

Identificarea si Configurarea resurselor PC

Cpuid. BIOS

LAB

ANCA APĂTEAN - AC - UTCN

Tematica LAB

ANCA APATEAN - UTCN

Introducere

Introducere – reprezentarea informatiei in calculator. Tipuri de calculatoare

Istoria calculatoarelor. Calculatorul von Neumann.

Arhitectura calculatoarelor personale/ PC. Istoria familiei de procesoare x86

Din interiorul PC-ului

Memoria in PC.
Memoria cache.

Echipamente periferice.
Control transfer de date.
Polling, Intreruperi, DMA.

Bus-uri si interfete folosite in PC.
ISA, PCI, PCIe,
IDE/ATA, SCSI, RS232,
USB, IEEE 1284, etc

Din exteriorul PC-ului

Echipamente de stocare date: FD, HDD, SSD, CD/DVD, Flash USB

Echipamente de intrare-iesire: monitor, tastatura, mouse, interfata grafica, interfete audio, etc

Identificarea si configurarea resurselor PC

Cresterea performantelor PC-ului

Clasificarea Flynn.
Paralelismul in prelucrarea datelor.
CISC vs RISC

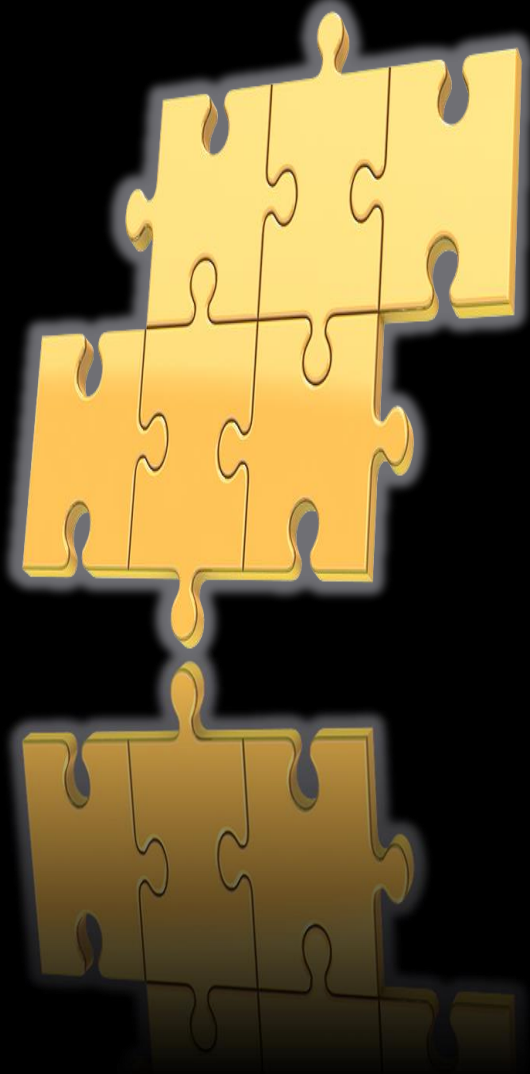
Arhitecturi VLIW, EPIC, Prelucrare secventiala si secvential-paralela

Pipeline/ Superpipeline.
Scalar/Superscalar

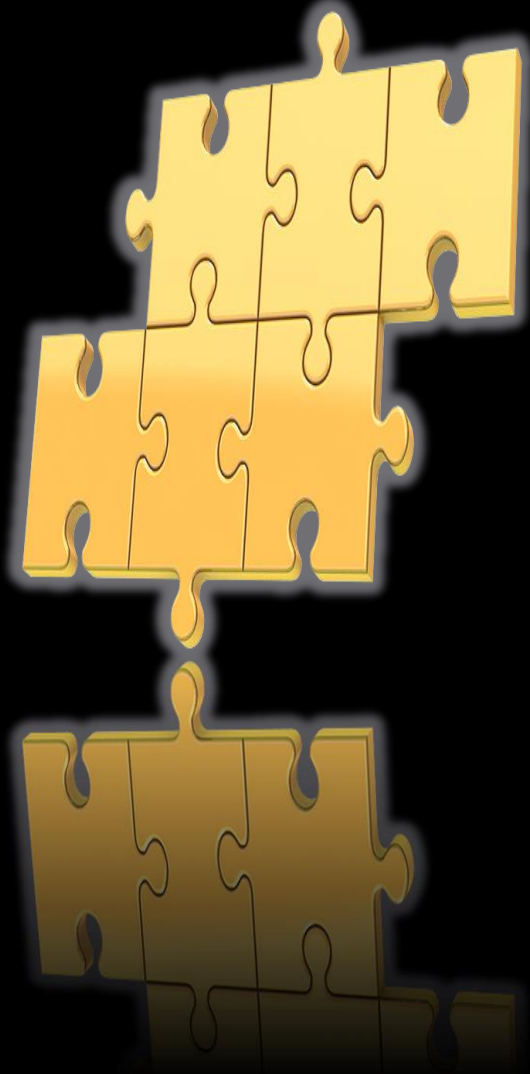
Comparatie arhitecturi procesoare de uz general (GPP), DSP, MicroC, DSC, SoC.

Evaluarea performantelor PC-ului

Evaluarea performantelor calculatoarelor. Benchmark-uri.



- Prezentarea notiunilor principale despre modul **cum se pot identifica resursele unui PC**
- Familiarizarea cu **instructiunea CPUID** si indrumarea spre exercitii si aplicatii ce folosesc aceasta instructiune
- Prezentarea notiunilor principale despre **configurarea resurselor unui PC**
- Familiarizarea cu notiunile **BIOS, EFI si UEFI.**

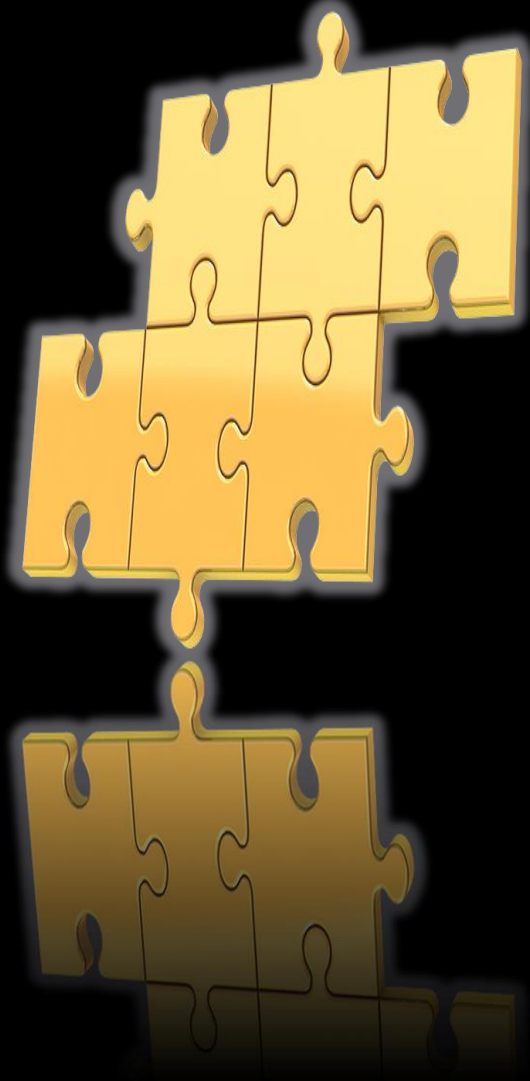


1. Identificarea resurselor PC

- instructiunea CPUID
- CPU-Z, AIDA64

2. Configurarea resurselor PC

- BIOS, EFI, UEFI



1. Identificarea resurselor PC

- instructiunea CPUID
- CPU-Z, AIDA64

2. Configurarea resurselor PC

- BIOS, EFI, UEFI

- **dintre cele mai folosite unelte la ora actuala:**
 - **CPU-Z, AIDA64**
 - furnizeaza informatii despre orice tip de procesor (universal)
(nu e o aplicatie specifica precum cele dezvoltate de Intel sau AMD)
 - **CPU-Z**
 - = unelta bazata pe S.O. Windows
 - foloseste instructiunea **CPUID** pentru a identifica diferite setari ale sistemului, in special cele legate de UCP
 - **AIDA64** (inainte Everest)
 - = unelta bazata pe S.O. Windows
 - identifica toate componentele din PC:
 - afiseaza atat informatii despre hardware
(inclusiv despre UCP, folosind instructiunea **CPUID**),
cat si despre software

AIDA64

ofera un set complet de unelte pentru:

- benchmark (testare, comparare),
- overclock (cresterea vitezei ceasului),
- monitorizare
- depanare
- pt sist. desktop si mobile

The screenshot displays the AIDA64 Extreme Edition interface. The main window shows a list of benchmarks for various system components. The 'CPU' section is expanded, showing a list of processors with their respective memory bandwidth, clock speeds, motherboard models, chipsets, and memory configurations. The 'Sempron 140' is highlighted in yellow. Below the list, a 'Field Value' table provides detailed specifications for the selected processor.

