BIOS

m@ʁ€Ⱪ Þud3£k0

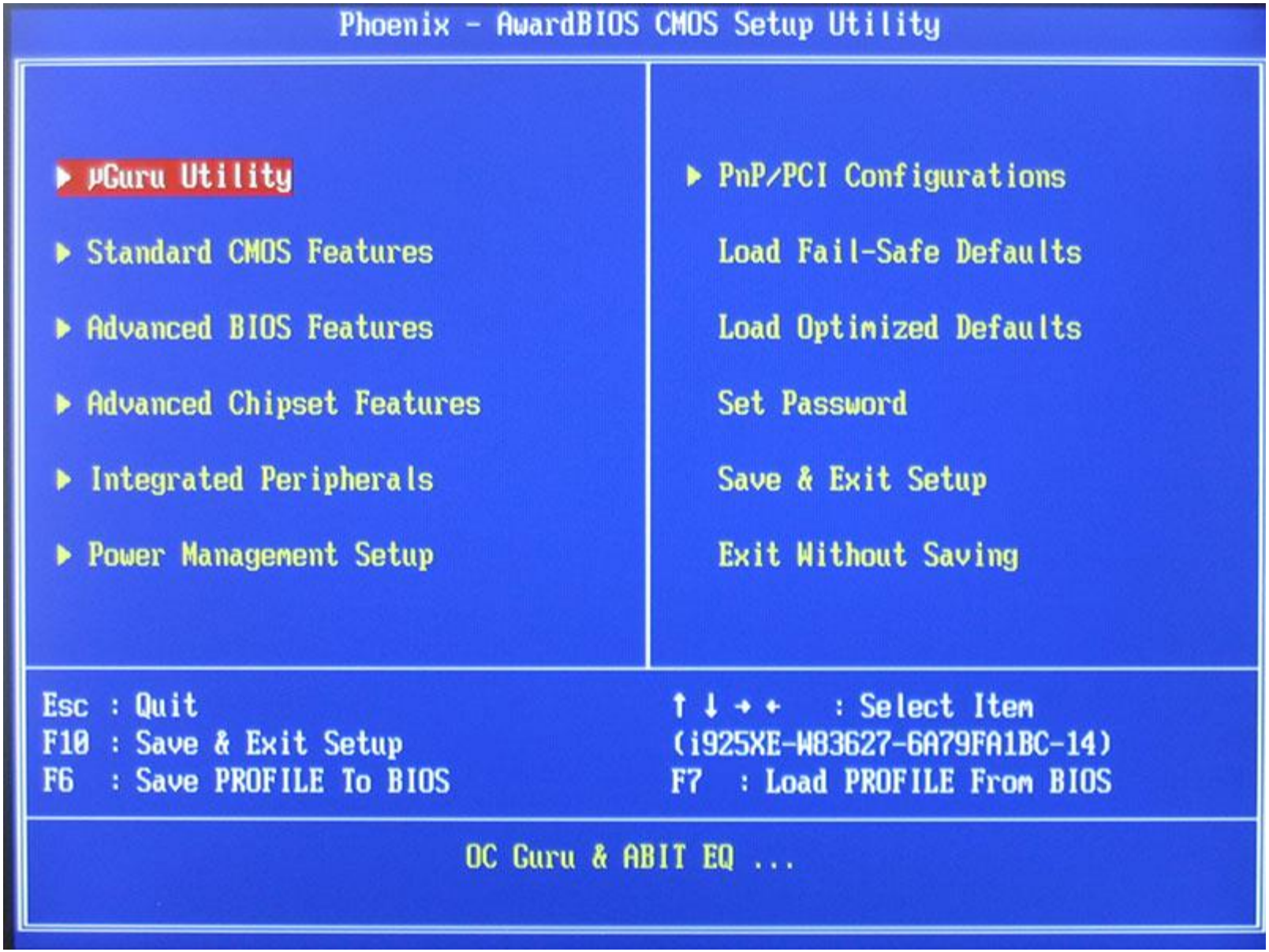
Urządzenia Techniki Komputerowej

Spis treści

BIOS

- **BIOS** (akronim ang. **Basic Input/Output System** - podstawowy system wejścia-wyjścia)
- Zapisany w pamięci stałej zestaw podstawowych procedur pośredniczących pomiędzy systemem operacyjnym a sprzętem.
  - Dla każdego typu płyty głównej komputera zestaw operacji jest inny.
- Program konfiguracyjny BIOS-u to BIOS-setup.
- Testuje sprzęt po włączeniu komputera, zajmuje się wstępną obsługą jego podzespołów.

- BIOS działa w środowisku 16-bitowym, w tzw. trybie rzeczywistym procesora.
- Jego możliwości są więc ograniczone z racji architektury
  - może użyć tylko 1 MB pamięci.
  - BIOS nie jest w stanie przygotować karty graficznej tak, by zwolnić system operacyjny od konieczności stosowania własnej autodetekcji.
  - Typowy BIOS zajmuje 4–8 MB.

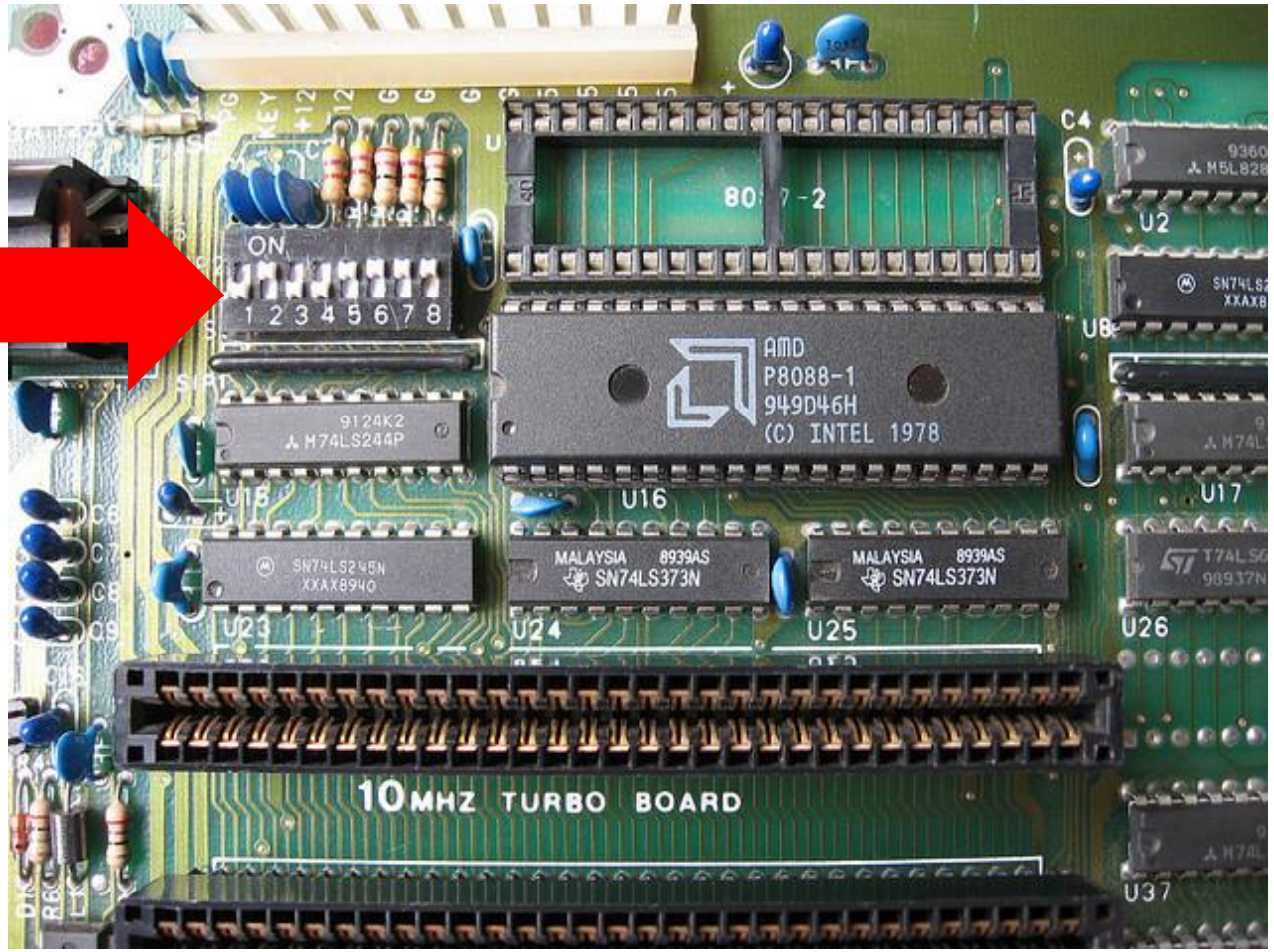

Phoenix - AwardBIOS CMOS Setup Utility
µGuru Utility
Standard CMOS Features
Advanced BIOS Features
Advanced Chipset Features
Integrated Peripherals
Power Management Setup
PnP/PCI Configurations
Load Fail-Safe Defaults
Load Optimized Defaults
Set Password
Save & Exit Setup
Exit Without Saving
Esc : Quit
F10 : Save & Exit Setup
F6 : Save PROFILE To BIOS
↑ ↓ → ← : Select Item
(i925XE-W83627-6A79FA1BC-14)
F7 : Load PROFILE From BIOS
OC Guru & ABIT EQ ...

AT BIOS


[F1 - HELP]
[Generic SETUP Version 3.0 2/88]
[80286]
Current SETUP Configuration
[0] Time
21:07:26_
[1] Date
08/20/2009
[2] Floppy Disk A:
DS/HD 1.2m 5¼""
[3] Floppy Disk B:
Not Installed
[4] Hard Disk 1 (C:)
Type 2
[5] Hard Disk 2 (D:)
Type 3
[6] Base Memory
640k
[7] Expansion Memory
2072k
[8] Math Coprocessor
Not installed
[9] Primary Display
Special (EGA)

Historia BIOSu cz.1

- Pierwsze PC nie miały BIOS-u
  - Wszystkie ustawienia realizowano za pomocą przełączników na płycie głównej.
  - Użytkownik ręcznie ustawiał konfigurację komputera.



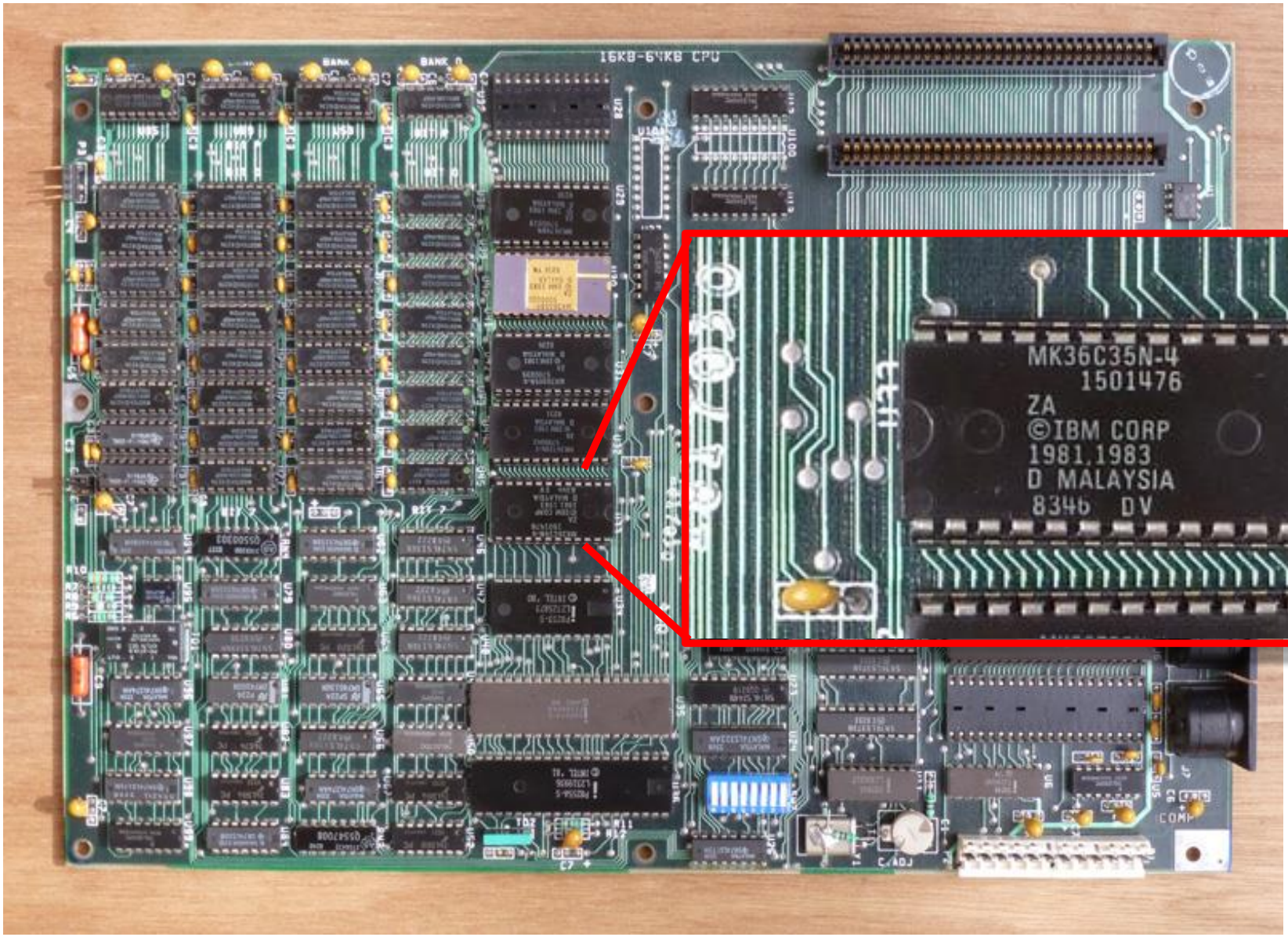
Historia BIOSu cz.2

- IBM podpisał z nieznaną firmą Microsoft umowę o dostarczenie systemu operacyjnego do komputera osobistego.
- Całość miała się składać z dwóch części:
  - Pierwsza część, system operacyjny, był dostępny na dysku (na początku na dyskietce). Ta część systemu operacyjnego została nazwana **Disk Operating System – *DOS***. *Część Microsoftu*.
  - Druga z nich (**Basic Input/Output System** – ***BIOS***) została dodana do sprzętu komputerowego w postaci pamięci tylko do odczytu (Read-Only-Memory – ROM). *Część IBM.*

Historia BIOSu cz.3

- IBM wprowadził model otwarty architektury komputerowej.
- Licencje na BIOS miał tylko IBM.
  - Nie pozwalał ani kopiować, ani używać przez innych producentów płyt głównych
  - Wytaczał procesy sądowe innym firmom

IBM 5150 – płyta z BIOSem



Historia BIOSu cz.4

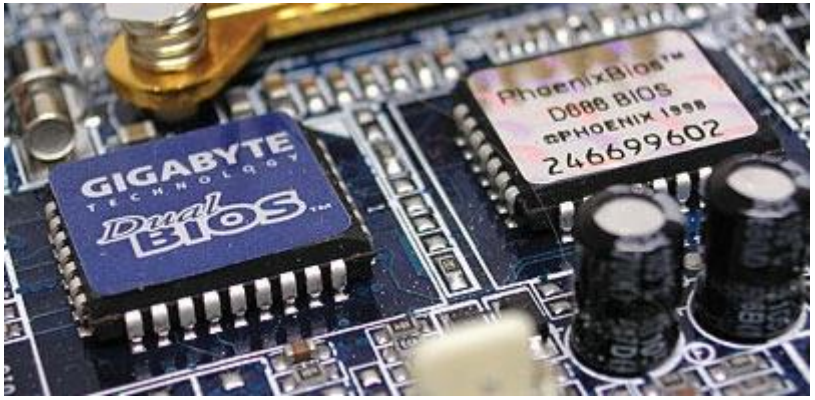
- Firmy postanowiły stworzyć własne BIOS-y.
- Użyto inżynierii wstecznej (metody czystego pokoju).
  - Udało się opracować BIOS-y zgodne z oryginalnym.

- 1983 - Texas Instruments
  - Jego pracownicy założyli później firmę Phoenix (1984)
- 1985 AMI (*American Megatrends Incorporated*)
- 1986 Award

- 1998 połączenie Phoenix i Award

BIOS

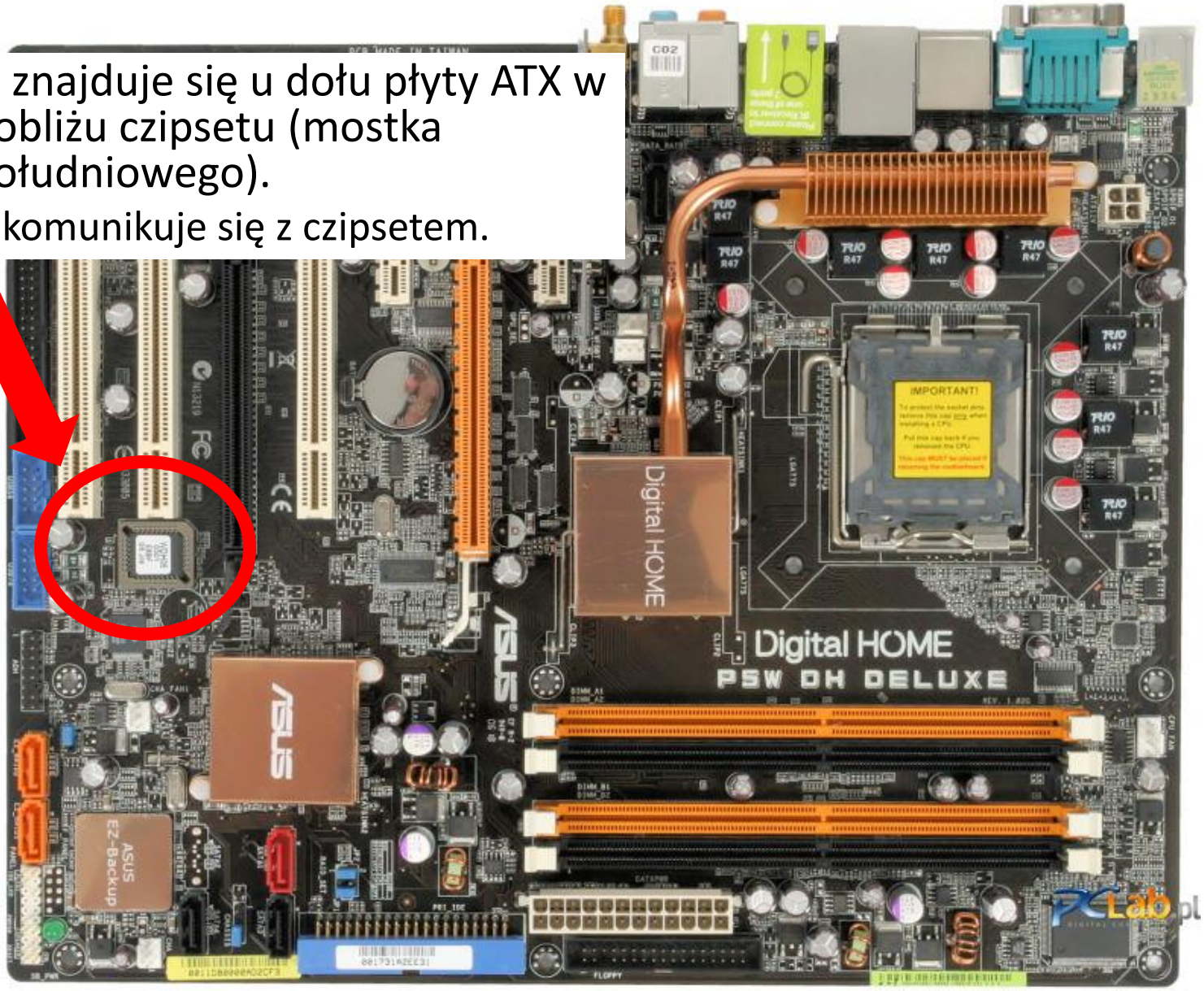
Nowoczesne układy BIOS



Położenie

BIOS znajduje się u dołu płyty ATX w pobliżu czipsetu (mostka południowego).

BIOS komunikuje się z czipsetem.



Występowanie BIOS-u

- Podzespoły komputerowe
  - Płyty główne
  - Kontroler SCSI
  - Karta graficzna
  - Karta sieciowa
- Inne urządzenia
  - konsole do gier (np. przenośna konsola Sony PSP, czy PlayStation 3)
  - odtwarzacze CD i DVD
  - telefony komórkowe
  - odtwarzacze mp3
  - tablety

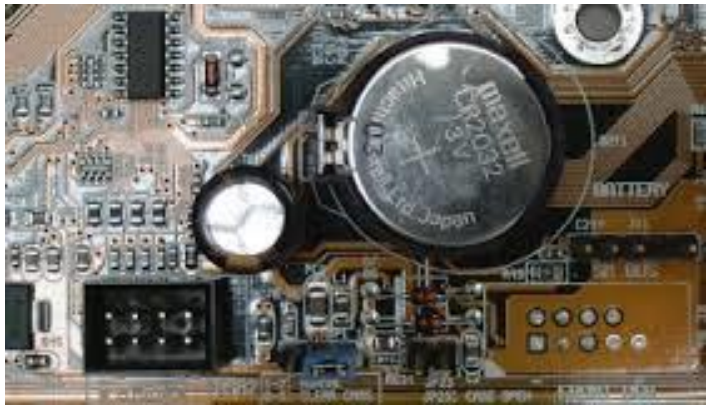
Zadania BIOS-u

1. Sprawdza czy wszystkie komponenty komputera działają prawidłowo. Testuje je przy każdym włączeniu komputera (Power-On-Self-Test – POST).
2. Po starcie systemu BIOS przejmuje kontrolę nad operacjami fundamentalnymi. Konfiguruje pamięć RAM, zasoby komputera i okresowo uruchamia funkcje porządkujące.
3. BIOS rezerwuje mały blok pamięci RAM nazywany ***BIOS Data Area***, gdzie przechowuje informacje o konfiguracji komputera, do których mogą odnosić się inne programy.
4. BIOS pozwala łączyć się programom (w tym systemowi operacyjnemu) ze sprzętem komputerowym.

Pamięć CMOS

- BIOS znajduje się w pamięci ROM
  - Zazwyczaj to pamięć EEPROM (electrically-erasable read-only memory) umożliwiająca ponowne nagrywanie zawartości BIOSu (flash BIOS).
- Ustawienia BIOS-u są zapisywane w pamięci, która nie może być wyczyszczona przy ponownym uruchomieniu komputera.
- Pamięć typu CMOS (Complementary Metal Oxide Semiconductor).
  - Często na pamięć BIOS-u mówi się "CMOS", ale pamięć typu CMOS jest używana również w innych częściach komputera. Kiedyś jedynym miejscem, w którym występowała, był BIOS - stąd brak nazwy własnej jego pamięci.
- W pamięci BIOS-u zachowywane są informacje o dacie systemowej, konfiguracji dysków oraz wszystkich innych ustawieniach, do których mamy dostęp przez program konfiguracyjny BIOS-u.
- Pamięć jest podtrzymywana przez baterię, ale ma bardzo małą pojemność – zazwyczaj jedynie 64 bajtów.

Ustawienia CMOS

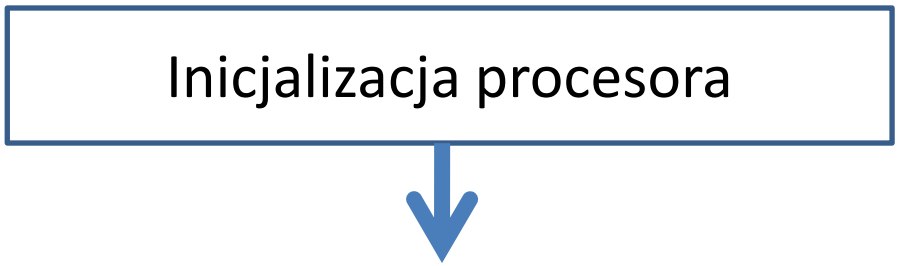


- Bateria

- Resetowanie ustawień BIOS-u

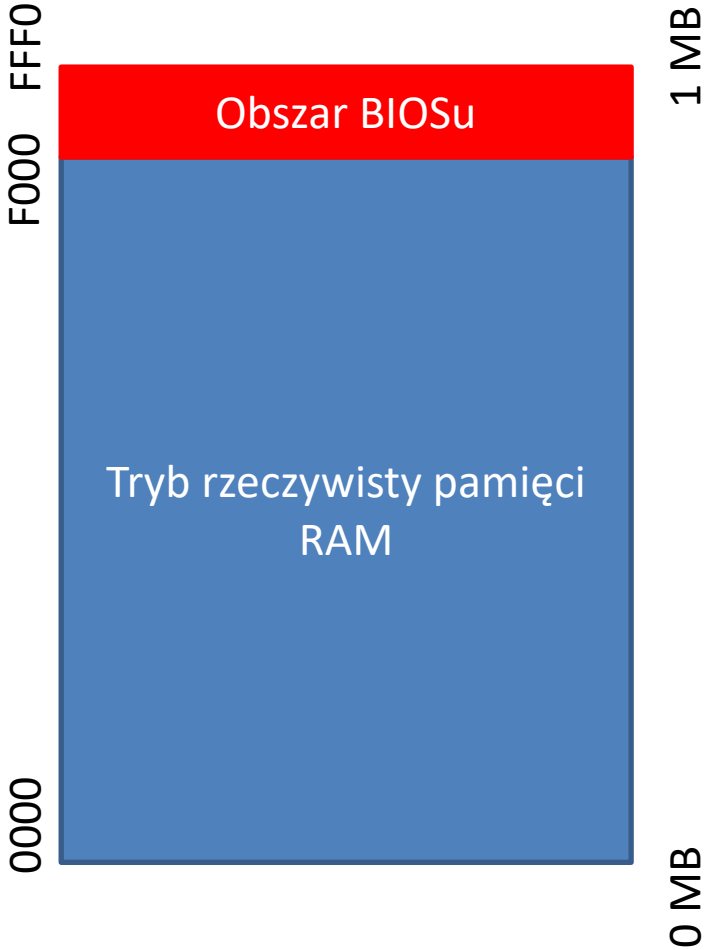
URUCHAMIANIE SYSTEMU

Start komputera



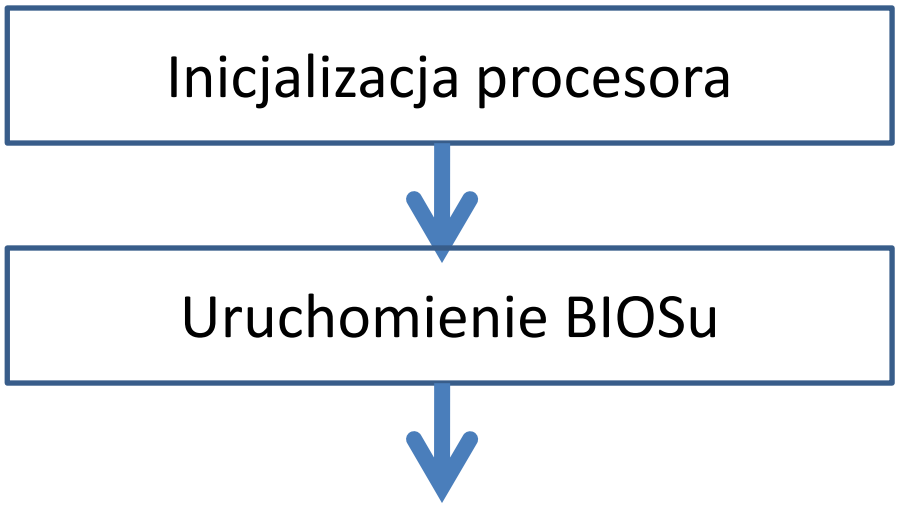
- Procesor inicjalizuje się samodzielnie. Rejestry CS i IP świeżo uruchomionego procesora zawierają wartości F000 i FFF0. Zaczyna przetwarzać kod zawarty między tymi adresami pamięci (F000h:FFF0h) - obszar zarezerwowany dla BIOSu.

F000:FFF0



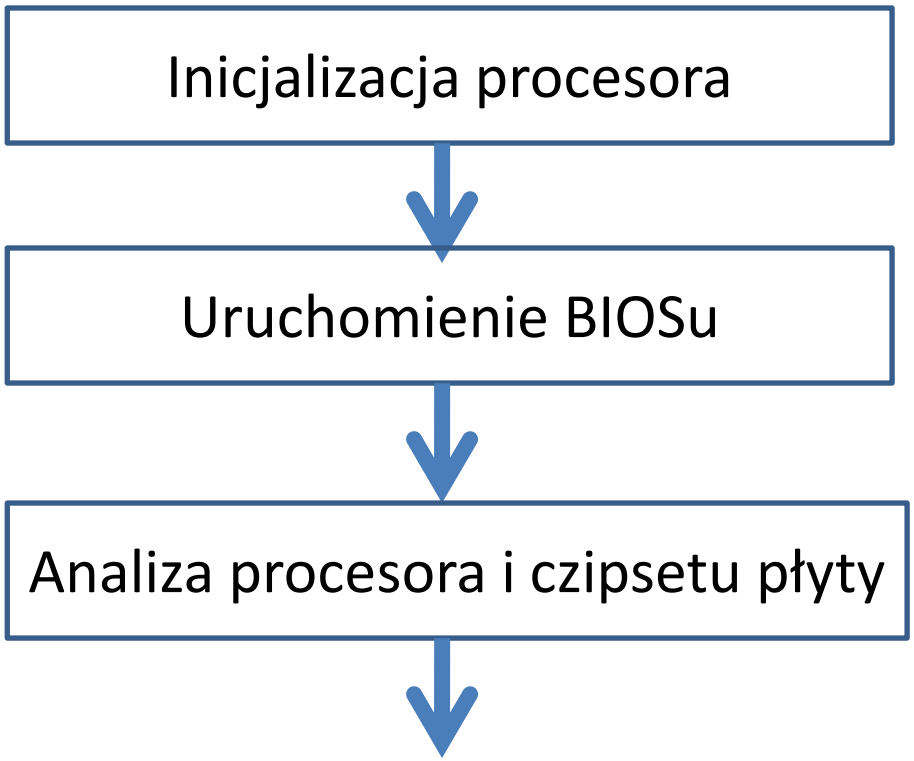
- Procesor jako pierwszą wykonuje instrukcję spod adresu F000:FFF0, czyli szesnaście bajtów przed górnym krańcem pamięci w trybie rzeczywistym (jest to jeden megabajt).
- Aby zachować kompatybilność wstecz, wszystkie procesory Intela uruchamiają się w trybie 16-bitowym.
- BIOS nie przełącza procesora w tryb 32-bitowy.
  - W fazie POST tryb ten może być testowany
- Przełączenie na stałe realizuje dopiero system operacyjny.

Uruchomienie BIOSu



- W obszarze pamięci zawartym w przedziale F000h:FFF0h znajduje się procedura uruchomienia BIOSu.
- Pierwsze zadanie BIOSu polega na wykryciu podłączonego sprzętu i przygotowaniu go do uruchamienia systemu.
- **Procedury diagnostyczne to Post (*Power On Self Test*).**
- Jeżeli komputer był po zwykłym restarcie bez odłączenia zasilania, pod adresem 0000:0472 znajduje się wartość 0x1234 i BIOS pomija niektóre testy.

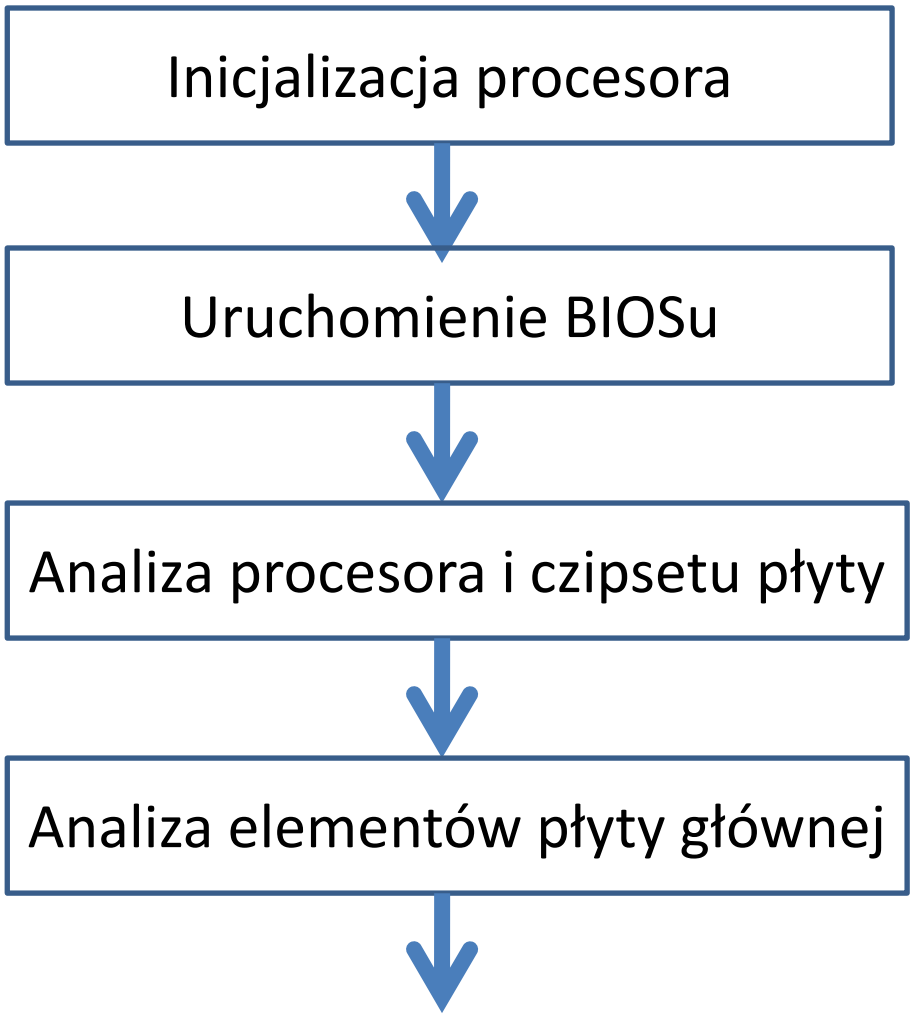
Procedury diagnostyczne POST



- Pierwszym krokiem jest analiza procesora.
- Następnie BIOS, przechodzi do inicjowania chipsetu płyty głównej.
- W pierwszej kolejności zostaje przygotowany kontroler pamięci, bo umożliwia rozpakowanie BIOS-u do pamięci roboczej peceta.
  - Przeważająca część kodu BIOS-u jest skompresowana, aby zajmowała mniej miejsca w pamięci.

