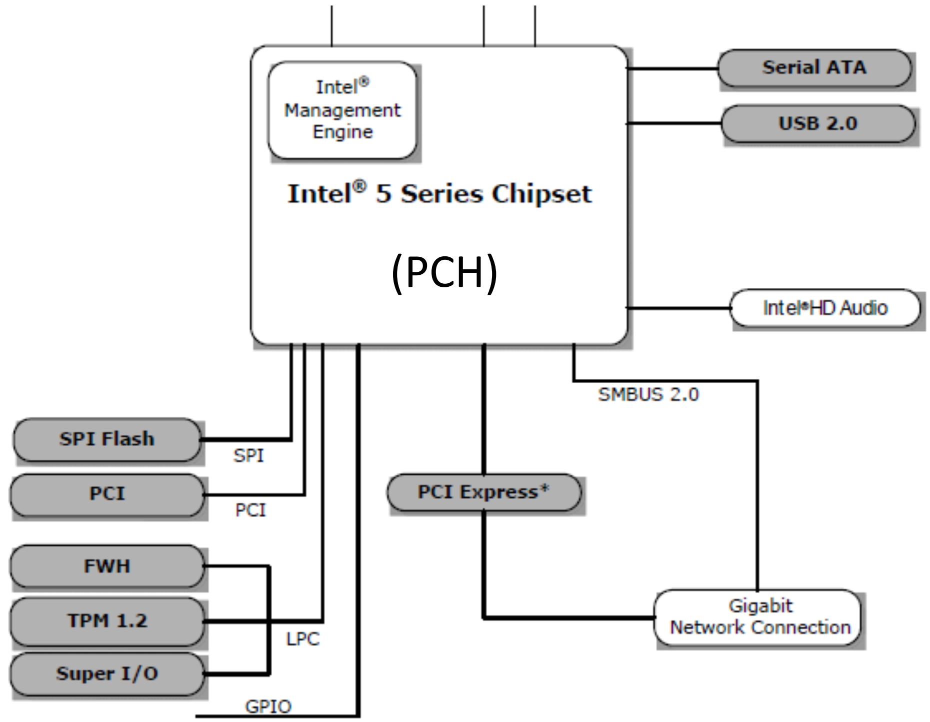
Now everything's just PCHy



- Shown here is the Intel 5-series chipset
- First iteration of the consolidation into a single Platform Controller Hub (PCH)
- AMD did similar in 2003, but I don't want to throw too many hardware diagrams at you (despite being different at the hardware level, logically they are similar if not the same)
- Better to show you just a few, explain why they are the way they are so then you can interpret new/different ones yourself
- Processor is starting to resemble a System On a Chip (SoC)

Intel Core i5-600, i3-500 Desktop Processor Series, Intel Pentium Desktop Processor 6000 Series datasheet

Platform Controller Hub (PCH)

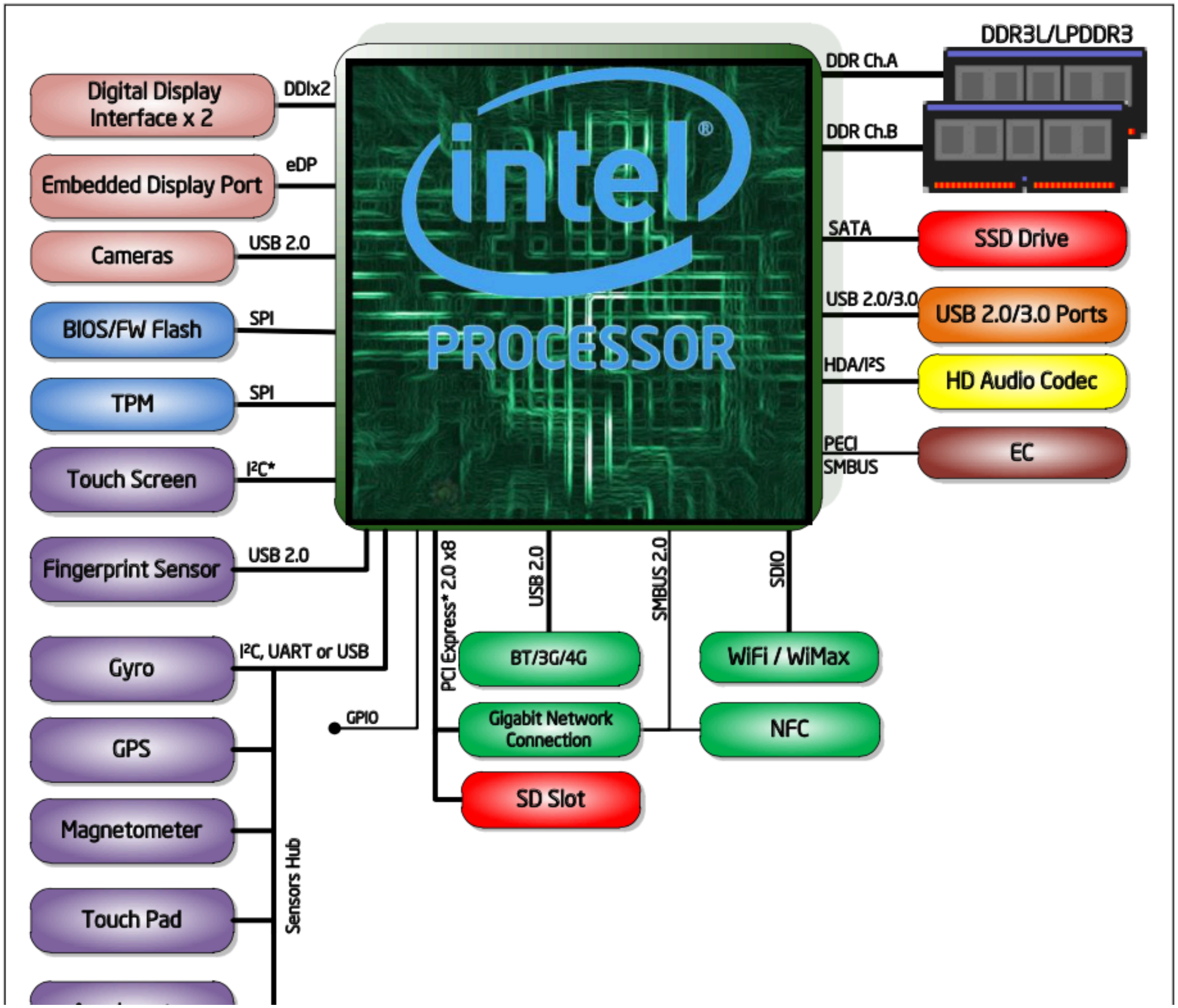


- All the ICH components that we cared about for this course are still present
  - From a software standpoint, even their mode of access is the same
- Functionally speaking, most of what we'll be looking at is agnostic as to whether its MCH/ICH or PCH
  - There are a few exceptions and those will be addressed as they crop up as well as how you account for them

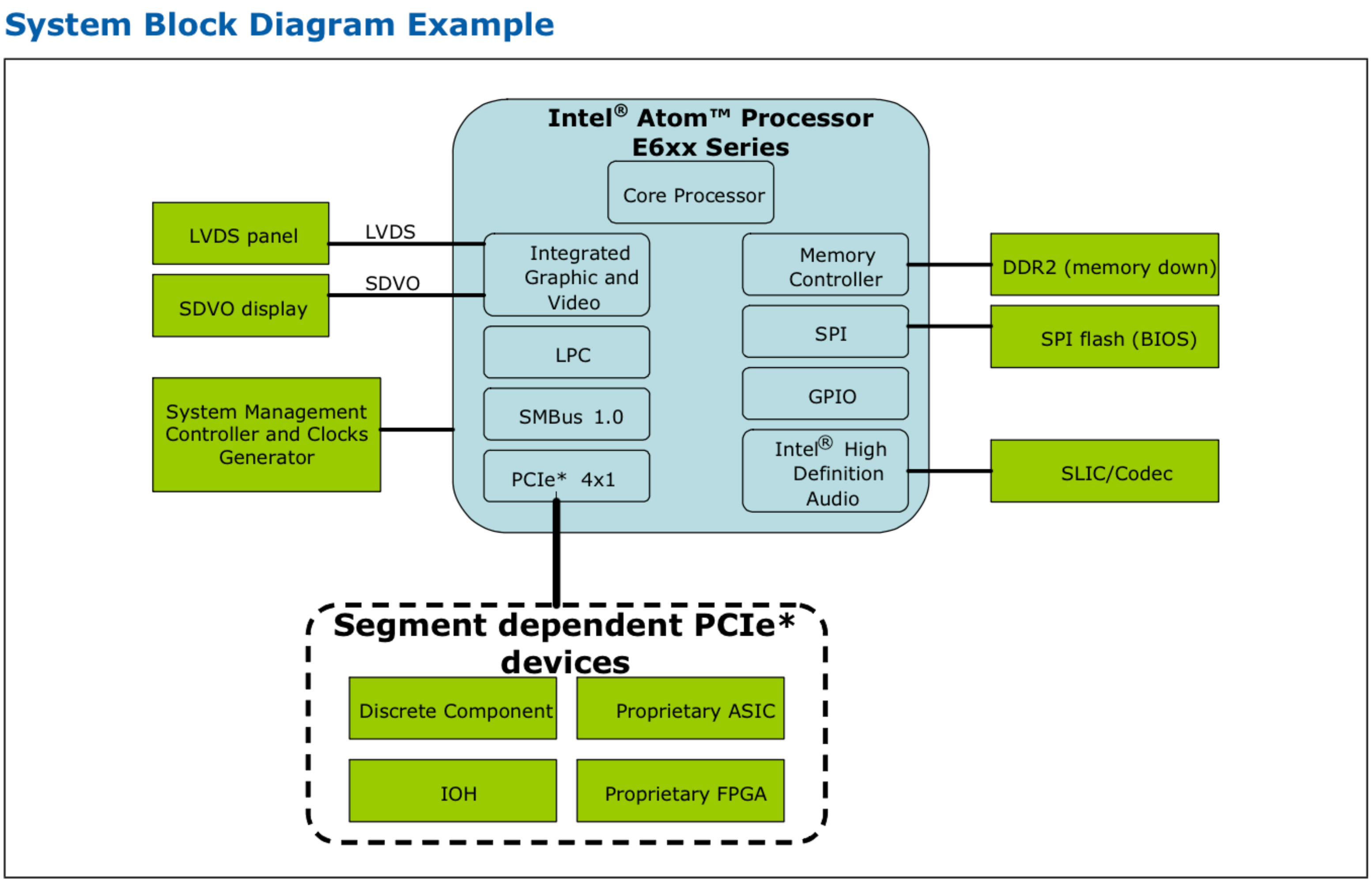
Intel Core i5-600, i3-500 Desktop Processor Series, Intel Pentium Desktop Processor 6000 Series datasheet