Field	Value
CPU Type	AMD Sempron 140 (Sargas)
CPU Platform / Stepping	Socket AM3 / DA-C2
CPU Clock	2712.0 MHz (original: 2700 MHz)
CPU Multiplier	13.5x
CPU FSB	200.9 MHz (original: 200 MHz)
Memory Bus	535.7 MHz
DRAM:FSB Ratio	16:6
Motherboard Chipset	AMD 890GX, AMD K10

At the bottom of the window, a status bar displays system information: Load Mem SSE PrefNTA SUB Back: 2.97 bytes/cycle (mask:00000001) | BDLL: 2.6.328-x64, CPU: 2711 MHz, TSC: 2711 MHz

Identificarea si configurarea resurselor PC

1. Identificarea resurselor PC – AIDA64 (2)

ANCA APATEAN - UTCN

AIDA64 - CPUID –

AMD vs Intel

AIDA64 CPUID

Processor	AMD Sempron 140				
Code Name	Sargas				
Platform	Socket AM3				
Stepping	DA-C2				
CPUID Vendor	AuthenticAMD	45 nm			
CPUID Name	AMD Sempron(tm) 140 Processor				
CPUID Rev.	01F	6	2	Core Voltage	1.344 V
CPU Clock	2710.0 MHz		L1 Instr. Cache	64 KB	
Multiplier	13.5x		L1 Data Cache	64 KB	
HTT Clock	200.7 MHz		L2 Cache	1 MB	
HTT Speed	2007.4 MHz		L3 Cache		
Instruction Set	x86, x86-64, MMX, MMX+, 3DNow!, 3DNow!+, 3DNow! Pro, SSE, SSE2, SSE3, SSE4A				
Motherboard	Gigabyte GA-890GPA-UD3H v2				
BIOS Version	FA				
Chipset	AMD 890GX, AMD K10				
Integr. Video	Active (ATI Radeon HD 4290)				
Memory Type	Unganged Dual Channel DDR3-1071 SDRAM (8-8-8-20 CR1)				
Memory Clock	535.3 MHz	DRAM:FSB Ratio	16:6		

CPU #1 AIDA64

AIDA64 CPUID

Processor	QuadCore Intel Core i7 Extreme 965 [ES]				
Code Name	Bloomfield				
Platform	LGA1366				
Stepping	C0/C1				
CPUID Vendor	GenuineIntel	45 nm			
CPUID Name	Genuine Intel(R) CPU 000 @ 3.20GHz				
CPUID Rev.	6	1A	4	Core Voltage	1.136 V
CPU Clock	3207.3 MHz		L1 Instr. Cache	32 KB	
Multiplier	24x		L1 Data Cache	32 KB	
QPI Clock	133.6 MHz		L2 Cache	256 KB	
QPI Speed	3207.3 MHz		L3 Cache	8 MB	
Instruction Set	x86, x86-64, MMX, SSE, SSE2, SSE3, SSSE3, SSE4.1, SSE4.2				
Motherboard	Asus P6T Deluxe				
BIOS Version	1611				
Chipset	Intel Tylersburg X58, Intel Nehalem				
Integr. Video	-				
Memory Type	Triple Channel DDR3-1333 SDRAM (9-9-9-24 CR1)				
Memory Clock	668.2 MHz	DRAM:FSB Ratio	5:1		

CPU #1 / Core #1 / HTT Unit #1 AIDA64

Identificarea si configurarea resurselor PC

1. Identificarea resurselor PC – CPU-Z vs AIDA64

ANCA APATEAN - UTCN

- CPUID -

CPU-Z vs AIDA64

CPU-Z

CPU Caches Mainboard Memory SPD Graphics About

Processor

Name	Intel Core i7 3930K		
Code Name	Sandy Bridge-E	Max TDP	130 W
Package	Socket 2011 LGA		
Technology	32 nm	Core Voltage	1.112 V

Specification: Genuine Intel(R) CPU @ 3.20GHz (ES)

Family	6	Model	D	Stepping	5
Ext. Family	6	Ext. Model	2D	Revision	C0

Instructions: MMX, SSE (1, 2, 3, 3S, 4.1, 4.2), EM64T, VT-x, AES, AVX

Clocks (Core #0)

Core Speed	3202.0 MHz
Multiplier	x 32.0 (12 - 32)
Bus Speed	100.1 MHz
Rated FSB	3202.0 MHz

Caches

L1 Data	6 x 32 KBytes	8-way
L1 Inst.	6 x 32 KBytes	8-way
Level 2	6 x 256 KBytes	8-way
Level 3	12 MBytes	16-way

Selection: Processor #1 Cores: 6 Threads: 12

Validate OK

Version 1.61.3

AIDA64 CPUID

Processor: QuadCore Intel Core i7 Extreme 965 [ES]
Code Name: Bloomfield
Platform: LGA1366
Stepping: C0/C1
CPUID Vendor: GenuineIntel 45 nm
CPUID Name: Genuine Intel(R) CPU 000 @ 3.20GHz

CPUID Rev.: 6 1A 4 Core Voltage: 1.136 V

CPU Clock: 3207.3 MHz
Multiplier: 24x
QPI Clock: 133.6 MHz
QPI Speed: 3207.3 MHz

L1 Instr. Cache: 32 KB
L1 Data Cache: 32 KB
L2 Cache: 256 KB
L3 Cache: 8 MB

Instruction Set: x86, x86-64, MMX, SSE, SSE2, SSE3, SSSE3, SSE4.1, SSE4.2

Motherboard: Asus P6T Deluxe
BIOS Version: 1611
Chipset: Intel Tylersburg X58, Intel Nehalem
Integr. Video: -
Memory Type: Triple Channel DDR3-1333 SDRAM (9-9-9-24 CR1)
Memory Clock: 668.2 MHz DRAM:FSB Ratio: 5:1

CPU #1 / Core #1 / HTT Unit #1 AIDA64 Save Close

Identificarea si configurarea resurselor PC

1. Identificarea resurselor PC – CPU-Z

ANCA APATEAN - UTCN

CPU-Z

- ofera informatii despre:

- UCP

- memoria cache

- P.B.

- memorie

- placa grafica

The screenshot shows the CPU-Z application window with the 'CPU' tab selected. The processor information is as follows:

Processor Name	Intel Mobile Core 2 Duo T7250		
Code Name	Merom	Brand ID	
Package	Socket P (478)		
Technology	65 nm	Core VID	0.900 V
Specification	Intel(R) Core(TM)2 Duo CPU T7250 @ 2.00GHz		
Family	6	Model	F
Ext. Family	6	Ext. Model	F
Stepping	D		
Revision	M0		
Instructions	MMX, SSE (1, 2, 3, 3S), EM64T, VT-x		

Cache information:

L1 Data	2 x 32 KBytes	8-way
L1 Inst.	2 x 32 KBytes	8-way
Level 2	2048 KBytes	8-way
Level 3		

Clocks (Core #0):

Core Speed	798.07 MHz
Multiplier	x 4.0
Bus Speed	199.53 MHz
Rated FSB	798.07 MHz

Selection: Processor #1 | Cores: 2 | Threads: 2

Buttons: Validate, OK

Version: CPU-Z Version 1.62.0.x32

CPU-Z

- ofera informatii despre:
 - CPU
 - memoria cache
 - P.B.
 - memorie
 - placa grafica

The screenshot shows the CPU-Z application window with the 'Caches' tab selected. The interface displays the following cache information:

Cache Type	Size	Descriptor
L1 D-Cache	32 KBytes x 2	8-way set associative, 64-byte line size
L1 I-Cache	32 KBytes x 2	8-way set associative, 64-byte line size
L2 Cache	2048 KBytes	8-way set associative, 64-byte line size
L3 Cache		

At the bottom of the window, the version 'CPU-Z Version 1.62.0.x32' is displayed, along with 'Validate' and 'OK' buttons.