Power-On-Self-Test

Testowanie elementów płyty głównej

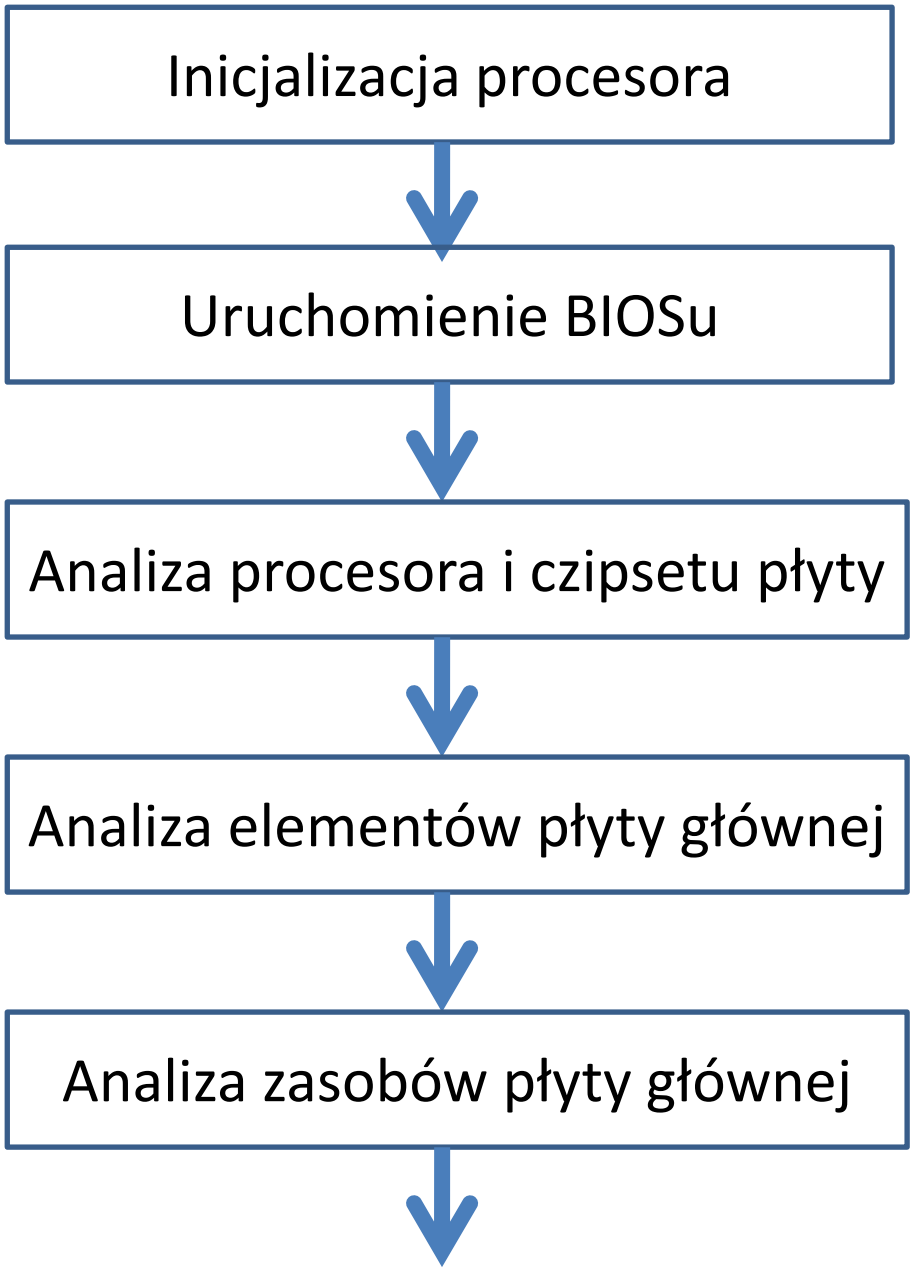


- Następnie BIOS testuje i inicjuje pozostałe podzespoły płyty głównej.
- Jednocześnie konfiguruje ich podstawowe ustawienia, które w większości przypadków są zgromadzone w rejestrach danych elementów.
  - Wartość pola ***CAS Latency Time*** zostaje pobrana przez procedurę Post i zapisana w rejestrze kontrolera pamięci.
  - Inne parametry konfiguracyjne określają właściwości samego BIOS-u. Na przykład ***kolejność sprawdzania napędów w poszukiwaniu systemu operacyjnego***.
- W trakcie testu można przejść do trybu konfiguracji BIOSu.

Sprawdzane elementy

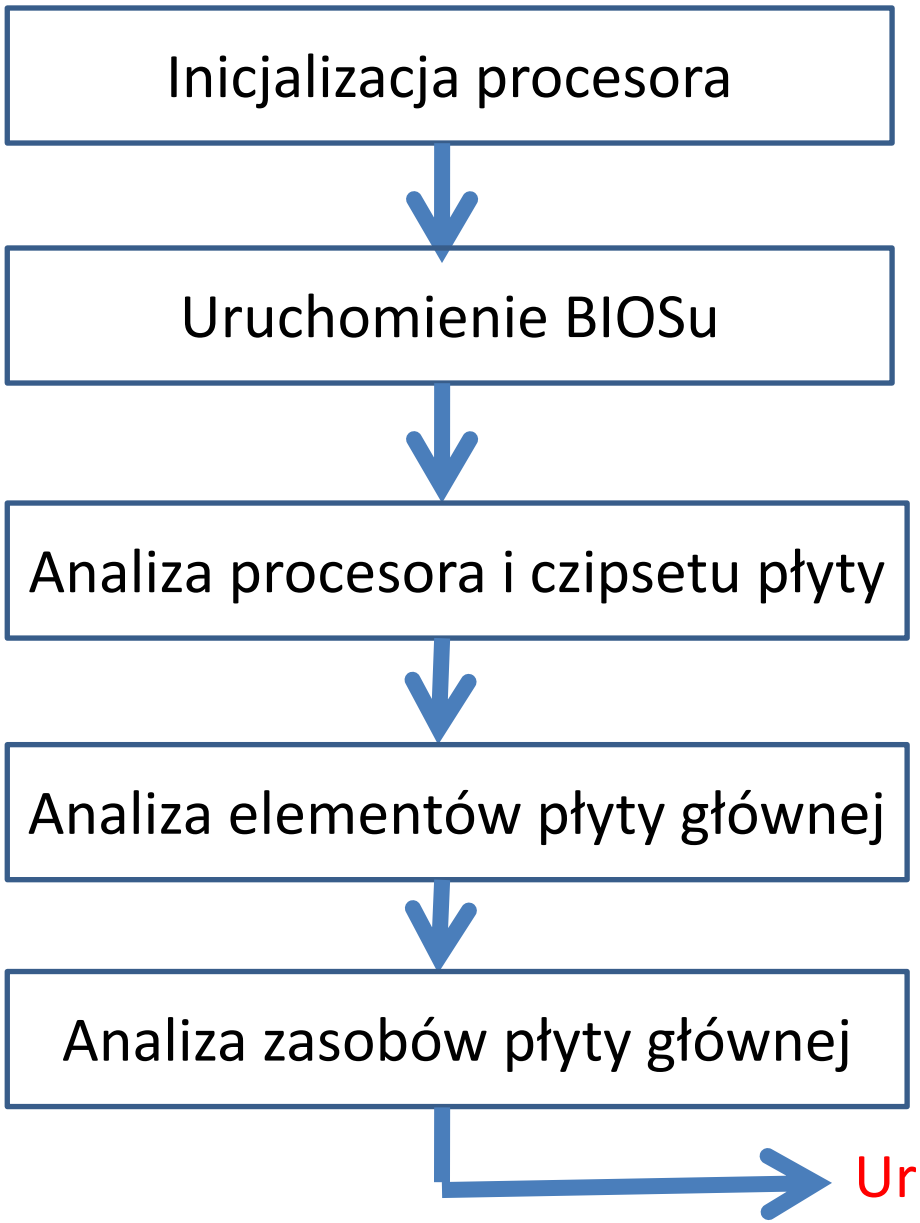
1. test rejestrów procesora
2. sprawdzenie sumy kontrolnej BIOSu
3. test sterownika klawiatury
4. test zegara systemowego
5. sprawdzenie dostępu do bazowych 64 kB pamięci
6. test pamięci cache
7. test sprawności baterii systemowej
8. test karty graficznej
9. test trybu chronionego
10. próba odczytu i zapisu do pamięci konwencjonalnej
11. test pamięci rozszerzonej
12. test sterownika DMA
13. sprawdzenie konfiguracji systemu

Wykrycie zasobów komputera



- Na końcu procedura Post wykrywa dostępne zasoby (pamięć, przerwania, porty We/Wy itd.).
- Później zostaną podzielone na urządzenia ***Plug & Play***.
- Jeżeli uruchamiany system operacyjny obsługujący Plug&Play, BIOS przydziela zasoby tylko tym podzespołom, które biorą udział w uruchamianiu systemu (np. kontrolerowi EIDE czy karcie sieciowej, lecz nie karcie dźwiękowej).

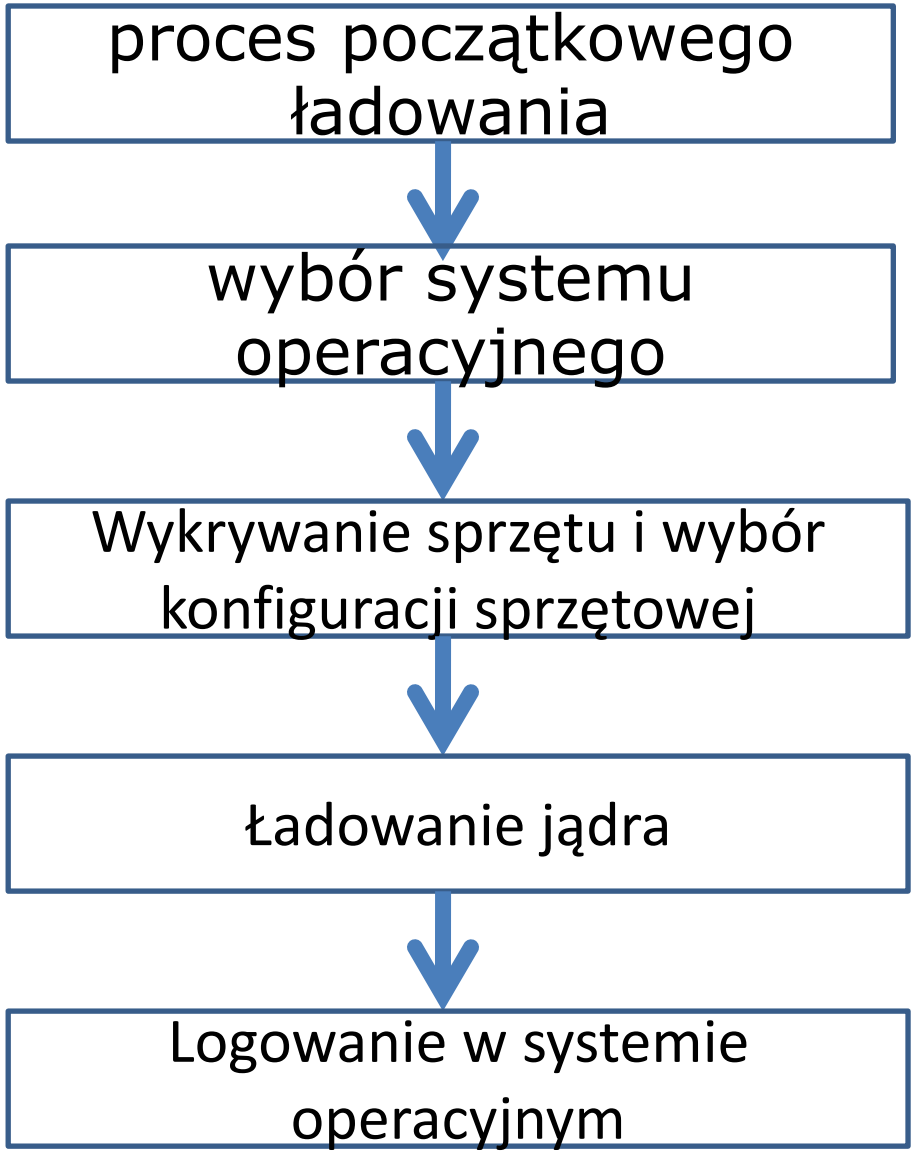
Uruchomienie systemu operacyjnego



- Po zakończeniu testowania, BIOS wywołuje przerwanie 0x19.
  - Próbuje załadować pierwszy sektor sektora MBR (Master Boot Record) z zerowej ścieżki urządzenia uruchamiającego, do pamięci.
  - W razie powodzenia operacji umieszcza go pod adresem 0000:7C00. Następnie BIOS skacze pod ten adres.
- Jeżeli ładowanie systemu nie powiedzie się z powodu braku sektora startowego, wywoływane jest przerwanie 0x18.
  - Wyświetlany jest tekst: "NO BOOT DEVICE AVAILABLE".

Start systemu operacyjnego

- Z MBR (lub GPT) jest wybierany system operacyjny (gdy jest ich więcej)
- BIOS przekazuje pałeczkę systemowi operacyjnemu.
  - W Windows rodziny NT sterowanie uruchamianiem przejmuje NTLdr (NT Loader).
  - W Linuksie jest to Grub lub Lilo.
  - Najpierw wykonuje program NTDETECT.COM, który dokonuje analizy komputera.
  - Jednocześnie pobiera informacje z BIOS-u i zapisuje je w Rejestrze (klucz "HKEY_LOCAL_MACHINE\Hardware\Description").

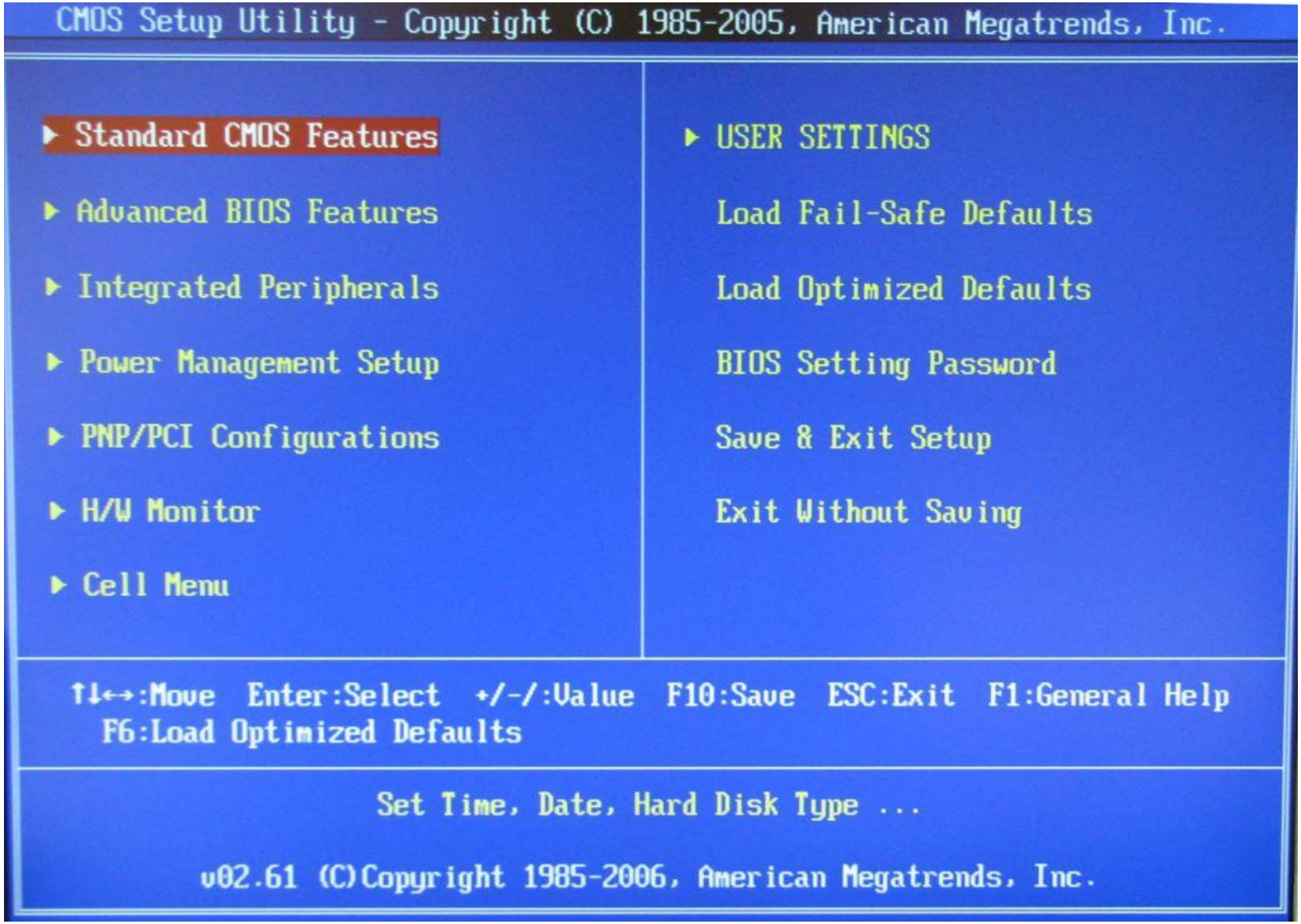


Shadowing

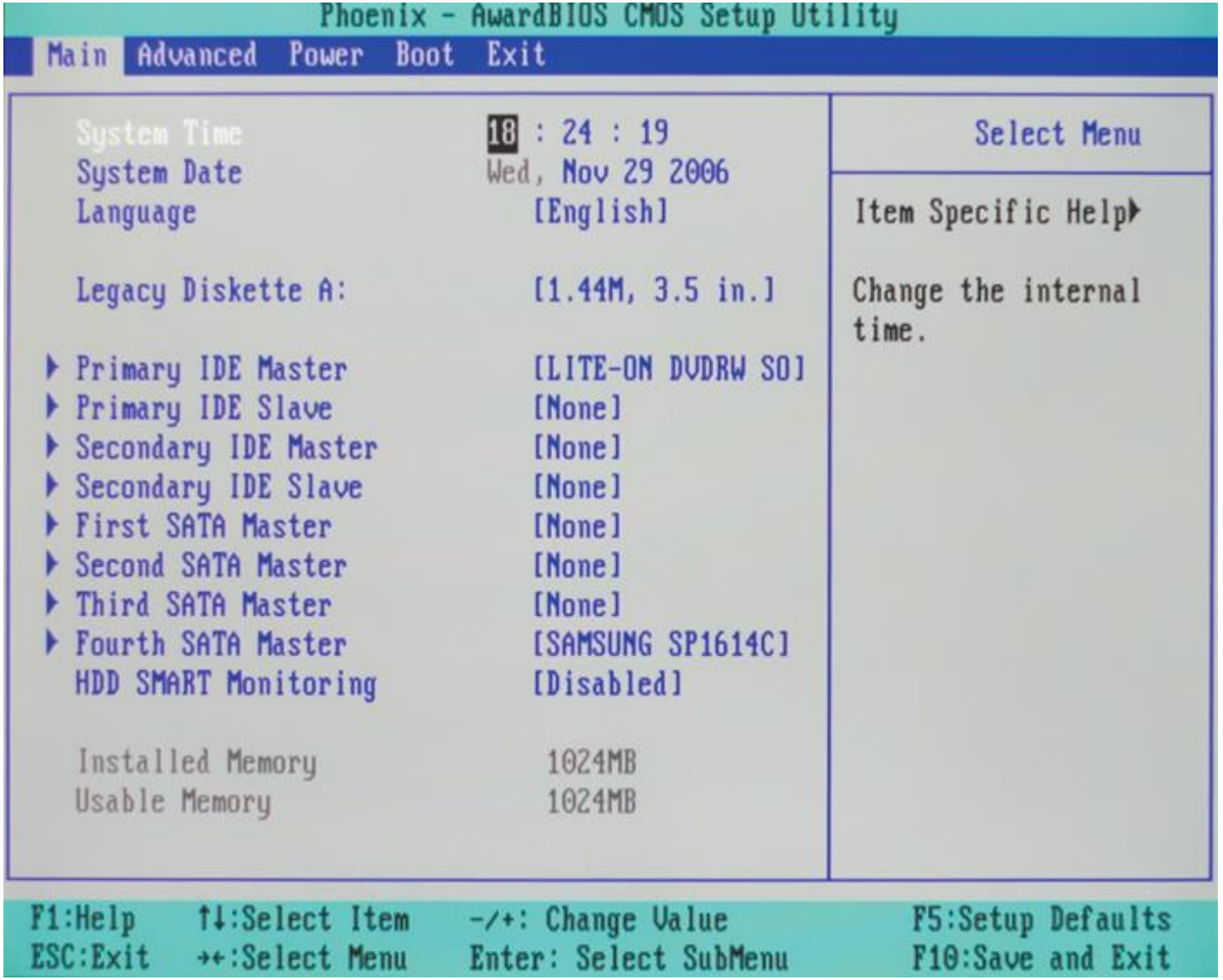
- Dostęp do pamięci RAM jest szybszy niż do ROM
  - Dostęp do pamięci ROM odbywa się w blokach ośmiobitowych, do pamięci RAM w blokach trzydziestodwubitowych.
  - Poza tym czas dostępu do pamięci ROM jest większy - od 150 do 200 nanosekund, dla pamięci RAM - od 60 do 70 nanosekund.
- Z tego powodu często spotykaną techniką jest kopiowanie kodu BIOSu do pamięci RAM podczas startu komputera - tak zwany *shadowing*.
  - Dostęp do pamięci ROM BIOS odbywa się poprzez adresy F000-FFFF. Ten sam zakres adresów istnieje także w pamięci RAM.
- Jeżeli *shadowing* jest aktywny, zawartość pamięci ROM BIOS jest kopiowana do pamięci RAM pod ten zakres adresów po uruchomieniu komputera.
- Istnieje ponadto opcja umieszczania w pamięci RAM BIOSu karty graficznej.
  - BIOS karty graficznej jest umieszczony na kościach ROM wbudowanych w kartę (w przypadku płyt głównych z wbudowaną kartą graficzną BIOS karty graficznej jest umieszczony razem z BIOSem płyty). Dostęp do BIOSu karty graficznej odbywa się zwykle przez adresy C000-C7FF.
- Niektóre BIOSy umożliwiają także umieszczanie w pamięci RAM BIOSów innych urządzeń, na przykład karty sieciowej.

PRODUCENCI

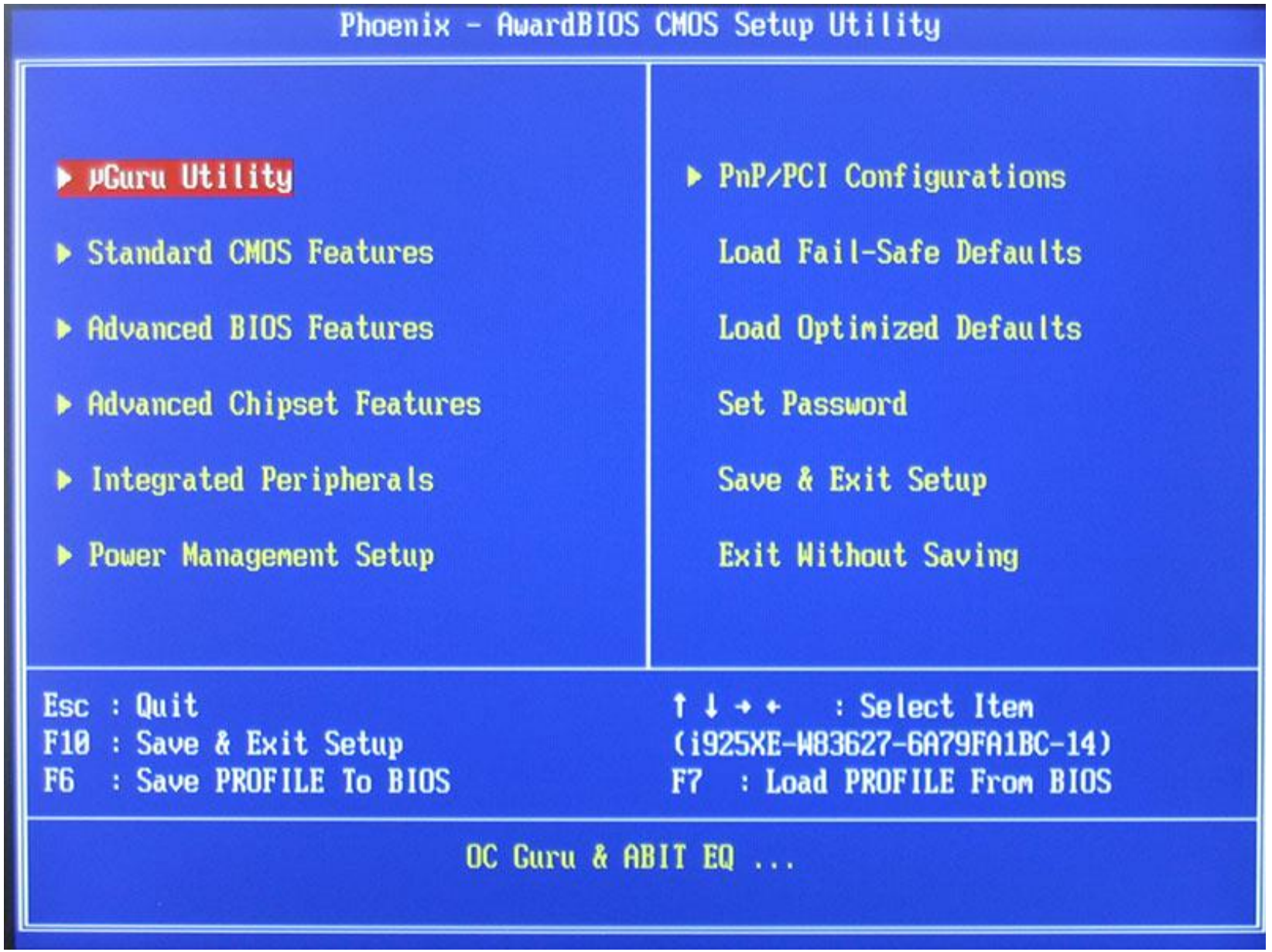
AMI BIOS


CMOS Setup Utility - Copyright (C) 1985-2005, American Megatrends, Inc.
Standard CMOS Features
Advanced BIOS Features
Integrated Peripherals
Power Management Setup
PNP/PCI Configurations
H/W Monitor
Cell Menu
USER SETTINGS
Load Fail-Safe Defaults
Load Optimized Defaults
BIOS Setting Password
Save & Exit Setup
Exit Without Saving
↑↓↔:Move Enter:Select +/-/:Value F10:Save ESC:Exit F1:General Help
F6:Load Optimized Defaults
Set Time, Date, Hard Disk Type ...
v02.61 (C)Copyright 1985-2006, American Megatrends, Inc.

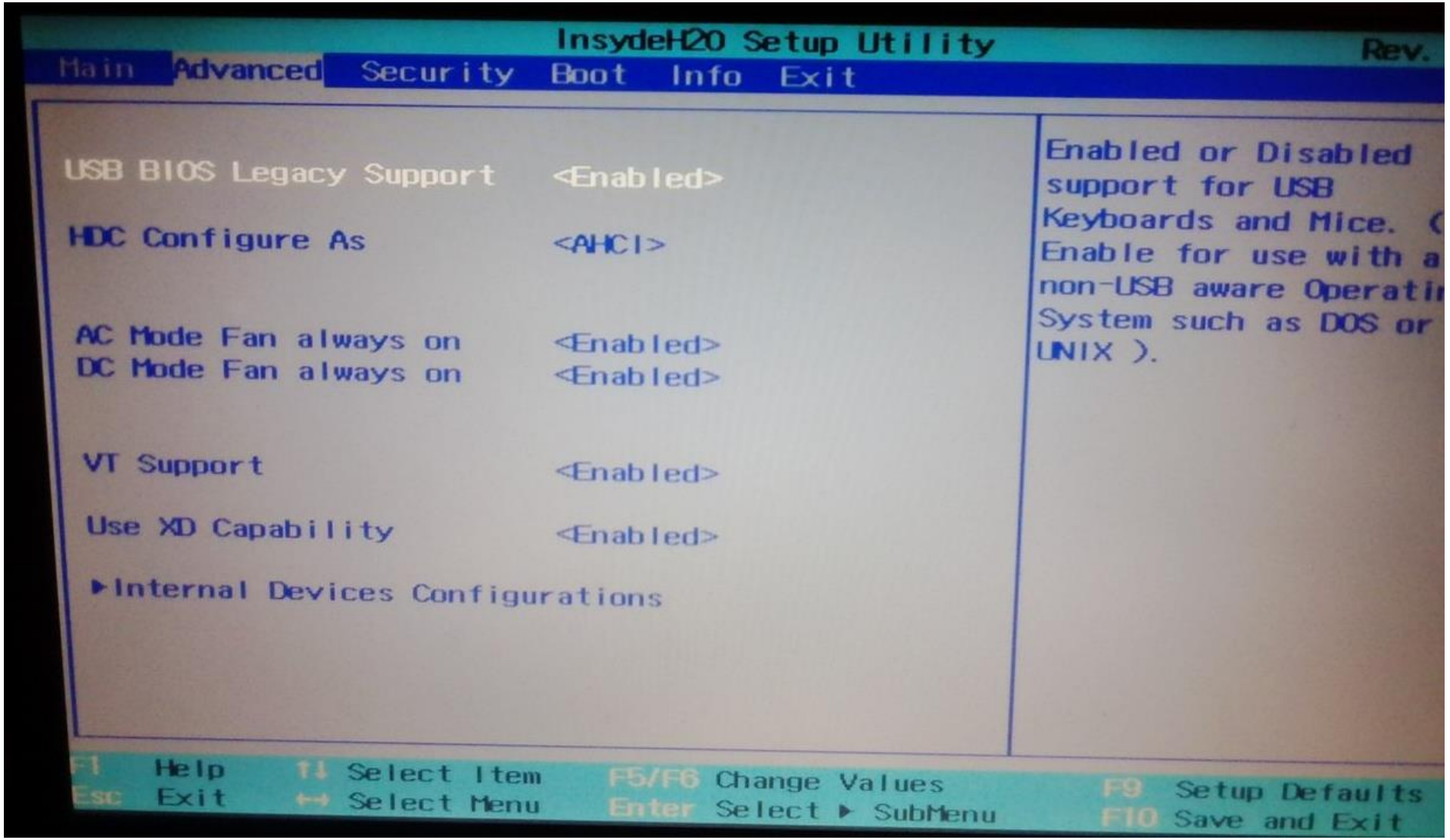
Phoenix BIOS



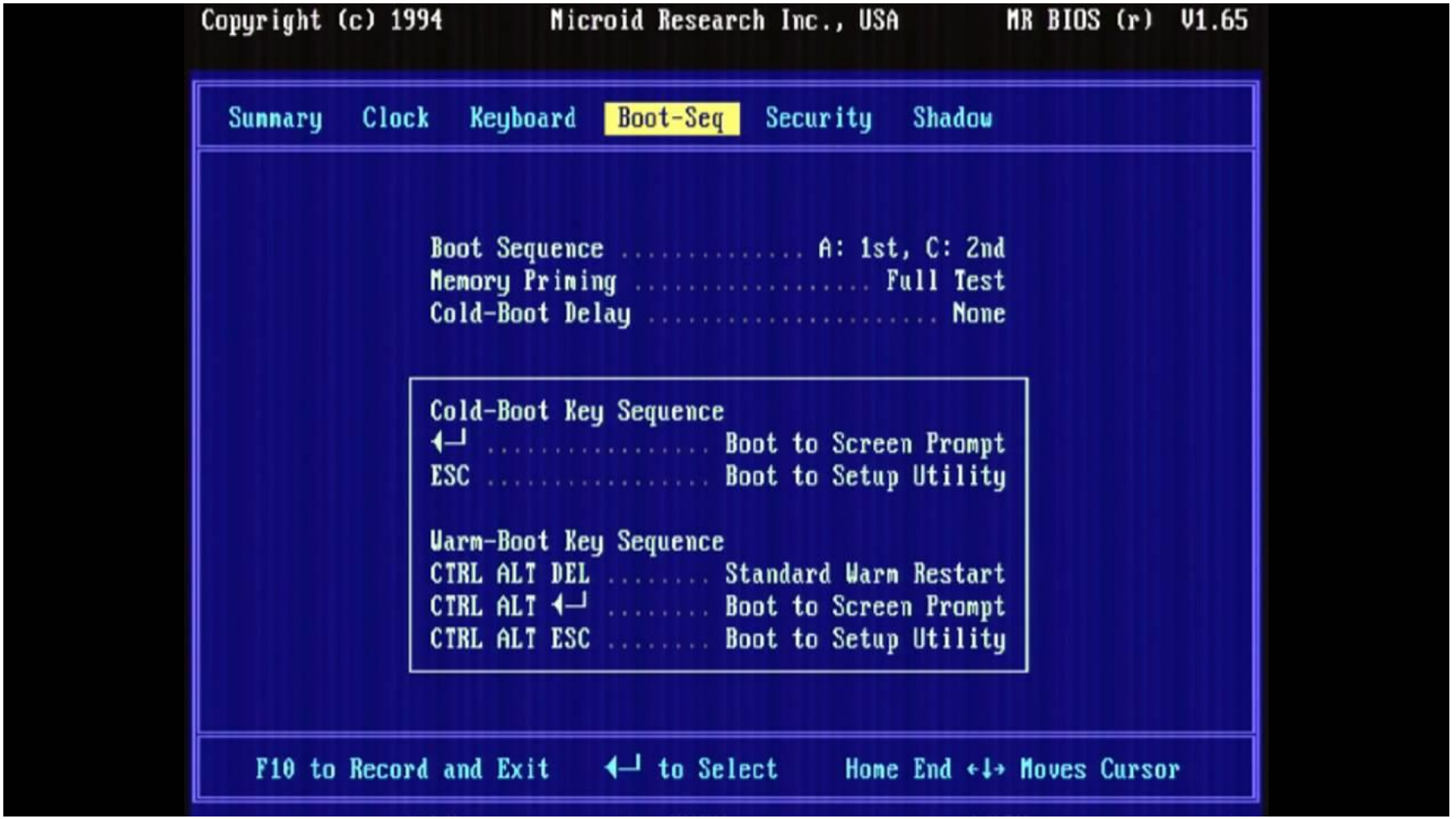
Award BIOS


Phoenix - AwardBIOS CMOS Setup Utility
µGuru Utility
Standard CMOS Features
Advanced BIOS Features
Advanced Chipset Features
Integrated Peripherals
Power Management Setup
PnP/PCI Configurations
Load Fail-Safe Defaults
Load Optimized Defaults
Set Password
Save & Exit Setup
Exit Without Saving
Esc : Quit
F10 : Save & Exit Setup
F6 : Save PROFILE To BIOS
↑ ↓ → ← : Select Item
(i925XE-W83627-6A79FA1BC-14)
F7 : Load PROFILE From BIOS
OC Guru & ABIT EQ ...