Aside: Yeah it's really getting SoCish:
Haswell/Broadwell mobile

Processor Platform Block Diagram

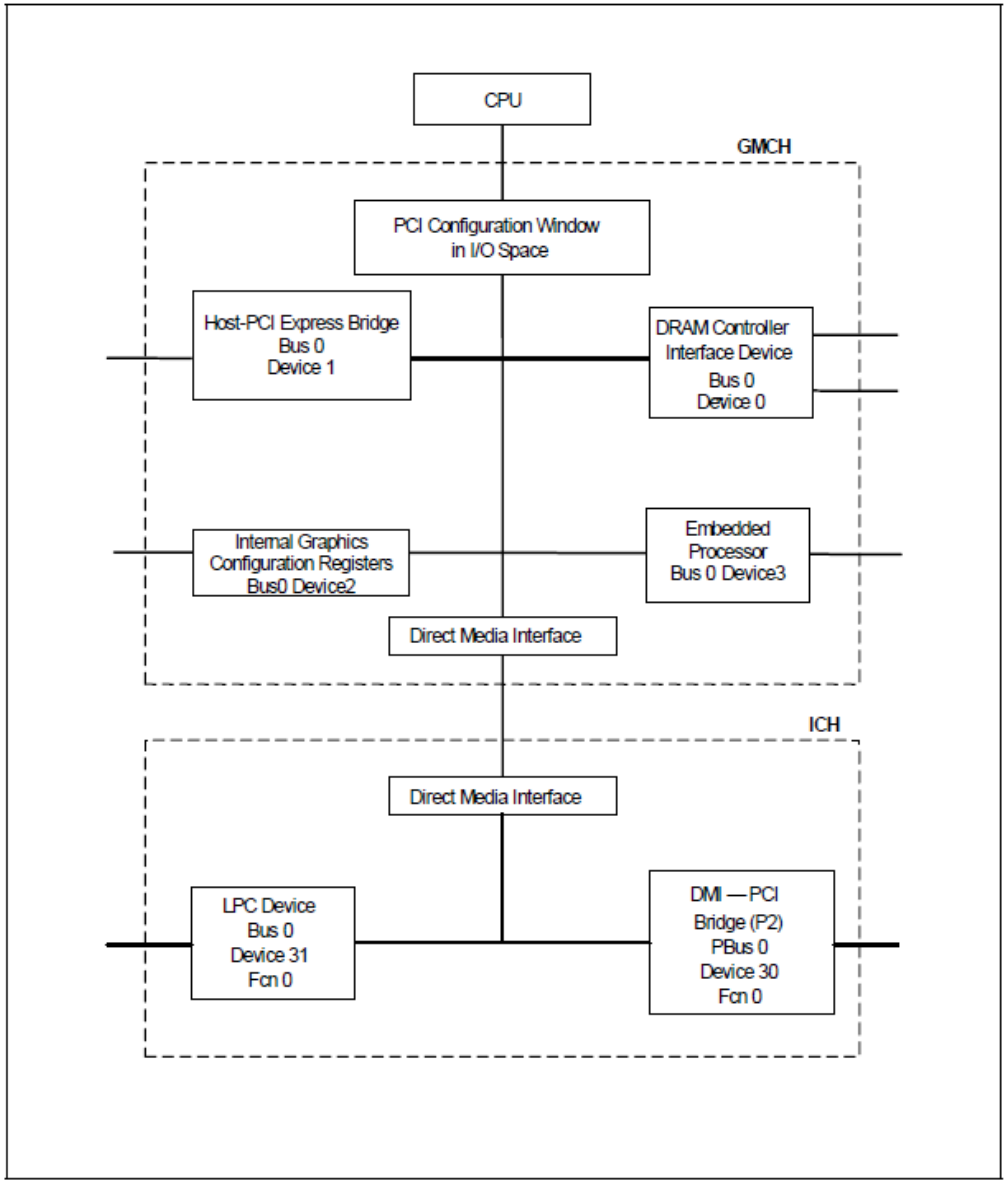


Aside: Intel does make some SoCs, their "Atom" series. Out of scope for today



From Intel® AtomTM Processor E6xx Series Datasheet

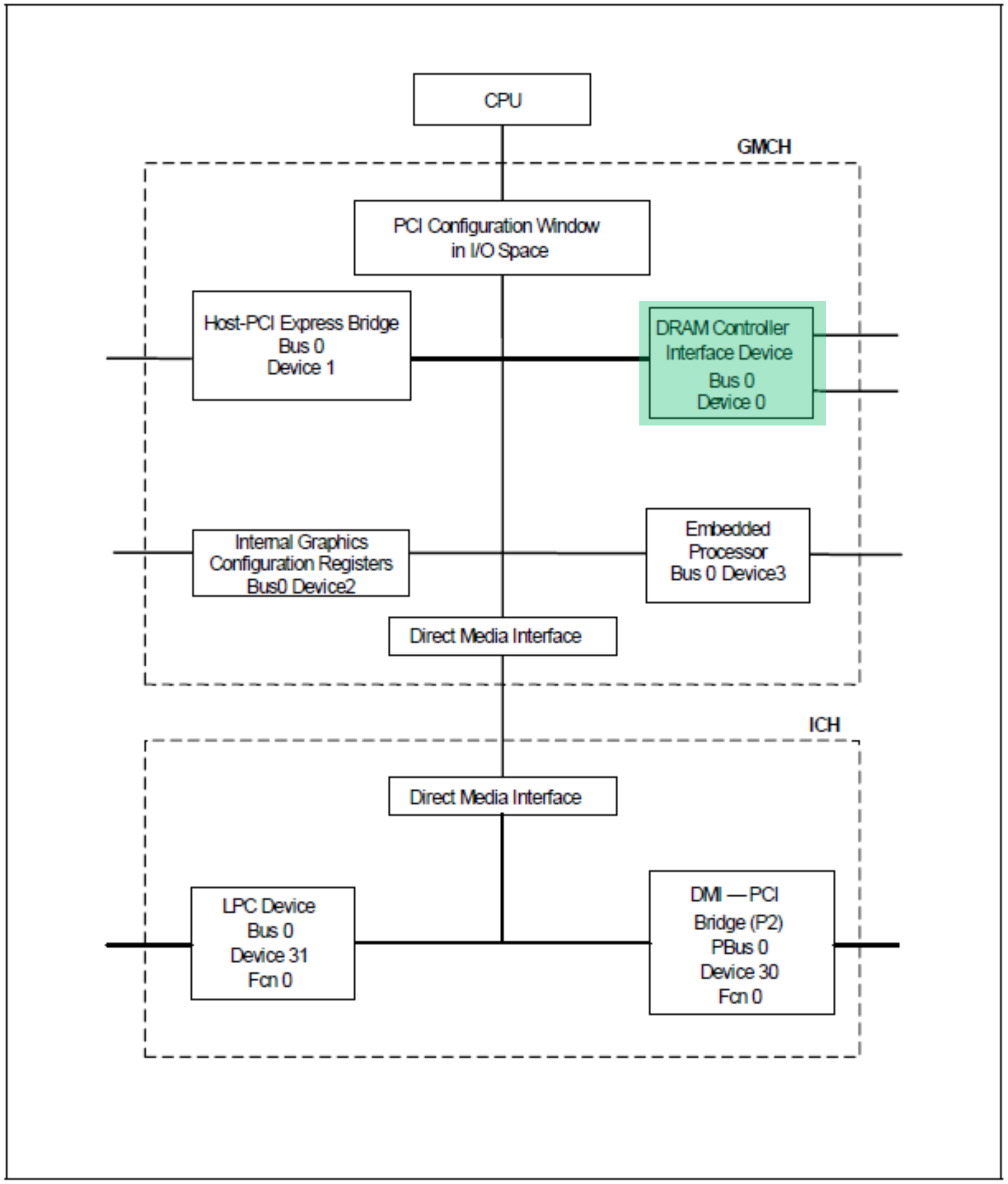
Software Model



- This is how the processor sees the chipset devices
- Not actually a complete diagram, there are more devices listed in the datasheet than what Intel included in this diagram
- Some devices have additional functions (it's a PCI-thing which we'll talk about)

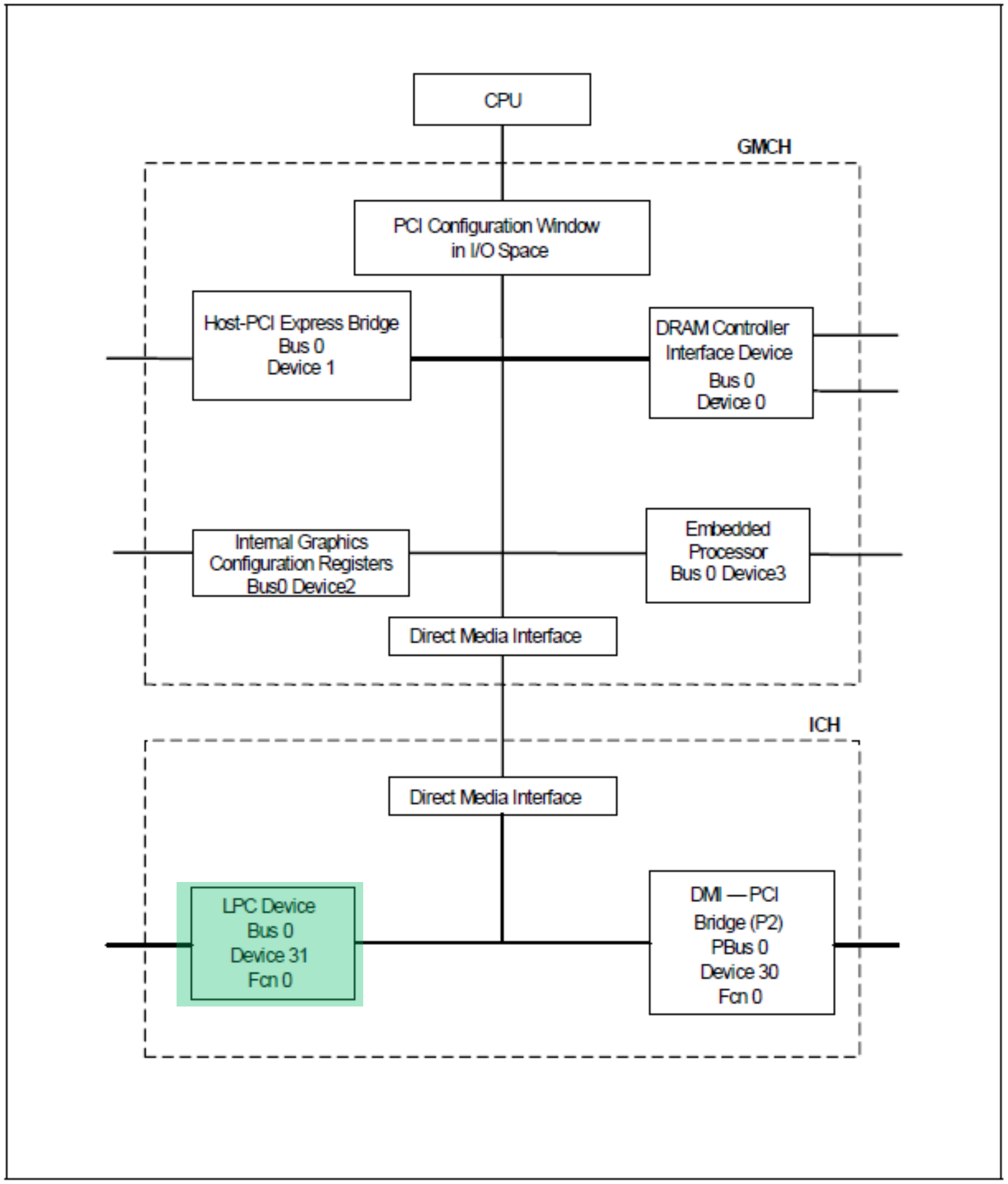
* Device 2 won't be implemented if there is an external graphics card.