CPU-Z

- ofera informatii despre:
 - CPU
 - memoria cache
 - P.B.
 - memorie
 - placa grafica

The screenshot shows the CPU-Z application window with the 'Mainboard' tab selected. The 'Motherboard' section contains the following information:

Manufacturer	Dell Inc.		
Model	0U990C		
Chipset	Intel	GM965	Rev. C0
Southbridge	Intel	82801HBM (ICH8-ME)	Rev. B0
LPCIO	NS		

The 'BIOS' section contains the following information:

Brand	Dell Inc.		
Version	A17		
Date	10/27/2009		

The 'Graphic Interface' section contains the following information:

Version			
Transfer Rate		Max. Supported	
Side Band			

At the bottom of the window, it displays 'CPU-Z Version 1.62.0.x32' and buttons for 'Validate' and 'OK'.

CPU-Z

- ofera informatii despre:
 - CPU
 - memoria cache
 - P.B.
 - memorie
 - placa grafica

CPU-Z Version 1.62.0.x32

Validate OK

Section	Parameter	Value
General	Type	DDR2
	Size	3072 MBytes
	Channels #	Dual
	DC Mode	Symmetric
Timings	DRAM Frequency	332.6 MHz
	FSB:DRAM	3:5
	CAS# Latency (CL)	5.0 clocks
	RAS# to CAS# Delay (tRCD)	5 clocks
	RAS# Precharge (tRP)	5 clocks
	Cycle Time (tRAS)	15 clocks
	Bank Cycle Time (tRC)	
Command Rate (CR)		
DRAM Idle Timer		
Total CAS# (tRDRAM)		
Row To Column (tRCD)		

CPU-Z

- ofera informatii despre:
 - CPU
 - memoria cache
 - P.B.
 - **memorie**
 - placa grafica

Memory Slot Selection

Slot #2	DDR2		
Module Size	1024 MBytes	Correction	None
Max Bandwidth	PC2-5300 (333 MHz)	Registered	
Manufacturer	Samsung	Buffered	
Part Number	M4 70T2864QZ3-CE6	SPD Ext.	AMP
Serial Number	762B6E5E	Week/Year	04 / 08

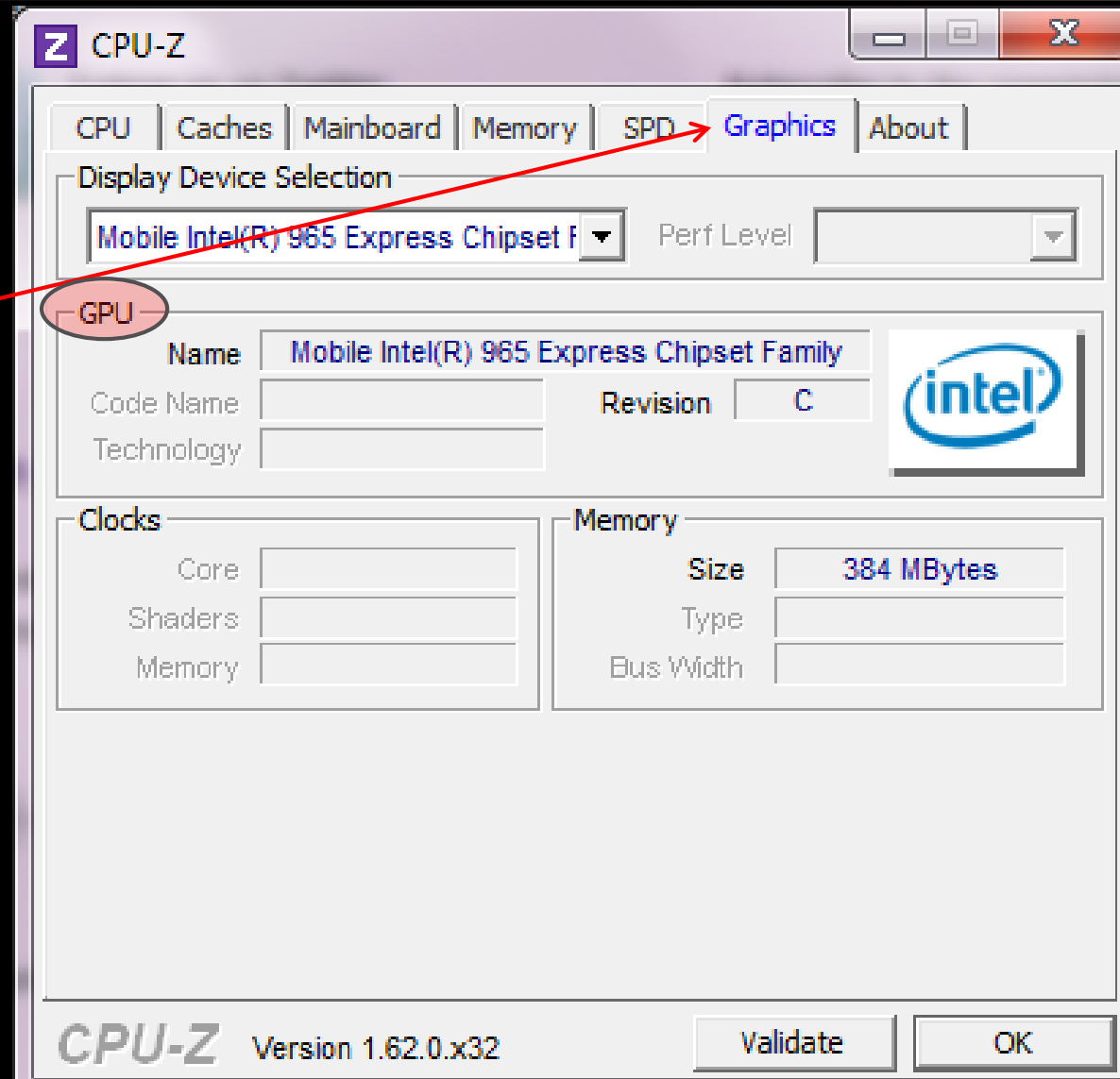
Timings Table

	JEDEC #1	JEDEC #2	JEDEC #3	AMP
Frequency	200 MHz	266 MHz	333 MHz	0 MHz
CAS# Latency	3.0	4.0	5.0	
RAS# to CAS#	3	4	5	-1073741824
RAS# Precharge	3	4	5	-1073741824
tRAS	9	12	15	-1073741824
tRC	12	16	20	-1073741824
Command Rate				
Voltage	1.80 V	1.80 V	1.80 V	

CPU-Z Version 1.62.0.x32 Validate OK

CPU-Z

- ofera informatii despre:
- CPU
- memoria cache
- P.B.
- memorie
- placa grafica




Z CPU-Z

CPU | Caches | Mainboard | Memory | SPD | **Graphics** | About

Display Device Selection

Mobile Intel(R) 965 Express Chipset f | Perf Level

GPU

Name	Mobile Intel(R) 965 Express Chipset Family	
Code Name		Revision C
Technology		

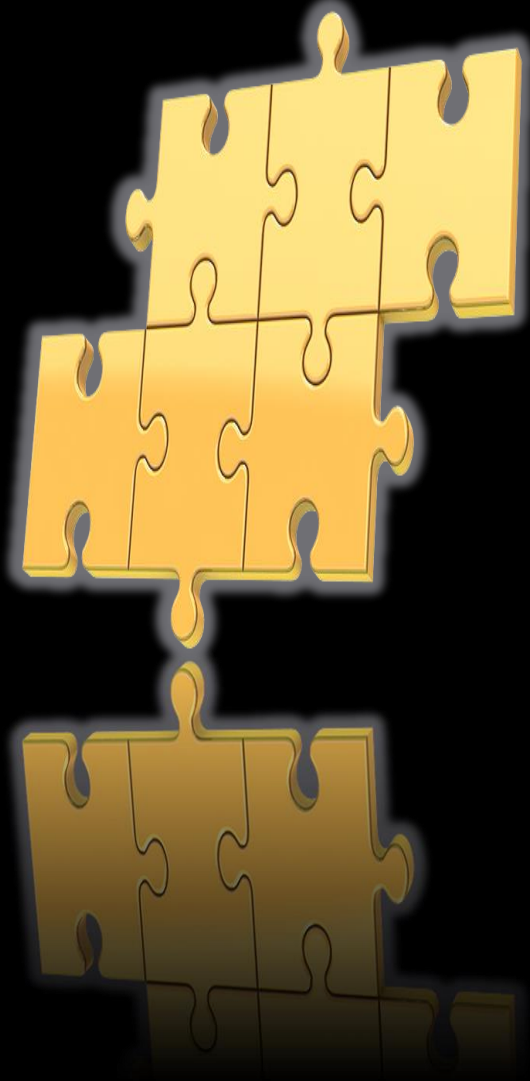
Clocks

Core	
Shaders	
Memory	

Memory

Size	384 MBytes
Type	
Bus Width	

CPU-Z Version 1.62.0.x32 Validate OK



1. Identificarea resurselor PC

- instructiunea CPUID
- CPU-Z, AIDA64

2. Configurarea resurselor PC

- BIOS, EFI, UEFI

CPUID (CPU IDentification)

= o instructiune x86 – Intel 1993 – unele 486↑

- codul operatiei (de la codificarea instructiunilor) = 0FA2h
- **nu are operanzi**, dar **are PARAMETRII la INTRARE** (inainte de executie): **registrul EAX (uneori si ECX)**
- valoarea din registrul **EAX** – specifica informatia returnata
- este specifica arhitecturii x86 (Intel si AMD), alte arhitecturi furnizand **registre “on-chip”**
ce pot fi citite si interpretate pt a obtine acelasi tip de informatii
- poate determina **tipul procesorului si prezenta caracteristicilor**
(precum FPU,MMX,SSE,PSN,...)