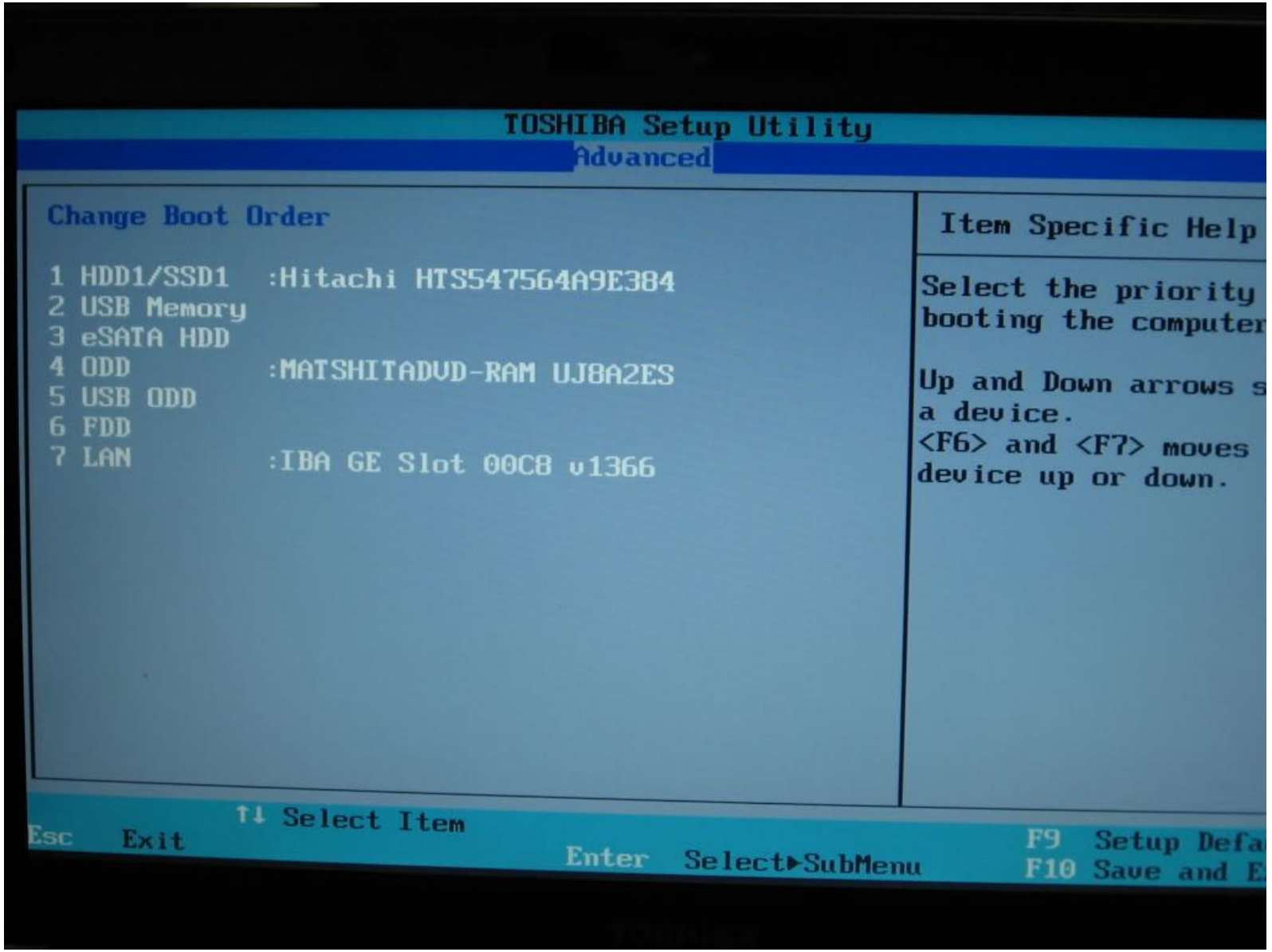
Insyde BIOS


InsydeH20 Setup Utility
Rev.
Main Advanced Security Boot Info Exit
USB BIOS Legacy Support <Enabled>
HDC Configure As <AHCI>
AC Mode Fan always on <Enabled>
DC Mode Fan always on <Enabled>
VT Support <Enabled>
Use XD Capability <Enabled>
▶Internal Devices Configurations
Enabled or Disabled support for USB Keyboards and Mice. (Enable for use with a non-USB aware Operati System such as DOS or UNIX).
F1 Help ↑↓ Select Item F5/F6 Change Values F9 Setup Defaults
Esc Exit ↔ Select Menu Enter Select ▶ SubMenu F10 Save and Exit

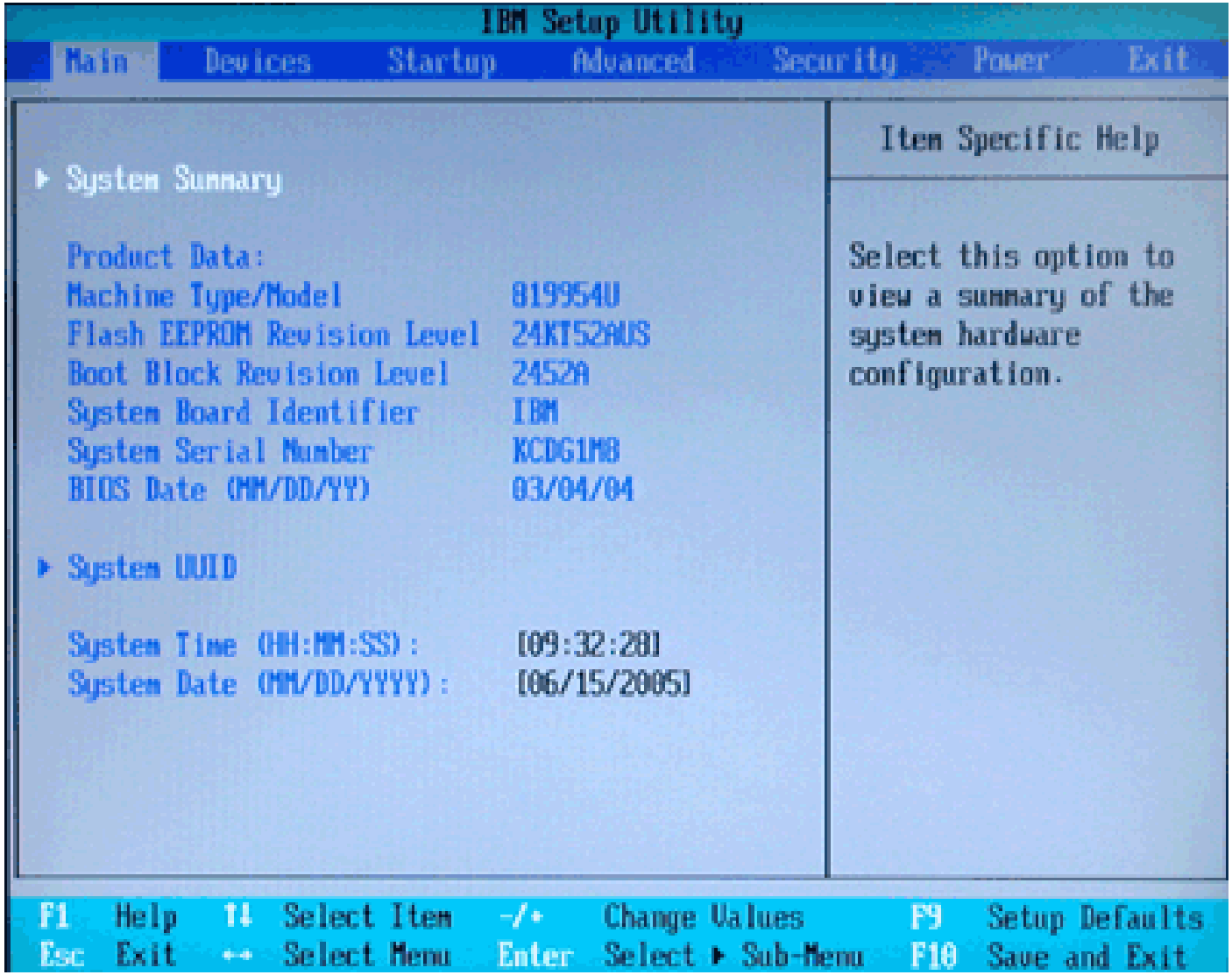
MicroID Research (MRBIOS)



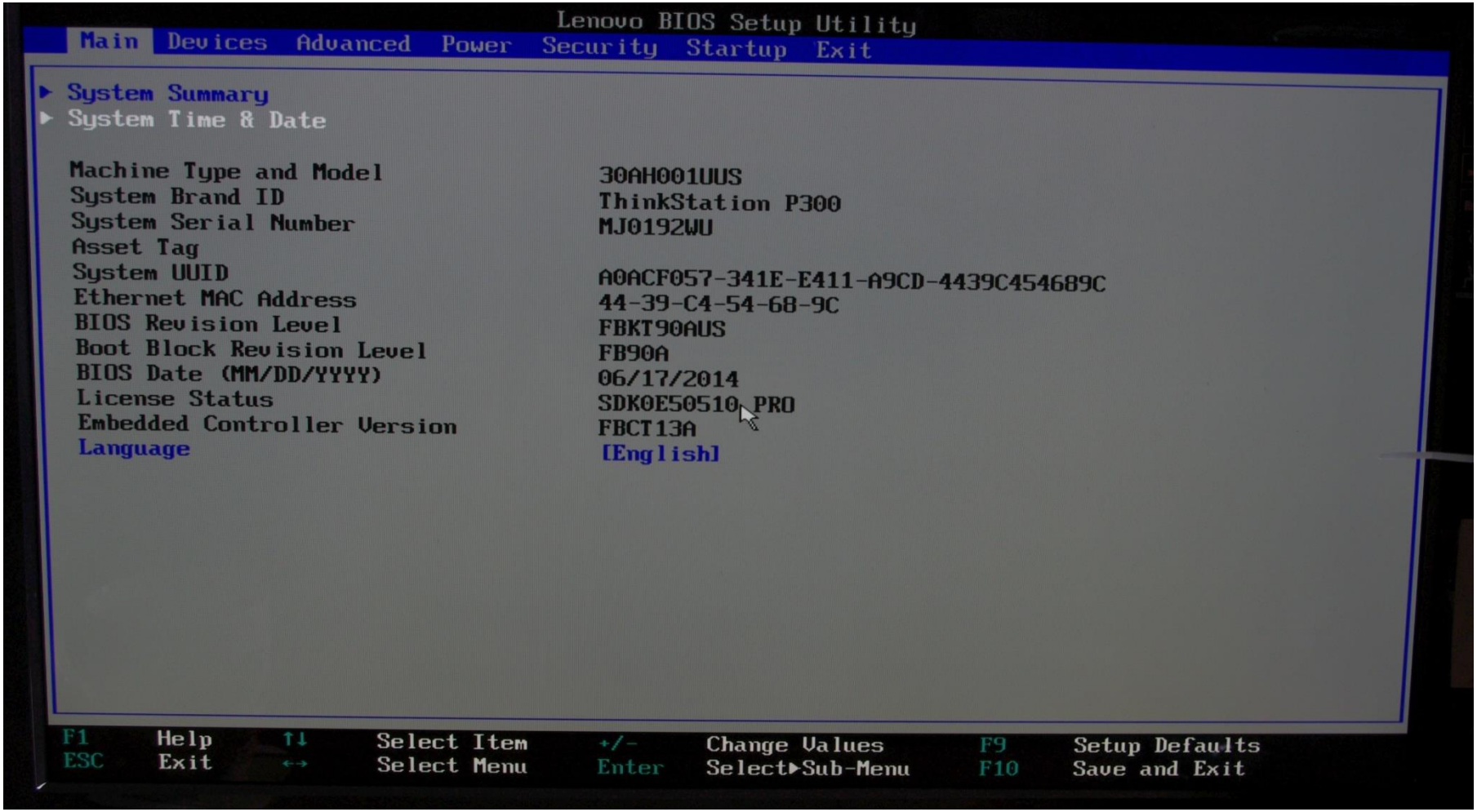
Toshiba BIOS



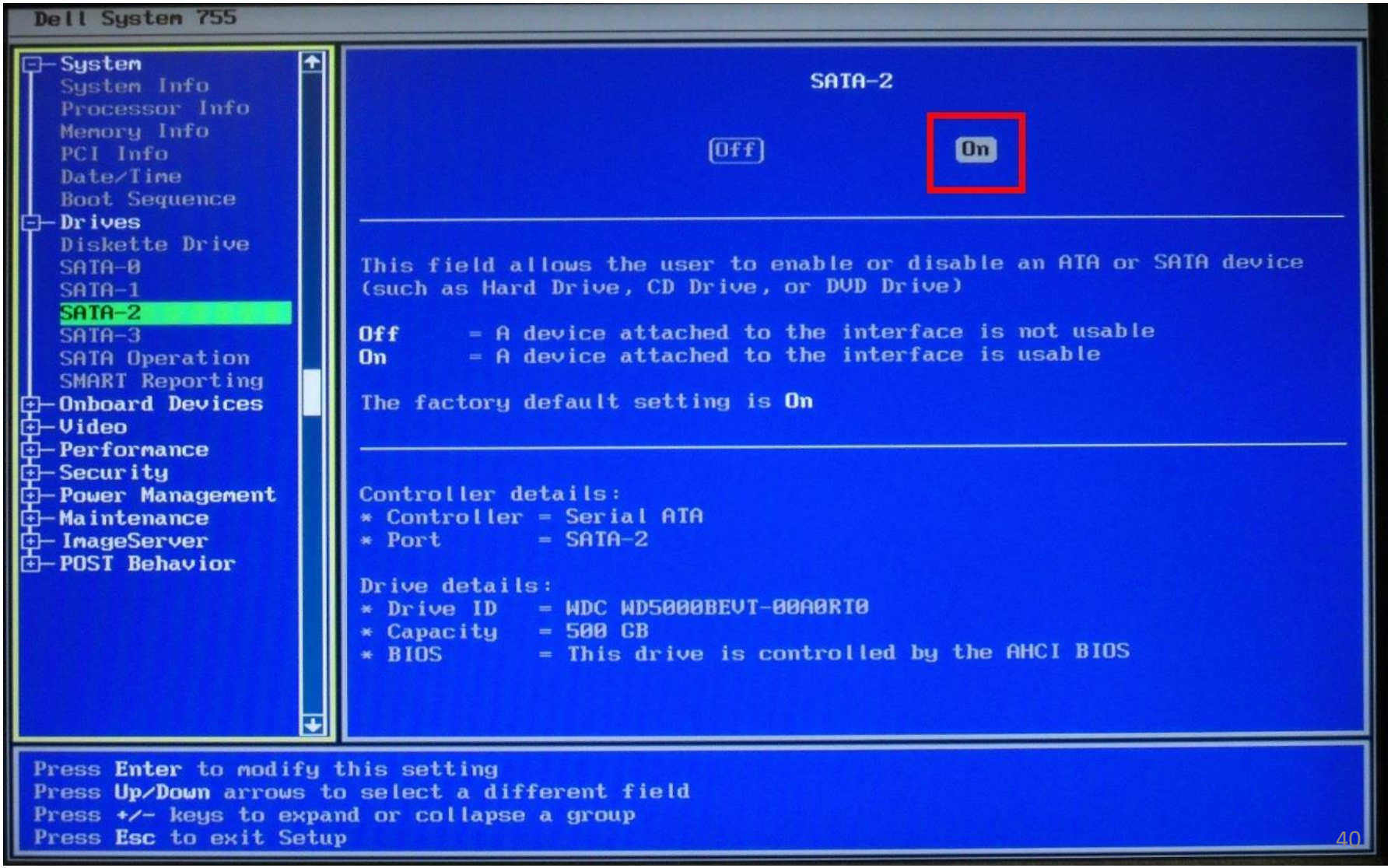
IBM BIOS


IBM Setup Utility
Main
Devices
Startup
Advanced
Security
Power
Exit
Item Specific Help
System Summary
Product Data:
Machine Type/Model 819954U
Flash EEPROM Revision Level 24KT52AUS
Boot Block Revision Level 2452A
System Board Identifier IBM
System Serial Number KCDG1M8
BIOS Date (MM/DD/YY) 03/04/04
System UUID
System Time (HH:MM:SS): [09:32:28]
System Date (MM/DD/YYYY): [06/15/2005]
Select this option to view a summary of the system hardware configuration.
F1 Help
Esc Exit
↑↓ Select Item
↔ Select Menu
-/+ Change Values
Enter Select ▸ Sub-Menu
F9 Setup Defaults
F10 Save and Exit

Lenovo BIOS


Lenovo BIOS Setup Utility
Main Devices Advanced Power Security Startup Exit
System Summary
System Time & Date
Machine Type and Model 30AH001UUS
System Brand ID ThinkStation P300
System Serial Number MJ0192WU
Asset Tag
System UUID A0ACF057-341E-E411-A9CD-4439C454689C
Ethernet MAC Address 44-39-C4-54-68-9C
BIOS Revision Level FBKT90AUS
Boot Block Revision Level FB90A
BIOS Date (MM/DD/YYYY) 06/17/2014
License Status SDK0E50510 PRO
Embedded Controller Version FBCT13A
Language [English]
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults
ESC Exit ↔ Select Menu Enter Select▶Sub-Menu F10 Save and Exit

Dell BIOS


Dell System 755
System
System Info
Processor Info
Memory Info
PCI Info
Date/Time
Boot Sequence
Drives
Diskette Drive
SATA-0
SATA-1
SATA-2
SATA-3
SATA Operation
SMART Reporting
Onboard Devices
Video
Performance
Security
Power Management
Maintenance
ImageServer
POST Behavior
SATA-2
Off
On
This field allows the user to enable or disable an ATA or SATA device (such as Hard Drive, CD Drive, or DVD Drive)
Off = A device attached to the interface is not usable
On = A device attached to the interface is usable
The factory default setting is On
Controller details:
* Controller = Serial ATA
* Port = SATA-2
Drive details:
* Drive ID = WDC WD5000BEVT-00A0RT0
* Capacity = 500 GB
* BIOS = This drive is controlled by the AHCI BIOS
Press Enter to modify this setting
Press Up/Down arrows to select a different field
Press +/- keys to expand or collapse a group
Press Esc to exit Setup

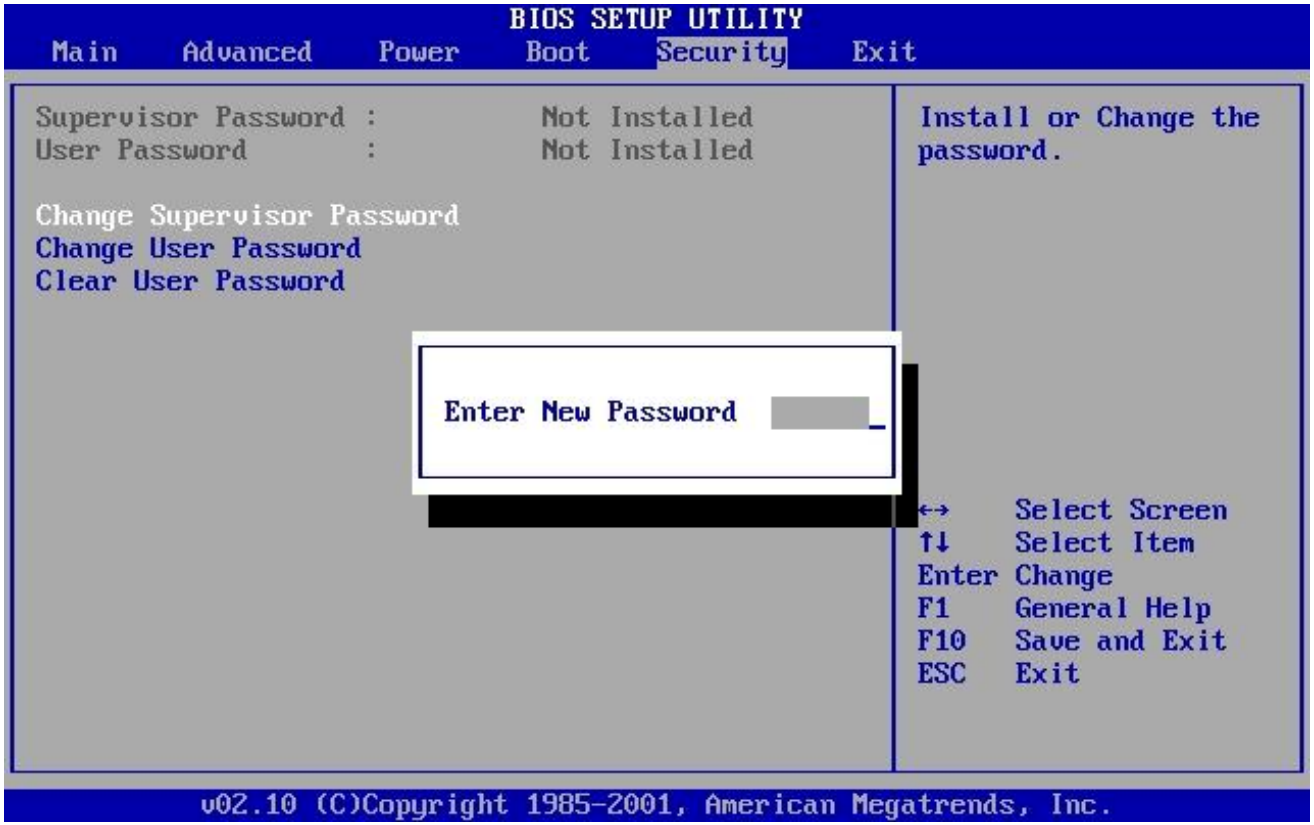
Compaq BIOS


Compaq Computer Corporation Setup Utility
Storage
Security
Power
Advanced
Device Configuration
Storage Options
IDE
Boot
Device Configuration
Hard Disk
▶IDE Primary 0 60.0 GB, WDC WD600AB-00CDB0
IDE Primary 1 34.2 GB, IBM-DPTA-373420
CD-ROM
IDE Secondary 0 COMPAQ DVD-ROM GD-8000
IDE Secondary 1 HL-DT-ST CD-RW GCE-8240B
Diskette
Legacy Diskette 0 3.5" 1.44 MB
Enter=Configure, ESC=Back

HASŁO W BIOSIE

Hasła w BIOSie

- W BIOSie występują dwa rodzaje haseł:
  - Superviser
  - User



Rodzaje haseł

- User (Użytkownik) - hasło ma zablokować uruchomienie się komputera (BIOSU oraz systemu operacyjnego). User nie może też grzebać w ustawieniach BIOSU.
- Superviser (Administrator) - ma pełen dostęp do wszystkich opcji BIOSu. Inne uprawnienia ma takie jak dla zwykłego użytkownika.

- W niektórych BIOSach możemy wybrać zasięg hasła:
  - Blokuje uruchomienie komputera.
  - Blokuje dostęp do wejścia do BIOSu.
  - Blokuje dostęp do modyfikacji ustawień BIOSu.

Hasła uniwersalne

- Do BIOSu można wejść używając tzw. haseł serwisowych (uniwersalnych).
- Pozwalają one na (niezależne od założonego przez użytkownika) dostanie się do ustawień lub uruchomienie komputera.

BIOS	Hasła
AMI	AMI, ami, bios, setup, cmos, AMIDECODE, A.M.I., AMI SW, AMI_SW, BIOS, PASSWORD, HEWITT RAND, A.M.I., AMI!SW, AMI?SW, HEWITT RAND, alfarome, efmukl
AWARD	01322222, 589589, 589721, 595595, 598598, aLLy, aLLY, ALLY, ALFAROME, alfaromeo, aPAf, AW, AWARD, _award, AWARD_HW, AWARD SW, AWARD_PS, AWARD PW, AWARD_SW, AWARD?SW, AWKWARD, awkward, BIOSTAR, CONCAT, Condo, d8on, djonet, HLT, J64, J256, J262, j332, KDD, LKWPETER, lkwpeter, PINT, pint, SER, SKY_FOX, SYXZ, Syxz, TTPTHA, ZAAADA, ZBAAACA, ZJAAADC
PHOENIX	BIOS, CMOS, PHOENIX, phoenix
Compaq	Compaq
Dell	Dell
VOBIS & IBM	merlin
IBM APTIVA	równocześnie nacisnąć dwa przyciski myszy
Biostar	Biostar
Enox	xo11nE
Epox	central
Siemens	SKY_FOX
Packard Bell	bell9
Freetech	Posterie
IWill	iwill
TMC	bigo
Jetway	spooml
QDI	QDI
SOYO	SOYO
Tinys	Tiny
Toshiba	Toshiba, lub w trakcie uruchamiana przytrzymać "Shift".

Zasada przechowywania haseł

- Hasła nie są przechowywane w pamięci BIOSu.
- BIOS przechowuje tylko tzw. sumę kontrolną.
  - Do każdego hasła jest wyznaczana dwubajtowa liczba zapamiętywana w komputerze.
  - Przy wpisywaniu hasła obliczana jest jego suma kontrolna i porównywana z tą zawartą w BIOSie.
- Suma kontrolna może być identyczna dla różnych haseł.
- Znając algorytm możemy obliczyć hasła uniwersalne.
- Na nowych płytach głównych niektóre hasła mogą nie działać.
  - Zmieniony (ulepszony) algorytm.
  - Odkryto nowe hasła uniwersalne.

Wpisywanie haseł

- BIOS zazwyczaj rozróżnia małe i wielkie litery.
- Należy korzystać z klawiatury programisty wpisując hasła.
- Dla układu klawiatury „polska – maszynistki” należy wprowadzać hasła według amerykańskiego układu klawiatury.
  - Przykładowo naciśnięcie klawisza _ powoduje wyświetlenie pytajnika ?
  - AWARD_SW i AWARD?SW występujące na niektórych listach to nie dwa oddzielne hasła, lecz jedno, zapisane raz dla klawiatury amerykańskiej i polskiej programisty, a za drugim razem dla polskiej maszynistki.

Programy do łamania haseł w BIOSach

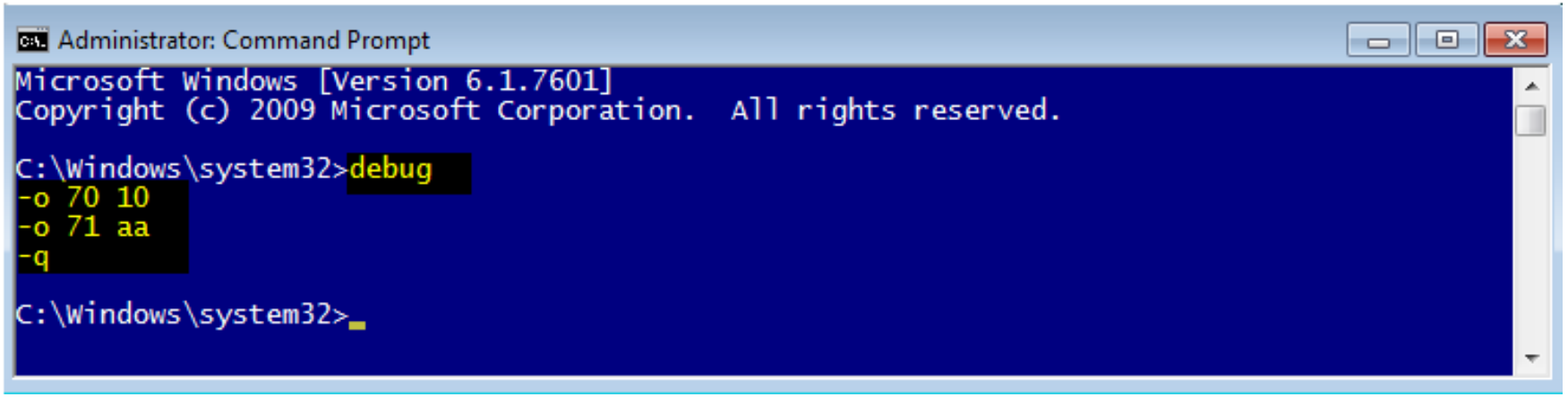
- Sprawdzają hasła serwisowe i popularne hasła.
- Próbują metody brute-force
  - BIOSy nie mają ograniczenia liczby logowań
- Odczytanie pamięci CMOS i poszukanie w niej hasła (lub jego sumy kontrolnej).
- Kasowanie i śmiecenie pamięci CMOS.

Program Debug

- Przy włączonym komputerze można wyczyścić pamięć CMOS za pomocą programu DEBUG.EXE
  - Dla Windows 95/98/Me poszukaj w katalogu \WINDOWS\COMMAND
  - Dla XP i nowszych użyj dyskietki startowej Windows 98.
- Po uruchomieniu wpisz następujące polecenia:

  o 70 2E
  o 71 0
  q

  usuwana jest suma kontrolna hasła i informacja o jego aktywności.
- Po restarcie systemu BIOS zauważy zmiany w pamięci CMOS i wyświetli komunikat `CMOS checksum error - Defaults loaded`.



Inne sposoby

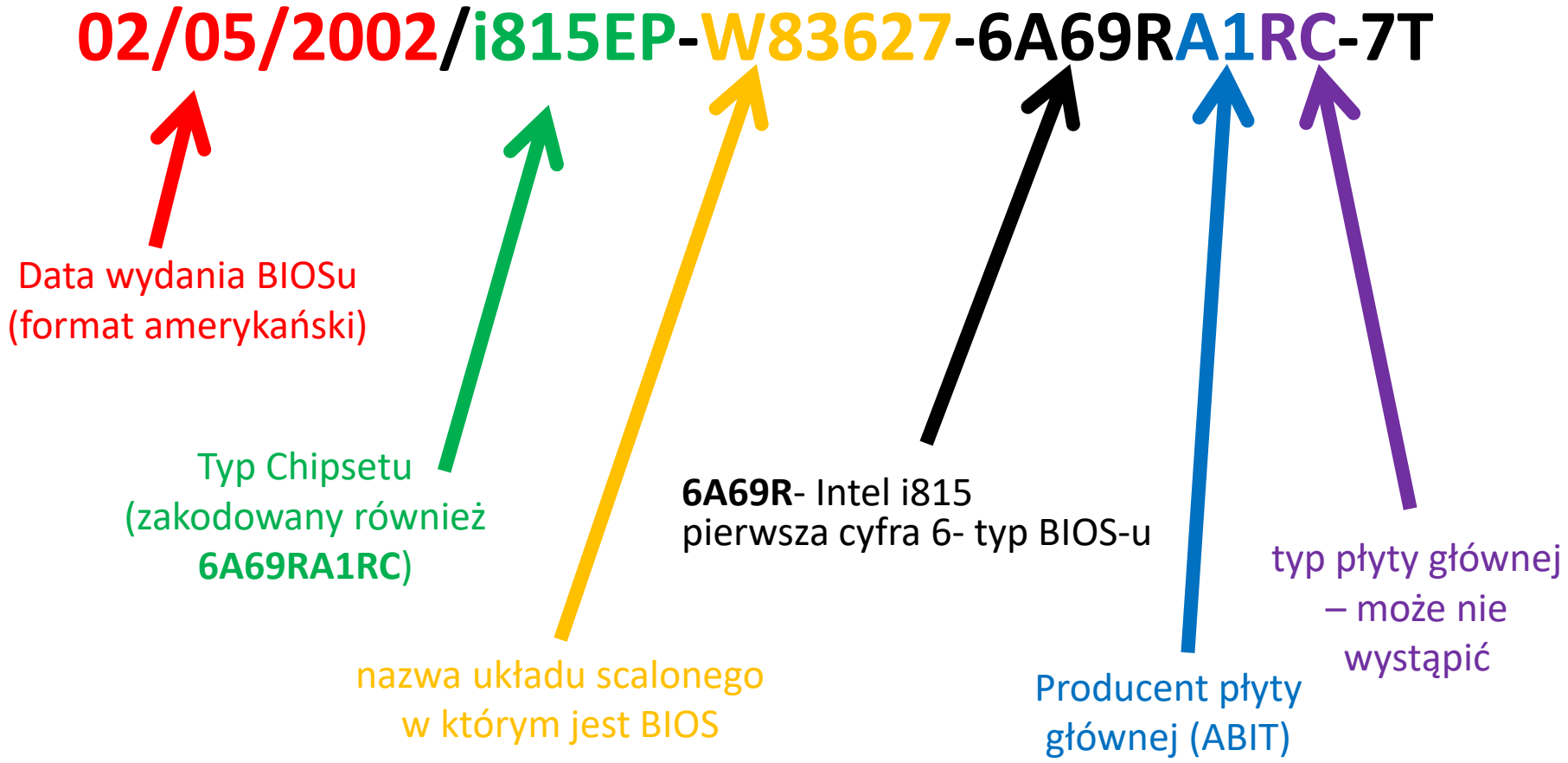
- Wyjęcie bateryjki BIOSu na kilka minut.
- Naciśnięcie przycisku resetującego BIOS
- Zwarcie zworki CLR_CMOS, PSWD (nie ma ich w niektórych laptopach)

Ćwiczenie

- Wyszukaj w twoim BIOSie gdzie można założyć lub zmienić hasło na BIOS.