Device 0: DRAM Controller



- Device 0 – DRAM Controller
- Configured by BIOS to define much of the memory map
  - SMM
  - PCI Express base address register space(PCIEXBAR)
  - Etc.

Device 31: LPC Interface Bridge



- Device 31 – Low Pin Count Interface (LPC) Bridge
- Located on ICH (or PCH if it's a PCH system)
- Implements various system management functions
- We reference this device a lot
- Spec: http://www.intel.com/design/chipsets/industry/25128901.pdf (*Low Pin Count Interface Specification*, Revision 1.1)

Datasheet will list all PCI Devices

Bus:Device:Function	Function Description
Bus 0:Device 30:Function 0	DMI-to-PCI Bridge
Bus 0:Device 31:Function 0	LPC Controller[1]
Bus 0:Device 31:Function 2	SATA Controller #1
Bus 0:Device 31:Function 5	SATA Controller #2[3]
Bus 0:Device 31:Function 6	Thermal Subsystem
Bus 0:Device 31:Function 3	SMBus Controller
Bus 0:Device 29:Function 0	USB FS/LS UHCI Controller #1
Bus 0:Device 29:Function 1	USB FS/LS UHCI Controller #2
Bus 0:Device 29:Function 2	USB FS/LS UHCI Controller #3
Bus 0:Device 29:Function 3	USB FS/LS UHCI Controller #6[2]
Bus 0:Device 29:Function 7	USB HS EHCI Controller #1
Bus 0:Device 26:Function 0	USB FS/LS UHCI Controller #4
Bus 0:Device 26:Function 1	USB FS/LS UHCI Controller #5
Bus 0:Device 26:Function 2	USB FS/LS UHCI Controller #6[2]
Bus 0:Device 26:Fucntion 7	USB HS EHCI Controller #2
Bus 0:Device 28:Function 0	PCI Express* Port 1
Bus 0:Device 28:Function 1	PCI Express Port 2
Bus 0:Device 28:Function 2	PCI Express Port 3
Bus 0:Device 28:Function 3	PCI Express Port 4
Bus 0:Device 28:Function 4	PCI Express Port 5
Bus 0:Device 28:Function 5	PCI Express Port 6
Bus 0:Device 27:Function 0	Intel® High Definition Audio Controller
Bus 0:Device 25:Function 0	Gigabit Ethernet Controller

NOTES:
1. The PCI-to-LPC bridge contains registers that control LPC, Power Management, System Management, GPIO, Processor Interface, RTC, Interrupts, Timers, and DMA
2. Device 26:Function 2 maybe configured as Device 29:Function 3 during BIOS Post.
3. SATA Controller 2 is only visible when D31:F2 CC.SCC=01h.

- So as I said, there are devices which were not included in the chipset diagram provided by Intel in the Mobile 4-Series datasheet.
- They're not all important from a security perspective, but provided here for reference

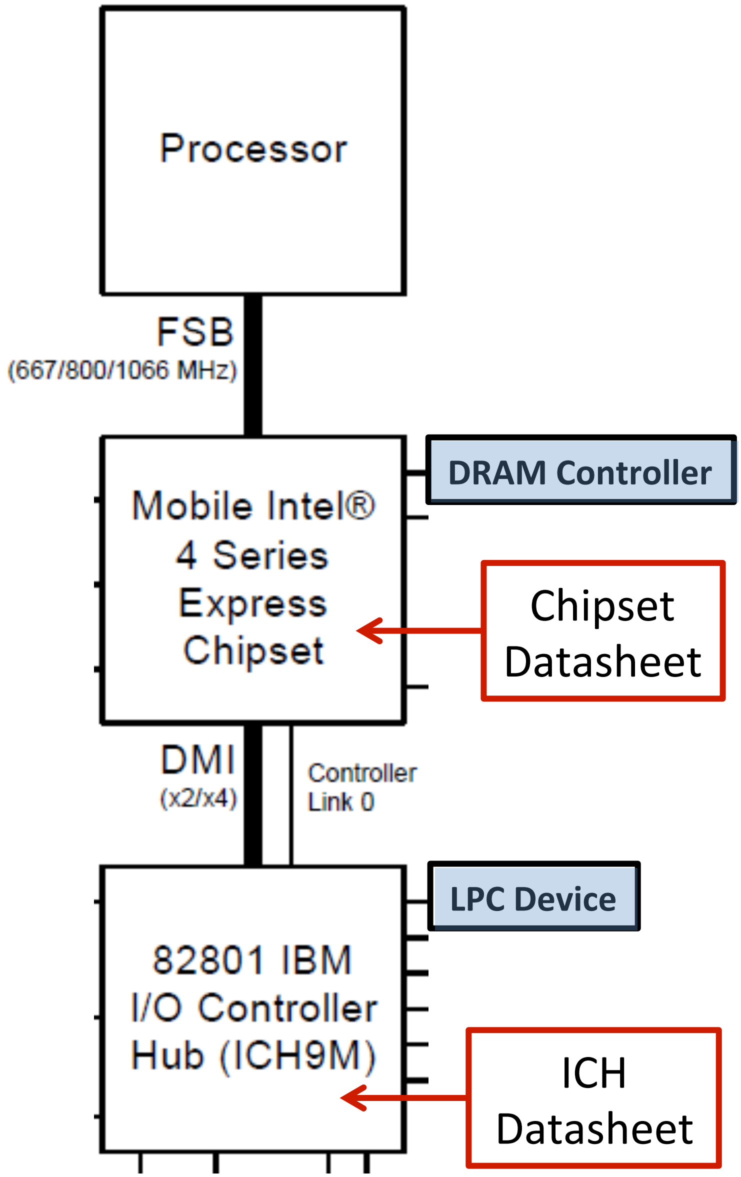
*Intel I/O Controller Hub 9 datasheet

Chipset Identification

- Goal: Identify the Chipset and/or Controller Hub
- Reasons: (1) To find the datasheet, and (2) know the locations of those registers which we will be probing to determine whether a system is vulnerable
  - Some have stayed the same (same name, same offset) over the years (LPC, BIOS_CNTL) while others have “bounced around a little”
  - Our demonstrations/slides are all on the Mobile 4-Series Chipset and IO Controller Hub Family 9
  - However, the functionality provided by these registers still exist in the latest architecture (assuming they aren’t just still the “same old registers”)
  - We want *you* to be able to locate/analyze these (ie: teaching you to fish)

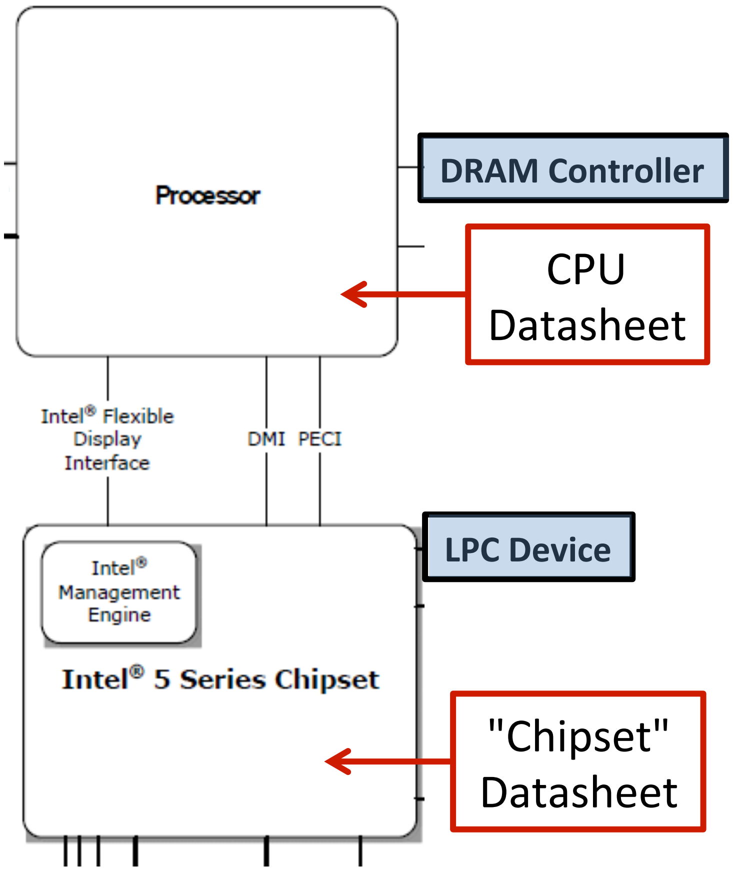
- Ok I’m convinced! So how do we find out?
  - We are “pretending” that we don’t have eyes on the platform itself:
  - In other words, we are using RW-Everything in this example, but RW-E accesses the PCI configuration space which we also could do programmatically

Strategy:



- Many of the registers we care about are located in two separate devices: (1) LPC Device, and (2) DRAM-Controller
- In legacy Chipsets the LPC device is located in the IO Controller Hub and the DRAM-Controller is located in the Memory Controller Hub
- The datasheet containing the information related to the DRAM controller will be found in the Chipset datasheet
- The datasheet containing the LPC-related information will be found in the "I/O Controller Hub" datasheet

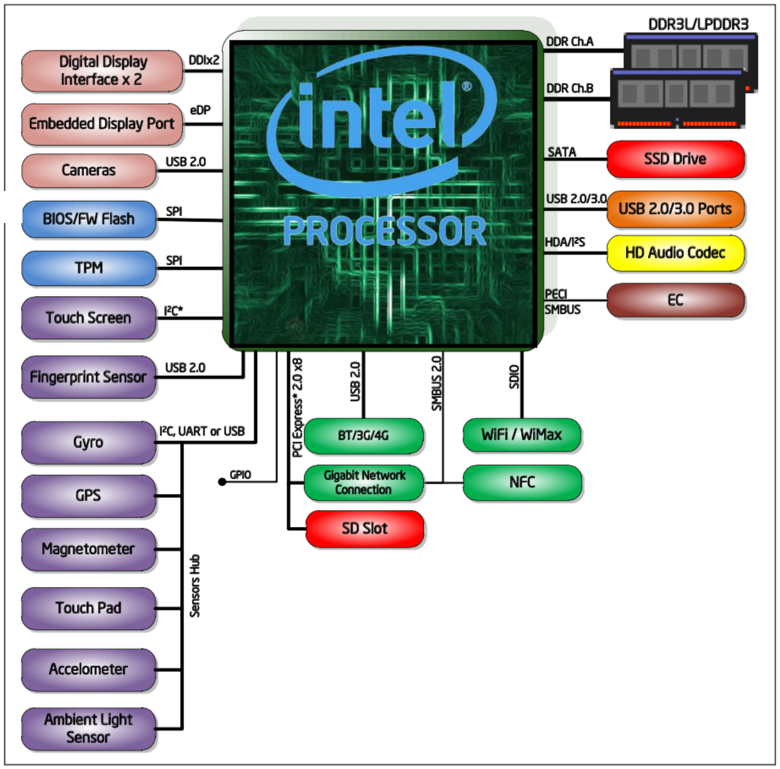
Strategy:



- Many of the registers we care about are located in two separate devices: (1) LPC Device, and (2) DRAM-Controller
- In Modern "Chipsets" (PCH) the LPC device is located in the Platform Controller Hub and the DRAM-Controller is located in the Processor
- The datasheet containing the information related to the DRAM controller will be found in the processor datasheet
- The datasheet containing the LPC-related information will be found in the Chipset datasheet

Strategy:

Processor Platform Block Diagram



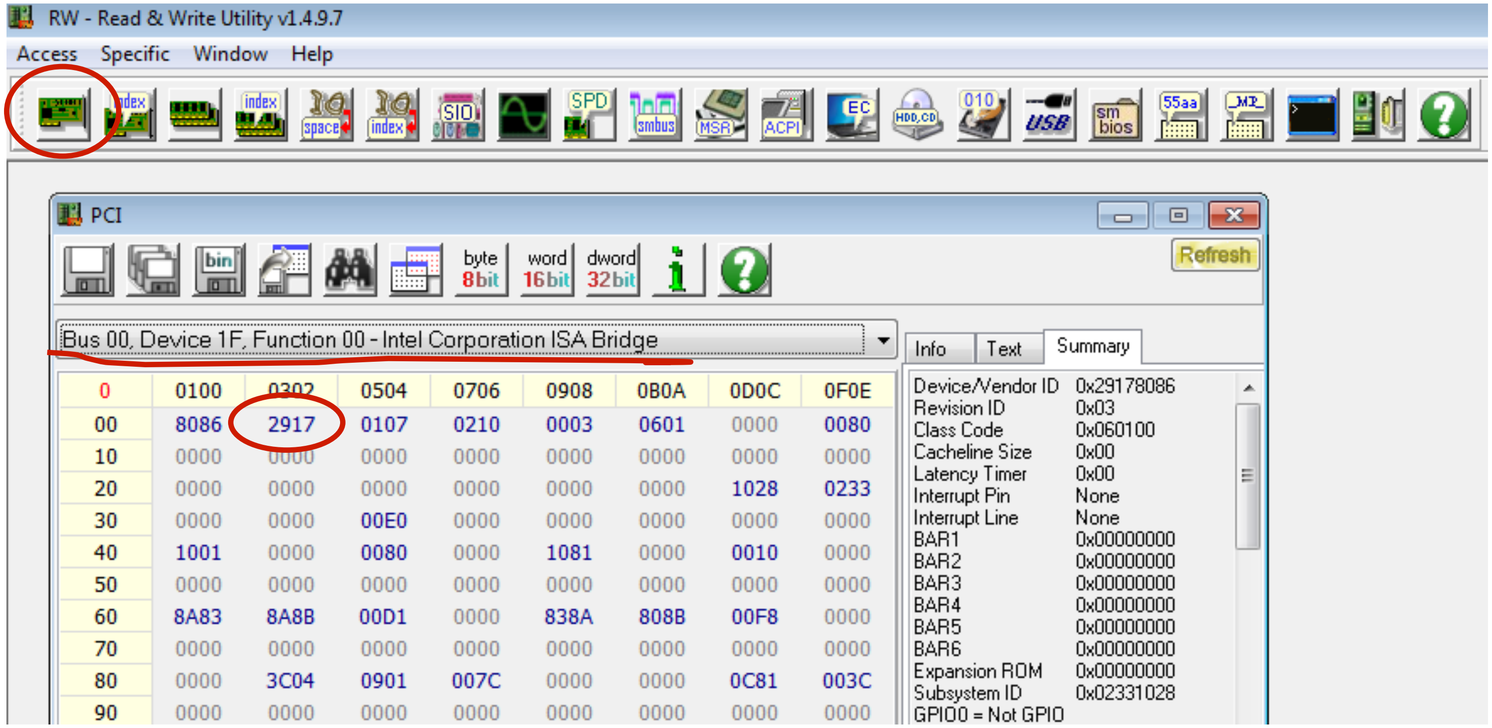
- If your PCI LCP device ID lookup says something like “Wildcat Point-LP”, that means you’re using a Broadwell/5th generation chip
- The DRAM controller / Host Device ID will still be in the CPU specification update
- The LCP device ID can be found in the CPU’s associated “IO datasheet”

Strategy: Additional Notes

1. You do not have to know in advance whether the architecture is a modern chipset or otherwise, the process of identifying the device ID's will tell you that

2. Because we're identifying PCI devices, this same strategy will work on an AMD system (which is completely left out in this course)
   – However, identifying the applicable registers and offsets is an exercise left to you (or me if I get my hands on an enterprise system with an AMD processor)

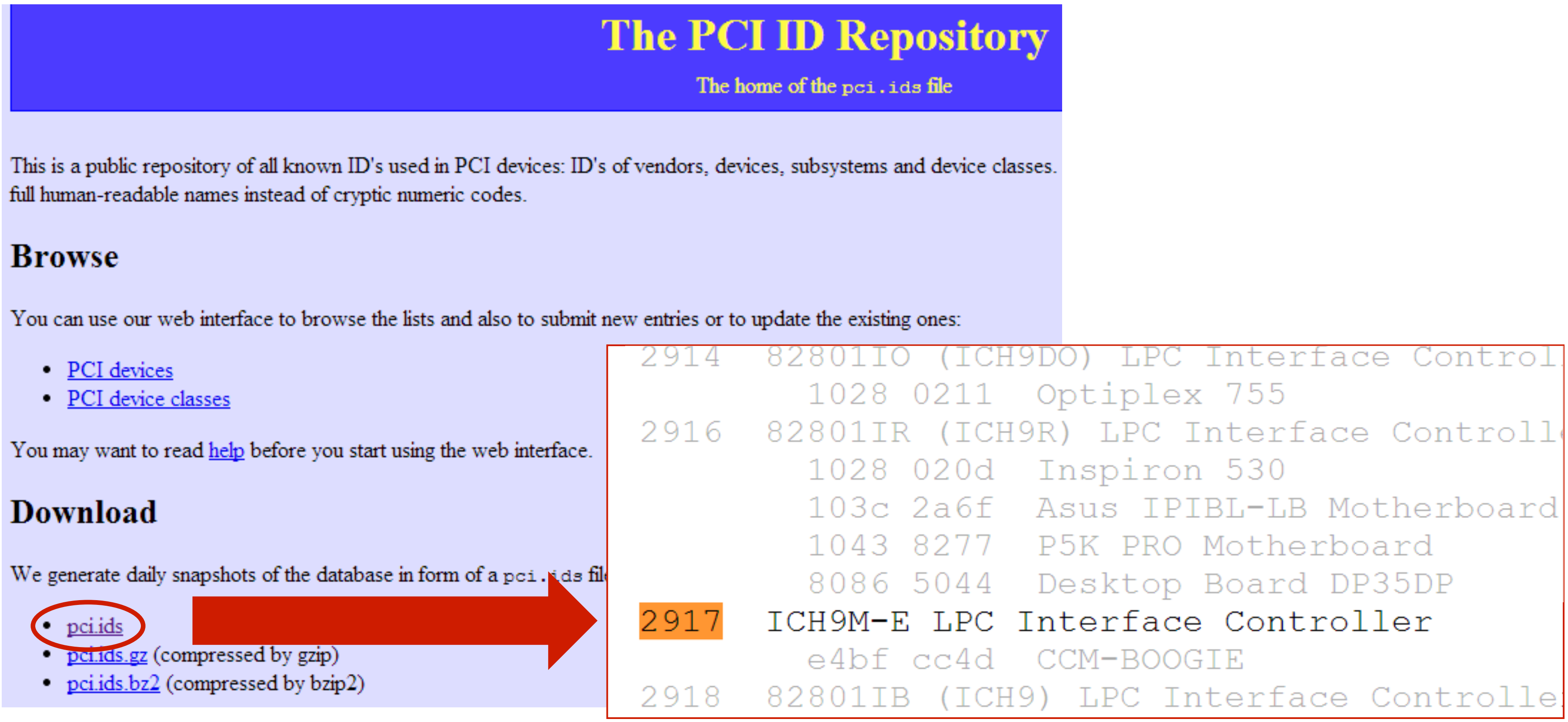
Get the LPC Device ID



- Will tell us the Controller Hub family (therefore either ICH datasheet if legacy or chipset datasheet otherwise)
- Bus 0, Device 31 (1Fh), Function 0, Offset 2 (2-bytes)
- Not sure where RW Everything gets the names of its PCI devices from
- In this example, the LPC Device ID is 0x2917

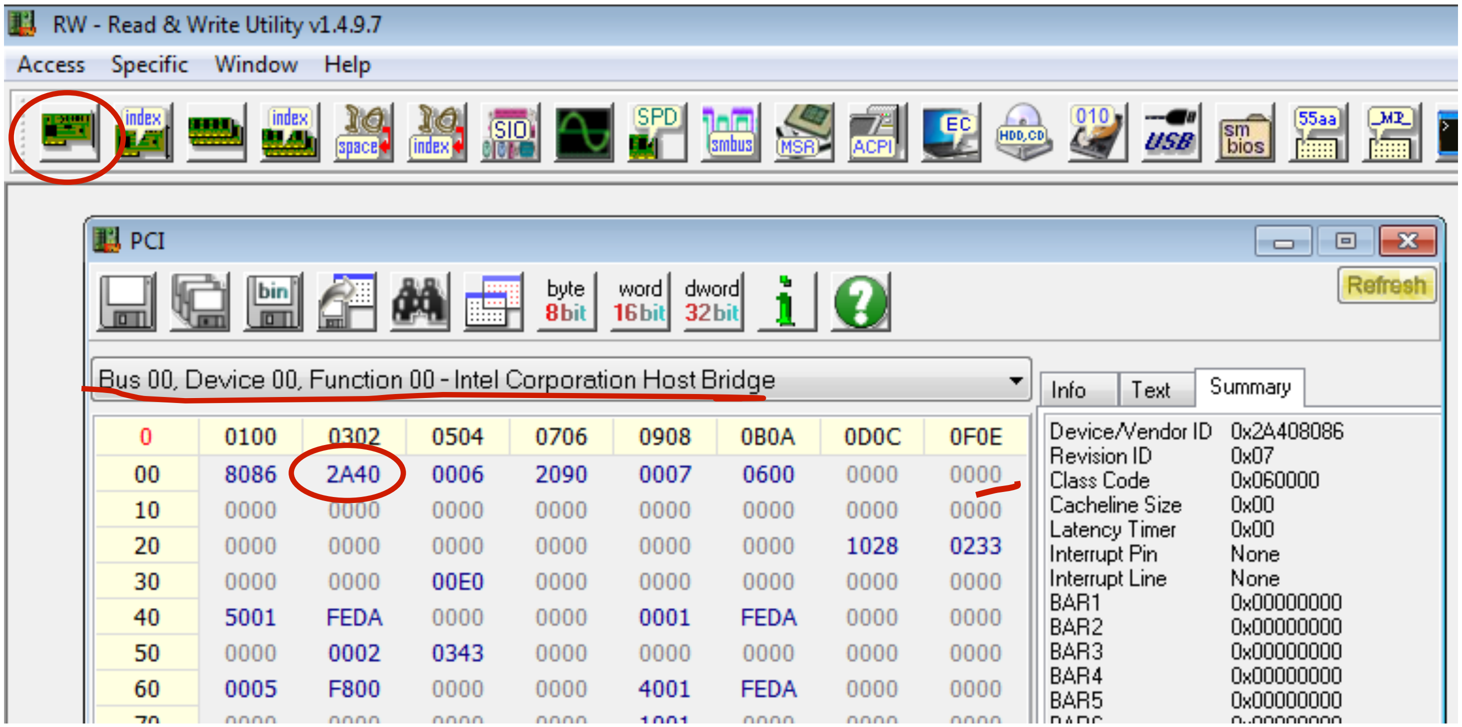
Device ID Lookup

- http://pciids.sourceforge.net
- http://pci-ids.ucw.cz/ (same site, alternate location)