Prima data :

-CPUID ar trebui executata cu **EAX = 0**

=> **EAX**=valoarea maxima suportata de CPUID = nr **functii standard**

-CPUID ar trebui executata cu **EAX = 80000000h** (b31=1)

=> **EAX**=valoarea maxima suportata de CPUID = nr **functii extinse**

CPUID (CPU IDentification)

Parametru	Informatia returnata de CPUID
EAX=0	EAX ← val. maxima recunoscuta de CPUID pentru functiile standard EBX:EDX:ECX ← sirul ASCII al producatorului
EAX=1	EAX ← semnatura procesorului= cei mai semnificativi 32 biti (bitii 95-64) din cei 96 ai numarului serial al procesorului (PSN) EBX ← Brand ID pe bitii 7..0 ECX,EDX ← flaguri de caracteristici ale procesorului (! Nu e PSW)
EAX=2	EAX:EBX:ECX:EDX ← informatii despre memoria cache si descriptorii TLB (Translation Lookaside Buffer)
EAX=3	EDX:ECX ← cei mai putin semnificativi 64 biti (bitii 63-0) din cei 96 ai numarului serial al procesorului (PSN)
!!! EAX=4,5,6,7,8,9,a,b,c,d !!	
EAX=8000_0000h	EAX ← valoarea maxima recunoscuta de CPUID pentru functiile extinse
EAX=8000_0001h	EAX ← semnatura extinsa a procesorului si ECX,EDX ← flaguri de caracteristici extinse ale procesorului
EAX=8000_0002/3/4h	EAX:EBX:ECX:EDX ← numele procesorului (Processor Brand String)
EAX=8000_0005h	EAX:EBX:ECX:EDX ← informatii despre memoria cache L1 / TLB
EAX=8000_0006h	EAX:EBX:ECX:EDX ← informatii despre memoria cache L2 / TLB
EAX=8000_0007h	EAX:EBX:ECX:EDX ← flaguri de caracteristici pentru controlul avansat al puterii
EAX=8000_0008h	EAX:EBX:ECX:EDX ← dimensiunea adresei virtuale si fizice (liniara)

EAX=0 -> **ID-ul producatorului (vendor ID)** = un sir ASCII de 12 caractere preluat din continutul reg **EBX, EDX, ECX** in aceasta ordine !

"AMDisbetter!"	— primele AMD K5
"AuthenticAMD"	— AMD
"CentaurHauls"	— Centaur
"CyrixInstead"	— Cyrix
"GenuineIntel"	— Intel
"TransmetaCPU"	— Transmeta
"GenuineTMx86"	— Transmeta
"Geode by NSC"	— National Semiconductor
"NexGenDriven"	— NexGen
"RiseRiseRise"	— Rise
"SiS SiS SiS "	— SiS
"UMC UMC UMC "	— UMC
"VIA VIA VIA "	— VIA
"Vortex86 SoC"	— Vortex

Bit	EDX		ECX	
0	FPU	Onboard x87 FPU	PNI	Prescott New Instructions (SSE3)
1	VME	Virtual mode extensions (VIF)	PCLMULQDQ	PCLMULQDQ support
2	DE	Debugging extensions (CR4 bit 3)	DTES64	64-bit debug store (edx bit 21)
3	PSE	Page size extensions	MONITOR	MONITOR and MWAIT instructions (SSE3)
4	TSC	Time Stamp Counter	DS_CPL	CPL qualified debug store
5	MSR	Model-specific registers	VMX	Virtual Machine eXtensions
6	PAE	Physical Address Extension	SMX	Safer Mode Extensions (LaGrande)
7	MCE	Machine Check Exception	EST	Enhanced SpeedStep
8	CX8	CMPXCHG8 (compare-and-swap) instruction	TM2	Thermal Monitor 2
9	APIC	Onboard Advanced PIC(ProgramableInterruptCtrller)	SSSE3	Supplemental SSE3 instructions
10		(RESERVED)	CID	Context ID
11	SEP	SYSENTER and SYSEXIT instructions		(RESERVED)
12	MTRR	Memory Type Range Registers	FMA	Fused multiply-add (FMA3)
13	PGE	Page Global Enable bit in CR4	CX16	CMPXCHG16B instruction
14	MCA	Machine check architecture	XTPR	Can disable sending task priority messages
15	CMOV	Conditional move and FCMOV instructions	PDCM	Perform & debug capability
16	PAT	Page Attribute Table		(RESERVED)
17	PSE36	36-bit page huge pages	PCID	Process context identifiers (CR4bit 17)
18	PSN	Processor Serial Number	DCA	Direct cache access for DMA writes
19	CLFLUSH	CLFLUSH instruction (SSE2)	SSE4_1	SSE4.1 instructions
20		(RESERVED)	SSE4_2	SSE4.2 instructions
21	DTS	Debug store: save trace of executed jumps	X2APIC	x2APIC support
22	ACPI	Onboard thermal control MSRs for ACPI	MOVBE	MOVBE instr. (big-endian, Intel Atom)
23	MMX	MMX instructions	POPCNT	POPCNT instruction
24	FXSR	FXSAVE, FXRESTOR instructions,CR4 bit 9	TSCDEADLINE	APIC -one-shot op. using a TSC deadline value
25	SSE	SSE instr.(a.k.a. Katmai New Instructions)	AES	AES instruction set
26	SSE2	SSE2 instructions	XSAVE	XSAVE, XRESTOR, XSETBV, XGETBV
27	SS	CPU cache supports self-snoop	OSXSAVE	XSAVE enabled by OS
28	HT	Hyper-threading	AVX	Advanced Vector Extensions
29	TM	Thermal monitor autom. limits temperature	F16C	CVT16 instr. set (half-precision) FP support
30	IA64	IA64 processor emulating x86	RDRND	RDRAND (on-chip random no. generator)
31	PBE	Pending Break Enable (PBE# pin) wakeup	HYPervisor	Running on a hypervisor (=0 on a real CPU)

Pentru ca o tehnologie sa functioneze pe PC ...

ANCA APĂTEAN - AC - UTCN

Analizati si Retineti:

“A processor with **VT** technology does not guarantee that **virtualization** works on your system. The **VT** technology requires a computer system with a **chipset**, **BIOS**, enabling **software** and/or **operating system**, **device drivers**, and **applications** designed for **this feature**.

If your **BIOS** includes a setting to *enable or disable* support for **Intel VT**, make sure **it is enabled**.”