OZNACZENIA BIOSU

Oznaczenia BIOSu



Kod producentów płyty głównej cz.1

ID	Firma	ID	Firma	ID	Firma	ID	Firma
A0	ASUS	B1	BEK-Tronic Technology	D2	Digital	EC	ENPC
A1	Abit (Silicon Star)	B2	Boser	D3	Digicom	F0	FIC (FICA)
A2	Atrend	B3	BCM	D4	DFI (Diamond Flower) (Crusader?)	F1	Flytech Group International
A3	Bcom (ASI)	C0	Matsonic	D7	Daewoo	F2	Free Tech or flexus?
A7	AVT (formerly Concord)	C1	Clevo	DE	Dual Tech	F3	Full Yes
A8	Adcom	C2	Chicony	DI	Domex (DTC)	F5	Fugutech
AB	AOpen	C3	Chaintech	DJ	Darter	F8	Formosa Industrial Computing
AD	Amaquest	C5	Chaplet	DL	Delta Electronics	F9	Fordlian
AK	Advantech	C9	Computrend	E1	ECS (Elitegroup)	FG	Fastfame Technology Co., Ltd.
AM	Achme	CF	Flagpoint	E3	EFA	FI	FIC (FICA)
AT	ASK Technology	CS	Gainward or CSS Laboratories	E4	ESPCo	G0	Giga-byte
AX	Achitec	D0	Dataexpert	E6	Elonex	G1	GIT???
B0	Biostar	D1	DTK	E7	Expen Tech	G3	Gemlight

Kod producentów płyty głównej cz.2

ID	Firma	ID	Firma	ID	Firma	ID	Firma
G5	GVC	IE	Itri	M0	Matra	P4	Asus
G9	Global Circuit Technology	J1	Jetway (Jetboard, Acorp)	M2	Mycomp (TMC) and Megastar	P6	Pro-Tech
GA	Giantec	J2	Jamicon (Twn)	M3	Mitac	P8	Azza
GE	Zaapa	J3	J-Bond	M4	Micro-star	P9	Powertech
H0	Hsing-Tech (PcChips)	J4	Jetta	M8	Mustek	PA	Epox & 2TheMax
H2	HOLCO (Shuttle)	J6	Joss	M9	Micro Leader Enterprises Corp. (MLE)	PC	Pine
HH	HighTech Information System	K0	Kapok	MH	Macrotek	PF	President (dead)
I3	IWill	K1	Kamei	N0	Nexcom	PN	Procomp Informatics Ltd.
I4	Inventa (Twn)	KF	Kinpo	N5	NEC	PS	Palmax (notebooks)
I5	Informtech	L1	Lucky Star	NM	NMC (New Media Communication)	PX	Pionix
I9	ICP	L7	Lanner Electronics Inc.	NX	Nexar	Q0	Quanta (Twn)
IA	Infinity (?)	L9	Lucky Tiger	O0	Ocean (Octek)	Q1	QDI
IC	Inventec(notebook)	LB	LeadTek	P1	PC-Chips	RA	RioWorks Solutions Inc

Kod producentów płyty głównej cz.3

ID	Firma	ID	Firma	ID	Firma	ID	Firma
R0	Mtech (Rise)	SL	Winco	TL	Transcend Information Inc.	V7	YKM (Dayton Micro)
R2	Rectron	SM	San-Li and Hope Vision, Superpower	TP	Commate, Ozzo (?)	W0	Wintec (Edom)
R3	Datavan International Corp.	SN	Soltek	U0	U-Board (?)	W1	WellJoin
S2	Soyo	SW	S&D A-Corp and Zaapa	U1	USI (Universal Scientific Industrial)	W5	Winco
S3	Smart D&M Technology Co.,	T0	Twinhead	U2	AIR (UHC)	W7	Win Lan Enterprise
S5	Shuttle (Holco)	T1	Taemung or Fentech or Trang Bow	U4	Unicorn	XA	ADLink Technology Inc.
S9	Spring Circle	T4	Taken	U5	Unico	X3	A-Corp
SA	Seanix	T5	Tyan	U6	Unitron	X5	Arima
SC	Sukjung (Auhua Electronics Co. Ltd.)	T6	Trigem	U9	Warp Speed Ink.	Y2	Yamashita
SE	Professional Technologies, Inc	TB	Taeil ???	V3	Vtech (PCPartner)	Z1	Zida (Tomato boards)
SH	SYE (Shining Yuan Enterprise)	TG	Tekram	V5	Vision Top Technology	Z2	???
SJ	Sowah	TJ	Totem	V6	Vobis	Z3	ShenZhen Zeling Industrial Co., Ltd

Oznaczenia BIOSu

- **Award Modular BIOS v.4.51, An Energy Star Ally**
  Copyright (C) 1984-2000, Award Software, Inc.
  W6163MJ V3.8 052900

- BIOS firmy AWARD (2 pierwsze linie, litera W przed 6163)
- Płyta 6163
- BIOS w wersji 3.8.
- Sześć ostatnich cyfr podaje datę emisji w formacie amerykańskim (miesiąc, dzień, rok). Tu jest to BIOS z 29 maja 2000 roku.

- **Press DEL to enter SETUP, ESC to skip memory test**
  05/29/2000 - i440BX - W977 - 2A69KM4KC - 00

- Pierwszy rząd znaków – data BIOSu
- Drugi – typ chipsetu
- Trzeci – W – Award
- Czwarty – informuje o typie chipsetu (znaki 1-5) i identyfikatorze producenta płyty (znaki 6-7).
- M4 – producentem firma MSI

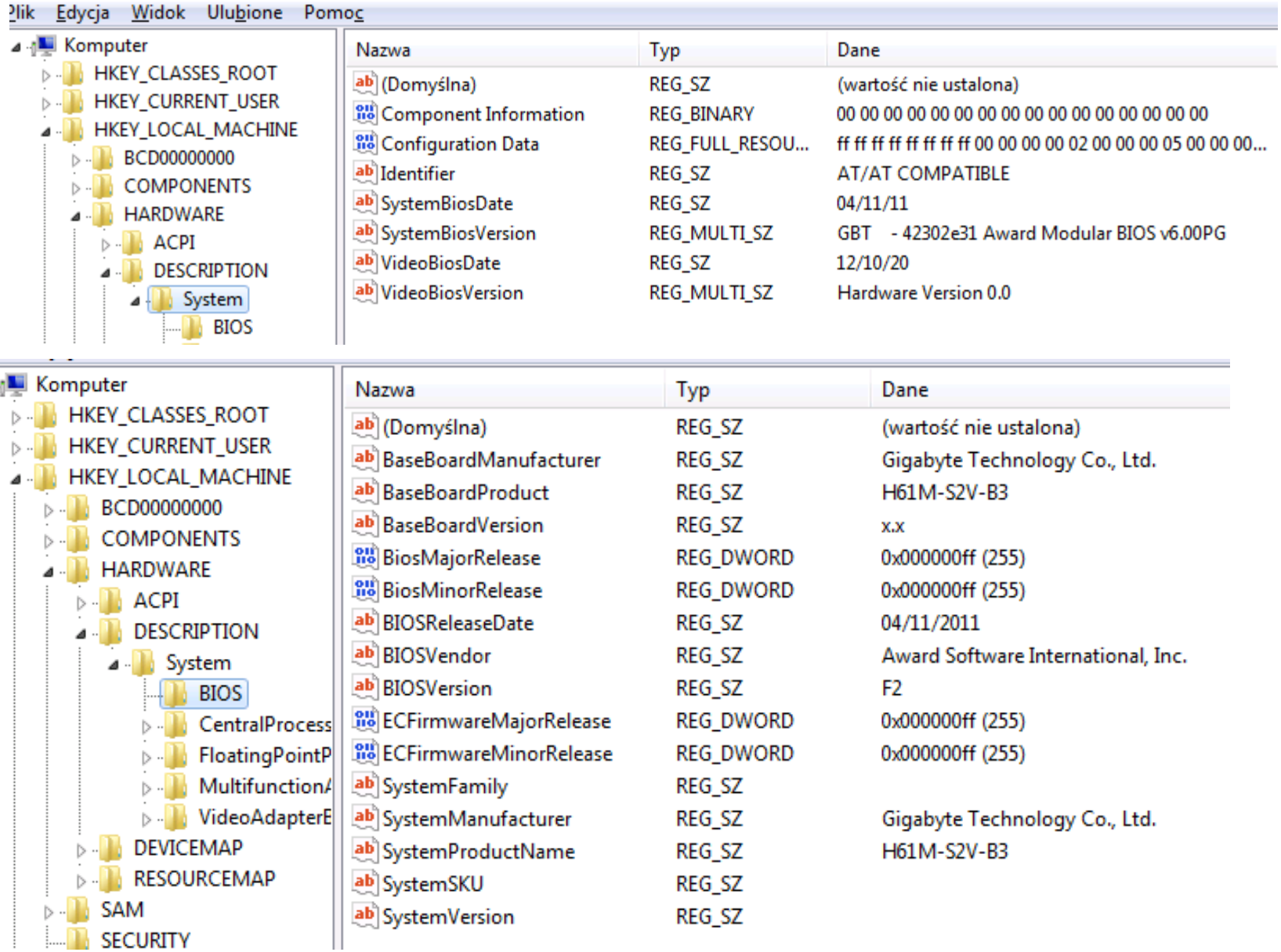
Oznaczenia BIOSu – Edytor rejestru

- **Windows 98/Me**
- Klucz "HKEY_LOCAL_MACHINE\ Enum\Root*PNP0C01\0000".
  - Wartość ciągu "BIOSDate" zdradza datę BIOS-u,
  - "BIOSName" nazwę producenta (np. Award),
  - "BIOSVersion" - bieżącą wersję BIOS-u.

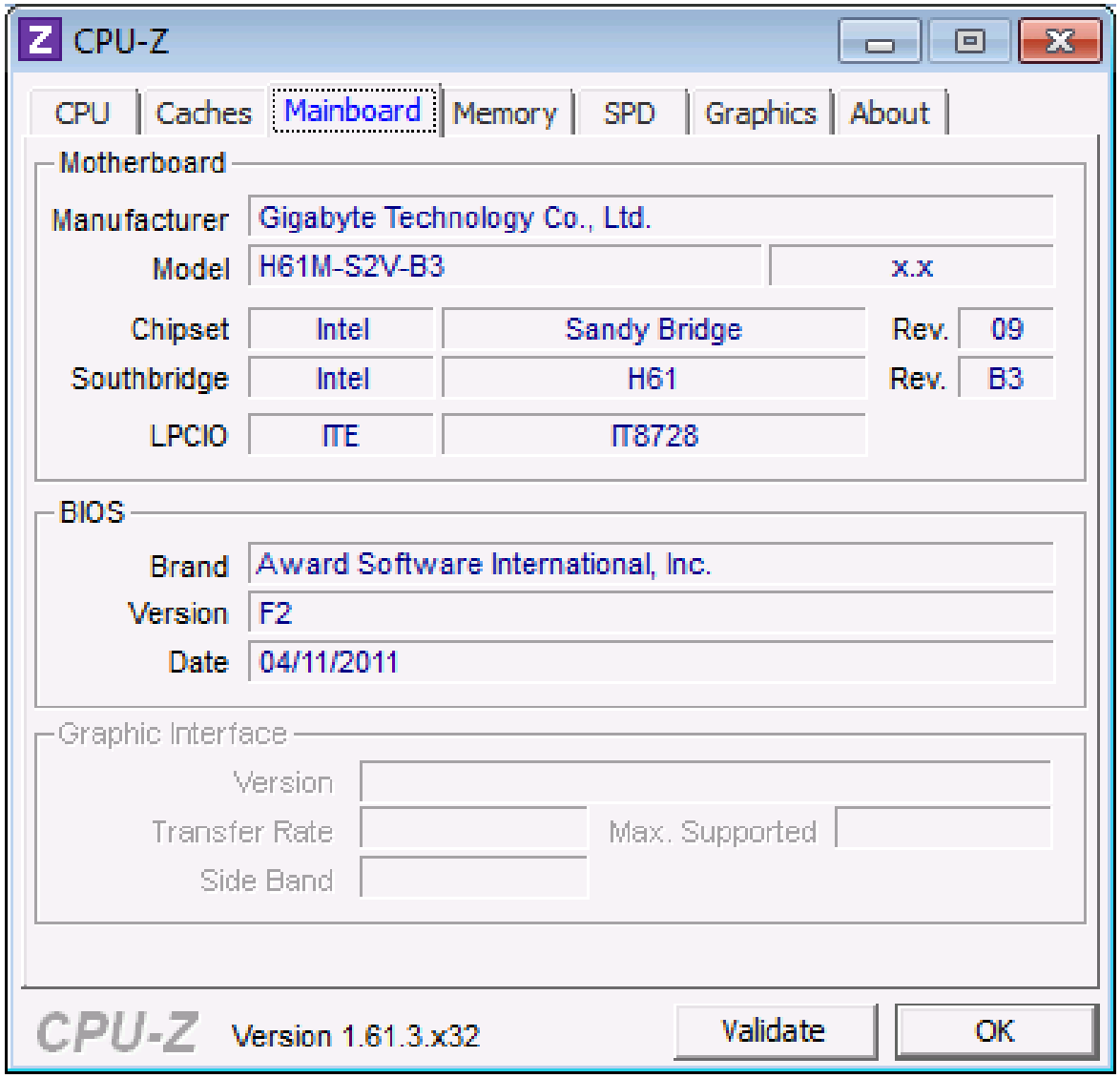
- **Windows NT i nowsze**
- Klucz "HKEY_LOCAL_MACHINE\Hardware\Description\System".
  - wartość "SystemBiosDate” podaje datę BIOS-u.
  - wartość " SystemBiosVersion ” podaje wersję BIOS-u.

- Klucz "HKEY_LOCAL_MACHINE\Hardware\Description\System\BIOS".

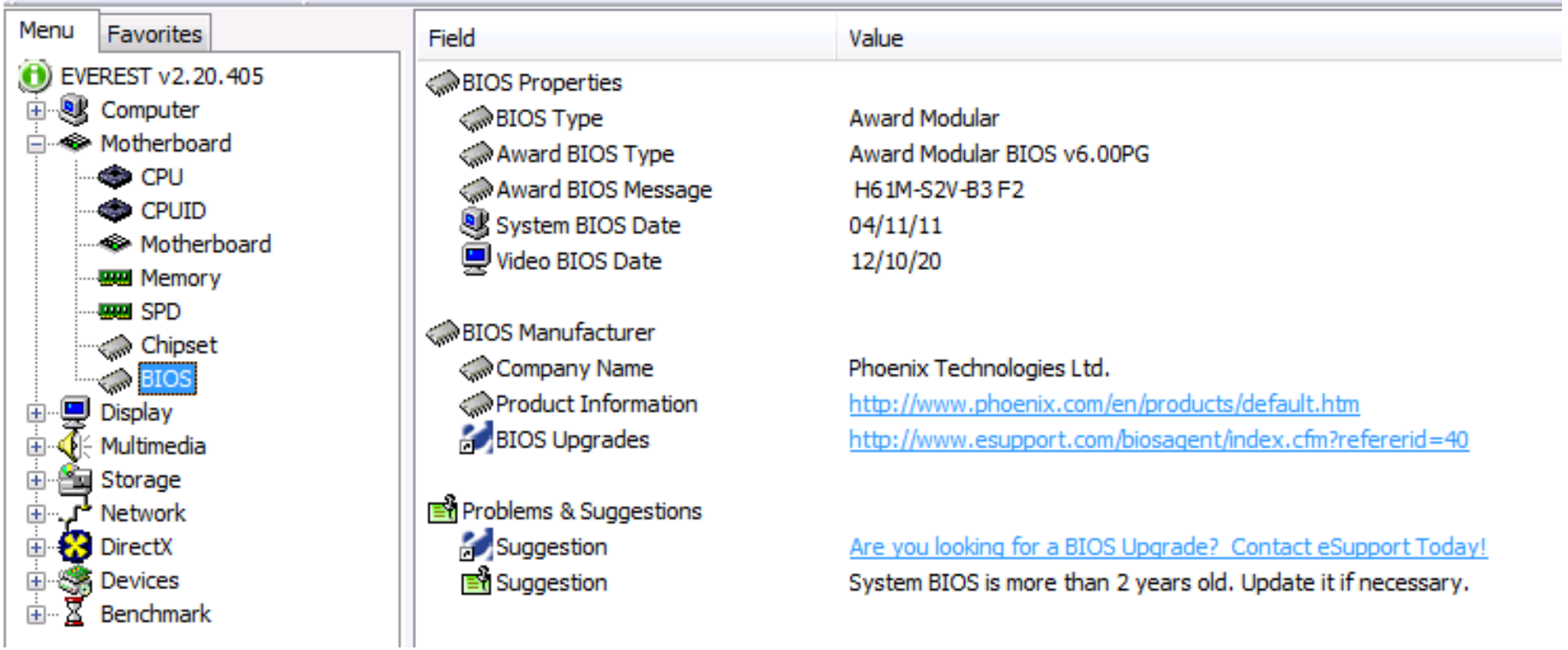
Oznaczenia BIOSu – Edytor rejestru



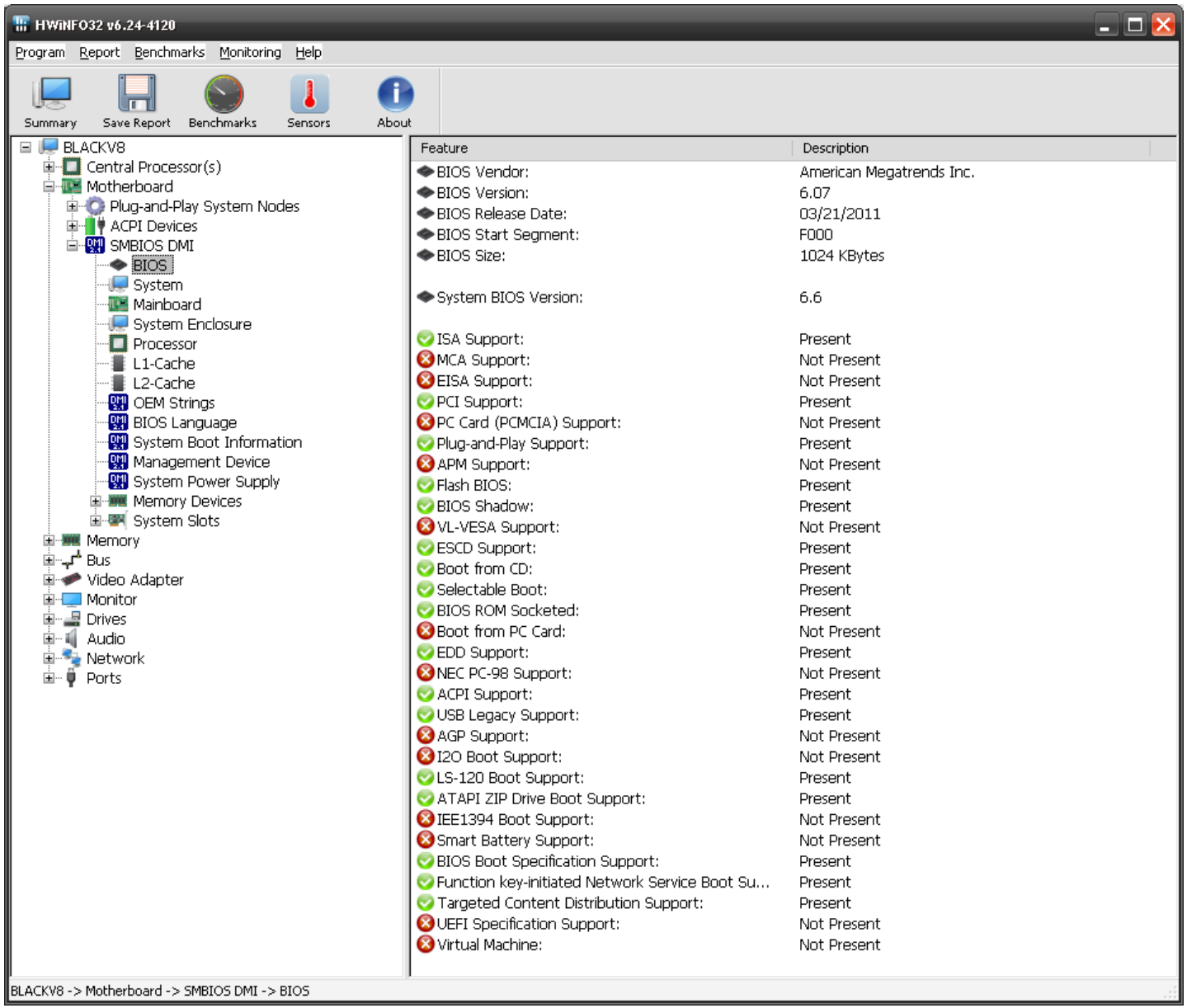
CPU-Z


CPU-Z
CPU
Caches
Mainboard
Memory
SPD
Graphics
About
Motherboard
Manufacturer
Gigabyte Technology Co., Ltd.
Model
H61M-S2V-B3
x.x
Chipset
Intel
Sandy Bridge
Rev.
09
Southbridge
Intel
H61
Rev.
B3
LPCIO
ITE
IT8728
BIOS
Brand
Award Software International, Inc.
Version
F2
Date
04/11/2011
Graphic Interface
Version
Transfer Rate
Max. Supported
Side Band
CPU-Z
Version 1.61.3.x32
Validate
OK

Everest

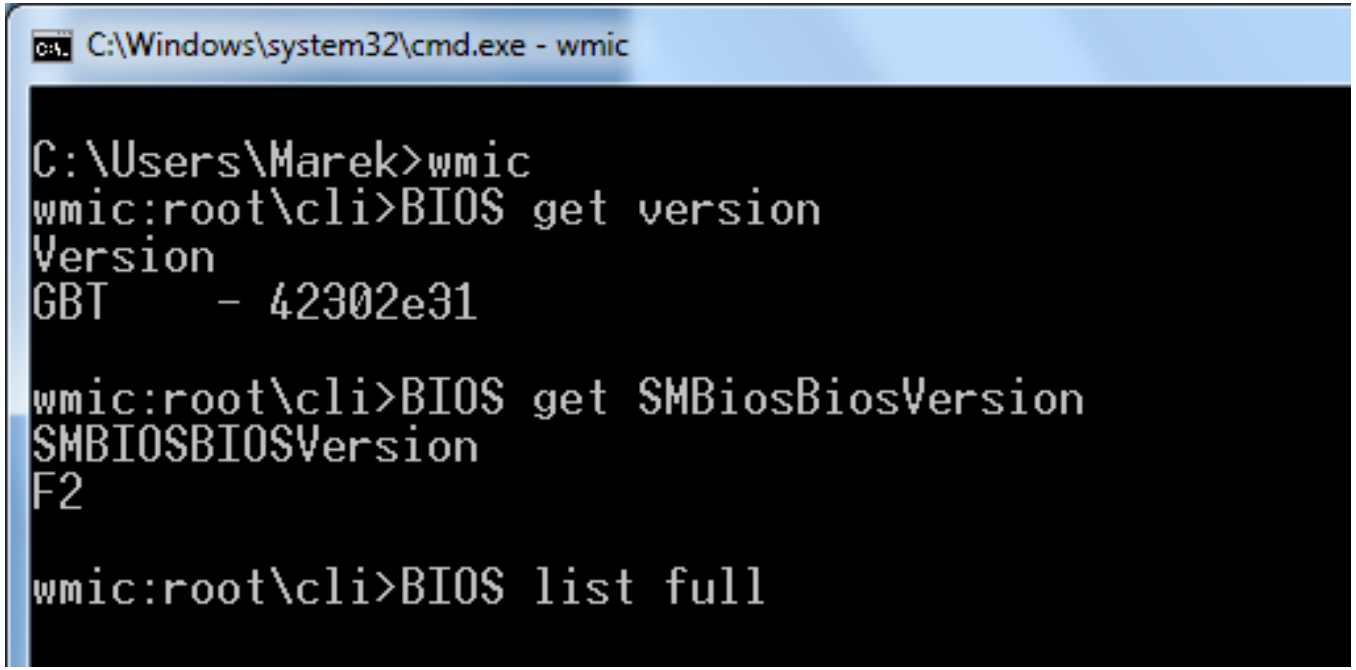

Menu
Favorites
EVEREST v2.20.405
Computer
Motherboard
CPU
CPUID
Motherboard
Memory
SPD
Chipset
BIOS
Display
Multimedia
Storage
Network
DirectX
Devices
Benchmark
Field
Value
BIOS Properties
BIOS Type
Award Modular
Award BIOS Type
Award Modular BIOS v6.00PG
Award BIOS Message
H61M-S2V-B3 F2
System BIOS Date
04/11/11
Video BIOS Date
12/10/20
BIOS Manufacturer
Company Name
Phoenix Technologies Ltd.
Product Information
http://www.phoenix.com/en/products/default.htm
BIOS Upgrades
http://www.esupport.com/biosagent/index.cfm?refererid=40
Problems & Suggestions
Suggestion
Are you looking for a BIOS Upgrade? Contact eSupport Today!
Suggestion
System BIOS is more than 2 years old. Update it if necessary.

HWInfo


HWiNFO32 v6.24-4120
Program Report Benchmarks Monitoring Help
Summary Save Report Benchmarks Sensors About
BLACKV8
Central Processor(s)
Motherboard
Plug-and-Play System Nodes
ACPI Devices
SMBIOS DMI
BIOS
System
Mainboard
System Enclosure
Processor
L1-Cache
L2-Cache
OEM Strings
BIOS Language
System Boot Information
Management Device
System Power Supply
Memory Devices
System Slots
Memory
Bus
Video Adapter
Monitor
Drives
Audio
Network
Ports
Feature
Description
BIOS Vendor: American Megatrends Inc.
BIOS Version: 6.07
BIOS Release Date: 03/21/2011
BIOS Start Segment: F000
BIOS Size: 1024 KBytes
System BIOS Version: 6.6
ISA Support: Present
MCA Support: Not Present
EISA Support: Not Present
PCI Support: Present
PC Card (PCMCIA) Support: Not Present
Plug-and-Play Support: Present
APM Support: Not Present
Flash BIOS: Present
BIOS Shadow: Present
VL-VESA Support: Not Present
ESCD Support: Present
Boot from CD: Present
Selectable Boot: Present
BIOS ROM Socketed: Present
Boot from PC Card: Not Present
EDD Support: Present
NEC PC-98 Support: Not Present
ACPI Support: Present
USB Legacy Support: Present
AGP Support: Not Present
I2O Boot Support: Not Present
LS-120 Boot Support: Present
ATAPI ZIP Drive Boot Support: Present
IEE1394 Boot Support: Not Present
Smart Battery Support: Not Present
BIOS Boot Specification Support: Present
Function key-initiated Network Service Boot Su... Present
Targeted Content Distribution Support: Present
UEFI Specification Support: Not Present
Virtual Machine: Not Present
BLACKV8 -> Motherboard -> SMBIOS DMI -> BIOS

WMIC (Windows Managament Instrumentation Console)

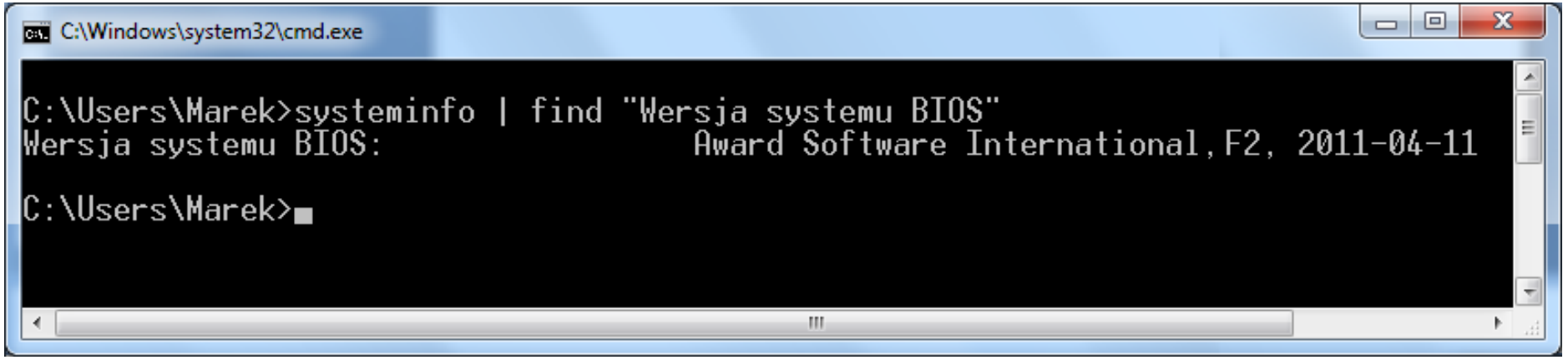
- Polecenie w wierszu poleceń
- `WMIC BIOS GET version`
- `WMIC BIOS GET SMBiosBiosVersion`
- `WMIC BIOS LIST FULL`



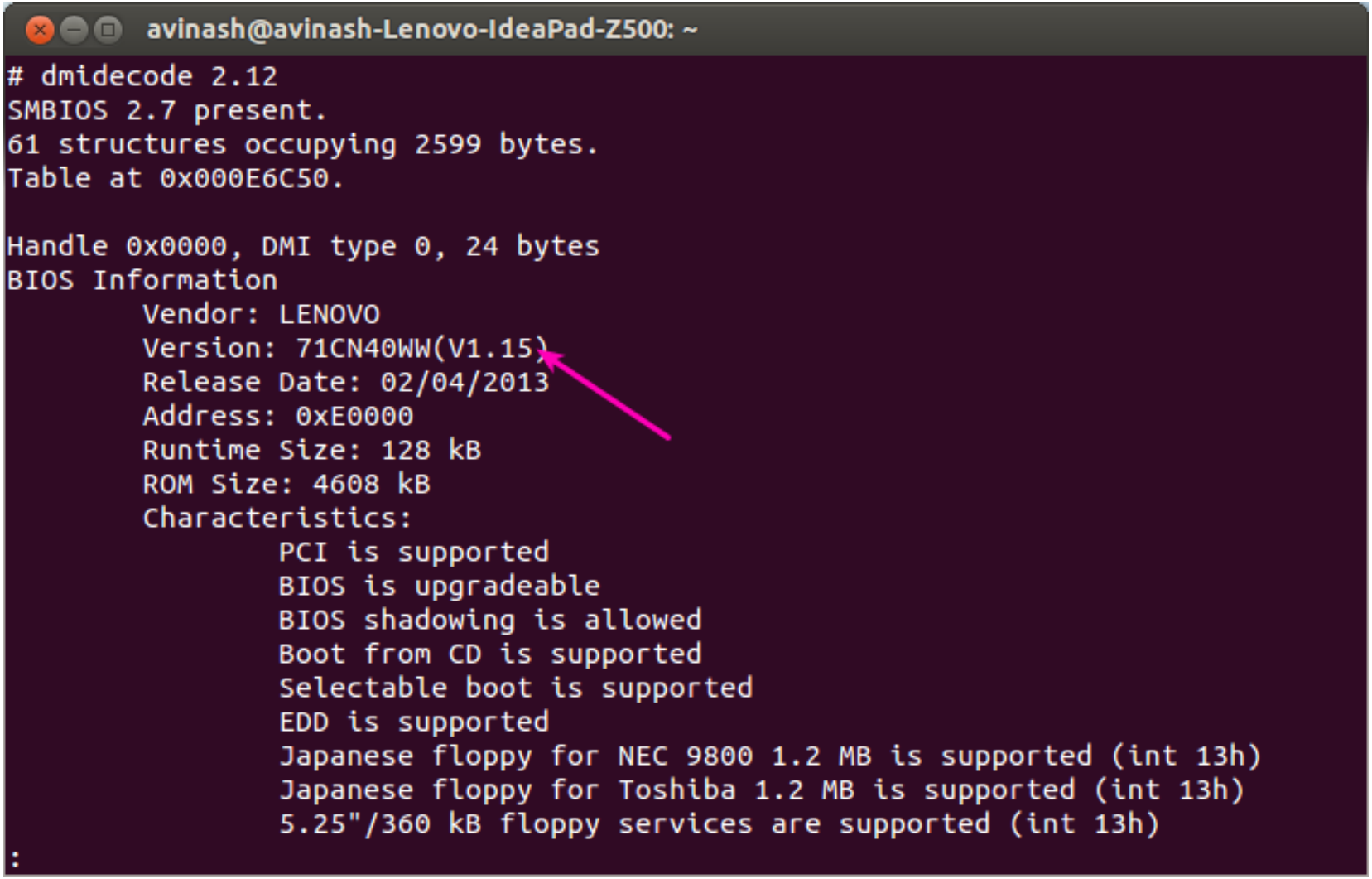
Konsola CMD (Command Line)

- Polecenie w wierszu poleceń

```
systeminfo | find ”Wersja systemu BIOS”
```



Linux-polecenie **dmidecode**

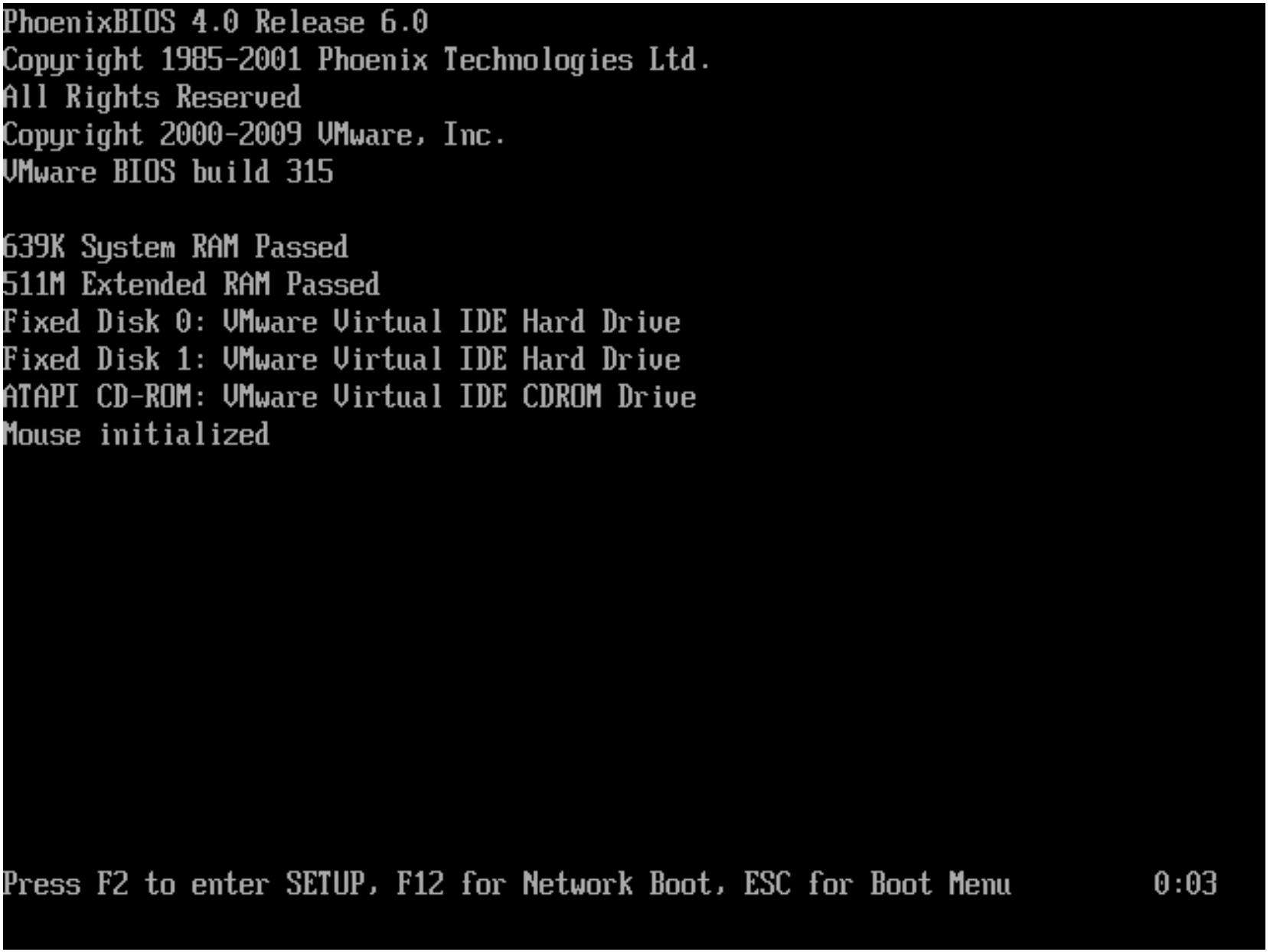


SETUP BIOS

Kody do wejścia do BIOSu

Producent	*Klawisz*	*Producent*	*Klawisz*
ABIT	Del	**DFI**	Del lub F8
Acer	F2 lub Ctrl Alt Esc	**Gigabyte**	Del
ASUS	Del lub F2	**Hewlett Packard**	F1, F2 gdy pojawi się logo HP lub F10 dla nowszych wersji
ASRock	Del lub F2	**IBM**	F1, Ins (wcisnąć i przytrzymać obydwa klawisze myszy)
American Megatrends (AMI)	Del lub F1	**NEC, Packard Bell, Amax, Micron, Aptiva, Sharp**	F1, F2
AST Advantage, Tandon	Ctrl Alt Esc	**Phoenix BIOS**	F1, F2, Ctrl Alt Ins, Ctrl S, Ctrl Alt Esc, Ctrl Alt S, Ctrl Alt Enter, Del
Award	Del lub F1	**Sony**	F3 potem F1 lub F2
Compaq	F10 gdy na ekranie w górnym rogu pojawi się mały kwadrat	**Toshiba**	Esc, F1, F2
Dell	Del, F2, F1, Ctrl Alt Enter, wcisnąć Reset dwa razy	**Zenith**	Ctrl Alt Ins