- Device ID 0x2917 is part of the ICH9M-E family
- http://www.intel.com/content/www/us/en/io/io-controller-hub-9-datasheet.html

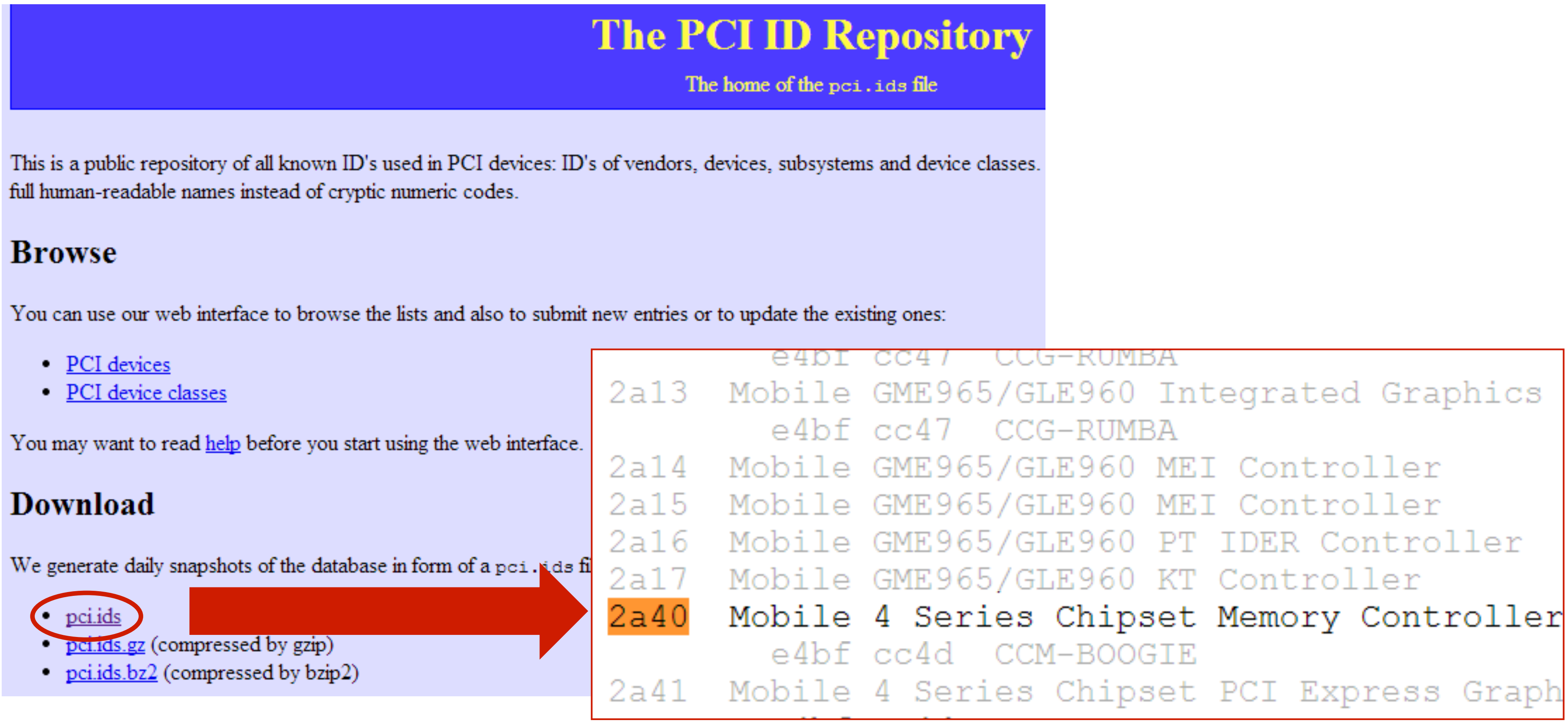
Get the Memory Controller Device ID



- Read the 2-byte Device ID of the Memory Controller:
- Bus 0, Device 0, Function 0, Offset 2
- In this case RW Everything calls it a Host bridge, but as you can see at offset 0x0E in it's header, it is not a bridge
  - PCI-related fact which we'll cover in PCI
- In this sample case the Memory Controller Device ID is 0x2A40

Device ID Lookup

- http://pciids.sourceforge.net
- http://pci-ids.ucw.cz/ (same site, alternate location)

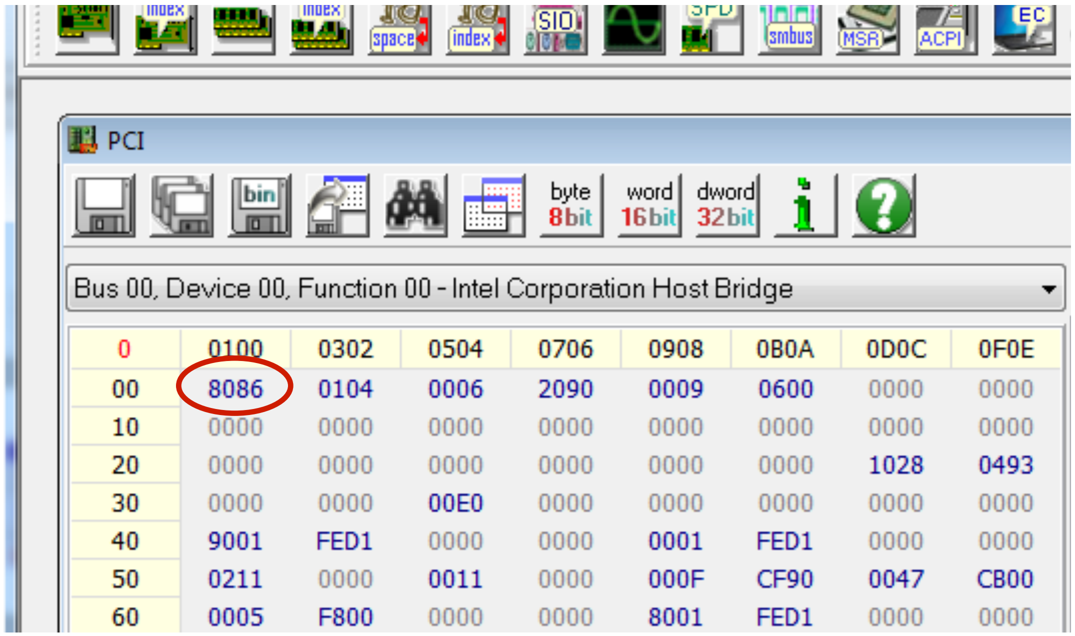


- Device ID 0x2a40 is part of the Mobile 4-Series chipset family
- http://www.intel.com/assets/PDF/datasheet/320122.pdf

So what we have learned about this E6400

- The LPC Device ID is 2917h
  - ICH9M-E Controller Hub
  - Member of the IO Controller Hub 9 family
- The Memory Controller Device ID is 2A40h
  - Mobile 4-Series Chipset Memory Controller
- Therefore this is a legacy chipset
  - DRAM controller is located in the chipset
  - LPC is located in the IO Controller Hub
- The same steps will work on a new system
  - The DRAM controller will be located on the processor
  - The LPC device will be located in the chipset (aka: platform controller hub)
- Sometimes there may be ambiguity. A discussion of how to resolve some forms of ambiguity was moved to the backup slides for this slide deck for time reasons.