[Intel, for VT-Virtualization Technology]

<http://www.intel.com/support/processors/sb/cs-030729.htm>



1. Identificarea resurselor PC – Exemplu CPUID (1)

Exemplu CPUID

EAX in	EAX	EBX	ECX	EDX
0000 0000	0000 0008	6874 7541	444d 4163	6974 6e65
0000 0001	0000 36eb	0102 0800	0000 e3bd	bfeb fbff
0000 0002	05b0 b101	0056 57f0	0000 0000	2cb4 307d
0000 0003	0000 0000	0000 0000	0000 0000	0000 0000
8000 0000	8000 0006	0000 0000	0000 0000	0000 0000

EAX=0

CPUID

EAX=8 (val. maxima recunoscuta de CPUID pentru functiile standard)

EAX=80000000h

CPUID

EAX=6 (val. maxima recunoscuta de CPUID pentru functiile extinse)

EAX=0

CPUID

EBX:EDX:ECX = AuthenticAMD (sirul ASCII al producatorului)

EBX=68 74 75 41 = h t u A

EDX=49 65 6e 69 = i t n e

ECX=6c 65 74 6e = D M A c

	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
50	51	52	53	54	55	56	57	58	59	5a					
P	Q	R	S	T	U	V	W	X	Y	Z					

	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f
	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
70	71	72	73	74	75	76	77	78	79	7a					
p	q	r	s	t	u	v	w	x	y	z					



1. Identificarea resurselor PC – Exemplu CPUID (2)

EAX=1 -> **EAX** - Versiunea (stepping), modelul, familia = semnatura procesorului
 = cei mai semnificativi 32 biti (bitii 95-64) din cei 96 ai **PSN**
 (PSN=nr serial al procesorului)

31	28	27	20	19	16	15	14	13	12	11	8	7	4	3	0	
Familie ext				Model ext				Tip proc.				Cod familie		Nr model		ID versiune

Exemplu

EAX in	EAX	EBX	ECX	EDX
0000 0000	0000 0008	6874 7541	444d 4163	6974 6e65
0000 0001	0000 36eb	0102 0800	0000 e3bd	bfeb fbff
0000 0002	05b0 b101	0056 57f0	0000 0000	2cb4 307d
0000 0003	0000 0000	0000 0000	0000 0000	0000 0000
8000 0000	8000 0006	0000 0000	0000 0000	0000 0000

EAX=1 → **CPUID** → **EAX = 0000 36eb** (semnatura procesorului)

ID versiune = b = 1011
Nr model = e = 1110
Cod familie = 6 = 0110
Tip procesor = 11



1. Identificarea resurselor PC – Exemplu CPUID (3)

ANCA APATEAN - UTCN

EAX=1 -> **EDX,ECX**

- **flaguri de caracteristici ale procesorului**

(! Nu e PSW)

a se consulta tabelul de pe slide-ul 20

Exemplu

EAX in	EAX	EBX	ECX	EDX
0000 0000	0000 0008	6874 7541	444d 4163	6974 6e65
0000 0001	0000 36eb	0102 0800	0000 e3bd	bfeb fbff
0000 0002	05b0 b101	0056 57f0	0000 0000	2cb4 307d
0000 0003	0000 0000	0000 0000	0000 0000	0000 0000
8000 0000	8000 0006	0000 0000	0000 0000	0000 0000

EAX=1

CPUID →

EDX = bfeb fbff = 1011 1111 1110 1011 1111 1011 1111 1111

b0 - FPU (unitate in virgula mobila) – suportat

b18 - PSN (processor serial number) – nu e suportat

b23 - MMX (multimedia extension) – suportat

EAX=1

CPUID →

ECX = 0000 e3bd = 0000 0000 0000 0000 1110 0011 1011 1101

b5 – VME (Virtual Machine eXtensions) - suportat



1. Identificarea resurselor PC – Exemplu CPUID (4)

EAX=1 -> EAX – semnatura procesorului = cei mai semnificativi 32 biti
(bitii 95-64) din cei 96 ai numarului serial al procesorului (PSN)

EAX=3 -> EDX:ECX - cei mai putin semnificativi 64 biti
(bitii 63-0) din cei 96 biti ai numarului serial al procesorului (PSN)

Exemplu

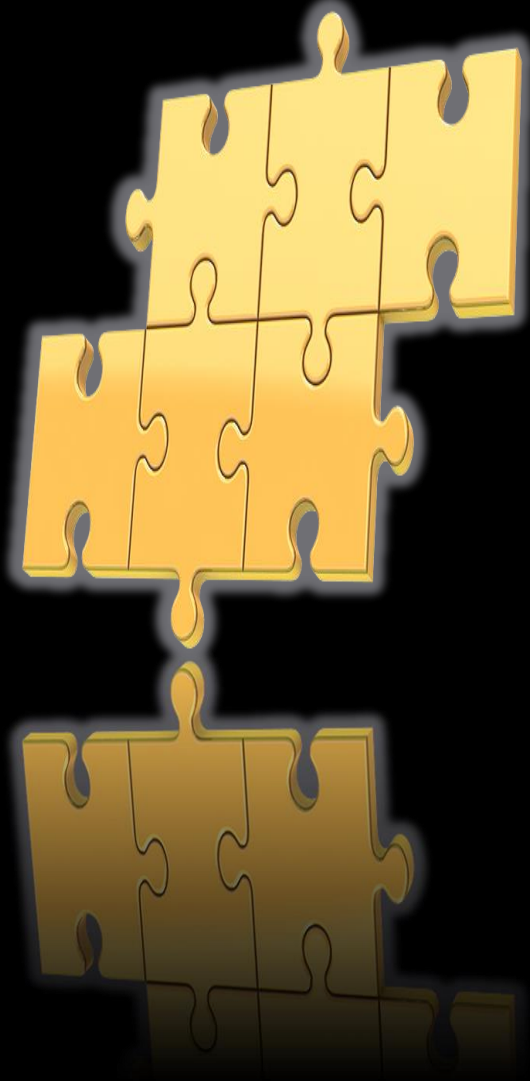
EAX in	EAX	EBX	ECX	EDX
0000 0000	0000 0008	6874 7541	444d 4163	6974 6e65
0000 0001	0000 36eb	0102 0800	0000 e3bd	bfeb fbff
0000 0002	05b0 b101	0056 57f0	0000 0000	2cb4 307d
0000 0003	0000 0000	0000 0000	0000 0000	0000 0000
8000 0000	8000 0006	0000 0000	0000 0000	0000 0000

EAX=1,3

CPUID

PSN = 0000 36eb 0000 0000 0000 0000

b18 - PSN (processor serial number) – nu e suportat, nu e valid !



1. Identificarea resurselor PC

- instructiunea CPUID
- CPU-Z, AIDA64

2. Configurarea resurselor PC

- BIOS, EFI, UEFI

BIOS Setup

Fiecare marcă/model de placă de bază conține un BIOS diferit, unii producători optând pentru introducerea unor opțiuni cu ajutorul cărora să se poate optimiza BIOS-ul, în vederea creșterii semnificative a performanței sistemului.

Toate BIOS-urile oferă **posibilitatea modificării unor parametri de funcționare** încă de la pornirea computerului.

Pentru a **intra în programul de tip meniu de Setup al BIOS-ului**, pe durata POST, este necesară **apăsarea unei taste/ combinații de taste**,

atunci când se afișează un mesaj care indică aceasta;

- de exemplu : „**Press DEL to enter Setup**”, dar poate să difere la anumite plăci, astfel:

- la BIOS **AMI** - Press F1 or Del (Delete) during POST;
- la BIOS **Phoenix BIOS** - Press F1 or F2 during POST;
- la BIOS **Award** - Press Del (Delete or Ctrl+Alt+Esc during POST);
- la BIOS **Microid Research (MR)** - Press Esc during POST.

Dacă secvența se derulează prea repede pe ecran, se poate apăsa tasta Pause pentru a îngheța ecranul și a vizualiza display-ul, iar apoi orice tastă (în general) pentru a continua.

-in meniul de **Setup BIOS**, există în general o **listă tip meniu** cu optiuni:

System Time/Date - setează sau modifică data și timpul;

Boot Sequence - ordinea în care BIOS-ul va încerca să încarce S.O. (să boot-eze)

Plug and Play - un standard pt auto-detectarea dispozitivelor conectate

Mouse/Keyboard - opțiuni "Enable Num Lock," "Enable the Keyboard," "Auto-Detect Mouse"

Drive Configuration - Configurează discurile hard, CD-ROM și floppy;

Memory - direcționează BIOS-ul să realizeze operația de mapare (shadow) la o anumită adresă de memorie;

Security - setează o parolă pentru accesul la computer;

Power Management – pentru managementul puterii, precum și timpul de standby sau suspend

Exit – salvează sau nu modificările, restaurează setările implicite.

Producătorii de BIOS-uri oferă, pe lângă opțiunile standard,

un **set de opțiuni adiționale**,

în funcție de capacitățile chipset-ului plăcii și de dotările oferite de acesta.