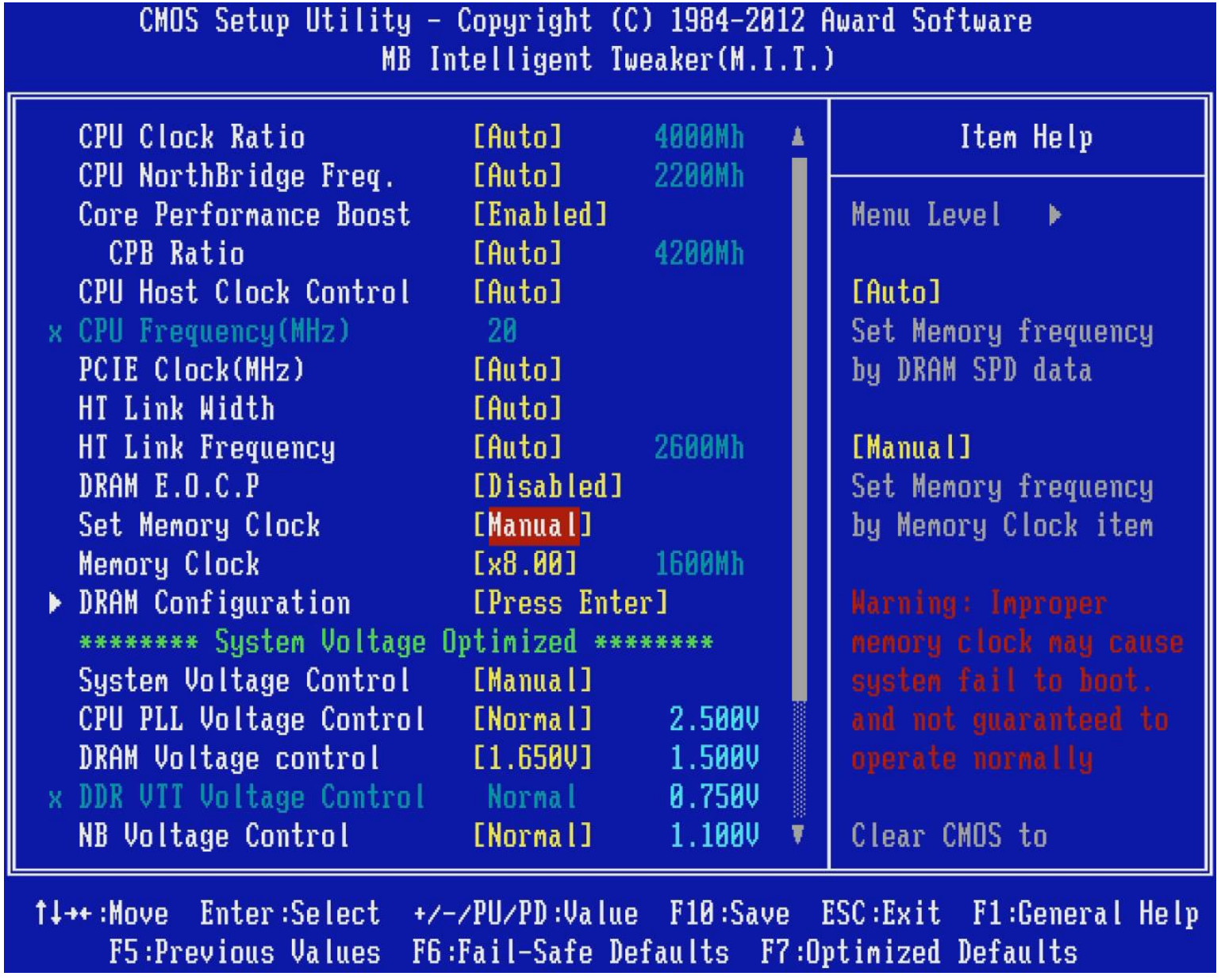
Wejście do BIOS-setup



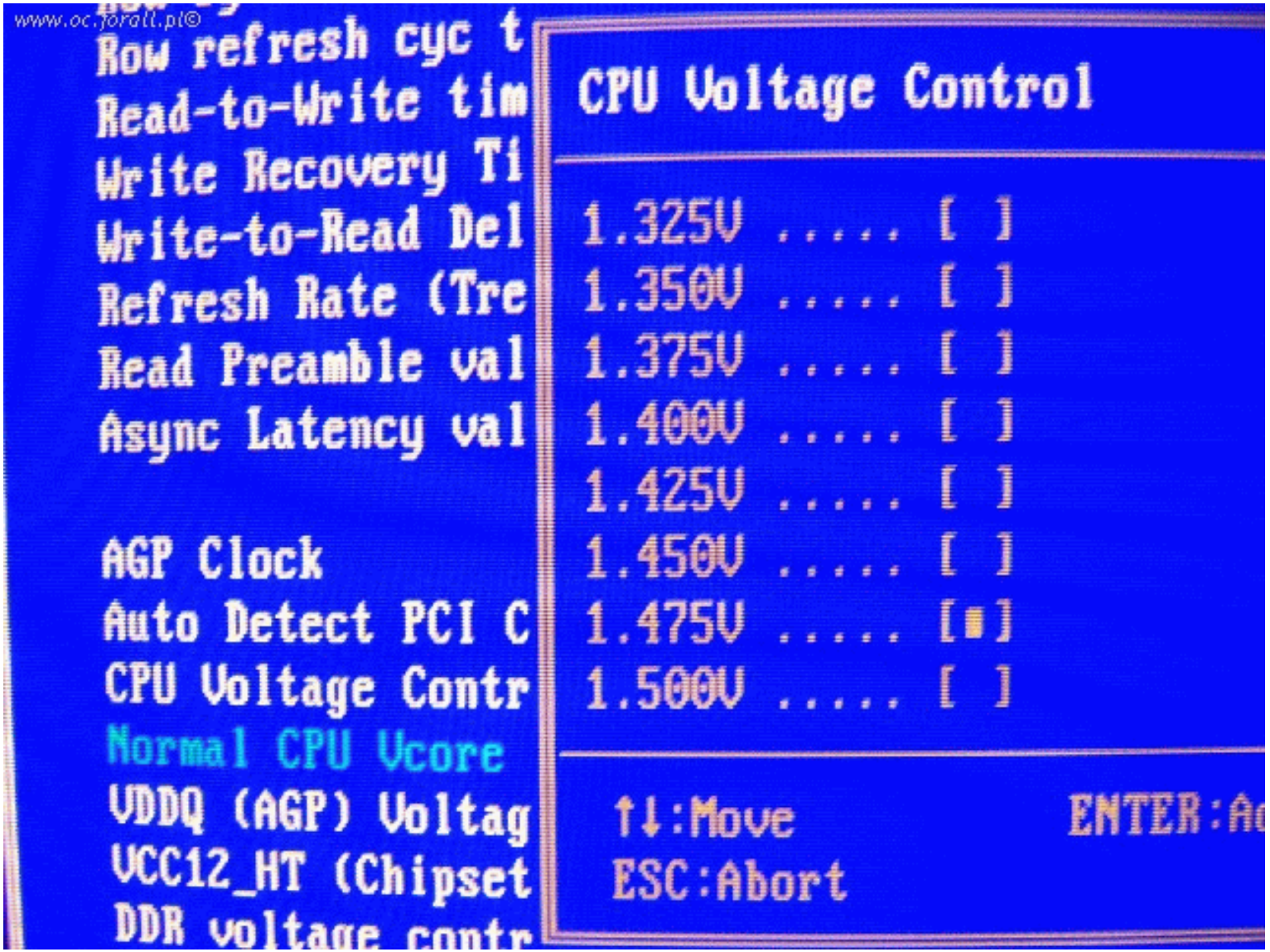
Jakich zmian można dokonać?

- Za pomocą wbudowanego w BIOS programu setup można zmieniać standardowe ustawienia BIOS-u
  - parametry podłączonych nośników pamięci
  - zachowanie się komputera po jego włączeniu
  - włączać/wyłączać niektóre elementy płyty głównej, np. porty komunikacyjne.
- Za pomocą BIOS-u można też przetaktowywać procesor i pamięć.

Zmiana parametrów procesora i pamięci



Zmiana napięcia zasilania procesora



Podstawowe parametry konfiguracyjne BIOSu

Date – data (mm.dd.yy.)

Time – czas (hh:mm:ss)

IDE Primary/Secondary Master/Slave - Tutaj znajdują się zdefiniowane samodzielnie przez użytkownika bądź przez BIOS, urządzenia przyłączone do wbudowanego w płytę główną kontrolera IDE.

IDE HDD Auto-Detection - Opcja wykrywająca automatycznie urządzenia przyłączone do kanałów np. twarde dyski, czy CD-ROMy.

IDE Primary (Secondary) Master/Slave - Tutaj możemy zadecydować, czy nasz BIOS będzie automatycznie ustawiał parametry dysku (Auto) czy też chcemy je sami ustawić (Manual). Jeżeli natomiast chcemy by nasz BIOS w danym kanale "nie widział" dysku, możemy się posłużyć funkcją: "None".

DRAM Timing By SPD - Opcja powodująca, że BIOS automatycznie dopasuje parametry pracy pamięci na podstawie informacji odczytanych z tzw. układu SPD (Procedura odczytu obsługiwana jest przez chipset płyty głównej).

SDRAM Clock - ustawienia częstotliwości pracy pamięci.

SDRAM CAS Latency Time - ustawienia czasu opóźnienia sygnału CAS dla pamięci SDRAM. (Ustawienie domyślne to 3, ustawienia inne dla pamięci o czasie CAS, który wynosi 3 może być przyczyną niestabilnego działania systemu).

CPU Internal Cache - Włącza/wyłącza pamięć cache (optymalizuje przesył danych do/z procesora).

Quick Power On Selt Test - Włącza/wyłącza przyśpieszoną procedurę testową sprzętu obsługiwanego przez komputer.

First/Second/Third Boot Device (Boot Sequence) - Ustala kolejność odczytywania nośników, z których BIOS ma uruchomić system operacyjny.

Boot Other Device - Włącza/wyłącza możliwość bootowania z urządzeń podłączonych do zewnętrznego kontrolera.

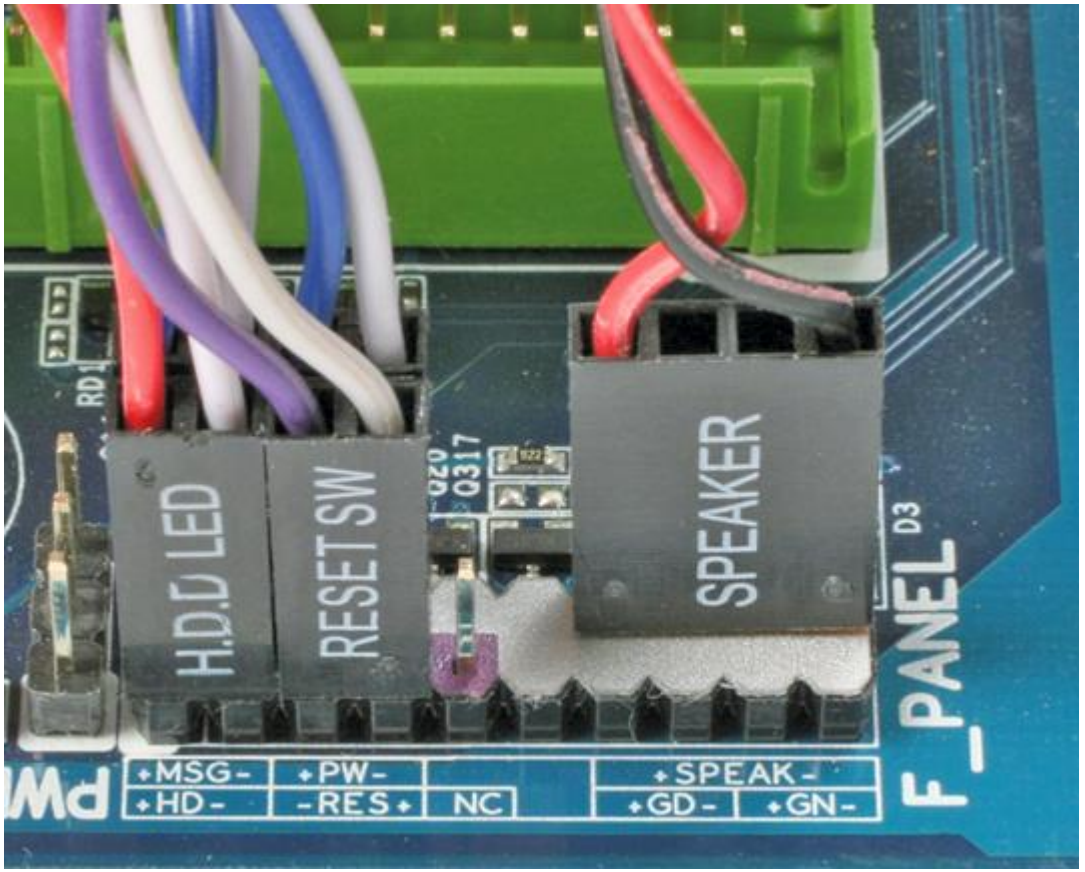
KODY DŹWIĘKOWE

Sygnalizacja dźwiękowa

- Jeśli procedury POST wykryją jakiś błąd przed zainicjalizowaniem karty graficznej niemożliwe jest wyświetlenie informacji o błędzie.
- Błędy są komunikowane za pomocą umieszczonego w obudowie głośniczka.
  - Ilość i czas emitowanych dźwięków pozwolą na zorientowanie się w rodzaju uszkodzenia.
- Poszczególni producenci BIOS-ów definiują własne zestawy takich sygnałów - mniej lub bardziej rozbudowanych.
  - Ami BIOS i Phoenix BIOS sygnalizują dość dużą ilość błędów,
  - BIOS-y Awarda są raczej lakoniczne.
- Oprócz sygnalizacji dźwiękowej błędu, kod ostatnio wykonywanej przez system czynności jest wysyłany do portu 80h, co wykorzystuje karta diagnostyczna.
  - Gdy komputer jest sprawny, zostaje wydany pojedynczy dźwięk i maszyna się uruchamia.

PC Speaker


SPEAKER


H.D.D LED
RESET SW
SPEAKER
F_PANEL
+MSG-
+HD-
+PW-
-RES+
NC
+SPEAK-
+GD-
+GN-

Award BIOS, sygnalizacja błędów

Rodzaj dźwięku	Znaczenie
Brak dźwięku	Uszkodzony głośniczek lub brak zasilania
1 krótki	wszystko w porządku
1 długi	błąd pamięci RAM
1 długi, 2 krótkie	błąd parzystości RAM
1 długi 2 krótkie	błąd karty graficznej
1 długi 3 krótkie	błąd pamięci karty graficznej lub jej brak
Powtarzający	błąd pamięci RAM
Zmienny niski i wysoki	błąd procesora
Podczas pracy komputera	przegrzanie procesora

AMI BIOS, sygnalizacja błędów

Rodzaj dźwięku	Znaczenie
1 krótki	błąd odświeżania pamięci RAM
2 krótkie	błąd parzystości pamięci RAM
3 krótkie	błąd w pierwszych 64KB pamięci RAM
4 krótkie	błąd zegara systemowego lub pierwszego wtyku pamięci
5 krótkich	błąd procesora
6 krótkich	błąd kontrolera klawiatury
7 krótkich	błąd trybu wirtualnego procesora
8 krótkich	błąd I/O pamięci karty graficznej
9 krótkich	błąd sumy kontrolnej BIOS-u
10 krótkich	błąd rejestru I/O pamięci CMOS
11 krótkich	błąd pamięci cache L2 procesora
1 długi, 2 krótkie	błąd karty graficznej
1 długi 3 krótkie	błąd pamięci RAM
1 długi 8 krótkie	problemy związane z wyświetlaniem obrazu przez kartę graficzną
Ciągły dźwięk	brak pamięci RAM lub karty graficznej

Phoenix BIOS, sygnalizacja błędów cz.1

Rodzaj dźwięku	Znaczenie
1-1-2	błąd procesora lub gdy niski ton błąd płyty głównej
1-1-3	błąd pamięci CMOS
1-1-4	błąd parzystości pamięci RAM
1-2-1	błąd zegara systemowego
1-2-2	błąd kontrolera DMA
1-2-3	błąd kontrolera DMA
1-3-1	błąd dotyczący odświeżania pamięci RAM
1-3-2	błąd testu pamięci RAM
1-3-3	błąd pierwszego wtyku pamięci RAM
1-3-4	błąd parzystości pamięci RAM w pierwszych 64 KB
1-4-1	błąd linii adresowej pamięci
1-4-2	błąd parzystości pamięci RAM
1-4-3 / 1-4-4	błąd magistrali EISA
2-x-x	błąd pamięci RAM
3-1-1	błąd kontrolera DMA (Slave)
3-1-2	błąd kontrolera DMA (Master)

Phoenix BIOS, sygnalizacja błędów cz.2

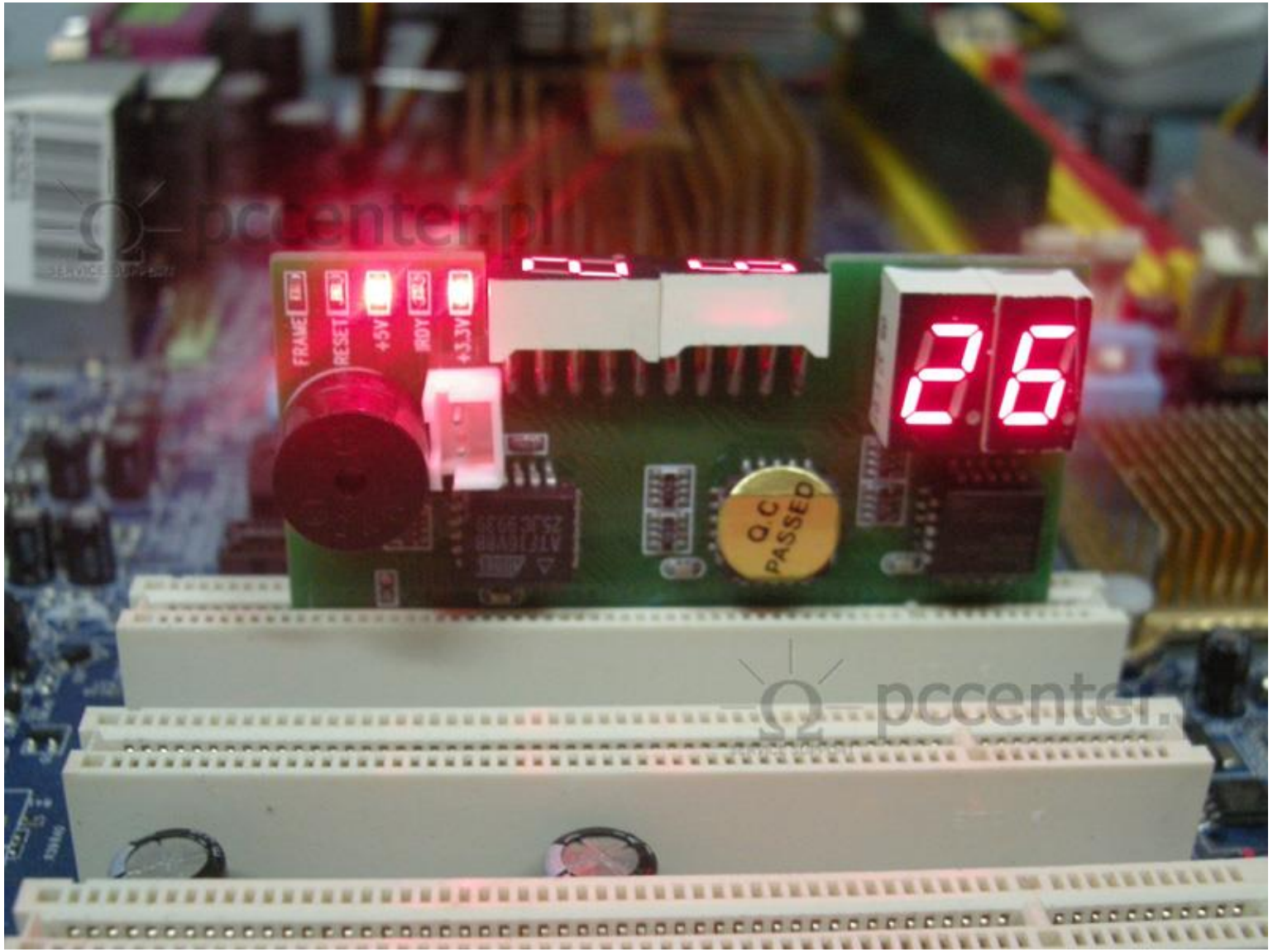
Rodzaj dźwięku	Znaczenie
3-1-3	błąd kontrolera przerwań (Master)
3-1-4	błąd kontrolera przerwań (Slave)
3-2-4	błąd kontrolera klawiatury
3-3-1	wyczerpała się bateria CMOS
3-3-2	błąd pamięci CMOS
3-3-4	błąd karty graficznej
3-4-1	błąd karty graficznej
4-2-1	błąd zegara systemowego
4-2-2	błąd pamięci CMOS
4-2-3	brak połączenia z klawiaturą
4-2-4	przerwany test procesora
4-3-1	błąd podczas testu pamięci RAM
4-3-3	błąd zegara systemowego
4-3-4	błąd zegara czasu rzeczywistego
4-4-1	błąd portu szeregowego
4-4-2	błąd portu równoległego
4-4-3	błąd procesora

Karta POST

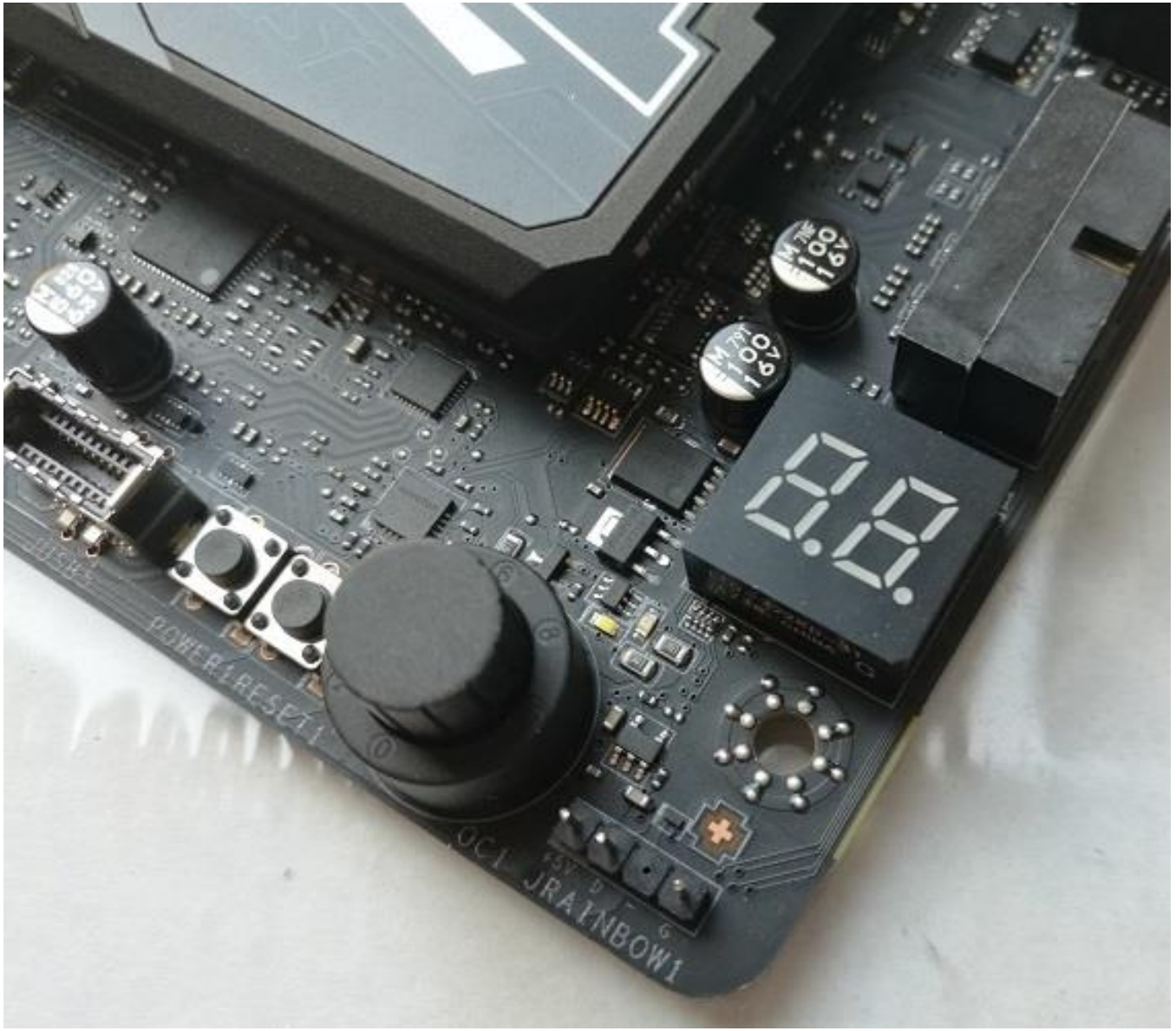
- BIOS w trakcie testowania systemu zapisuje rezultaty do portu 0x80. (wysyła do niego kody diagnostyczne POST).
- Karta POST służy do zbierania informacji o przebiegu testowania komputera przez BIOS.

- Informacje są zapisywane do portu, na co reaguje odpowiednia karta podłączona do komputera. Karta pozwala na znalezienie błędów płyty głównej.
- Kartę wpina się do portu PCI, PCI-Express lub miniPCI.
- Karty POST bywają wykorzystywane przez programistów. Jeżeli piszą programy systemowe działające w trybie pełnych uprawnień do procesora, wysyłają różne wartości do karty POST i na podstawie tych informacji testują swoje programy.

Karta POST



Płyta główna z sygnalizatorem POST



https://i.pcmag.com/imagery/articles/03GaWBJDU6tulmVetkPtzNp-24..1569470613.jpg

AKTUALIZACJA BIOSU

Powody aktualizacji BIOSU

- Nowe rozwiązania techniczne
  - Nowe generacje procesorów
  - Szybsze protokoły komunikacyjne (Thunderbolt, USB 3.2, USB 4)
  - Obsługa nowych standardów
  - Lepsza współpraca z pamięcią RAM
  - System nie obsługuje dużych dysków
- Błędy w pracy płyty głównej
  - Istotne usterki w pracy systemu
  - Usuwanie luk w zabezpieczeniach
- Poszerzenie umiejętności informatycznych

Sposoby aktualizacji

Aktualizacja dla Windows 7 i nowsze

- Ustalenie modelu płyty głównej
  - Dokumentacja płyty głównej
  - Napis pojawiający się przy starcie komputera
  - Program do badania zawartości komputera lub aktualizacji BIOSu
- Ściągnięcie pliku z nowym BIOSem
- Użycie programu do aktualizacji BIOSu
  - Operacja ta może być dokonana z poziomu systemu operacyjnego
- Program robi kopię starej wersji i nadpisuje BIOS nową wersją.
- Po restarcie komputer powinien już korzystać z nowej wersji BIOSu.

Aktualizacja dla starszych modeli

- Starsze modele wymagały aktualizacji z dyskietki (lub później z CD lub pendrive'a)
- Konieczne były 2 dyskietki:
  - Systemowa
  - Pusta na którą nagrywało się program i obraz BIOSu.
- W ustawieniach BIOSu trzeba było wyłączyć opcję "*System BIOS Cacheable*"(wyłączenie kopiowania BIOSu do pamięci RAM)
- Uruchomienie systemu z dyskietki startowej
- Po ukazaniu się znaku zachęty A:\ wkładamy do stacji drugą dyskietkę.
- W tym momencie trzeba zrobić kopię aktualnego obrazu BIOSu (niekonieczne, ale przydatne).
  - Większość programów do aktualizacji BIOSu ma taką opcję.
  - Spowoduje to utworzenie na dyskietce nowego pliku (na przykład o nazwie backup.bin).
- Uruchom program do aktualizacji BIOSu.
  - Całą procedura wgrywania nowego BIOSu do pamięci flash trwa około kilkanaście sekund.
- Przy braku problemów uruchom komputer ponownie.

Aktualizacja starych komputerów

- Jeżeli układ scalony jest wlutowany w płytę główną trzeba go wylutować lub kupić nową płytę główną.
- W wypadku nieprogramowalnych układów należy wymienić na nowe u producenta.

Problemy aktualizacji

- Niezgodność z systemem operacyjnym
  - Konieczność reinstalacji OS
- Nie wykrycie nowego BIOSu
  - Przywrócenie starej wersji
- Problemy z BIOSem
  - Przywrócenie ustawień fabrycznych

Programy do identyfikacji i aktualizacji BIOSu

- Programy dostarczane przez producentów BIOSu
  - **AwdFlash** - program firmy Award
  - **AmiFlash** - program firmy American Megatrends
  - **AMI Motherboard Identification Utility**
- Programy dostarczane przez producentów płyt głównych
  - **AFlash** - program firmy ASUS
- Programy uniwersalne
  - **Unicore BIOS Agent**
  - **CTBIOS**
  - **UniFlash** - uniwersalny program do uaktualniania BIOSu, dostępny razem z kodem źródłowym

UniFlash


UniFlash v1.28 (c) 2002 Rainbow Software (http://rainbow.ht.st)
Original version by Pascal van Leeuwen & Galkowski Adam
(1F08,FFFF) Flash ROM chip: Atmel AT49x002(N)T series (5V/3V/2.7V)
Organisation: sectored: 1x128k,1x96k,2x8k,1x16k (256K)
PCI chipset: VIA Apollo Pro (Plus/133(A|T))
Last write status: not available
Write backup BIOS image to file
Flash BIOS image file to Flash ROM
Flash backup BIOS image to Flash ROM
Redetect Flash ROM
CMOS submenu
ESCD (PnP) submenu
ADVANCED submenu
Quit
ROM base: FFFC0000, memory dump at FFFC0000-->(ED246C2D)

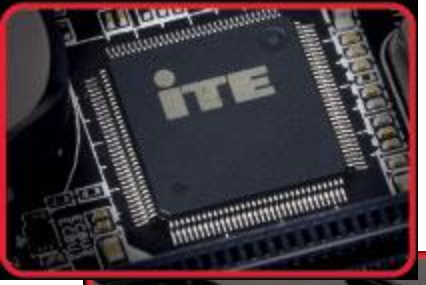
GIGABYTE @BIOS

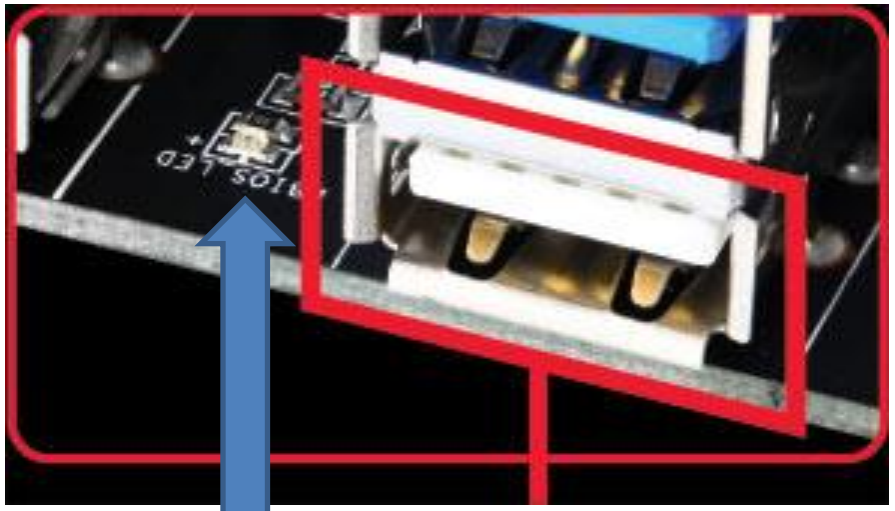
- GIGABYTE @BIOS to oprogramowanie w Windows do aktualizacji BIOS.
  - Potrafi ściągnąć właściwą wersję z Internetu i zainstalować ją automatycznie.
  - Wykrywa model płyty głównej i pomaga dobrać odpowiednią wersję BIOS-u.

Q-Flash Plus

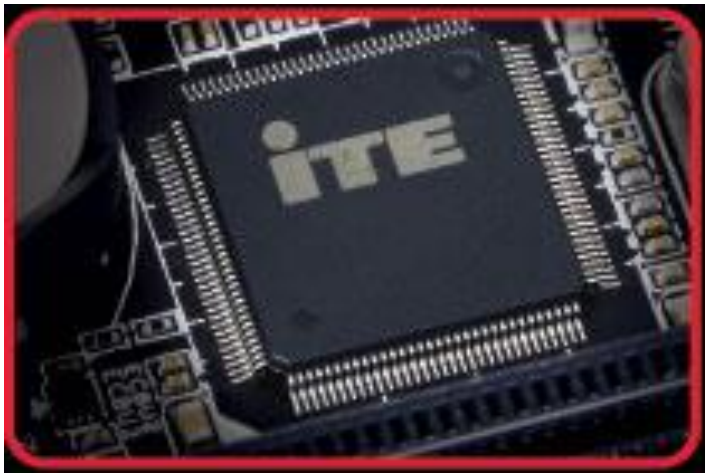
- Q-Flash Plus to technologia pozwalająca na aktualizację płyty głównej bez zainstalowanego procesora lub pamięci RAM.
  - Wymaga podłączenia do zasilania
- Stosowane w sytuacji, gdy płyta główna nie jest w stanie obsłużyć najnowszego procesora lub nowych kości pamięci.
- BIOS jest aktualizowany z zewnętrznego napędu USB.
  - Pendrive należy wcześniej skonfigurować w innym komputerze. Skopiować na niego plik z obrazem BIOSu.
  - Gotowy pendrive należy umieścić w specjalnym gnieździe USB na aktualizowanej płycie.
  - Kontroler automatycznie rozpozna nośnik USB w gnieździe i rozpocznie aktualizację.
  - Zakończenie aktualizacji zostanie zasygnalizowane świeceniem się odpowiedniej diody LED.
  - Po restarcie płyta będzie korzystać już z nowego BIOSu
- Rozwiązanie stworzone przez firmę Gigabyte po raz pierwszy dla płyt z chipsetem X99.
  - Wykorzystuje specjalny kontroler ITE EC 8951E.