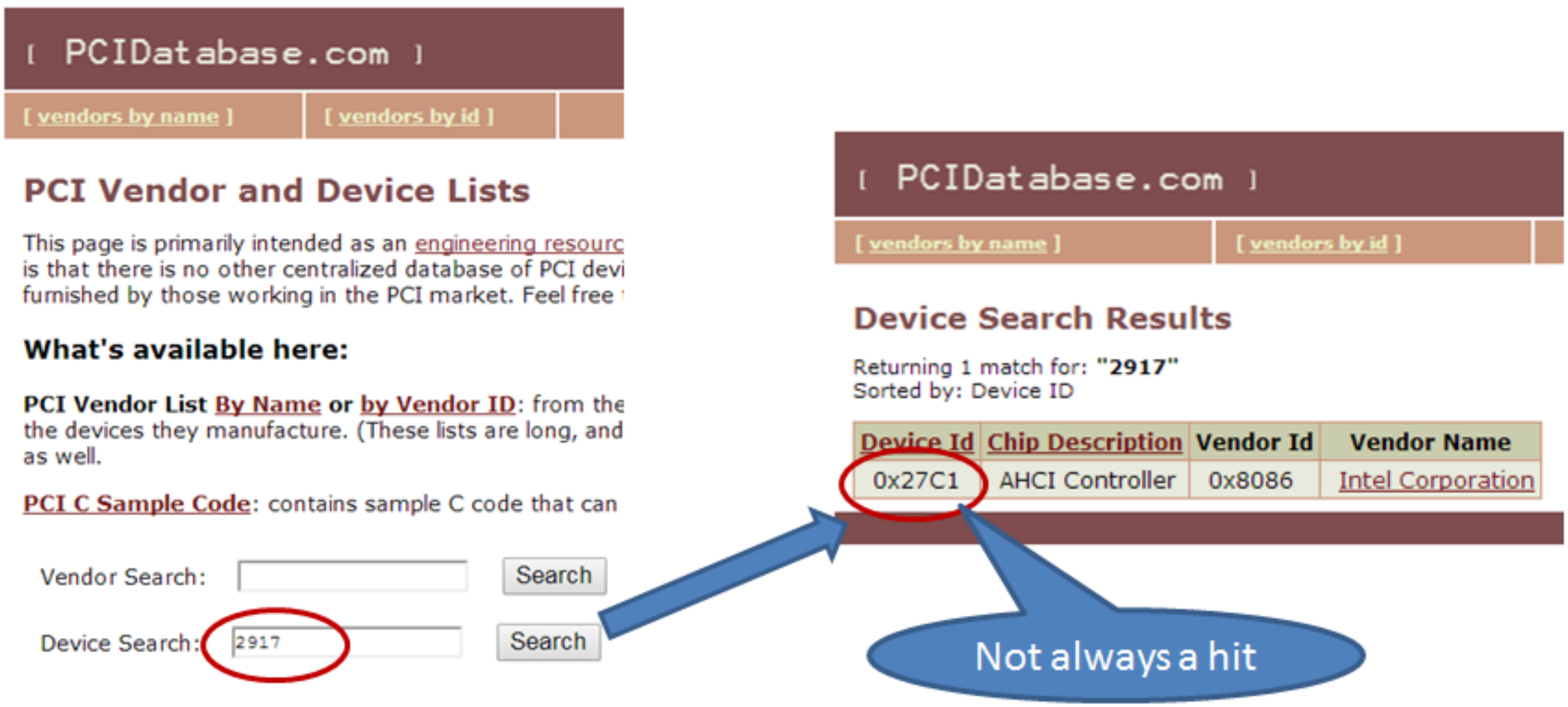
Beware: Gotcha #1



- Verify the Device ID you look up is for the correct vendor
  - Different Vendors can use the same Device IDs
  - Vendor ID's are allocated by the PCI SIG and are always unique
- The above Memory Controller Device ID of 0104h returns multiple hits on http://pci-ids.ucw.cz
  - But it's the 8086h (Intel) one that we want

Beware: Gotcha #2

- It's good to cross-reference more than one source...
- Where one fails (either returns an incorrect device, or finds no device at all), another may succeed
- www.PCIDatabase.com



Specification Updates

- For an Intel system, a given device family (Processor, IO Controller Hub, Chipset) will have a separate datasheet entitled "Specification Update"
- The spec update provides typo-fixes and such but also provides the device ID's for each revision within that particular device family

ICH Family 9 Specification Update

Device Function	Description	Intel® ICH9 Dev ID[1]	ICH9 A2 Rev ID	ICH9 A3 Rev ID	Comments
	LPC	2912h	02h	N/A	ICH9DH
		2914h	02h	N/A	ICH9DO
		2916h	02h	N/A	ICH9R
		2918h	02h	N/A	ICH9
		2917h	02h	03h	ICH9M-E
		2919h	02h	03h	ICH9M

In Summary

- DRAM Controller / Host Bridge PCI “Device IDs” can be found in MCH or CPU datasheets
  – This device will be used to find SPI flash programming registers
- LPC Controller PCI “Device IDs” can be found in the ICH, PCH, or CPU’s “IO” “specification update” datasheets
  – This device will be used to find SPI flash access control registers
- These two device IDs together provide all the information we need for identification of hardware for BIOS security checks

Device IDs

- I’m starting to get tired of spending the time it takes to have everyone look this up, so I’ve started to make a cheat sheet ;)

DRAM Controller/Host Bridge

- Cheat sheet

02–03h	DID	Device Identification	29C0h	RO

MCH/3-series-chipset-family-datasheet.pdf

Bit	Access & Default	Description
15:0	RO	**Device Identification Number (DID):**
	29B0h	29B0h = Intel® 82Q35 GMCH
	29C0h	29C0h = Intel® 82G33/82P35 (G)MCH
	29D0h	29D0h = Intel® 82Q33 GMCH

MCH/3-series-express-chipset-family-datasheet.pdf

The Intel 4 Series Chipset (G)MCH may be identified by the following register contents:

Stepping	Vendor ID[1]	Device ID[2]		Revision Number[3]
A2	8086h	82Q45/82Q43 GMCH	2E10h	02h
		82G45/82G43 GMCH	2E20h	
		82P45/82P43 MCH		
		82G41 GMCH	2E30h	
A2	8086h	82P45/82P43 MCH	2E20h	03h
A3	8086h	82Q45/82Q43 GMCH	2E10h	03h
		82G45/82G43 GMCH	2E20h	
		82G41 GMCH	2E30h	
		82B43 GMCH (Base)	2E40h	
		82B43 GMCH (Soft Sku)	2E90h	

MCH/4-series-chipset-family-datasheet.pdf

Device Identification	DID	2	3	2A40h	RO

MCH/4-series-express-chipset-family-datasheet.pdf

DID - Device Identification

B/D/F/Type: 0/0/0/PCI
Address Offset: 2-3h
Default Value: 0044h
Access: RO
Size: 16 bits

This register combined with the Vendor Identification register uniquely identifies any PCI device.

Bit	Access	Default Value	Description
15:0	RO	0044h	**Device Identification Number (DID)** Identifier assigned to the processor core/primary PCI device.

CPU/1stGen(Nehalem)/Mobile/core-mobile-datasheet-vol-2.pdf

Processor Stepping	Vendor ID[1]	Device ID[2]	Revision ID[3]
C-2	8086h	0044h	12h

CPU/1stGen(Nehalem)/Mobile/core-mobile-spec-update.pdf

DID: Device Identification Register

Register:DID Device:0(DMI) 3, 5 (PCIe) Function: 0 Offset:02h			
Bit	**Attr**	**Default**	**Description**
15:0	RO	See Table 3-1	**Device Identification Number** Identifier assigned to the product. Integrated I/O will have a unique device ID for each device.

CPU/2ndGen(SandyBridge)/Mobile/2nd-gen-core-family-mobile-vol-2-datasheet.pdf

Processor Stepping	Vendor ID[1]	Device ID[2]	Revision ID[3]
B-1	8086h	D132h	11h

CPU/2ndGen(SandyBridge)/Mobile/core-i7-900-mobile-ee-and-mobile-processor-series-spec-update.pdf

DID—Device Identification Register

This register, combined with the Vendor Identification register, uniquely identifies any PCI device.

B/D/F/Type:	**0/0/0/PCI**
Address Offset:	**2–3h**
Reset Value:	**0100h**
Access:	**RO-FW, RO-V**
Size:	**16 bits**

Bit	Attr	Reset Value	RST/ PWR	Description
15:4	RO-FW	010h	Uncore	**Device Identification Number MSB (DID_MSB)** This is the upper part of device identification assigned to the processor.
3:2	RO-V	00b	Uncore	**Device Identification Number SKU (DID_SKU)** This is the middle part of device identification assigned to the processor.
1:0	RO-FW	00b	Uncore	**Device Identification Number LSB (DID_LSB)** This is the lower part of device identification assigned to the processor.

CPU/2ndGen(SandyBridge)/Mobile/2nd-gen-core-family-mobile-vol-2-datasheet.pdf

Stepping	Vendor ID[1]	Host Device ID[2]	Processor Graphics Device ID[3]	Revision ID[4]
D-2	8086h	0104h	GT1: 0106h GT2: 0116h GT2 (>1.3 GHz Turbo): 126h	09h
J-1	8086h	0104h	GT1: 0106h GT2: 0116h GT2 (>1.3 GHz Turbo): 126h	09h

CPU/2ndGen(SandyBridge)/Mobile/2nd-gen-core-family-mobile-specification-update.pdf

DID—Device Identification Register

This register combined with the Vendor Identification register uniquely identifies any PCI device.

B/D/F/Type:	**0/0/0/PCI**
Address Offset:	**2–3h**
Reset Value:	**0150h**
Access:	**RO-FW, RO-V**
Size:	**16 bits**

Bit	Access	Reset Value	RST/ PWR	Description
15:4	RO-FW	015h	Uncore	**Device Identification Number MSB (DID_MSB)** This is the upper part of device identification assigned to the processor.
3:2	RO-V	00b	Uncore	**Device Identification Number SKU (DID_SKU)** This is the middle part of device identification assigned to the processor.
1:0	RO-FW	00b	Uncore	**Device Identification Number LSB (DID_LSB)** This is the lower part of device identification assigned to the processor.

CPU/3rdGen(IvyBridge)/Mobile/3rd-gen-core-family-mobile-vol-2-datasheet.pdf

Stepping	Vendor ID[1]	Host Device ID[2]	Processor Graphics Device ID[3]	Revision ID[4]
E-1	8086h	0154h	0166h	09h
L-1	8086h	0154h	0166h	09h

CPU/3rdGen(IvyBridge)/Mobile/3rd-gen-core-family-mobile-specification-update.pdf

3.1.2 DID—Device Identification

This register combined with the Vendor Identification register uniquely identifies any PCI device.

B/D/F/Type: 0/0/0/CFG			Access: RO; RO_V	
Size: 16	Default Value: 0C00h		Address Offset: 2h	
Bit Range	**Acronym**	**Description**	**Default**	**Access**
15:4	DID_MSB	Device Identification Number MSB: This is the upper part of device identification assigned to the processor.	0C0h	RO
3:2	DID_SKU	Device Identification Number SKU: This is the middle part of device identification assigned to the processor.	0h	RO_V
1:0	DID_LSB	Device Identification Number LSB: This is the lower part of device identification assigned to the processor.	0h	RO

4th-gen-core-family-mobile-m-h-processor-lines-vol-2-datasheet.pdf

3.1.2 DID—Device Identification

This register combined with the Vendor Identification register uniquely identifies any PCI device.

B/D/F/Type: 0/0/0/CFG			Access: RO; RO_V	
Size: 16	Default Value: 0C00h		Address Offset: 2h	
Bit Range	**Acronym**	**Description**	**Default**	**Access**
15:4	DID_MSB	Device Identification Number MSB: This is the upper part of device identification assigned to processor Intel Reserved Text The value of this field can be changed for soft SKU IDs. Reset value is written to 0x0A0 on processor-ULT by pcode fuse distribution	0C0h	RO
3:2	DID_SKU	Device Identification Number SKU: This is the middle part of device identification assigned to the processor.	0h	RO_V
1:0	DID_LSB	Device Identification Number LSB: This is the lower part of device identification assigned to the processor	0h	RO

continued...