ASUS EFI BIOS Utility - EZ Mode Exit/Advanced Mode

23:37
Monday[11/15/2010]

P8P67 DELUXE
BIOS Version : 0304
CPU Type : Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz
Total Memory : 4096 MB (DDR3 2201MHz)

English ▼
Build Date : 10/21/2010
Speed : 3226 MHz

Temperature

CPU	+111.2°F/+44.0°C
MB	+95.0°F/+35.0°C

Voltage

CPU	1.192V	5V	5.160V
3.3V	3.408V	12V	12.288V

Fan Speed

CPU_FAN	1601RPM	PWR_FAN1	N/A
CHA_FAN1	N/A	CHA_FAN2	N/A

System Performance

Quiet ▲ Performance ▲ Energy Saving ▲ Normal ▲

Boot Priority

Use the mouse to drag or keyboard to navigate to decide the boot priority.

Boot Menu(F8) Default(F5)

2011: **Extensible Firmware Interface (EFI)** a inceput sa inlocuiasca vechiul BIOS

diferenta nu este sesizata in randul utilizatorilor obisnuiti,

=> inca se mai foloseste termenul universal BIOS (cuprinzand si EFI).

(specificatiile UEFI - versiunea 2.4, Iulie 2013)

2005 -> **Unified EFI (UEFI)** = un standard ce defineste o interfata intre

S.O. (pe de o parte) si

hardware-ul si software-ul sistemului (pe de alta parte).

-> s-a concretizat intr-un standard in industrie pt **rularea aplicatiilor de bootare**, **incarcarea unui S.O.** si **furnizarea driverelor** ce trebuie activate pe durata incarcarii sistemului.

EFI a fost creat initial de Intel (incepand cu 2000), in 2003 au adus la zi specificatiile, iar 2 ani mai tarziu s-a dezvoltat **forumul UEFI**, o organizatie non-profit din care faceau parte reprezentanti ai **11 companii** (AMD, AMI, Apple, Dell, HP, IBM, Insyde, Intel, Lenovo, Microsoft si Phoenix Technologies)

cu rol de a promova standardul UEFI

E posibil ca unele implementari ale firmware-ului EFI/UEFI sa arate ca un BIOS standard, insa majoritatea celor actuale ofera o **interfata grafica** (la care se poate folosi si mouse-ul) (“*mouse-driven*”) combinata cu **diferite caracteristici care nu existau la BIOS-urile mai vechi**, precum:

- **Diagnostics** – mai cuprinzator decat POST, testeaza inclusiv memoria si HDD
- **Live Update** – poate intra pe site-ul web producatorului pt a verifica daca exista o versiune de BIOS mai recenta, iar apoi sa realizeze update in mod automat
- **HDD Backup** – posibilitatea de a face backup sau clona un HDD dinafara S.O.
- **Overclocking** – utilitati de overclocking
- **BOOT logo** – pt update/ modificare de logo grafic ce apare (se vede pe monitor) la pornirea sistemului

- In realitate:

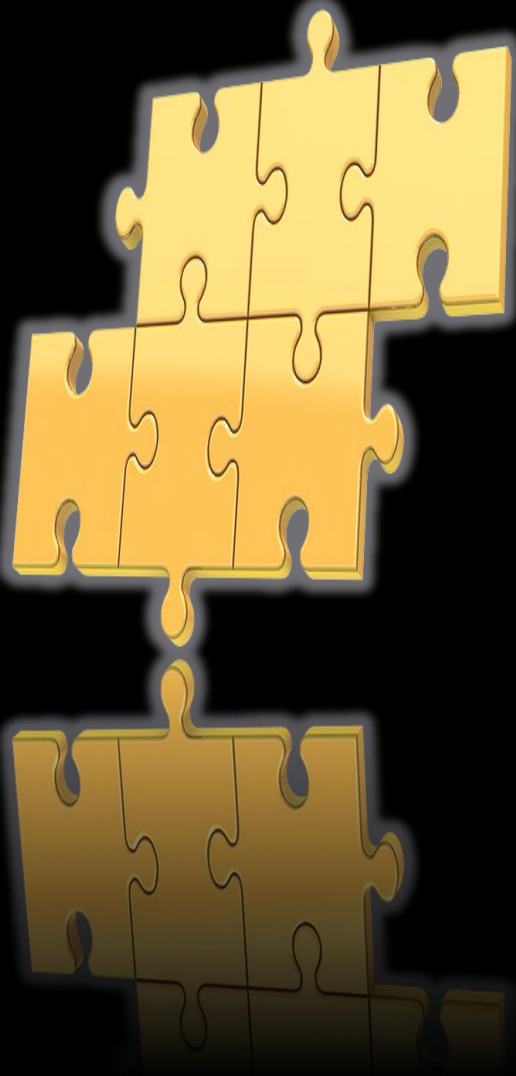
abia din 2008 PC-urile au suportat UEFI

(primul S.O. ce suporta UEFI a fost Windows Vista SP1 x64)

- doar din 2011 (odata cu introducerea seriei de chipseturi Intel 6x)

a aparut implementat in sisteme ca o caracteristica standard.

- au existat unele P.B. experimentale cu firmware UEFI (se numea **Click BIOS**) inca din 2008.



- pentru a identifica resursele unui PC se poate folosi instructiunea **CPUID (CPU IDentification)**
 - > prin intermediul reg EAX functionand ca parametru la intrare cpuid poate furniza informatii complexe despre producatorul CPU, seria, familia din care face parte, diferite caracteristici suportate, etc
- pentru a configura resursele unui PC se foloseste **BIOS-ul sistemului** (denumit si firmware)
 - BIOS-ul este sistemul de baza de intrare-iesire, iar in prezent aproape orice componenta din PC contine propriul firmware
 - in timp, s-au folosit mai multe tipuri de memorii pt BIOS, precum ROM, PROM, EPROM, EEPROM sau FlashROM
 - pentru configurarea sistemului se foloseste un program de **Setup** al BIOS care poate fi diferit de la un sistem la altul, in functie de specificatiile oferite de producatorul PB si al chipsetului



TEME set 1

1. urmariti Materialul de laborator (slide-ul 21) si explicati cum s-a obtinut sirul Ascii al producatorului
2. urmariti Materialul de laborator (slide-ul 22) si explicati cum s-au extras informatiile despre procesor:
ID versiune , nr model, Cod familie, Tip procesor din semnatura
3. Analizati in Materialul de laborator slide-ul 11, identificand campurile de la punctul 2 pe captura
4. rulati CPU-z pe PC-ul propriu si realizati o captura pe fereastra obtinuta, iar apoi explicati campurile din semnatura procesorului de la punctul 2
5. in Materialul de laborator pe slide-ul 23 urmariti caracteristicile procesorului si identificati-le pe tabelul de pe slide-ul 20.
6. in Materialul de laborator pe slide-ul 24 urmariti cum a fost aflat numarul de serie al procesorului si cum s-a verificat validitatea lui.



TEME set 2

1. Pentru datele din tabelul alaturat, stabiliti:

EAX in	EAX	EBX	ECX	EDX
0000 0000	0000 000a	756e 6547	6c65 746e	4965 6e69
0000 0001	0000 06fd	0102 0800	0000 e3bd	bfeb fbff
0000 0002	05b0 b101	0056 57f0	0000 0000	2cb4 307d
0000 0003	0000 0000	0000 0000	0000 0000	0000 0000
8000 0000	8000 0006	0000 0000	0000 0000	0000 0000

- val max pt nr de functii standard
- val max pt nr de functii extinse
- sirul ASCII al producatorului
- semnatura procesorului
- nr serial al procesorului
- daca procesorul suporta caracteristicile:
FPU, MMX, APIC, x2APIC, PSN, DCA, IA64, HT, SS(S)E(2,3,4_1,4_2).



2. Consultand Materialul de laborator, identificati circuitul din figura alaturata precizand tipul circuitului si capacitatea in octeti (folositi si catalog online).

3. Consultand Materialul de laborator, specificati care este capacitatea (in octeti, bytes) unei memorii Flash CMOS de tip W29C512AP-90.



4. Identificati **registrul** si **bitul** ce furnizeaza informatii despre caracteristicile **PSN, MMX, SSE, SSE2, HT** prin intermediul instructiunii **cpuid**.

Ce valoare ar trebui sa aiba bitul respectiv pt a fi activata/prezenta caracteristica?

5. Executati aplicatia CPU-Z pe sistemul propriu si identificati caracteristicile acestuia.

6. Repetati cerinta de a punctul 5 pentru AIDA64.

7. Studiati fenomenul de **overclocking**: La ce se foloseste? Cand a aparut? De ce este posibil? De ce nu toate UCP pot fi imbunatatite cu acelasi factor ?