Q-Flash Plus





Q-Flash USB Port



Q-Flash Plus kontroler

Q-Flash Plus LED sygnalizator

PROBLEMY BIOSU

Powody awarii BIOSu

- Atak wirusa,
- Niewłaściwa aktualizacja,
- Przerwa w dostawie prądu w czasie aktualizacji,
- Zapisanie innego BIOSu niż być powinien,
- Inne eksperymenty (edycja itd.)

Wirusy atakujące BIOS

- Ponieważ Flash-BIOS można zapisywać to również może to zrobić szkodliwe oprogramowanie.
- Najczęściej wirus kasuje zawartość BIOSu blokując działanie komputera.
- Znanych jest co najmniej pięć wirusy atakujących BIOS:
  - CIH (Czernobyl)
  - Demonstracyjny wirus autorstwa John Heasmana
  - Demonstracyjny wirus – autorzy: Anibal Sacco i Alfredo Orteg
  - Mebromi
  - Lojax (UEFI)

CIH

- Wirus CIH był znany jako Czernobyl. Powodem była data ataku 26 kwietnia 1999 roku – 13 rocznica wybuchu w elektrowni atomowej w Czernobylu.
  - Napisany został rok wcześniej, ale potrzebował czasu na powielenie się.
- Był to bardzo groźny wirus.
  - Infekował pliki wykonywalne *.exe systemów Windows 32-bitowych z rodziny Windows 95. Po uruchomieniu zarażonego programu, wirus zarażał komputer przez zagnieżdżenie się w pamięci. 26-tego każdego miesiąca kasuje te pliki.
  - Mógł zniszczyć zawartość BIOSu, jeżeli ten znajdował się w kości typu Flash, unieruchamiając w ten sposób płyty główne.
  - Dotyczyło to zwłaszcza płyt z czipsetem Intel i430TX. Windows 95 pozwalał wszystkim programom na bezpośredni dostęp do warstwy sprzętowej (a więc i BIOSu).
- Po około roku od pojawienia się wirusa, 26 kwietnia 1999 roku „bomba” w kodzie wirusa wywołała komputerową katastrofę.
  - Około miliona komputerów zostało uszkodzonych z powodu infekcji: we wszystkich przypadkach utracono dane na dysku twardym, w wielu zniszczony został FlashBios na płycie głównej oraz dyski twarde.

CIH

- Został napisany przez Chen Ing Hau (陳盈豪) z Tajwanu. We wrześniu 2000 roku został aresztowany za szkody wyrządzone przez jego wirusa. Otrzymał 5 lat więzienia.

http://www.sophos.com/images/eng/misc/cihauthor.jpg

Dysk zaatakowany przez wirus CIH

http://news.bbc.co.uk/olmedia/325000/images/_327903_cih_300.j

Mebromi

- Mebromi to pierwszy (działający w prawdziwym świecie) wirus atakujący przede wszystkim BIOS.
- Atakuje tylko BIOS firmy Award.
  - Dogrywa do niego szkodliwe oprogramowanie pozwalające mu modyfikować sektor MBR.
  - Dzięki temu może infekować procesy *winlogon.exe* lub *winnt.exe* podczas uruchamiania systemów z rodziny Windows NT.
  - Kolejnym krokiem jest ściągnięcie z Internetu rootkita, który zapobiegnie wyczyszczeniu rekordu startowego przez program antywirusowy.
- Całość procesu odbywa się po każdym uruchomieniu komputera.

Lojax.A

- Lojax to pierwszy wirus atakujący UEFI.
- Wirus zagnieżdża się w jednym z układów scalonych na płycie głównej komputera, gdzie przechowywane jest UEFI.
  - LoJax, po przejęciu kontroli nad systemem operacyjnym, nadpisuje UEFI złośliwym kodem.
  - Za każdym razem gdy użytkownik uruchamia komputer, aktywuje (konia trojańskiego) w systemie operacyjnym.
  - Ten komunikuje się z serwerem cyberprzestępców C&C i pobiera z niego, a następnie instaluje w systemie docelowe zagrożenie.
- Autorem Lojaksa jest grupa cyberprzestępcza Sednit (znana też jako APT28, Fancy Bear, Sofacy lub STRONTIUM), która ma na swoim koncie ataki na placówki dyplomatyczne i instytucje finansowe na całym świecie. Wirus atakuje głównie użytkowników z Europy Środkowej i Wschodniej.
- Ochrona UEFI
  - Formatowanie dysku, a nawet jego wymiana, nie eliminują wirusa z zainfekowanego komputera. Wirus ukrywa się w układzie scalonym płyty głównej.
  - Konieczny jest antywirus mający możliwość analizy i zabezpieczenia przed infekcją UEFI. Przykładem jest produkt firmy ESET.
- Jedynym skutecznym sposobem usunięcia **Lojax.A** jest przywrócenie UEFI do ustawień fabrycznych, czyli tzw. *reflashing firmware*.

Zagrożenia

- Niektóre programy antywirusowe nie są w
- stanie sprawdzić BIOSu.
- Wyczyszczenie dysku, a nawet jego wymiana nie gwarantuje usunięcia szkodnika.
- Mogą ominąć niektóre zabezpieczenia (hasła, szyfrowanie plików).
- Mogą być wbudowane na etapie produkcji.
- EFI mające być jednolitym standardem to dobre środowisko dla nowych wirusów.

Przeciwdziałanie

- Mnogość typów płyt głównych i BIOSów utrudnia działanie wirusów ograniczanych do danego typu układu i BIOSu.
- Niektóre płyty główne mają zworkę uniemożliwiającą aktualizację BIOSu.
- Wgranie firmware'u od nowa.

Pierwsza pomoc

Reanimacja BIOSu

- Jeśli przydarzyła nam się jakaś awaria to na pewno zauważymy.
  - komputer prawdopodobnie się nie uruchomi.
- Jeśli na samym początku uruchomienia pali się kontrolka w stacji dyskietek, to znaczy że zachował się tzw. „Boot Block” i reanimacja jest możliwa.
- Aby jej dokonać należy przygotować dyskietkę „do przywracania BIOSa”.
- Dysk należy włożyć do komputera i odpalić sprzęt.
- Powinien się rozpocząć automatyczny „recover”.
- Po skończonej operacji nastąpi długi pisk.
- Włączamy ponownie komputer i mamy z powrotem naszego starego BIOSa.

Hot Swapping

- W wypadku awarii BIOSu można spróbować zapisać go „na gorąco” (Hot Swapping).
- Należy znaleźć kogoś, kto ma dokładnie ten sam typ płyty głównej.
- Warunkiem operacji jest zabranie układu scalonego z BIOSem i dyskietki ratującej.

1. Należy zdjąć obudowę komputera i uruchomić go.
2. W BIOSie należy zmienić opcje ‘System BIOS Cacheable’ i ‘Video BIOS Cacheable’ (obydwie na Enabled).
3. Wkładamy dyskietkę, restartujemy komputer i uruchamiamy system z dyskietki.
4. Kolejny krok to uruchomienie programu do flash-u i zrobienie kopii BIOSu do nowego pliku (np. bios_kopia.bin).
5. Ponowne uruchomienie programu ma za zadanie zapisanie tej kopii do kości BIOSu. Program *czeka* na odpowiedź, czy ma zapisać dane z pliku do BIOS-u.
6. W tym momencie następuje najważniejszy moment procesu. **Cały czas *przy włączonym komputerze wyjmujesz kość* układu scalonego BIOS-u kumpla a na jego miejsce *wstawiasz* swoją**.
7. Dopiero w tym momencie wciskasz ‘Y’ na zezwolenie zaprogramowania.
8. Komputer nie powinien się zorientować na "podmiance" i zapisze dane już do Twojego BIOS-u.
9. Po zapisaniu uruchamia ponownie komputer sprawdzając, czy BIOS został zapisany i czy jest sprawny.
10. Jeśli tak, wyłączamy komputer i bierzemy BIOS do domu.

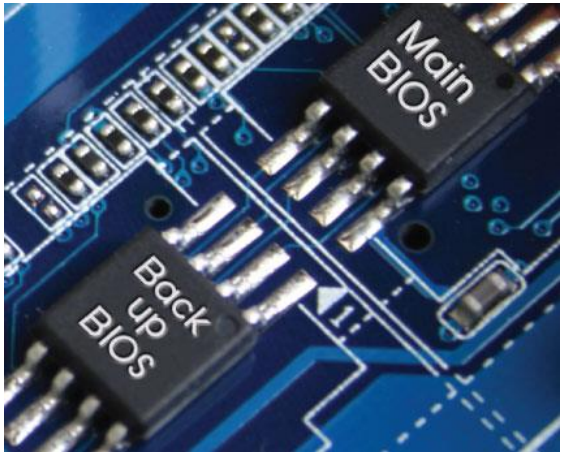
Systemy ochrony BIOSu

- Dual BIOS,
- Quad BIOS,
- DieHard BIOS

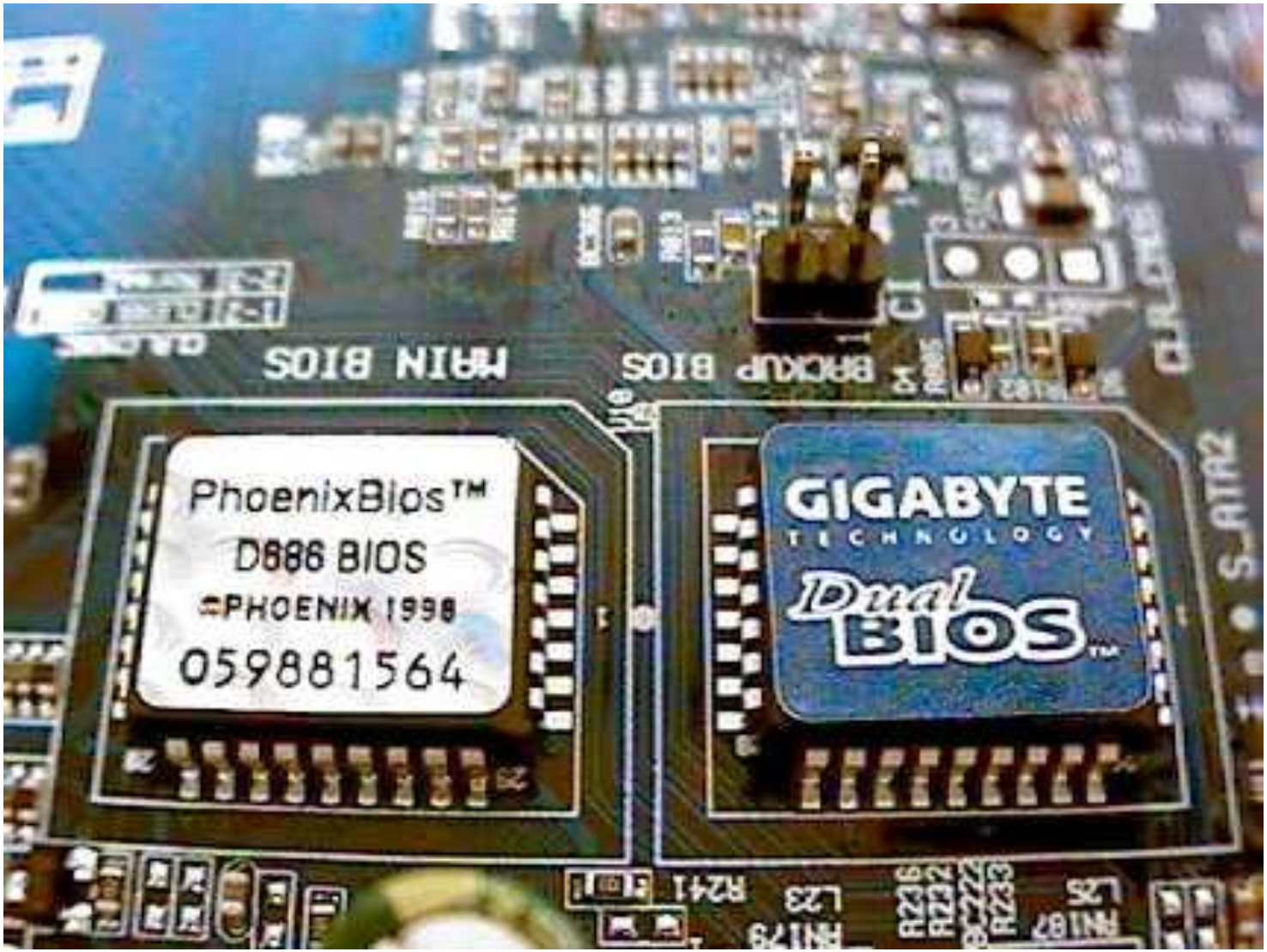
Dual BIOS

- Dual BIOS™ to dwa oddzielne układy BIOS na płycie głównej, z których jeden pełni rolę "głównego", drugi natomiast jest układem "zapasowym".

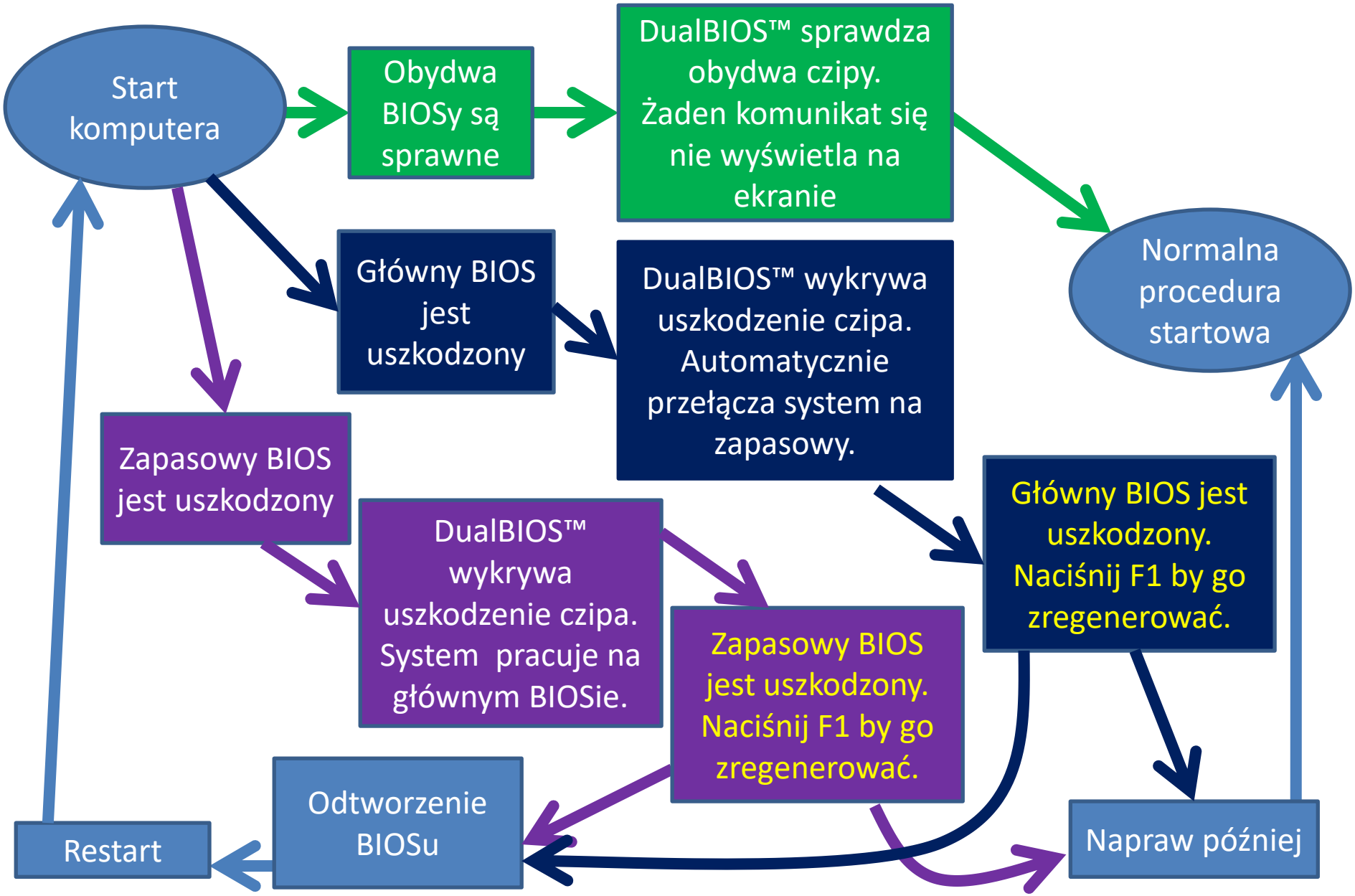
- Gdy "główny" chip ulegnie uszkodzeniu, "zapasowy" automatycznie przejmuje jego zadania.
  - Możliwe jest uruchomienie systemu komputerowego i dalsze działanie bez konieczności wymiany uszkodzonego BIOS-u.
- Proces przywracania operatywności systemu jest automatyczny i niemal natychmiastowy.



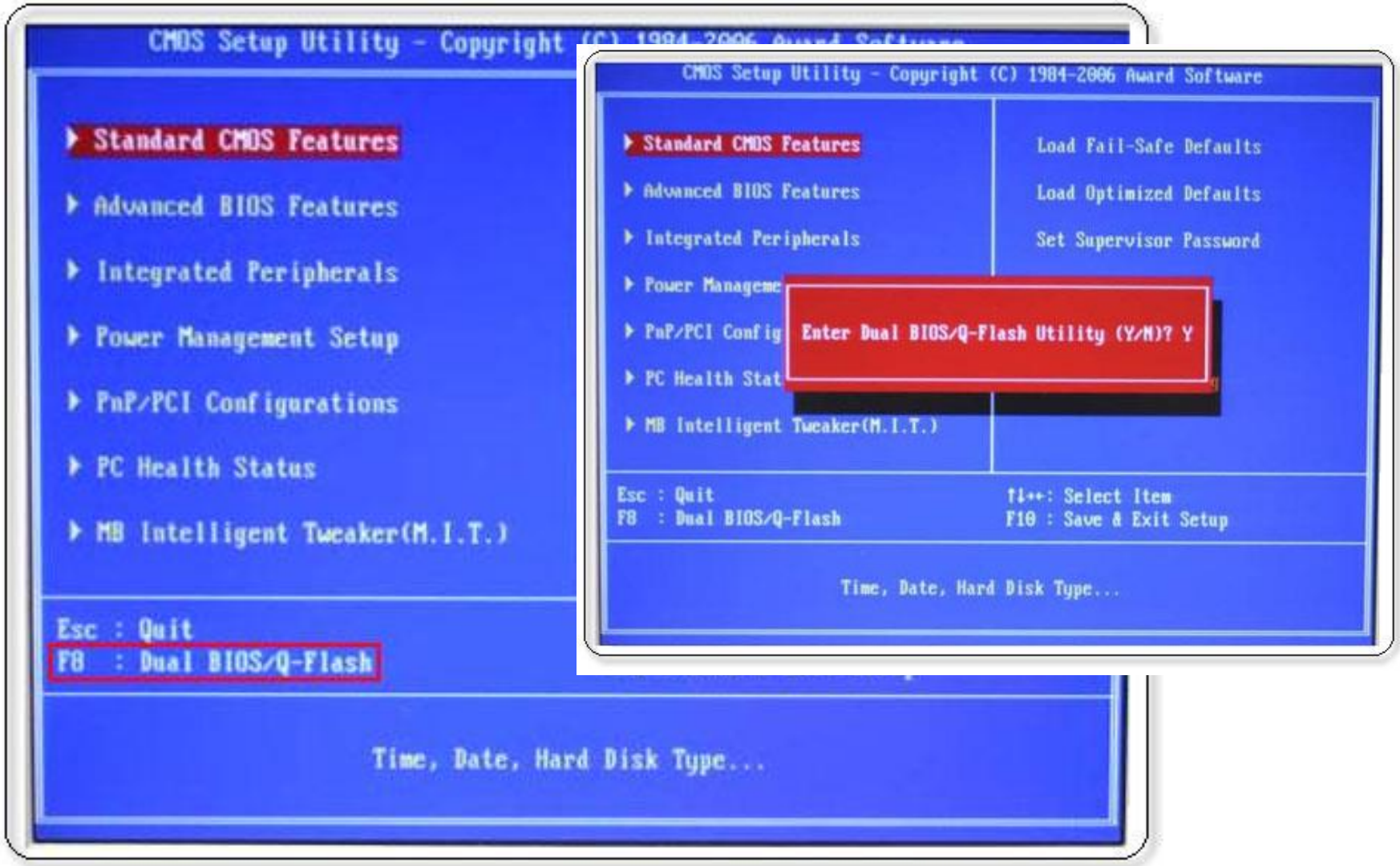
Dual BIOS


MAIN BIOS
BACKUP BIOS
PhoenixBios™
D686 BIOS
PHOENIX 1998
059881564
GIGABYTE
TECHNOLOGY
Dual
BIOS™

Jak działa Dual BIOS?



Dual BIOS


CMOS Setup Utility - Copyright (C) 1984-2006 Award Software
Standard CMOS Features
Advanced BIOS Features
Integrated Peripherals
Power Management Setup
PnP/PCI Configurations
PC Health Status
MB Intelligent Tweaker(M.I.T.)
Esc : Quit
F8 : Dual BIOS/Q-Flash
Time, Date, Hard Disk Type...
CMOS Setup Utility - Copyright (C) 1984-2006 Award Software
Standard CMOS Features
Advanced BIOS Features
Integrated Peripherals
Power Manageme
PnP/PCI Config
PC Health Stat
MB Intelligent Tweaker(M.I.T.)
Load Fail-Safe Defaults
Load Optimized Defaults
Set Supervisor Password
Enter Dual BIOS/Q-Flash Utility (Y/N)? Y
Esc : Quit
F8 : Dual BIOS/Q-Flash
↑↓++: Select Item
F10 : Save & Exit Setup
Time, Date, Hard Disk Type...

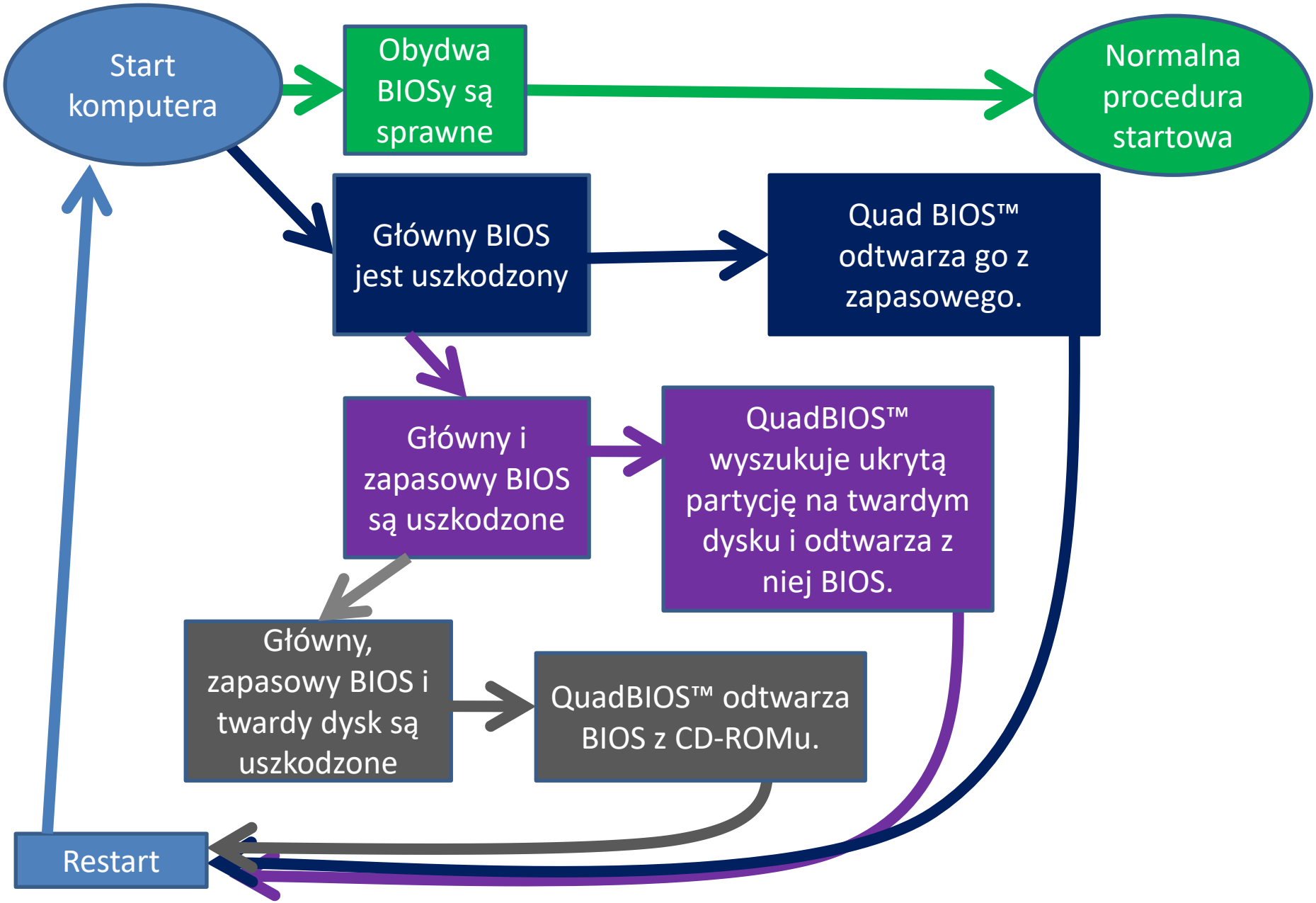
Zalety i wady Dual BIOSu

- Zalety technologii DualBIOS™:
  1. Natychmiastowa naprawa BIOSu
  2. Nie wymaga ingerencji użytkownika
  3.Minimalny czas naprawy

QuadBIOS

- Quad BIOS – rozwiązanie firmy Gigabyte tworzące cztery kopie zawartości BIOSu.
  - na płycie głównej znajdują się dwa układy BIOS, zawierające dwie kopie programu BIOS;
  - trzecią kopię oprogramowanie zapisuje na dysku twardym,
  - Czwartą umieszczono na płycie CD.
- Quad BIOS łączy rozwiązania
  - DualBIOS™
  - i Express BIOS Rescue Technology

Jak działa QuadBIOS?



Quad BIOS

GIGABYTE

6-QUAD

Motherboard

Ultra Durable 2

Quad BIOS | Quad Cooling | Quad eSATA 2 | Quad Triple Phase | Quad Core Optimized | Quad DDR3 Slots

<TAB>:POST Screen<DEL>:BIOS Setup/Q-Flash<F9>:XpressRecovery2<F12>:Boot Menu<End>:Qflash

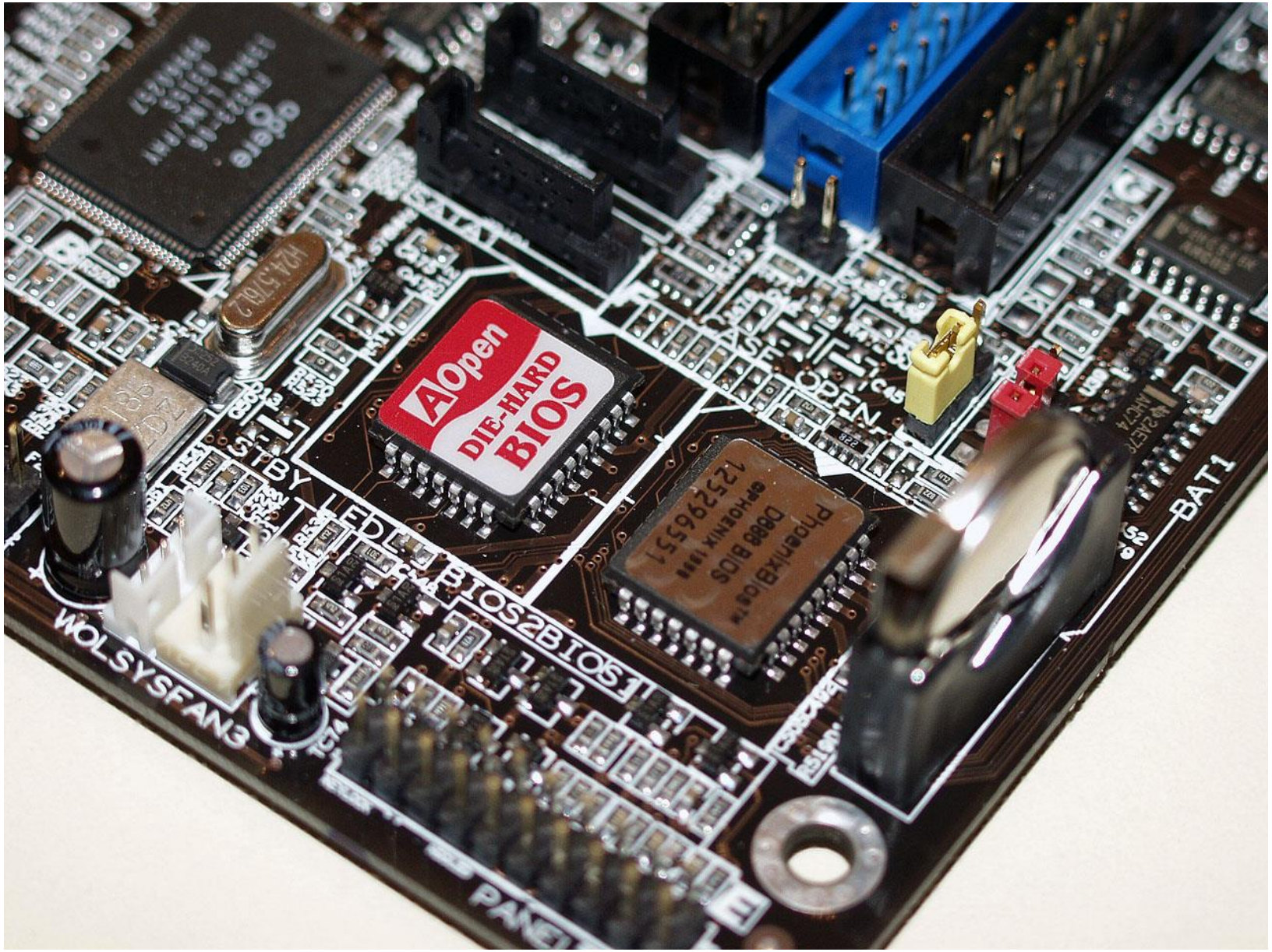
Die-Hard BIOS

- Na płytach głównych AOpen firmy ASUS znajdują się 2 układy BIOS.
- W razie awarii jednego z nich, użytkownik naciska przycisk, który kopiuje zawartość sprawnego do uszkodzonego.

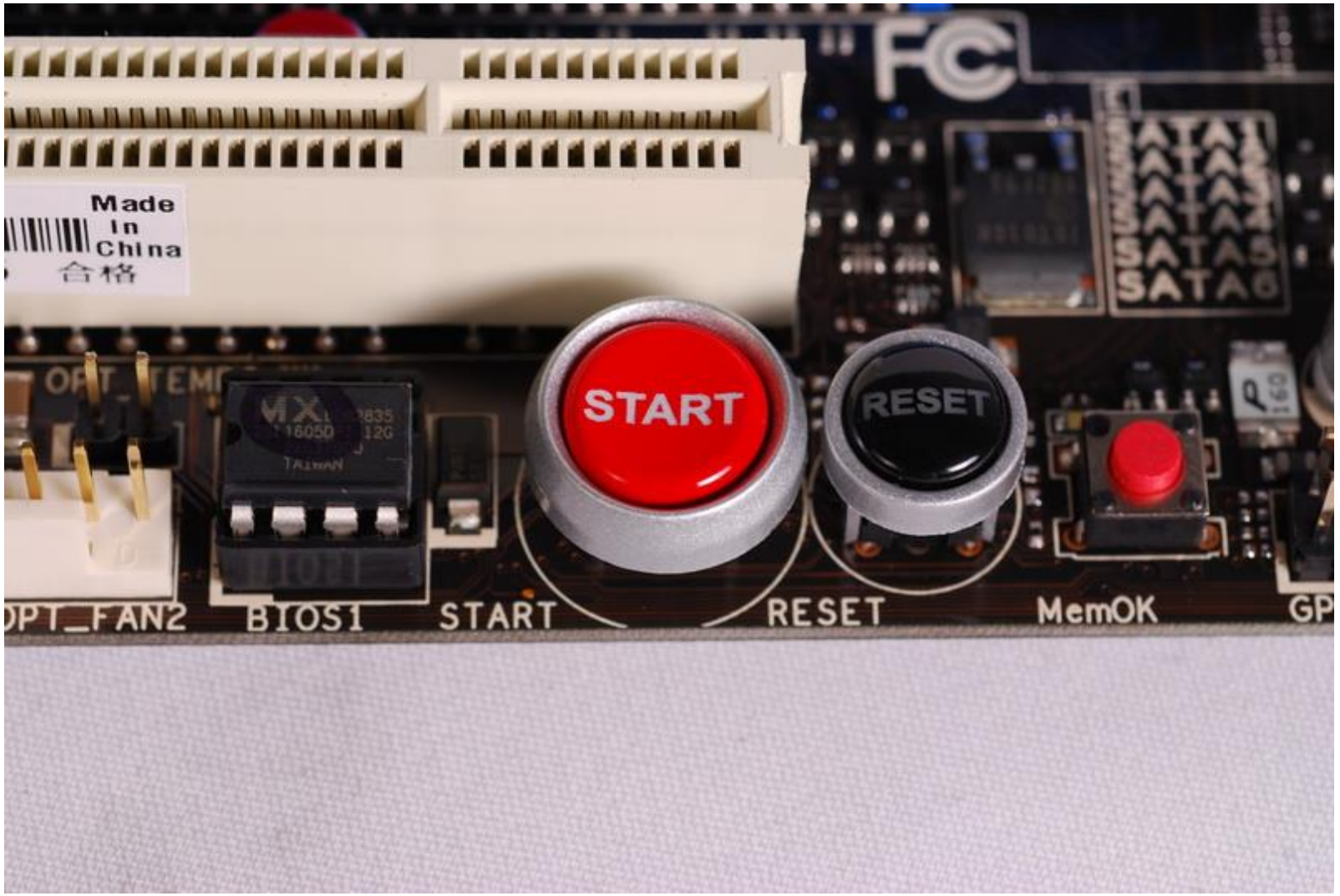
Die-Hard BIOS

- Na płytach głównych AOpen firmy ASUS znajdują się 2 układy BIOS.
- W razie awarii jednego z nich, użytkownik naciska przycisk, który kopiuje zawartość sprawnego do uszkodzonego.