Processor Identification by Register Contents

Processor line	Stepping	Vendor ID[1]	Host Device ID[2]	Processor Graphics Device ID[3]	Revision ID[4]	CRID
M-Processor Series	C-0	8086h	0C04h	GT1 = 0406h GT2 = 0416h	06h	06h
H-Processor Series	C-0	8086h	0C04h	GT2=0416h	06h	06h
H-Processor Series (BGA) with GT3 Graphics	C-0	8086h	0D04h	GT3 = 0D26h	08h	08h
U-Processor Series	C-0	8086h	0A04h	GT1 = 0A06h GT2 = 0A16h GT3 = 0A26h	GT1 = 0Bh GT2 = 0Bh GT3 = 09h	GT1 = 0Bh GT2 = 0Bh GT3 = 09h
U-Processor Series	D-0	8086h	0A04h	GT1 = 0A06h GT2 = 0A16h GT3 = 0A26h	GT1 = 0Bh GT2 = 0Bh GT3 = 09h	GT1 = 0Bh GT2 = 0Bh GT3 = 09h
Y-Processor Series (SDP = 6W)	C-0	8086h	0A04h	GT2 = 0A16h	GT2 = 0Bh	GT2 = 0Bh
Y-Processor Series (SDP = 6W)	D-0	8086h	0A04h	GT2=0A16h	GT2 = 0Bh	GT2 = 0Bh
Y -Processor Series (SDP = 4.5W)	D-0	8086h	0A04h	GT1 = 0A06h GT2 = 0A16h	GT1 = 0Bh GT2 = 0Bh	GT1 = 0Bh GT2 = 0Bh

CPU/4thGen(Haswell)/Mobile/4th-gen-core-family-mobile-specification-update.pdf

3.1.2 DID—Device Identification

This register combined with the Vendor Identification register uniquely identifies any PCI device.

B/D/F/Type: 0/0/0/CFG			Access: RO; RO_V	
Size: 16	Default Value: 0C00h		Address Offset: 2h	
Bit Range	**Acronym**	**Description**	**Default**	**Access**
15:4	DID_MSB	Device Identification Number MSB: This is the upper part of device identification assigned to the processor.	0C0h	RO
3:2	DID_SKU	Device Identification Number SKU: This is the middle part of device identification assigned to the Processor.	0h	RO_V
1:0	DID_LSB	Device Identification Number LSB: This is the lower part of device identification assigned to the Processor.	0h	RO

CPU/5thGen(Broadwell)/5th-gen-core-family-datasheet-vol-2.pdf

Processor Identification by Register Contents

Processor Line	Stepping	Vendor ID	Host Device ID	Processor Graphics Device ID	Revision ID	Compatibility Revision ID
5th Generation Intel® Core™ Processor	E-0	8086h	1604h	GT1 = 1606h GT2 = 1616h	8	8
5th Generation Intel® Core™ Processor	F-0	8086h	1604h	GT1 = 1606h GT2 = 1616h	9	9
Intel® Core™ M Processor	E-0	8086h	1604h	GT2 = 161Eh	8	8
Intel® Core™ M Processor	F-0	8086h	1604h	GT2 = 161Eh	9	9

CPU/5thGen(Broadwell)/5th-gen-core-family-spec-update.pdf

LPC Device datasheets

Device Function	Description	Intel® ICH 7 Dev ID[1]	Intel® ICH 7 A1 Rev ID	Intel® ICH 7 B0 Rev ID	Comments
D31, F0	LPC	27B8h	01h	N/A	Intel® ICH7, ICH7R
		27B9h	01h	02h	Intel® ICH7M, ICH7U
		27BDh	01h	02h	Intel® ICH7M DH
D31, F1	IDE	27DFh	01h	02h	

ICH/io-controller-hub-7-datasheet.pdf

Device Function	Description	Intel® ICH8 Dev ID[1]	ICH8 B0 Rev ID	ICH8 B1 Rev ID	ICH8 B2 Rev ID	Comments
D31:F0	LPC	2810h	02h	N/A	N/A	ICH8, ICH8R
		2815h	02h	03h	04h	ICH8M
		2812h	02h	N/A	N/A	ICH8DH
		2814h	02h	N/A	N/A	ICH8DO
		2811h	02h	03h	04h	ICH8M-E

ICH/io-controller-hub-8-datasheet.pdf

Device Function	Description	Intel® ICH9 Dev ID[1]	ICH9 A2 Rev ID	ICH9 A3 Rev ID	Comments
	LPC	2912h	02h	N/A	ICH9DH
		2914h	02h	N/A	ICH9DO
		2916h	02h	N/A	ICH9R
		2918h	02h	N/A	ICH9
		2917h	02h	03h	ICH9M-E
		2919h	02h	03h	ICH9M

ICH/io-controller-hub-9-datasheet.pdf

Device Function	Description	Intel® ICH 10 Dev ID	Intel® ICH 10 B0 Rev ID	Comments
D31:F0	LPC	3A14h	02h	ICH10DO
		3A1Ah	02h	ICH10D
D31:F0	LPC	3A16h	00h	ICH10R
		3A18h	00h	ICH10 (Consumer Base)

ICH/io-controller-hub-10-datasheet.pdf

Intel® 5 Series Chipset and Intel® 3400 Series Chipset Device and Revision ID Table (Sheet 1 of 2)

Device Function	Description	Dev ID[1]	B2 Rev ID	B3 Rev ID	Comments
D31:F0	LPC	3B02h	05h	06h	Intel® P55 Chipset
		3B03h	05h	06h	Intel® PM55 Chipset
		3B06h	n/a	06h	Intel® H55 Chipset
		3B07h	n/a	06h	Intel® QM57 Chipset
		3B08h	n/a	06h	Intel® H57 Chipset
		3B09h	n/a	06h	Intel® HM55 Chipset
		3B0Ah	n/a	06h	Intel® Q57 Chipset
		3B0Bh	n/a	06h	Intel® HM57 Chipset
		3B0Fh	n/a	06h	Intel® QS57 Chipset
		3B12h	05h	n/a	Intel® 3400 Chipset
		3B14h	05h	06h	Intel® 3420 Chipset
		3B16h	n/a	06h	Intel® 3450 Chipset

PCH Device and Revision ID Table (Sheet 1 of 3)

Device Function	Description	Dev ID	B2 Rev ID	B3 Rev ID	Comments
D31:F0	LPC	1C4Eh		05h	Intel® Q67 Chipset
		1C4Ch		05h	Intel® Q65 Chipset
		1C50h		05h	Intel® B65 Chipset
		1C4Ah	04h	05h	Intel® H67 Chipset
		1C44h		05h	Intel® Z68 Chipset
		1C46h	04h	05h	Intel® P67 Chipset
		1C5Ch		05h	Intel® H61 Chipset
		1C52h		05h	Intel® C202 Chipset
		1C54h		05h	Intel® C204 Chipset
		1C56h		05h	Intel® C206 Chipset
		1C4Fh		05h	Intel® QM67 Chipset
		1C47h		05h	Intel® UM67 Chipset
		1C4Bh	04h	05h	Intel® HM67 Chipset
		1C49h	04h	05h	Intel® HM65 Chipset
		1C4Dh		05h	Intel® QS67 Chipset

PCH/6-series-chipset-c200-chipset-datasheet.pdf

PCH Device and Revision ID Table (Sheet 1 of 3)

Device Function	Description	Dev ID	C1 RID	Comments
		1E47h	04h	Intel® Q77 Express Chipset
		1E48h	04h	Intel® Q75 Express Chipset
D31:F0	LPC	1E47h	04h	Intel® Q77 Express Chipset
		1E48h	04h	Intel® Q75 Express Chipset
		1E49h	04h	Intel® B75 Express Chipset
		1E44h	04h	Intel® Z77 Express Chipset
		1E46h	04h	Intel® Z75 Express Chipset
		1E4Ah	04h	Intel® H77 Express Chipset
		1E53h	04h	Intel® C216 Chipset
		1E55h	04h	Mobile Intel® QM77 Express Chipset
		1E55h	04h	Mobile Intel® QM77 Express Chipset
		1E58h	04h	Mobile Intel® UM77 Express Chipset
		1E57h	04h	Mobile Intel® HM77 Express Chipset
		1E59h	04h	Mobile Intel® HM76 Express Chipset
		1E5Dh	04h	Mobile Intel® HM75 Express Chipset
		1E5Eh	04h	Mobile Intel® HM70 Express Chipset
		1E56h	04h	Mobile Intel® QS77 Express Chipset
		1E5Fh	04h	Mobile Intel® NM70 Express Chipset
		1E5Eh	04h	Mobile Intel® HM70 Express Chipset
		1E56h	04h	Mobile Intel® QS77 Express Chipset

PCH/7-series-chipset-pch-datasheet.pdf

Device Function	Descrip-tion	Dev ID	C1 SRID	Comments
D31:F0	LPC	8C41h	04h	LPC Controller (Mobile Full Featured Engineering Sample).
		8C42h	04h	LPC Controller (Desktop Full Featured Engineering Sample).
		8C44h	04h	LPC Controller (Z87 SKU).
		8C46h	04h	LPC Controller (Z85 SKU).
		8C49h	04h	LPC Controller (HM86 SKU).
		8C4Ah	04h	LPC Controller (H87 SKU).
		8C4Bh	04h	LPC Controller (HM87 SKU).
		8C4Ch	04h	LPC Controller (Q85 SKU).
		8C4Eh	04h	LPC Controller (Q87 SKU).
		8C4Fh	04h	LPC Controller (QM87 SKU).
		8C50h	04h	LPC Controller (B85 SKU).
		8C52h	04h	LPC Controller (C222 SKU).
		8C54h	04h	LPC Controller (C224 SKU).
		8C56h	04h	LPC Controller (C226 SKU).
		8C5Ch	04h	LPC Controller (H81 SKU).

PCH/8-series-chipset-pch-datasheet.pdf

D31:F0	LPC	8CC2h	00h	LPC Controller (Full Featured Engineering Sample).
		8CC4h	00h	LPC Controller (Z97 SKU).
		8CC6h	00h	LPC Controller (H97 SKU).