INTREBARI

1. Care este denumirea noului "tip" de BIOS aparut in anii 2000 ?

2. Ce reprezinta UEFI? R: un standard/ un tip de bus/ un periferic ?

3. Prin ce se deosebeste UEFI de BIOS-ul vechi? ... a se vedea fisierul cu intrebari QUIZ

(Quiz BIOS si Quiz CPUID)

Instrucțiunea CPUID

returnează și informații despre mărimea și caracteristicile memoriei cache interne:

când registrul **EAX** este **initializat cu 2**, instrucțiunea CPUID încarcă regiștrii EAX, EBX, ECX și EDX cu **descriptori** ce arată caracteristicile cache-ului procesorului.

Cei 8 biți “low” din registrul EAX (adica **registrul AL**) conțin o **valoare** care identifică **de câte ori trebuie executată instrucțiunea CPUID** pentru a obține o **imagine completă a cache-ului procesorului**.

Exemplu: pentru un procesor Pentium Pro

se obtine valoarea 1 în registrul AL al registrului EAX

=> instrucț CPUID trebuie executată o singură dată (cu EAX=2) pt a obține o imagine completă a cache-ului procesorului

Restul registrului EAX și regiștrii EBX, ECX și EDX conțin pe cate 8 biți **descriptori valizi** (daca **bitul 31=0**).

Memoria si interfata ei in PC

LAB Identificarea caracteristicilor memoriei cache prin instructiunea cpuid (2)

ANCA APATEAN - AC - UTCN

Restul registrului EAX și regiștrii EBX, ECX și EDX conțin pe cate 8 biți **descriptori valizi** (daca bitul 31=0).

Valoarea descriptor	Descriere cache	Valoarea descriptor	Descriere cache
00h	Nul	50h	TLB Instructiuni, pagini de 4Ko/2Mo/4Mo , total asoc, 64 intrari
01h	Instructiune TLB, pagini de 4k, asociativ 4 căi, 32 intrări	51h	TLB Instructiuni, pagini de 4Ko/2Mo/4Mo, total asoc, 128 intrari
02h	Instructiune TLB, pagini de 4M, full asociativ, 2 intrări	52h	TLB Instructiuni, pagini de 4Ko/2Mo/4Mo, total asoc, 256 intrari
03h	Date TLB, pagini de 4k, asociativ 4 căi, 64 intrări	5bh	TLB date, pagini de 4Ko/4MB, total asociativ, 64 intrari
04h	Date TLB, pagini de 4M, asociativ 4 căi, 8 intrări	5ch	TLB date, pagini de 4Ko/4MB, total asociativ, 128 intrari
06h	Cache Instructiuni, 8k, asociativ 4 căi, linii de lungime 32 octeți	5dh	TLB date, pagini de 4Ko/4MB, total asociativ, 256 intrari
08h	Cache Instructiuni, 16k, asociativ 4 căi, linii de lungime 32 octeți	66h	Cache date 8ko, sectorizat, asociativ pe 4 căi, linii de lungime 64o
0Ah	Cache date, 8k, ă asociativ pe 2 căi, linii de lungime 32 octeți	70h	Cache Trace de instructiuni 12ko uOps, asociativ pe 4 căi
0Ch	Cache date, 16k, ă asociativ pe 4 căi, linii de lungime 32 octeți	79h	Cache L2 128k, asociativ pe 8 căi, linii de lungime 64 octeți
40h	Nu are cache de nivel L2 (la familia P6) sau L3 (la P4)	7ah	Cache L2 256k, asociativ pe 8 căi, linii de lungime 64 octeți
41h	Cache unificat, linii de lungime 32 octeți, asociativ pe 4 căi, 128k	7bh	Cache L2 512k, asociativ pe 8 căi, linii de lungime 64 octeți
42h	Cache unificat, linii de lungime 32 octeți, asociativ pe 4 căi, 256k	7ch	Cache L2 1M, asociativ pe 8 căi, linii de lungime 64 octeți
43h	Cache unificat, linii de lungime 32 octeți, asociativ pe 4 căi, 512k	82h	Cache unificat, linii de lungime 32 octeți, asociativ pe 8 căi, 512k
44h	Cache unificat, linii de lungime 32 octeți, asociativ pe 4 căi, 1M	84h	Cache unificat, linii de lungime 32 octeți, asociativ pe 8 căi, 1M
45h	Cache unificat, linii de lungime 32 octeți, asociativ pe 4 căi, 2M	85h	Cache unificat, linii de lungime 32 octeți, asociativ pe 8 căi, 2M

Exemplu:

Pentru un procesor **Pentium 4**, dupa executia instructiunii cpuid se returneaza urmatoarele valori in regiștrii EAX, EBX, ECX, EDX:

EAX= **665B5001**h -> b31=0 => descriptori valizi , **AL=01** -> trebuie executata o sg data

EBX=00000000h

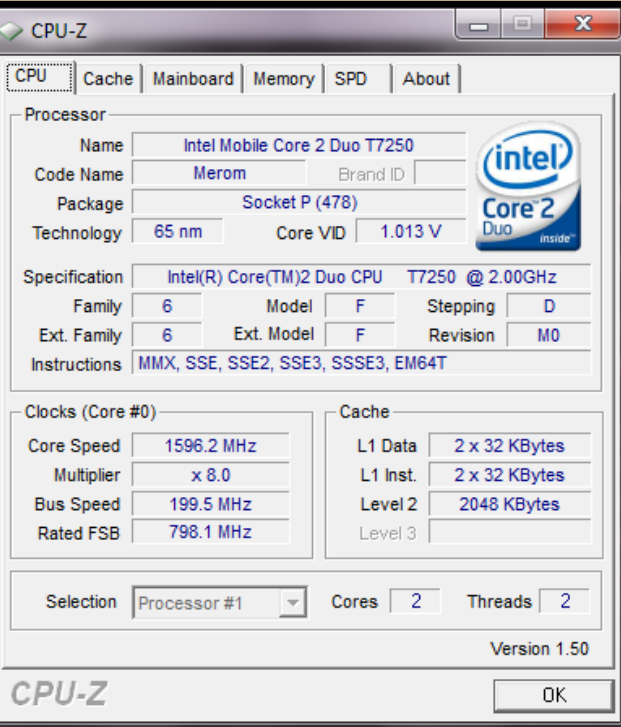
ECX=00000000h

EDX=00**7A70**40h

Memoria si interfata ei in PC

LAB Identificarea caracteristicilor *memoriei* cu ajutorul aplicatiei *CPU-Z*

ANCA APATEAN - AC - UTCN



CPU-Z Processor tab

Processor

Name: Intel Mobile Core 2 Duo T7250
Code Name: Merom
Package: Socket P (478)
Technology: 65 nm
Core VID: 1.013 V

Specification

Intel(R) Core(TM)2 Duo CPU T7250 @ 2.00GHz
Family: 6
Model: F
Stepping: D
Ext. Family: 6
Ext. Model: F
Revision: M0
Instructions: MMX, SSE, SSE2, SSE3, SSSE3, EM64T

Clocks (Core #0)

Core Speed: 1596.2 MHz
Multiplier: x 8.0
Bus Speed: 199.5 MHz
Rated FSB: 798.1 MHz

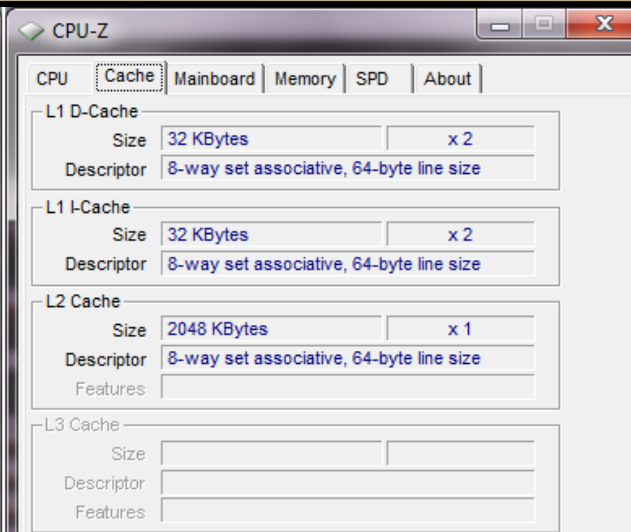
Cache

L1 Data: 2 x 32 KBytes
L1 Inst: 2 x 32 KBytes
Level 2: 2048 KBytes
Level 3:

Selection: Processor #1 | Cores: 2 | Threads: 2

Version 1.50

OK



CPU-Z Cache tab

L1 D-Cache

Size: 32 KBytes x 2
Descriptor: 8-way set associative, 64-byte line size

L1 I-Cache

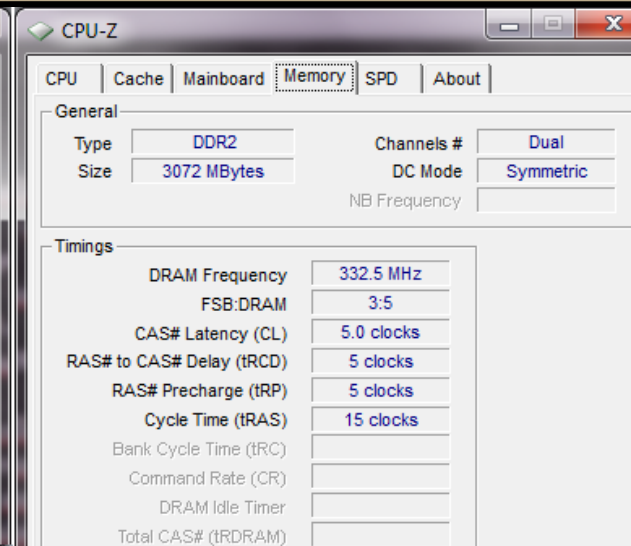
Size: 32 KBytes x 2
Descriptor: 8-way set associative, 64-byte line size

L2 Cache

Size: 2048 KBytes x 1
Descriptor: 8-way set associative, 64-byte line size

L3 Cache

Size:
Descriptor:
Features:



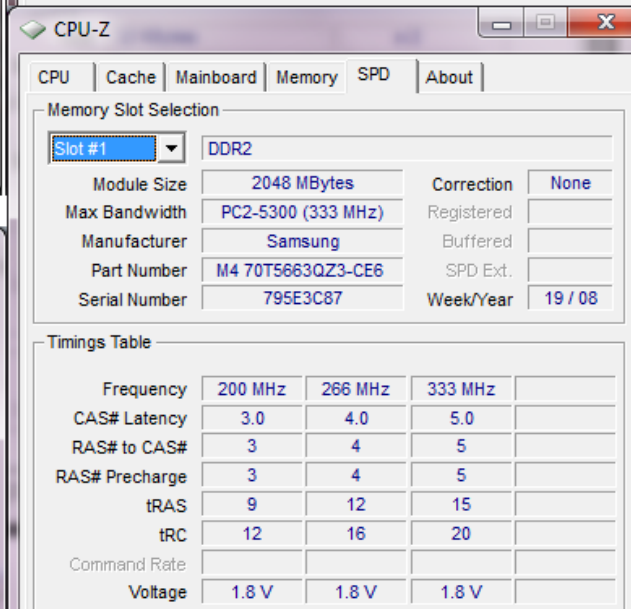
CPU-Z Memory tab

General

Type: DDR2
Size: 3072 MBytes
Channels #: Dual
DC Mode: Symmetric
NB Frequency:

Timings

DRAM Frequency: 332.5 MHz
FSB:DRAM: 3:5
CAS# Latency (CL): 5.0 clocks
RAS# to CAS# Delay (tRCD): 5 clocks
RAS# Precharge (tRP): 5 clocks
Cycle Time (tRAS): 15 clocks
Bank Cycle Time (tRC):
Command Rate (CR):
DRAM Idle Timer:
Total CAS# (tRDRAM):



CPU-Z Memory Slot Selection tab

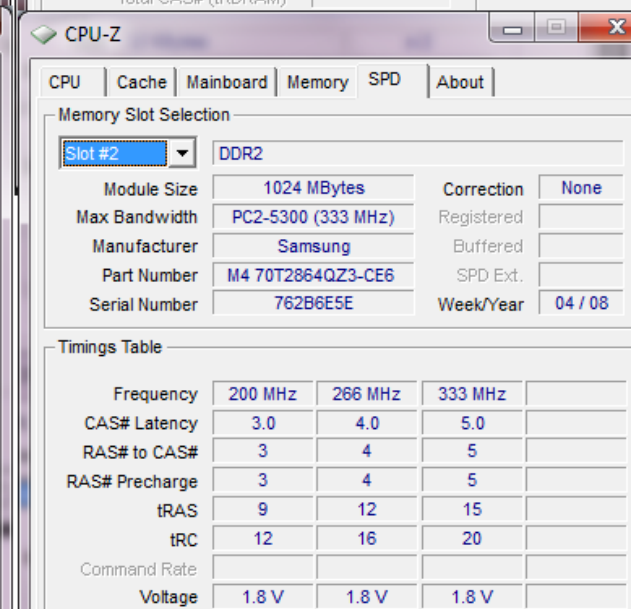
Slot #1: DDR2

Module Size: 2048 MBytes
Max Bandwidth: PC2-5300 (333 MHz)
Manufacturer: Samsung
Part Number: M4 70T5663QZ3-CE6
Serial Number: 795E3C87

Correction: None
Registered:
Buffered:
SPD Ext.:
Week/Year: 19 / 08

Timings Table

	200 MHz	266 MHz	333 MHz
Frequency	200 MHz	266 MHz	333 MHz
CAS# Latency	3.0	4.0	5.0
RAS# to CAS#	3	4	5
RAS# Precharge	3	4	5
tRAS	9	12	15
tRC	12	16	20
Command Rate			
Voltage	1.8 V	1.8 V	1.8 V



CPU-Z Memory Slot Selection tab

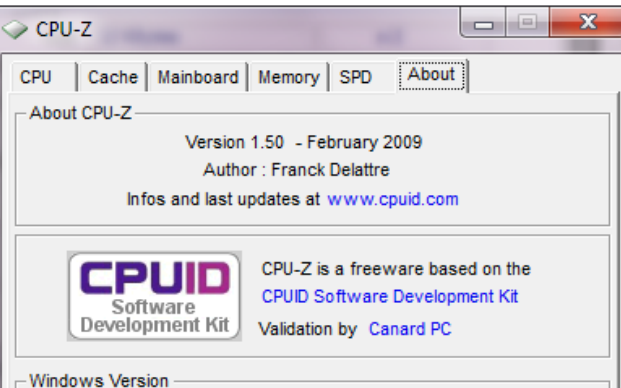
Slot #2: DDR2

Module Size: 1024 MBytes
Max Bandwidth: PC2-5300 (333 MHz)
Manufacturer: Samsung
Part Number: M4 70T2864QZ3-CE6
Serial Number: 762B6E5E

Correction: None
Registered:
Buffered:
SPD Ext.:
Week/Year: 04 / 08

Timings Table

	200 MHz	266 MHz	333 MHz
Frequency	200 MHz	266 MHz	333 MHz
CAS# Latency	3.0	4.0	5.0
RAS# to CAS#	3	4	5
RAS# Precharge	3	4	5
tRAS	9	12	15
tRC	12	16	20
Command Rate			
Voltage	1.8 V	1.8 V	1.8 V



CPU-Z About tab

About CPU-Z

Version 1.50 - February 2009
Author: Franck Delattre
Infos and last updates at www.cpubid.com

CPUID Software Development Kit

CPUI-Z is a freeware based on the CPUID Software Development Kit
Validation by Canard PC

Windows Version



[Barr2005] – Mostafa Abd-El-Barr, Hesham El-Rewini

– “Fundamentals of Computer Organization and Architecture”, 2005

[Baruch2000] - Zoltan Baruch

– “Arhitectura calculatoarelor”, Editura Todesco, 2000

[Brey1997] - Barry B. Brey

- “The Intel Microprocessors”, 4th edition, 1997

[Hennessy2009] - John Hennessy, David Patterson

– “Computer Architecture – A quantitative Approach”, 2009, 5th edition

[Hide2001] - Randall Hide

– “The Art of Assembly Language”, beta edition

[Lupu2012] – Eugen Lupu, Simina Emerich , Anca Apatean

– “Initiere in Limbaj de Asamblare x86. Lucrari practice, teste si probleme”, Ed. Galaxia Gutenberg, 2012

[Mueller2012] - Scott Mueller

– “Upgrading and Repairing PCs”, 20th edition, 2012

[Null2003] - Linda Null, Julia Lobur

– “The essentials of Computer Organization and Architecture”, 2003

[Patterson2009] – David Patterson, John Hennessy

– “Computer Organization and Design – the hardware/software interface”, 4th edition, 2009

[Tarnoff2007] - David Tarnoff

– “Computer Organization and Design Fundamentals”, editia intai revizuita, 2007