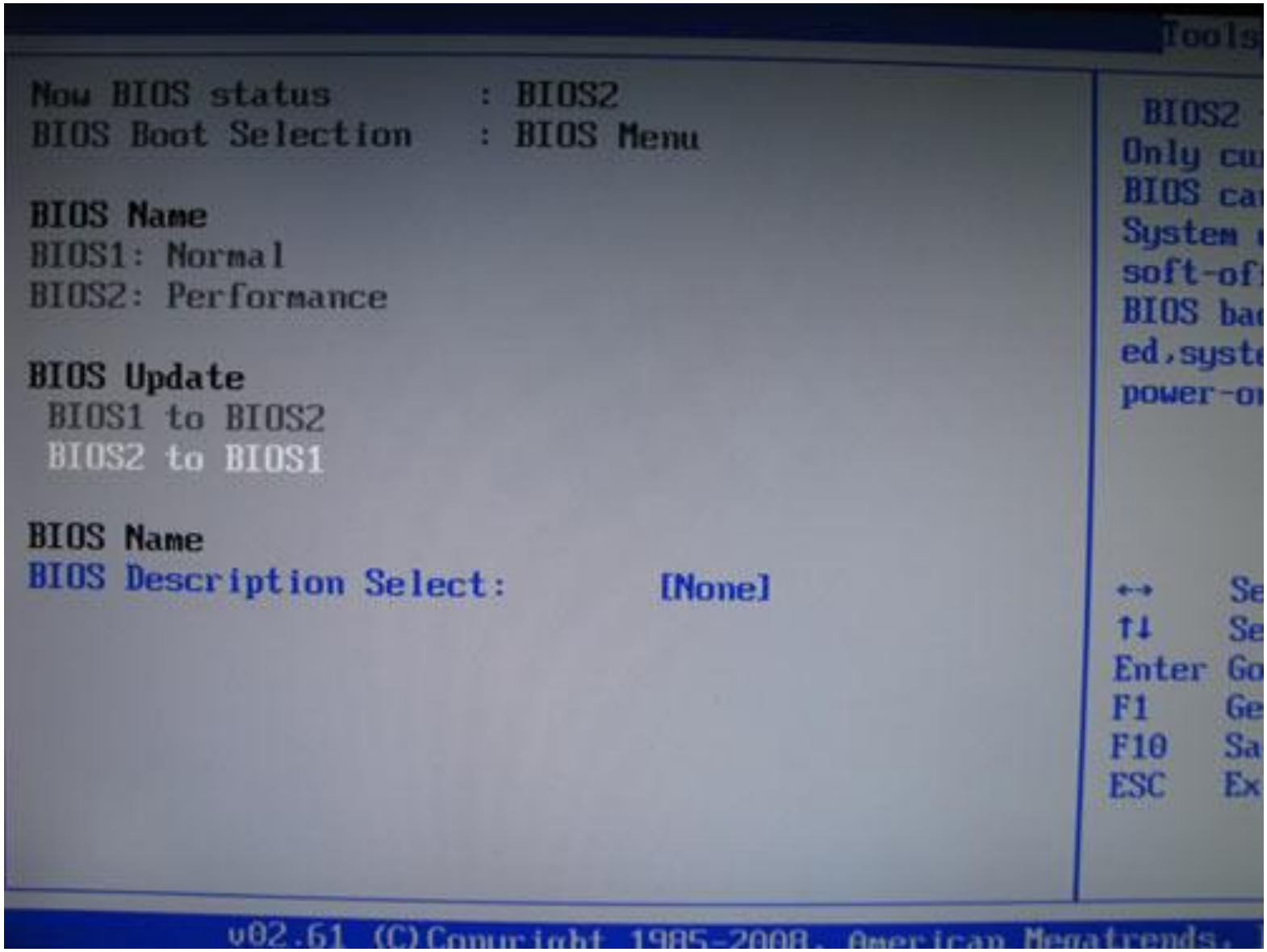
Die-Hard BIOS



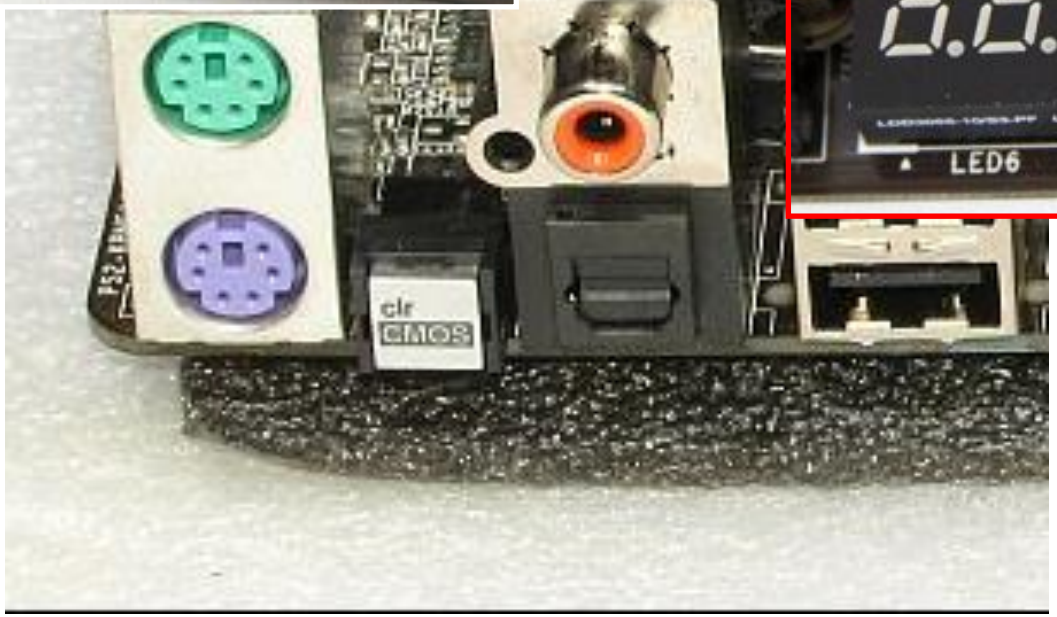
Die-Hard BIOS



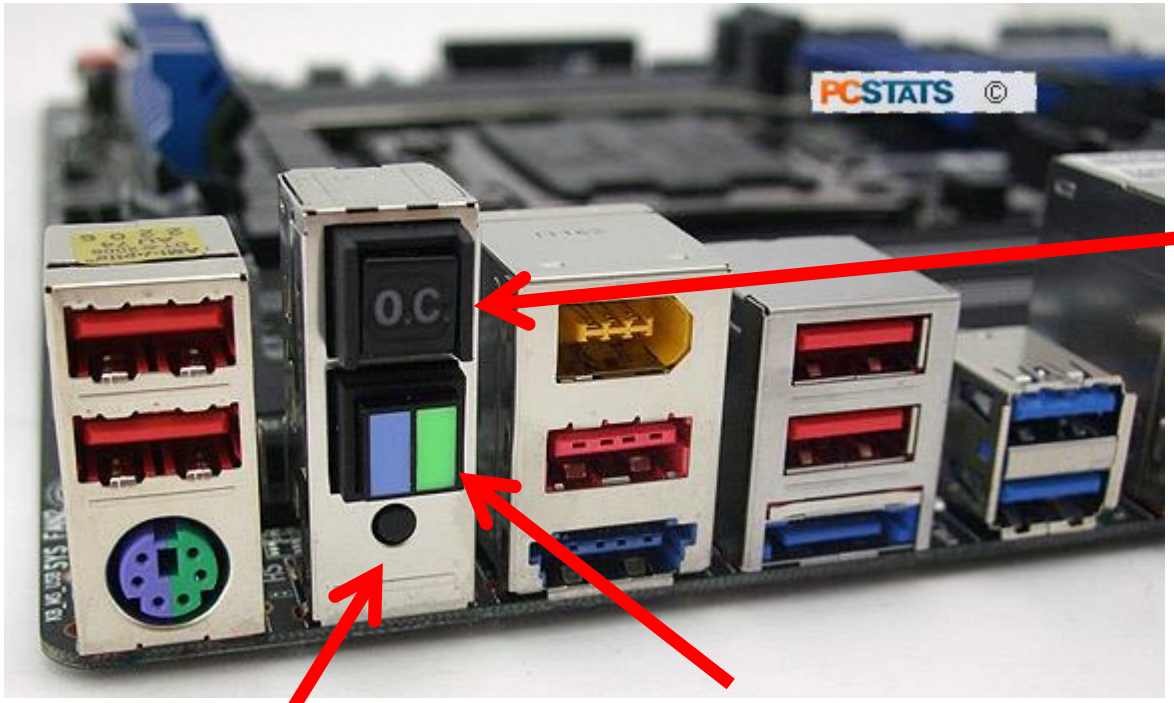
Aktualizacja BIOSu w BIOS-setup



Reset ustawień BIOSu



Reset ustawień BIOSu
Gigabyte GA-X79-UD5 Intel X79



CPU overclocking button (OC)

BIOS switch button (blue/green)

Clear CMOS jumper (small black dot)

INNE ROZWIĄZANIA

OpenBIOS

- **OpenBIOS** – wolna, przenośna wersja BIOS zawierająca zestaw instrukcji niezależnych od urządzenia.
- Pozwoli to uruchamiać system z dowolnych kart rozszerzeń.
- Ma pracować na wszystkich popularnych platformach, jak x86, Alpha, AMD64, PowerPC, ARM, Sparc, Mips IPF.
  - Serwery, stacje robocze, systemy wbudowane (zagnieżdżone)
  - Jednakowy firmware znacznie ułatwi przenośność.
- Open Firmware można znaleźć w wielu serwerach, istnieją też komercyjne implementacje SUN, Firmworks, CodeGen, Apple, IBM.

- http://www.openfirmware.info/Welcome_to_OpenBIOS

OpenBIOS


PA256 OpenBIOS Version 2.01
AOPEN INC.
Video Memory Clock : 333 MHz
Core Chip Clock : 200 MHz
Chip Voltage : 2.85 V
V-Ref Voltage : 1.25 V
Memory Voltage : 2.50 V
Boot-Up Display : TV.Monitor
TV-Out Format : NTSC-M
AGP4X Mode : Enable
AGP Sideband : Enable
Fan Speed : 4800 RPM
GPU Temperature : 45 'C
Post Up Delay : 2 Sec
Post Up Prompt : ON
Restore Setting
↑↓←→: Select & Modify
ESC : Exit Without Saving
F2 : Save & Reboot
F4 : Save & Exit Setup
F3 : Set Clock & Volt.
F5 : Load Default

ASUS AOpen Aeolus FX5600S - pierwsza karta graficzna z OpenBIOS

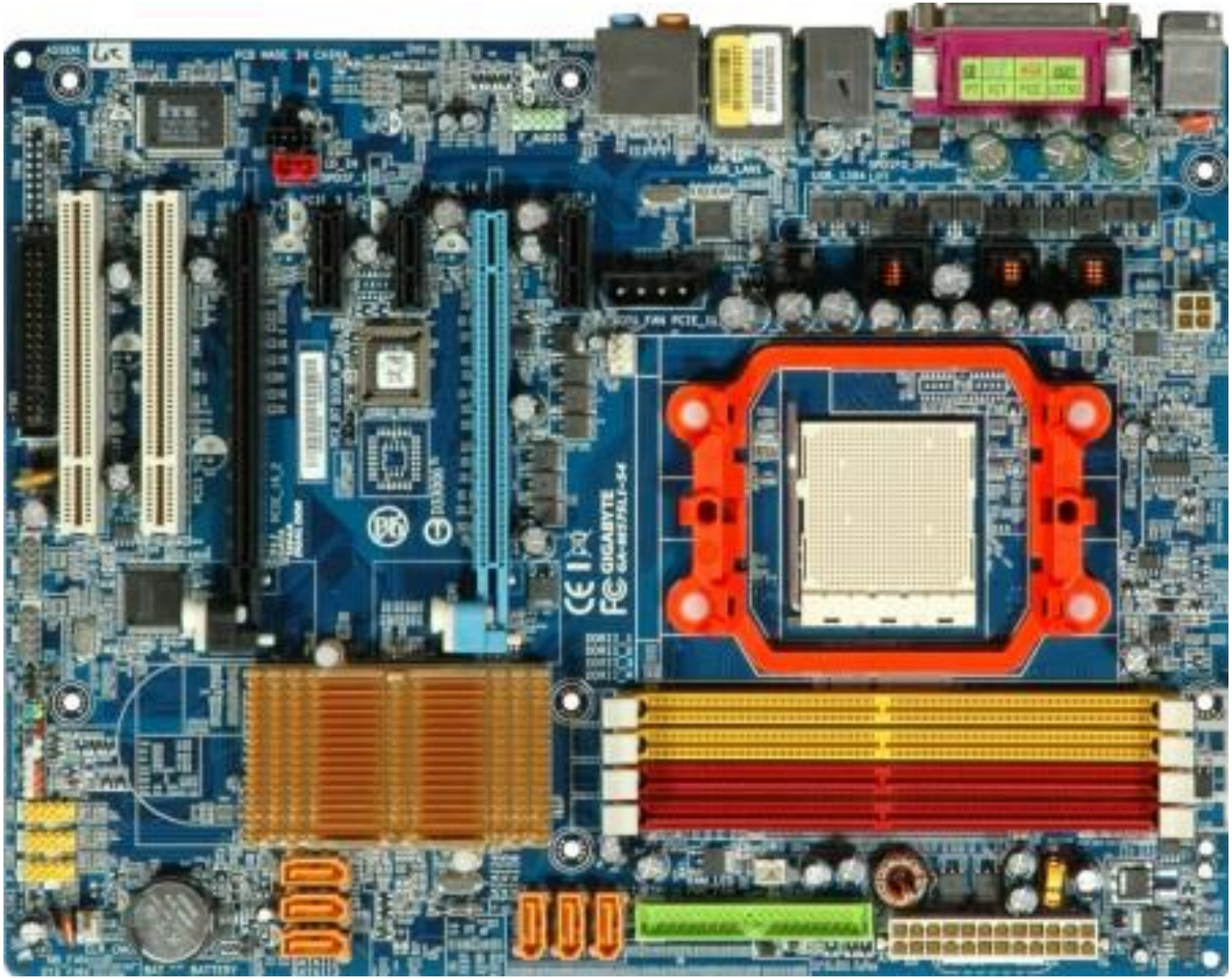
LinuxBIOS

- LinuxBIOS to nieco zmodyfikowany system operacyjny Linux zainstalowany jako BIOS na popularnych komputerach.
  - Nie różni się on bardzo od samego Linuksa, jest to dodatkowe 500 linii kodu w asemblerze i 5000 w C.
- LinuxBIOS powstał, by ułatwić zarządzanie komputerami połączonymi w klaster.
  - LinuxBIOS jest pełnym systemem operacyjnym, uruchamianym przy włączaniu komputera.
  - Nie wymaga dyskietek, ani dysków twardych
  - Pozwalana automatyzację zmiany konfiguracji na wielu komputerach
- LinuxBIOS umożliwia
  - Uruchamianie innego systemu operacyjnego przez lokalną sieć
  - Połączenia sieciowe - LinuxBIOS może otworzyć szyfrowane połączenie z innym komputerem i np. pobrać oraz załadować jądro systemu; może również korzystać z sieciowych systemów plików
  - Możliwość uruchamiania komputera bez stacji dysków, twardego dysku, napędu CD-ROM - wystarczy jedynie jednostka centralna i pamięć.
  - Szybkie uruchamianie systemu operacyjnego - udało się osiągnąć czas poniżej trzech sekund!

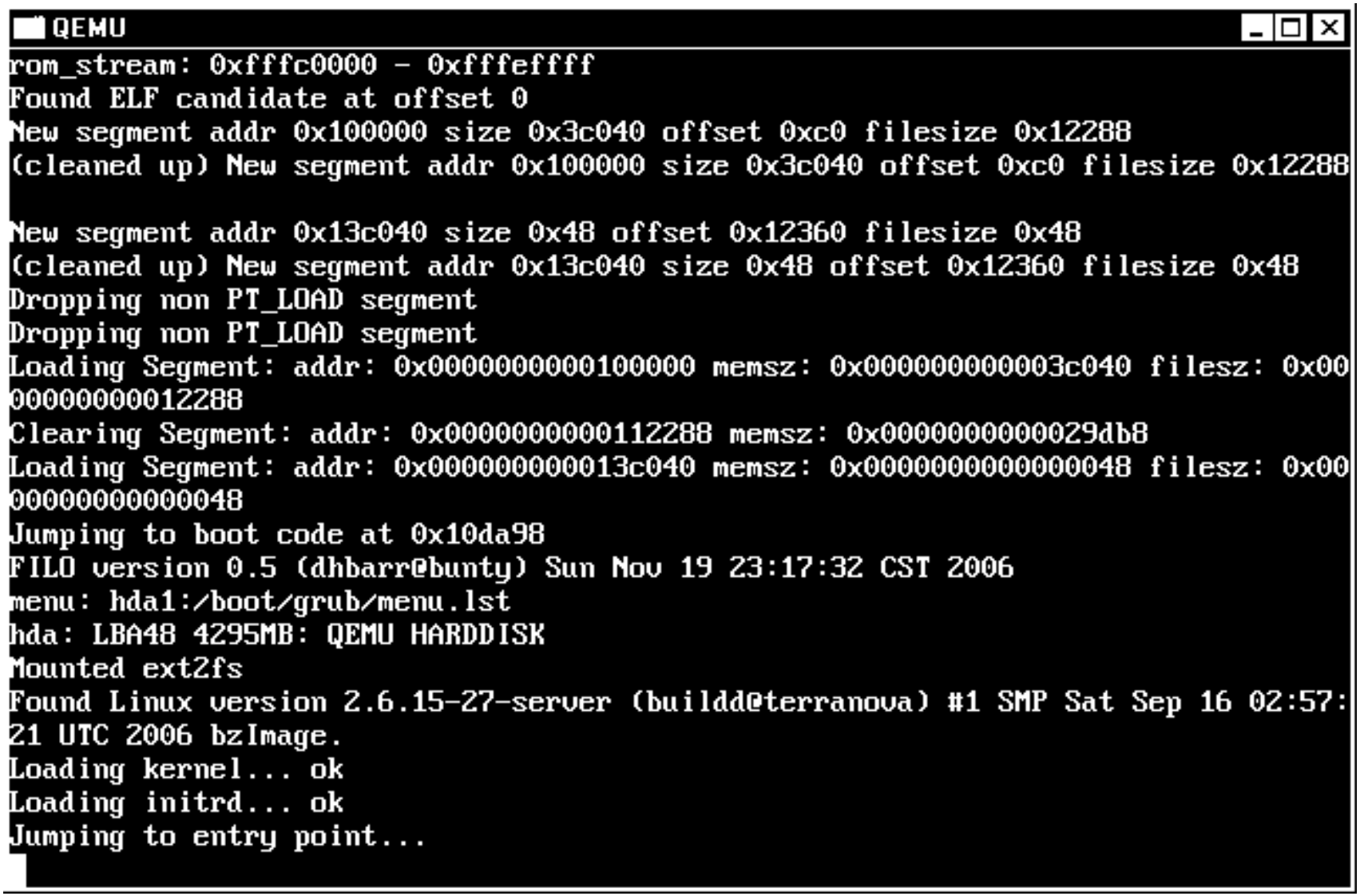
LinuxBIOS

- LinuxBIOS nie jest możliwy do zainstalowania na komputerze z dowolną płytą główną. Dzieje się tak z wielu powodów:
  - Niektóre firmy odmówiły współpracy z LinuxBIOS, brakuje dokumentacji
  - Istnieją płyty główne, w których sterowanie niektórymi urządzeniami jest bardzo trudne
  - Nie ma wystarczającej liczby chętnych do przeniesienia systemu na rzadko używane płyty główne

Gigabyte GA-M57SLI-S4
-pierwsza płyta główna na LinuxBIOS



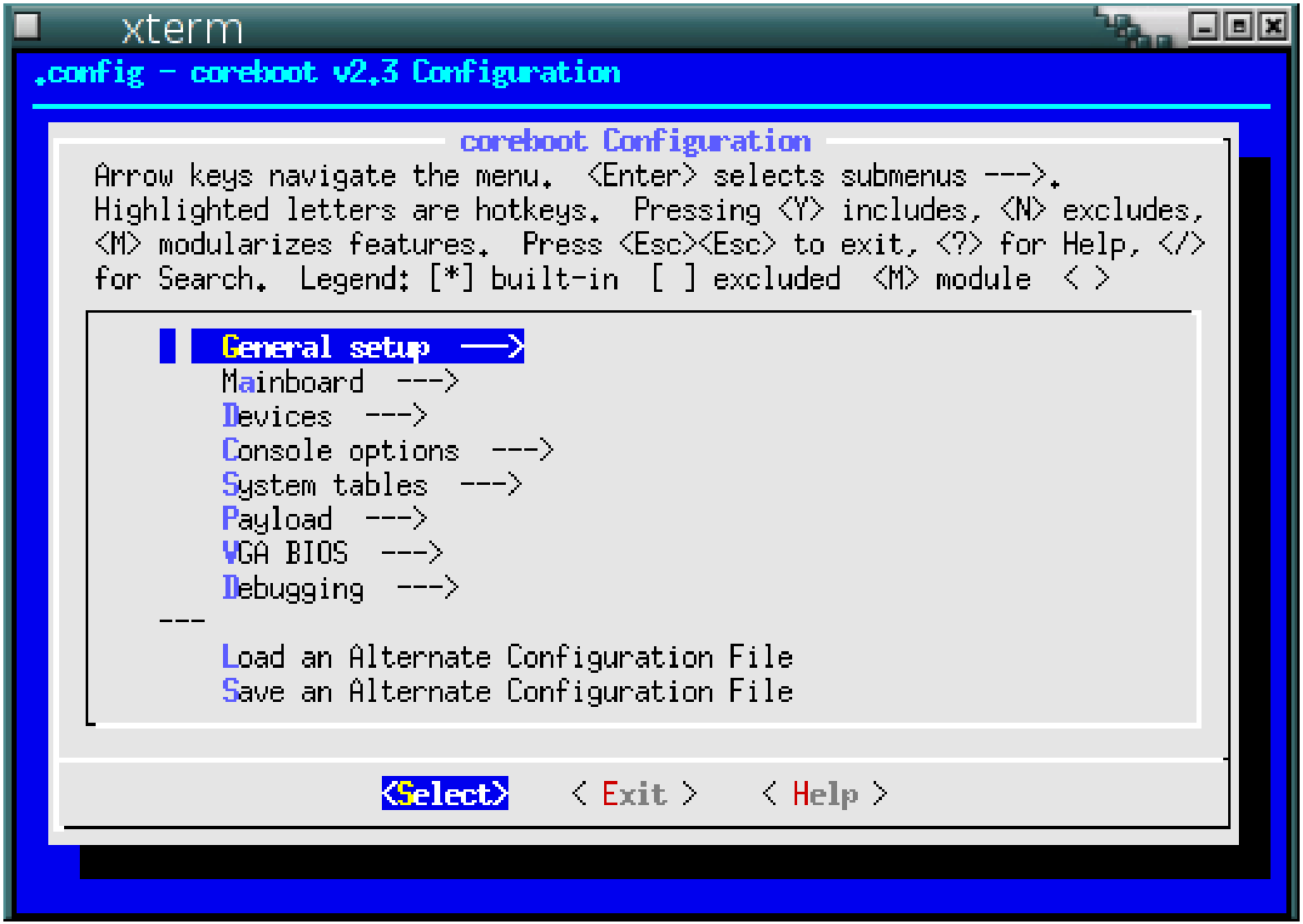
linuxbios boots qemu



Core Boot

- Coreboot to rozwinięcie LinuxBIOSu.
- Ma zastąpić tradycyjny BIOS lżejszym, otwartym oprogramowaniem. Coreboot współpracuje z 32-bitowymi i 64-bitowymi systemami operacyjnymi.
- Zrywa z kompatybilnością z tradycyjnym, 16-bitowym BIOSem.
  - nie wspiera bezpośrednio funkcji BIOS
  - nie może ładować bezpośrednio systemów, które z nich korzystają
- Coreboot potrafi załadować prawie każdy system operacyjny
  - Zawierający jądro Linuksa lub plik ELF
  - Etherboot, pozwalający załadować jądro poprzez sieć
  - SeaBIOS pozwalający załadować Windows 2000/XP/Vistę/7 oraz *BSD.
  - Systemy korzystające z funkcji BIOS wymagają SeaBIOS.
- Coreboot szybciej ładuje nowoczesne systemy. Dokonuje tylko inicjalizacji sprzętu, której nie może zrobić system operacyjny.

Coreboot


xterm
.config - coreboot v2.3 Configuration
coreboot Configuration
Arrow keys navigate the menu. <Enter> selects submenus --->.
Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes,
<M> modularizes features. Press <Esc><Esc> to exit, <?> for Help, </>
for Search. Legend: [*] built-in [ ] excluded <M> module < >
General setup --->
Mainboard --->
Devices --->
Console options --->
System tables --->
Payload --->
VGA BIOS --->
Debugging --->

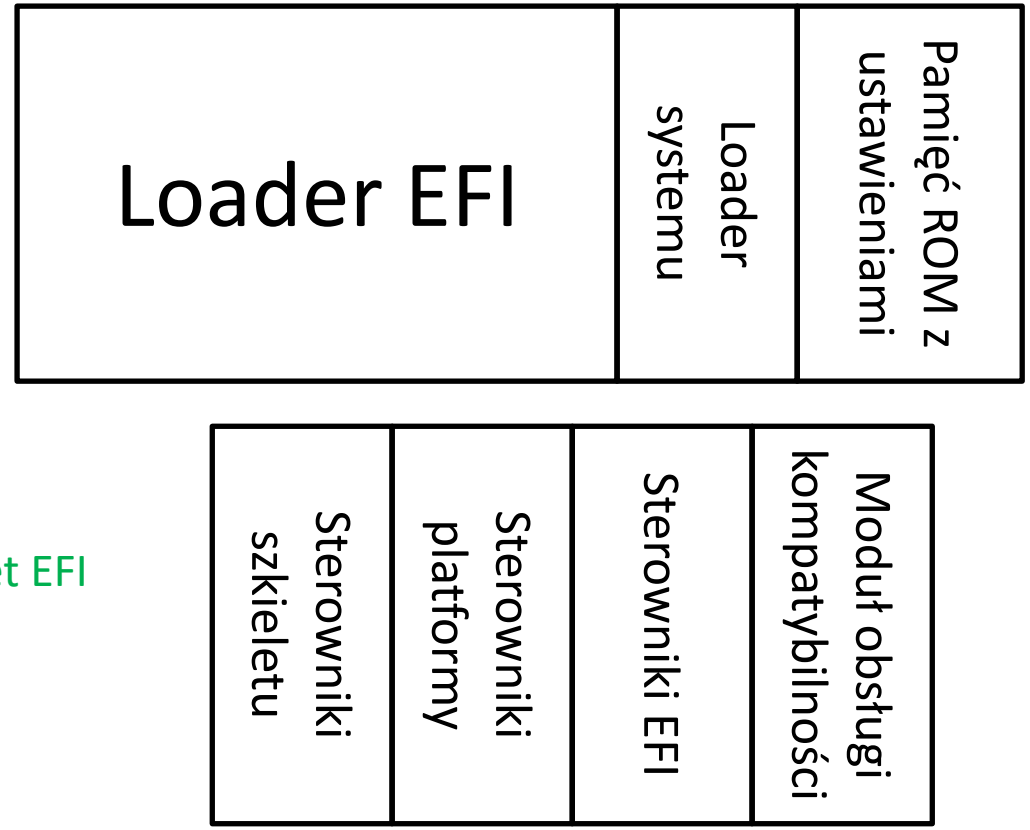
Load an Alternate Configuration File
Save an Alternate Configuration File
<Select> < Exit > < Help >

Płyta z Coreboot – AMD Pademelon

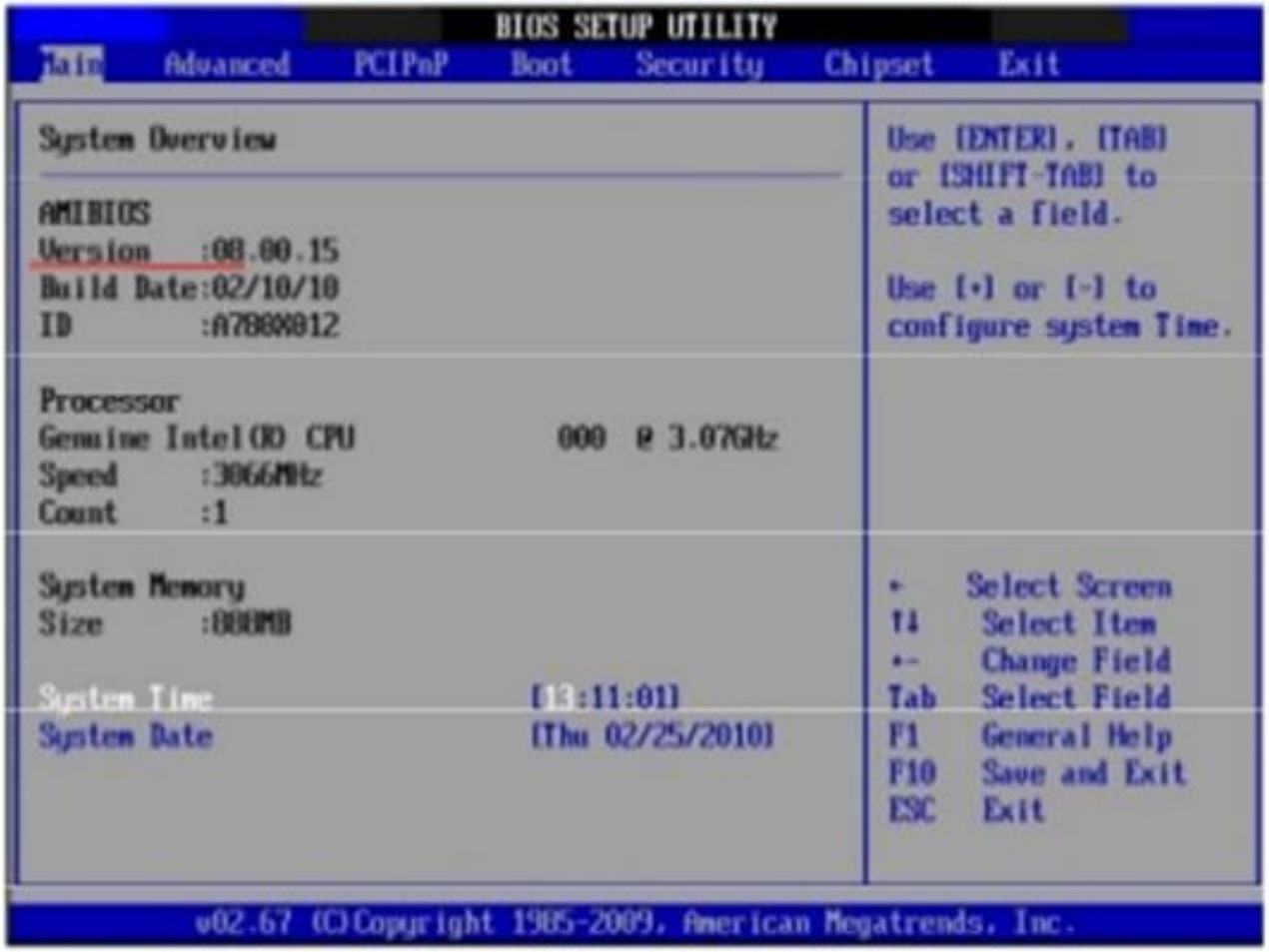
AMI Core 8

- AMI Core 8 to niedoszły następca BIOSu tworzony przez AMI, Microsoft oraz Intel.
- W skład AMI Core 8 miał wchodzić loader EFI, który odpowiada za uruchamianie szkieletu. Szkielet za pomocą wbudowanych sterowników i modułu obsługi kompatybilności uruchamiał podzespoły w komputerze za pośrednictwem interfejsu sprzętowego.
  - Przy wykorzystaniu AMI 8 komputer ma się uruchamiać szybciej, a system ma być wygodniejszy w obsłudze.
  - Core 8 miał być wspierany przez system Microsoft Windows Vista.
- Firma Phoenix, proponowała rozwiązanie – CME (Core Management Environment), które znalazło zastosowanie w notebookach i miało trafić do komputerów stacjonarnych.

Ami Core 8


Loader EFI
Loader systemu
Pamięć ROM z ustawieniami
Szkielet EFI
Sterowniki szkieletu
Sterowniki platformy
Sterowniki EFI
Moduł obsługi kompatybilności
Interfejs sprzętowy
Firmware
Platforma sprzętowa
Hardware

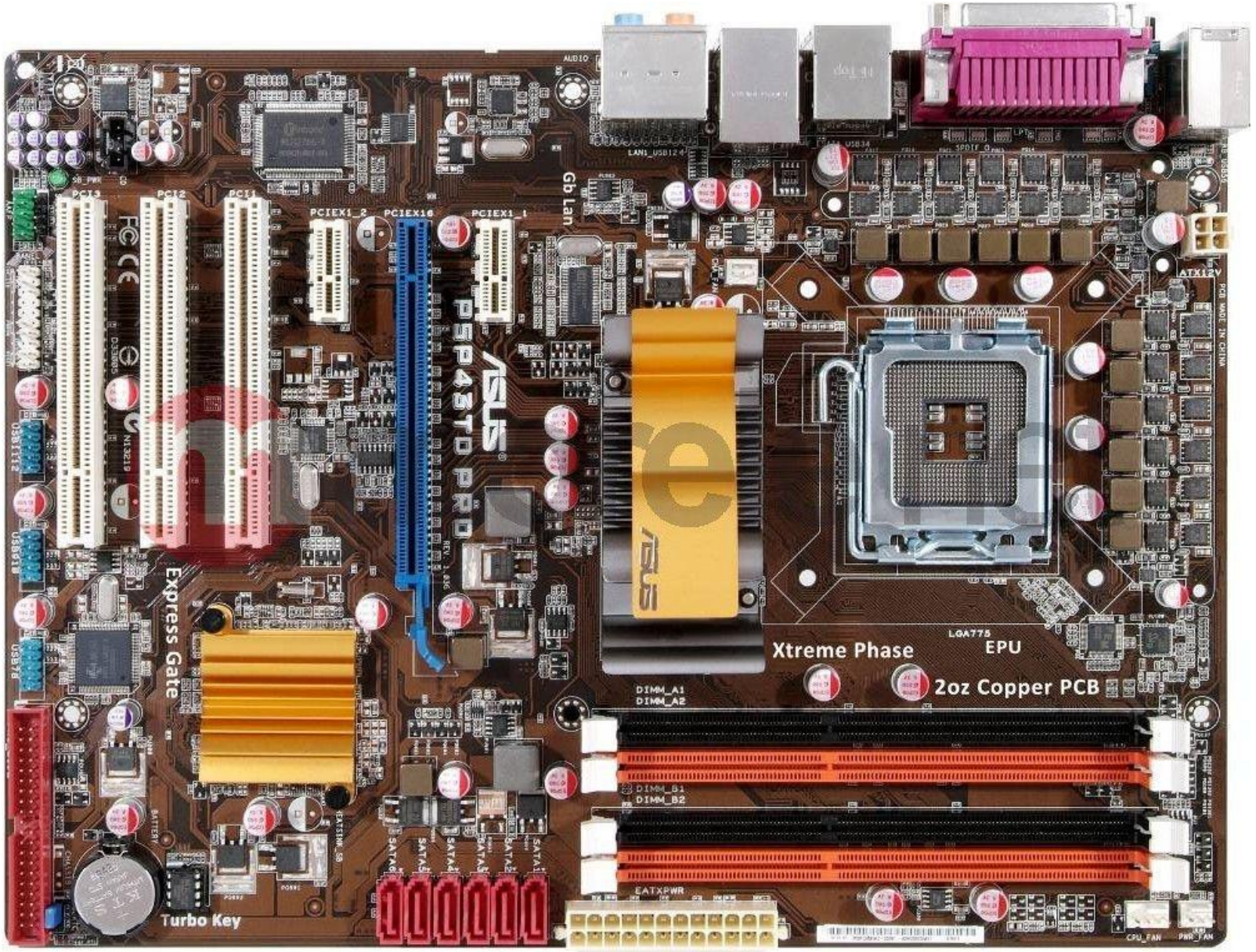
B.2 AMI Core 8



Example: AIMB-766/767/769/780; PCA-6011/6012;
PCE-5124/5125

BIOS tools: SPI programmer or Advspi v1.13 or Afudos (BIOS.rom)

Płyta z AMI BIOS - ASUS P5P43TD



EFI

EFI

- EFI- Extensible Firmware Interface.
- EFI to interfejs pośredniczący między oprogramowaniem podzespołów komputera a systemem operacyjnym.
- System współpracuje ze sprzętem różnych producentów i nie zawiera ograniczeń jakie posiada BIOS.
- EFI jest wyposażony w zestaw własnych ministerowników do sprzętu, a każdy producent może dopisać do niego własne moduły.