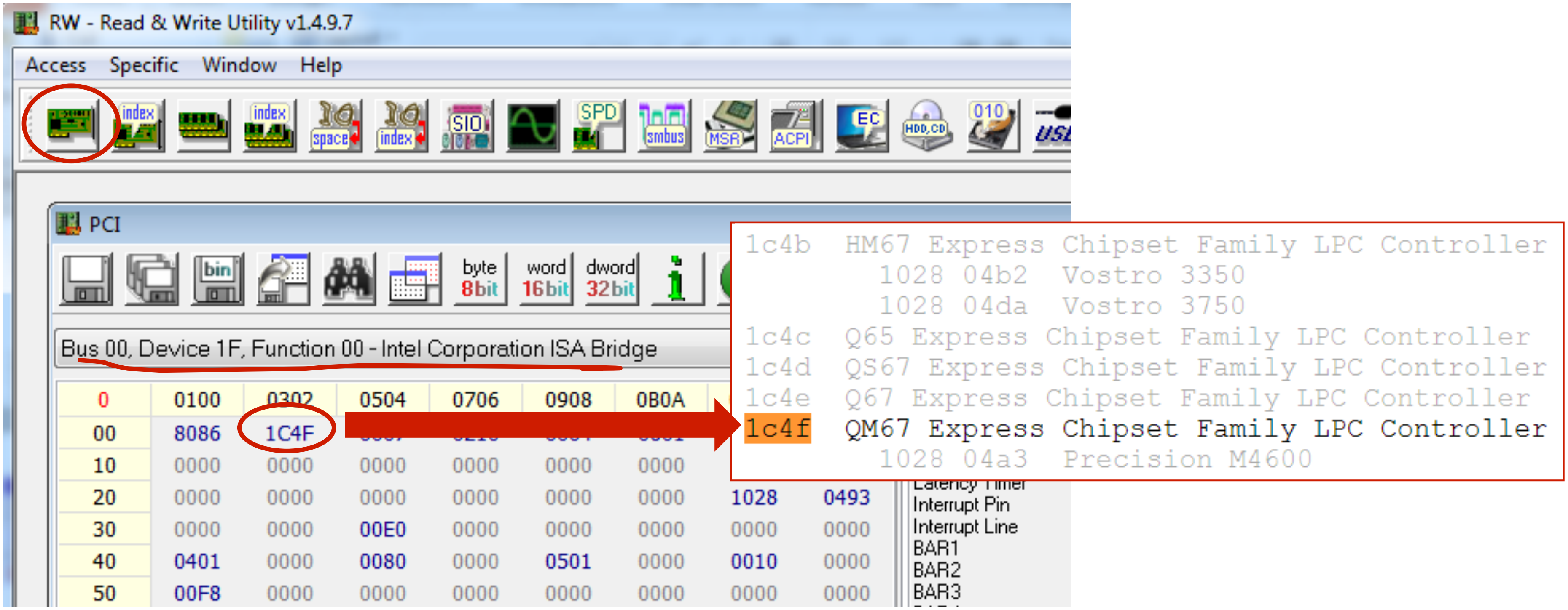
PCH/9-series-chipset-pch-datasheet.pdf

D31:F0	LPC	9CC1h	03h	LPC Controller (Full Featured Engineering Sample with U-Processor Line).
		9CC2h	03h	LPC Controller (Full Featured Engineering Sample with U-Processor Line).
		9CC3h	03h	LPC Controller (Premium SKU with U-Processor Line)
		9CC5h	03h	LPC Controller (Base SKU with U-Processor Line)
		9CC6	03h	LPC Controller (Full Featured Engineering Sample with the Intel® Core™ M processor).
		9CC7h	03h	LPC Controller (Premium SKU with the Intel® Core™ M processor)
		9CC9h	03h	LPC Controller (Base SKU with the Intel® Core™ M processor)

CPU/5thGen(Broadwell)/5th-gen-core-family-platform-i-o-datasheet.pdf

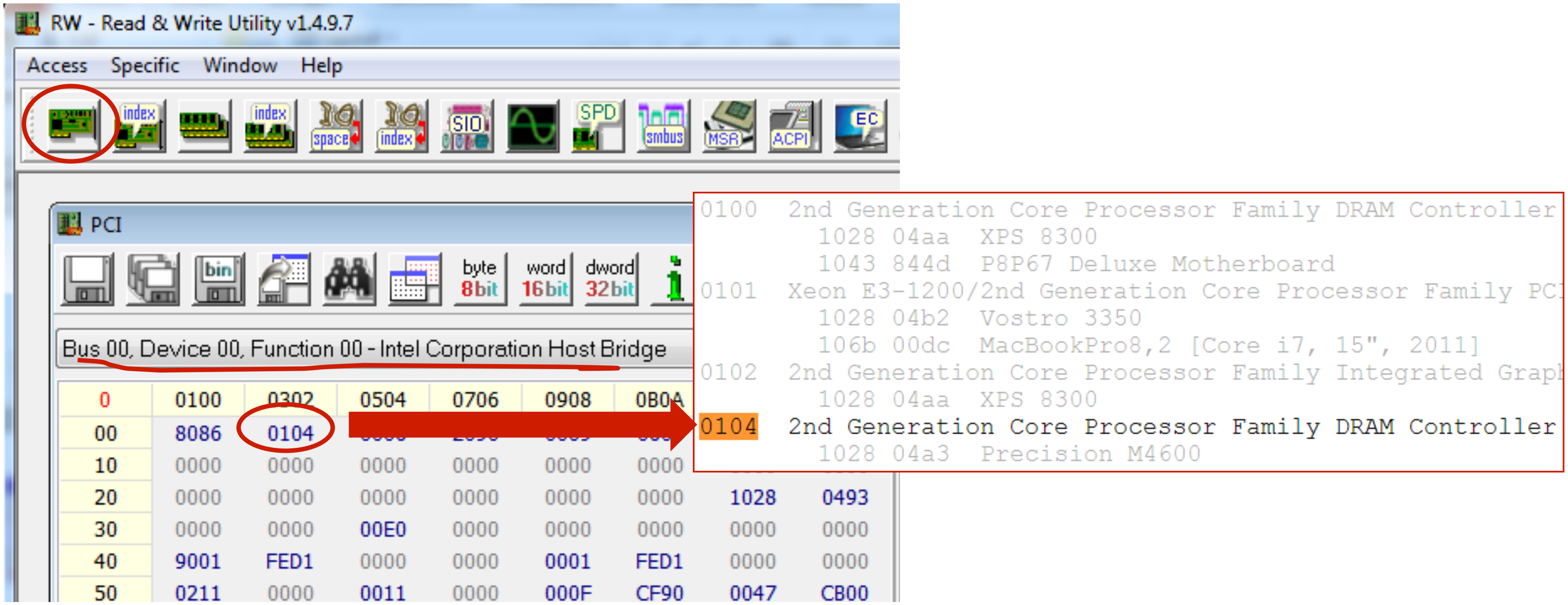
Backup

Solving Ambiguity: Get LPC Device



- As before, Read the 2-byte Device ID of the LPC device:
- Bus 0, Device 31d (1Fh), Function 0, Offset 2
- If the Controller Hub is referred to as the Chipset, it’s a PCH device.
- So in a PCH system, the LPC controller will tell us the chipset family
- So this is a QM67 Express Chipset (6-series chipset)
- Datasheet: http://www.intel.com/content/www/us/en/chipsets/6-chipset-c200-chipset-datasheet.html

Identify the MCH Device ID



- As before, Read the 2-byte Device ID of the MCH (DRAM Controller):
- Bus 0, Device 0, Function 0, Offset 2
- In this sample case the Memory Controller Device ID is 0x0104
- 2nd Generation Core processor Family
- However there are separate datasheets for the 2nd generation Mobile and Desktop family datasheets
- To identify the CPU, we have to download the Specification updates for each

Hmm…Either Mobile or Desktop* CPU

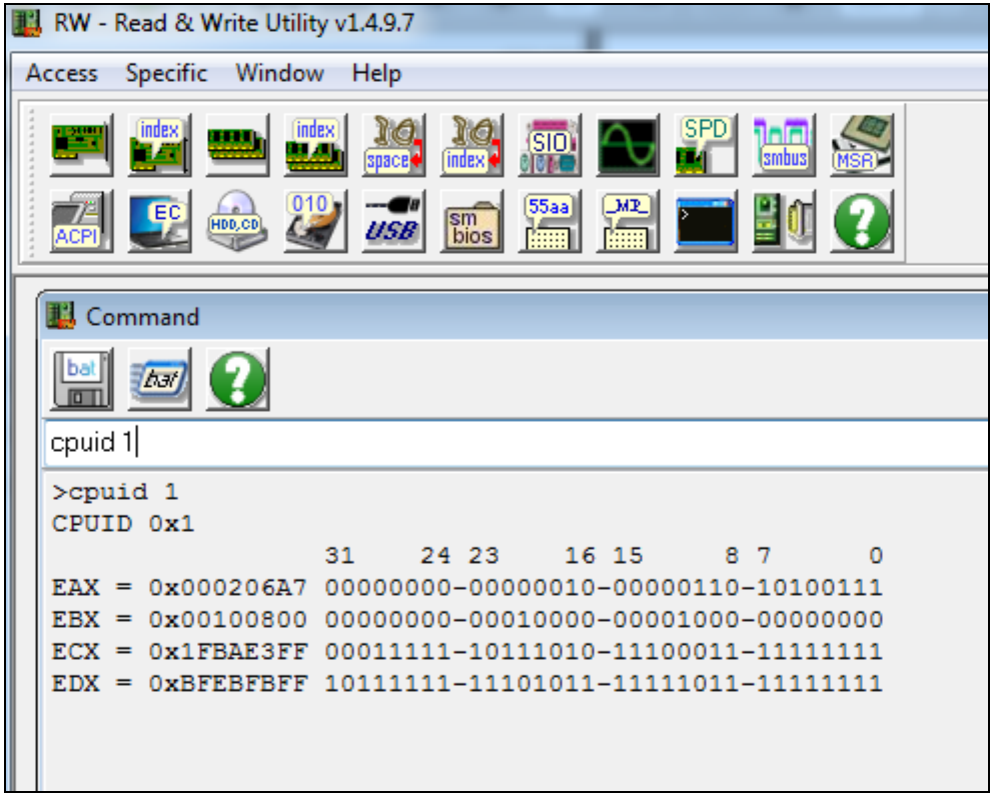
- Download the Specification Updates for both the Desktop and Mobile family (2nd generation Core series processor)
  - http://www.intel.com/content/dam/www/public/us/en/documents/specification-updates/2nd-gen-core-family-mobile-specification-update.pdf
  - http://www.intel.com/content/dam/www/public/us/en/documents/specification-updates/2nd-gen-core-desktop-specification-update.pdf

Stepping	Vendor ID[1]	Host Device ID[2]	Processor Graphics Device ID[3]	Revision ID[4]
D-2	8086h	0104h	GT1: 0106h GT2: 0116h GT2 (>1.3 GHz Turbo): 126h	09h
J-1	8086h	0104h	GT1: 0106h GT2: 0116h GT2 (>1.3 GHz Turbo): 126h	09h

- In this case, the DRAM Controller (MCH) device ID of 0104h is defined in the Mobile series specification update

*We're operating under the assumption that this is being done remotely so we can't just "look."

Get the CPU Stepping Information



- When EAX initialized with a value of ‘1’, CPUID returns the Extended Family, Extended Model, Processor Type, Family Code, Model Number and Stepping ID value (in EAX)
- You can run CPUID in RW Everything
  - CPUID requires no privileges to run

Identify the CPU Stepping Information

Reserved	Extended Family[1]	Extended Model[2]	Reserved	Processor Type[3]	Family Code[4]	Model Number[5]	Stepping ID[6]
31:28	**27:20**	**19:16**	**15:14**	**13:12**	**11:8**	**7:4**	**3:0**
	00000000b	0010b		00b	0110	1010b	xxxxb

Gen2 Core Specification Update Datasheet

```
>cpuid 1
CPUID 0x1
                   31      24 23     16 15      8 7       0
EAX = 0x000206A7 00000000-00000010-00000110-10100111
EBX = 0x00100800 00000000-00010000-00001000-00000000
ECX = 0x1FBAE3FF 00011111-10111010-11100011-11111111
EDX = 0xBFEBFBFF 10111111-11101011-11111011-11111111
```

- Extended family tells you which processor family the CPU is of (Pentium, Pentium Pro, Intel Core, etc.)
- Extended Model identifies the particular model within the family
- Processor Type tells you if it's OEM, etc.
- Family Code corresponds to EDX bits [11:8] at system reset
- The Model Number corresponds to EDX bits [7:4] at system reset
  - This is a PCH example and so this CPUID return will differ from our EDX value from the entry vector portion of the course which was of the E6400

– Stepping ID is the revision number of this CPU model