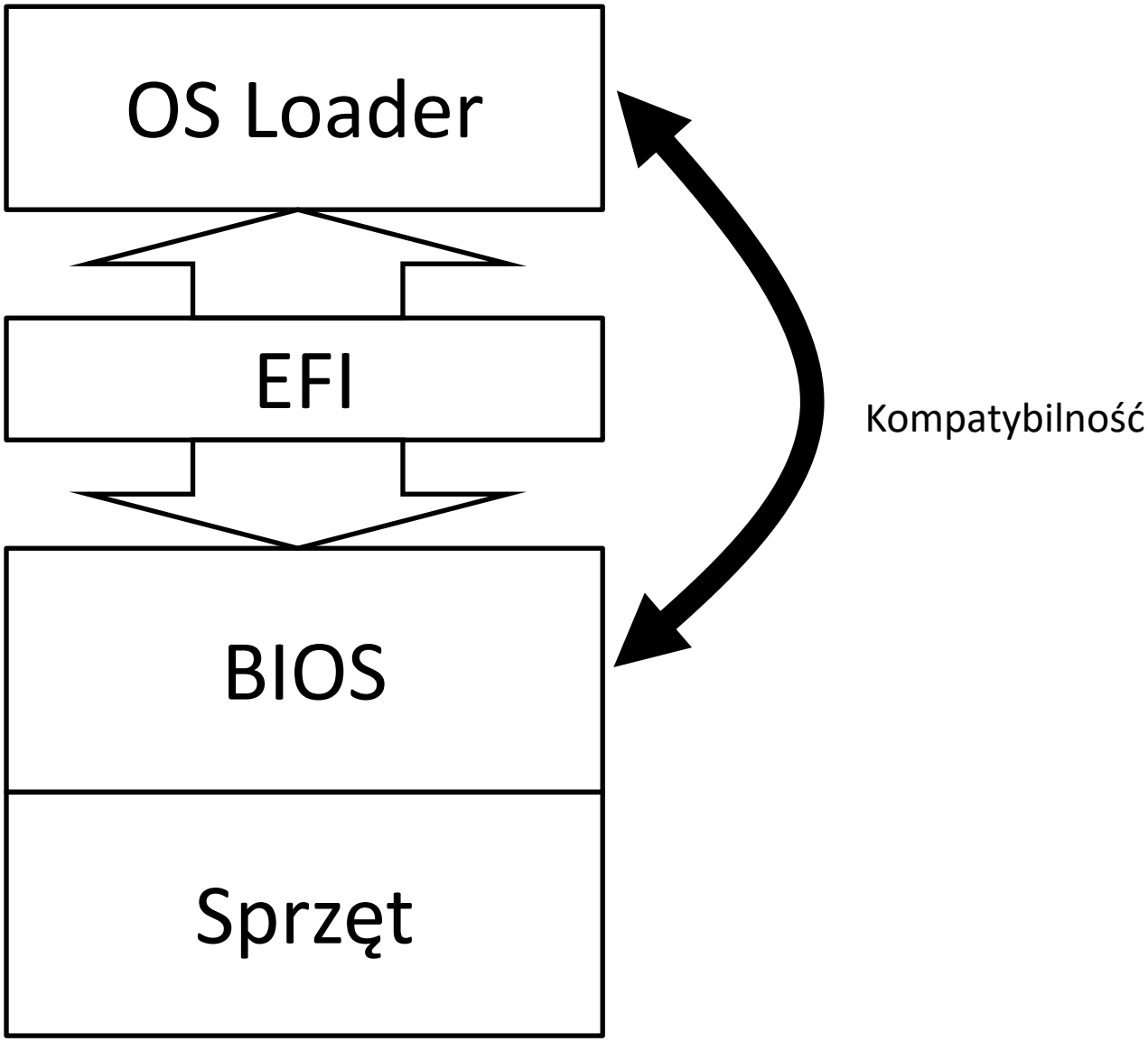
EFI - właściwości

- EFI działa w tym samym 32-, 64-bitowym trybie co system operacyjny.
- Moduły pamięci dla EFI mają po kilkadziesiąt MB.
- Pośrednicząc między OS-em a firmware'em sprzętu, jest w stanie przejąć część ustawień na siebie. System może je skopiować, nie tracąc czasu na wykonywanie własnych procedur.
  - Powoduje to znaczne przyśpieszenie startu komputera.
  - EFI jest wykrywane przez menedżer startu Linuksa, GRUB2 oraz sam Linux
- EFI jest rozszerzalny przez moduły.
  - Napisanie dodatkowego programu wzbogaci go o konkretną funkcję (np. moduł łączenia się z serwerami w sieci).

EFI - właściwości

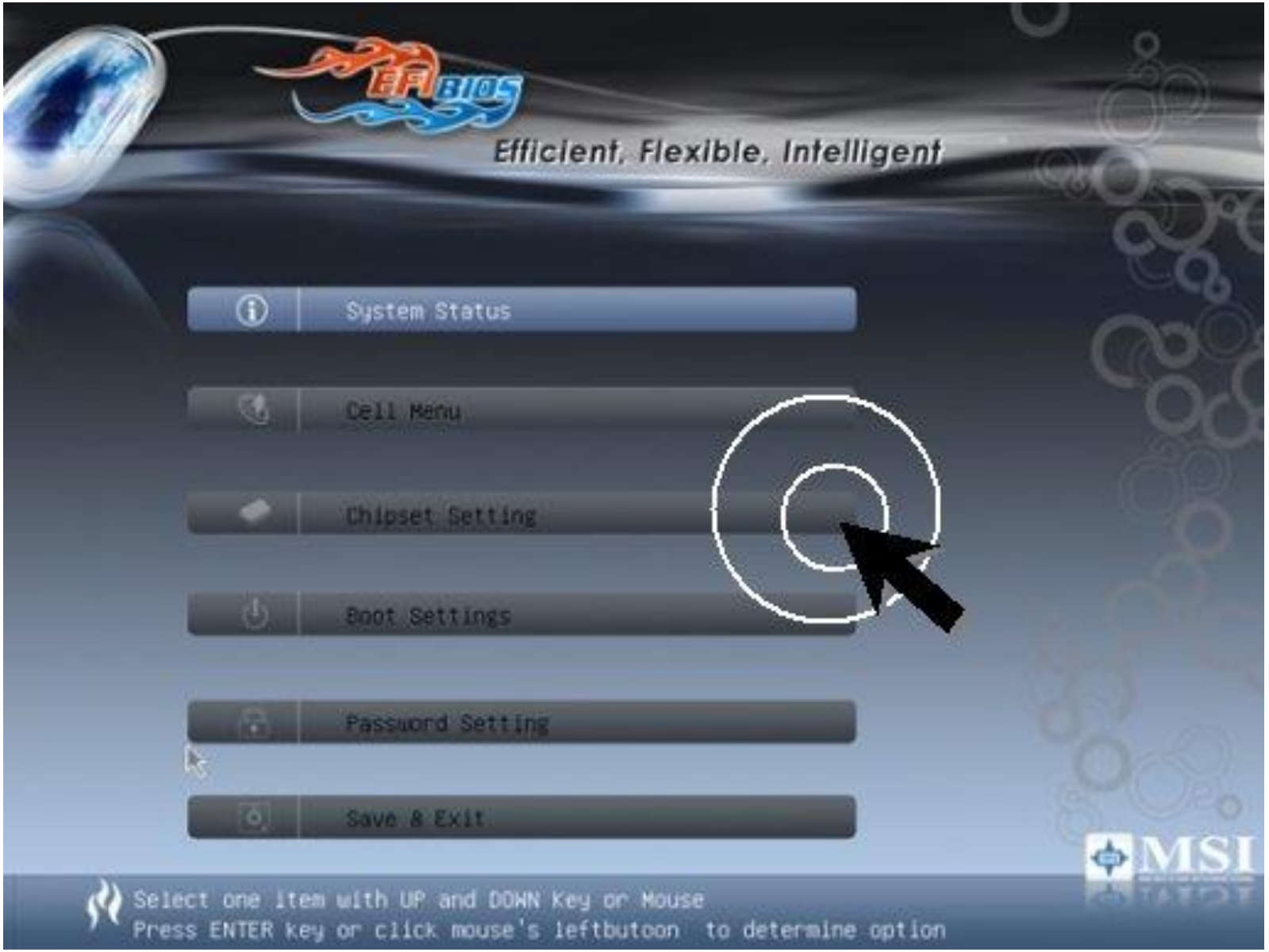
- EFI pozwala na obsługę dysków większych niż 2 TB (maksymalnie 8192 EB)
  - Używa GPT (GUID Partition Table), a nie MBR
  - Wymagany 64-bitowy system operacyjny
- Posiada jednolity interfejs programistyczny
- Niezależność od typu CPU i sterowników do niego
- Wsteczna zgodność z BIOS-em
- EFI ma graficzne, obsługiwane przez mysz interfejsy użytkownika.
  - Nie uprości to samej konfiguracji – parametry będą te same
  - system pomocy i objaśnień będzie można znacznie rozbudować.
  - Da się też tworzyć profile wyświetlania różnej szczegółowości opcji zależnie od wiedzy użytkownika.

Budowa EFI



Pierwsza płyta z EFI – MSI P35-Neo3

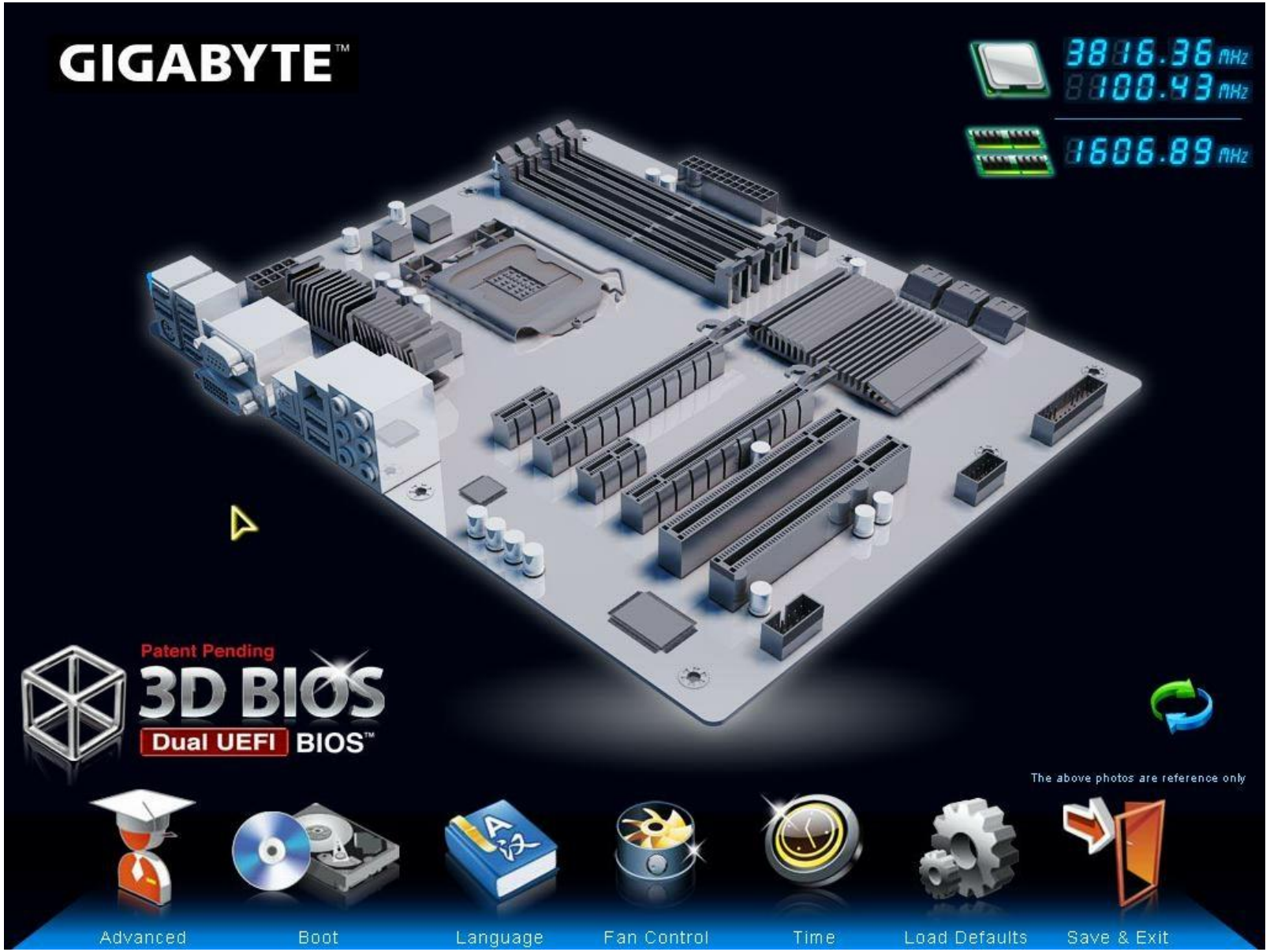
EFI na płycie MSI P35-Neo3



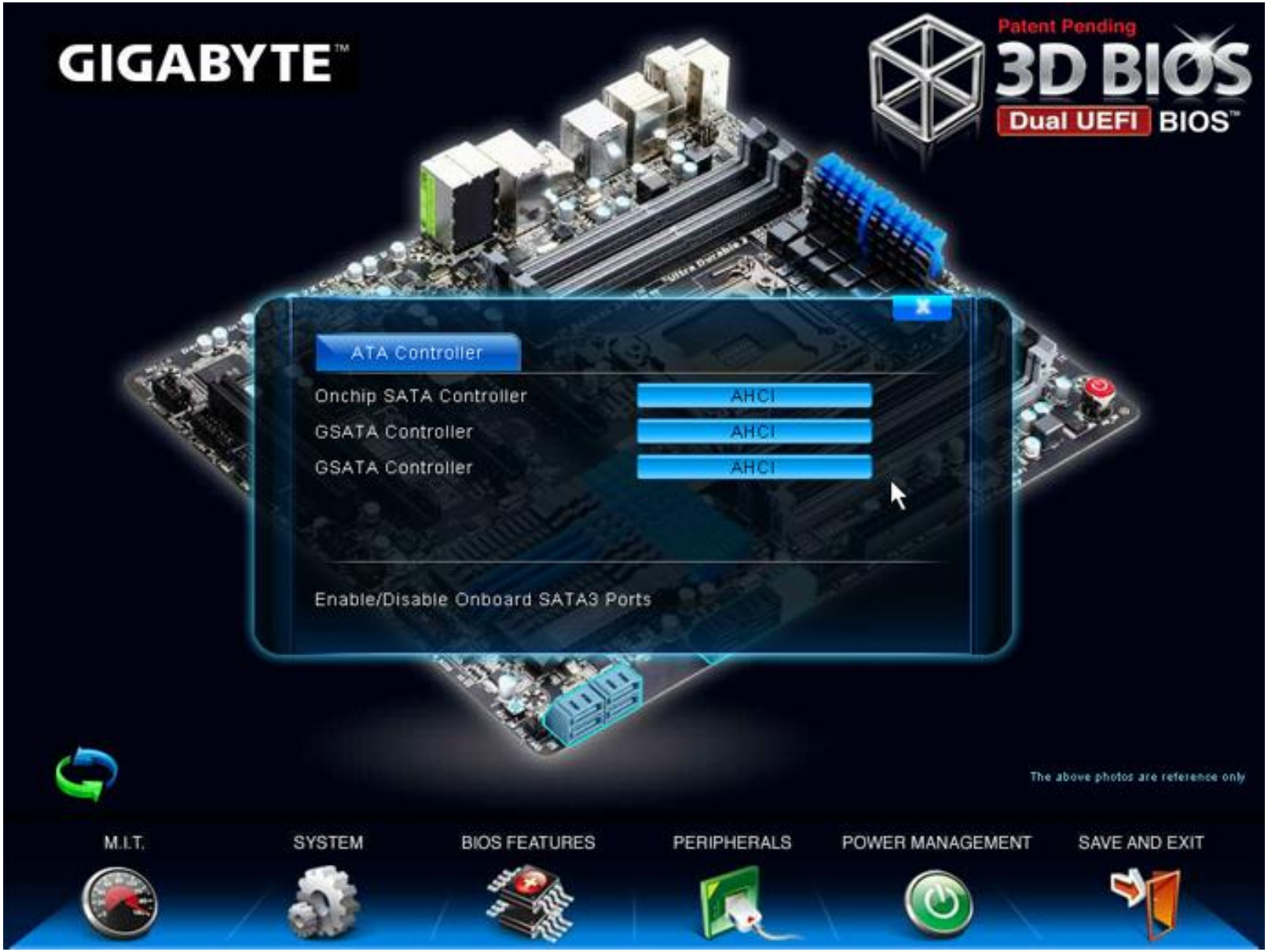
ClickBIOS


CLICKBIOS Efficient,Flexible,Intelligent
Back
Narzędzia
Live
Update
Test pamięci
Live Update
Ekran uruchamiania
Nawigacja za pomocą klawiszy strzałek lub myszki. F1 - Pomoc, F4 = Specyfikacja CPU
F5 = Memory-Z, F6 = Załaduj Ustawienia Domyślne, F10 = Zapisz i Wyjdź, Esc = Wyjdź bez zapisywania ustawień
msi

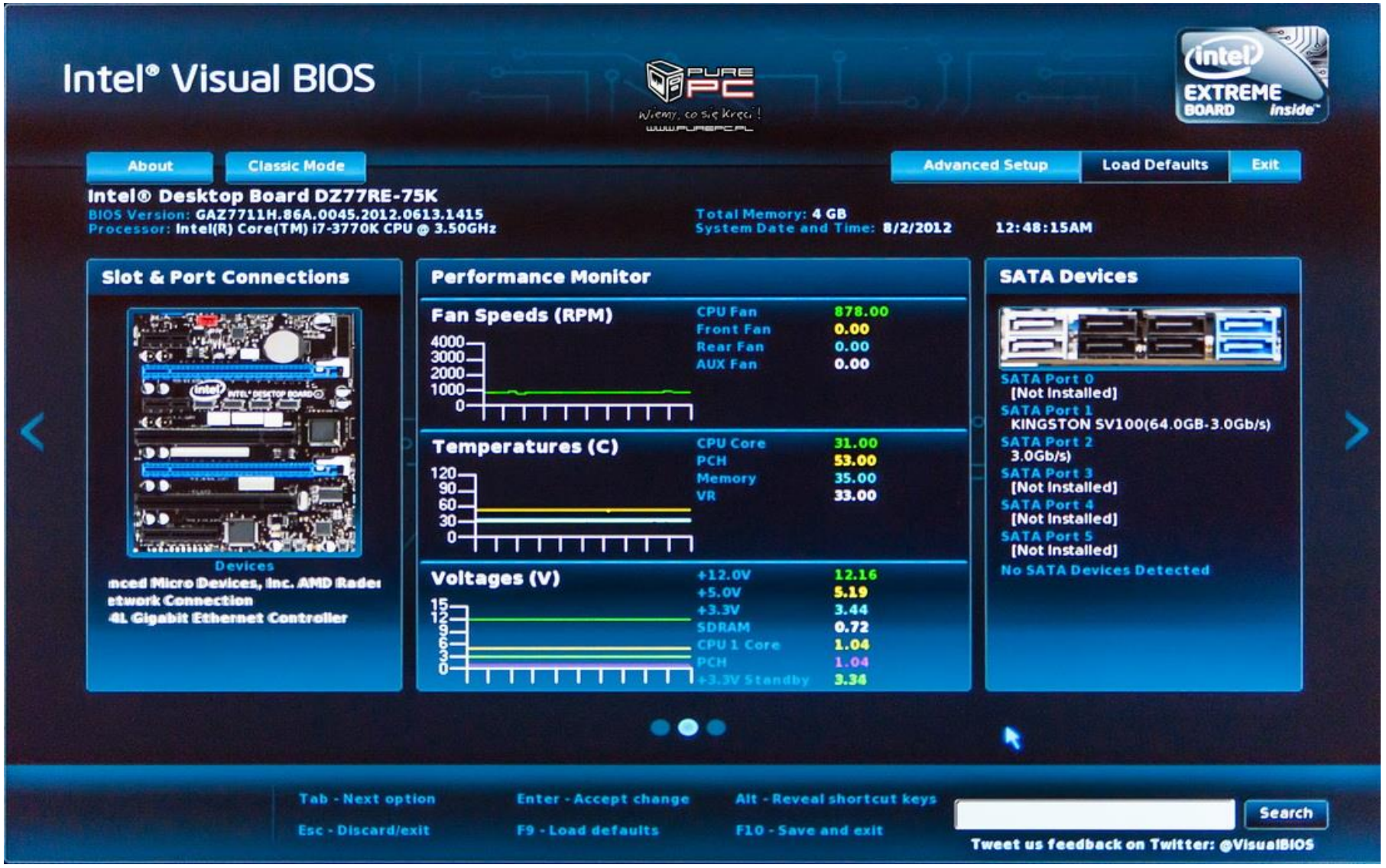
3D BIOS


GIGABYTE™
3816.36 MHz
100.43 MHz
1606.89 MHz
Patent Pending
3D BIOS
Dual UEFI BIOS™
The above photos are reference only
Advanced
Boot
Language
Fan Control
Time
Load Defaults
Save & Exit

3D BIOS

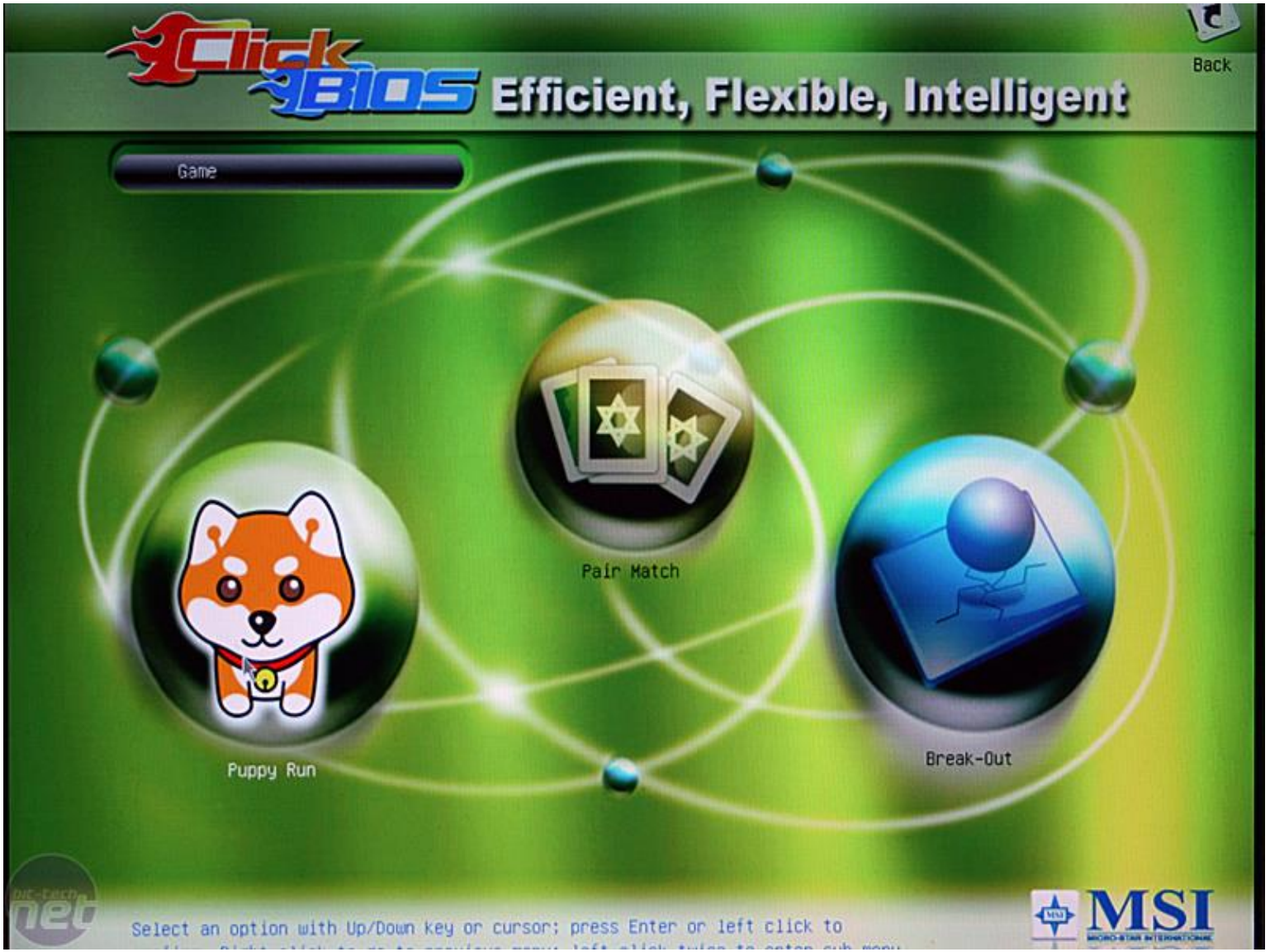

GIGABYTE™
Patent Pending
3D BIOS
Dual UEFI BIOS™
ATA Controller
Onchip SATA Controller
AHCI
GSATA Controller
AHCI
GSATA Controller
AHCI
Enable/Disable Onboard SATA3 Ports
The above photos are reference only
M.I.T.
SYSTEM
BIOS FEATURES
PERIPHERALS
POWER MANAGEMENT
SAVE AND EXIT

Intel Visual BIOS

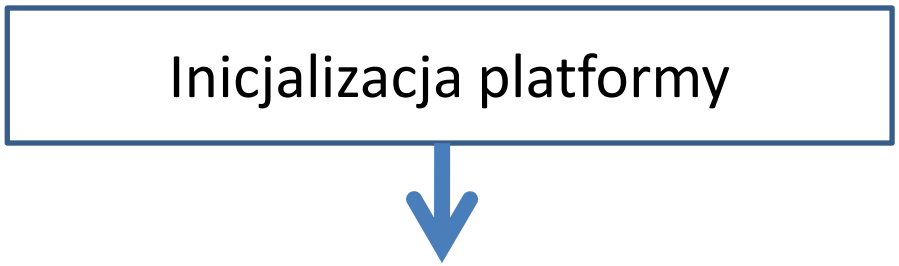


UEFI Dual BIOS

Gra pod UEFI

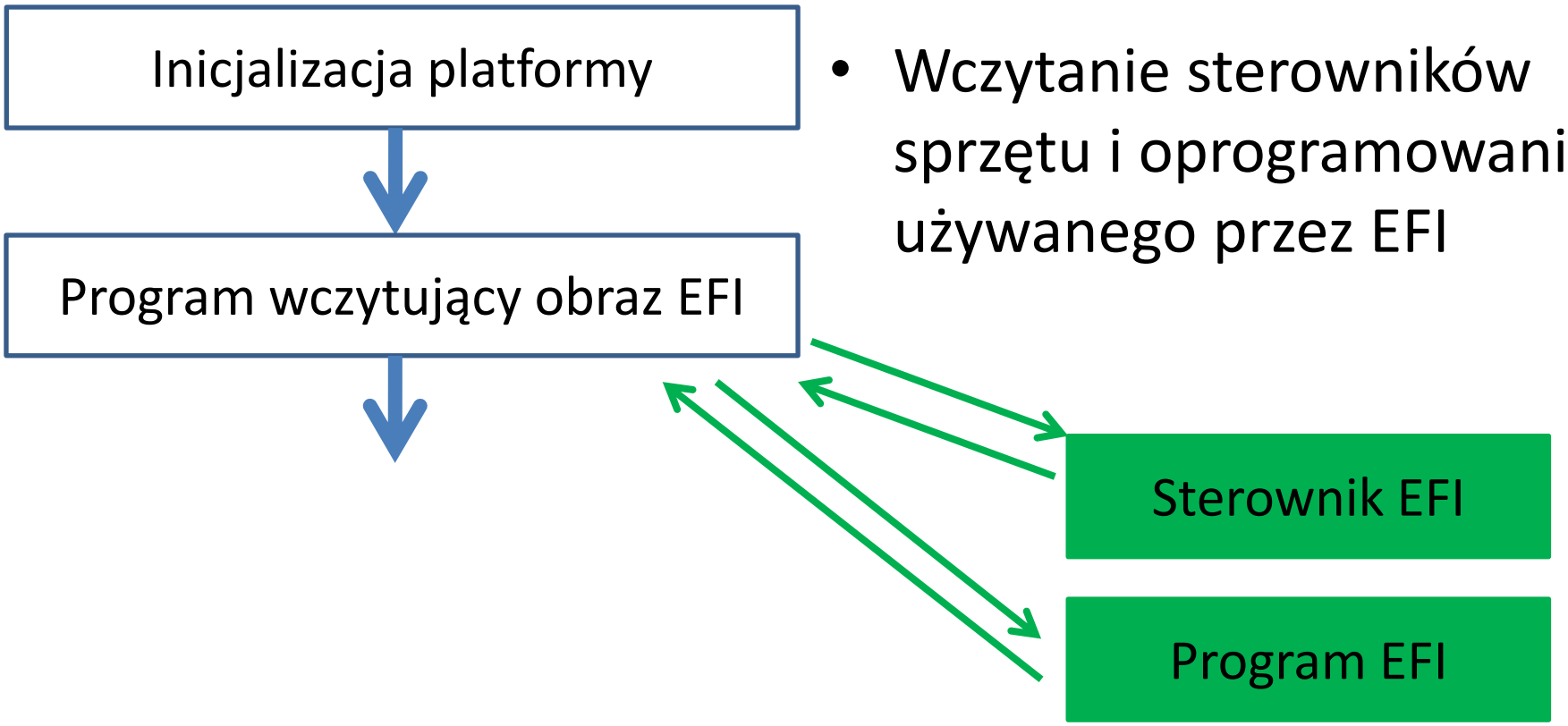

Click BIOS
Efficient, Flexible, Intelligent
Back
Game
Pair Match
Puppy Run
Break-Out
Select an option with Up/Down key or cursor; press Enter or left click to
MSI

Start komputera



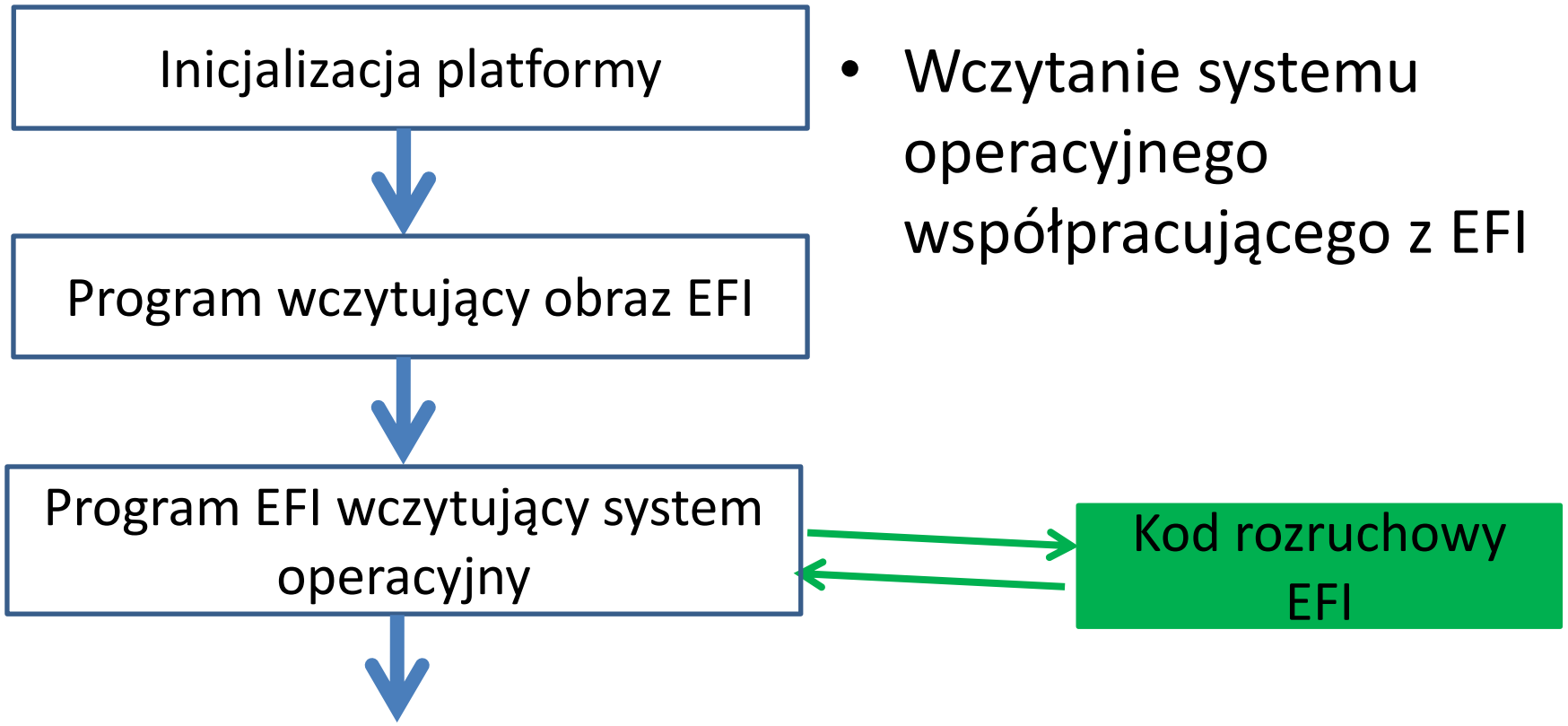
- Standardowe uruchomienie platformy sprzętowej: procesor, pamięć RAM, chipset, płyta główna itd.

Wczytanie oprogramowania EFI



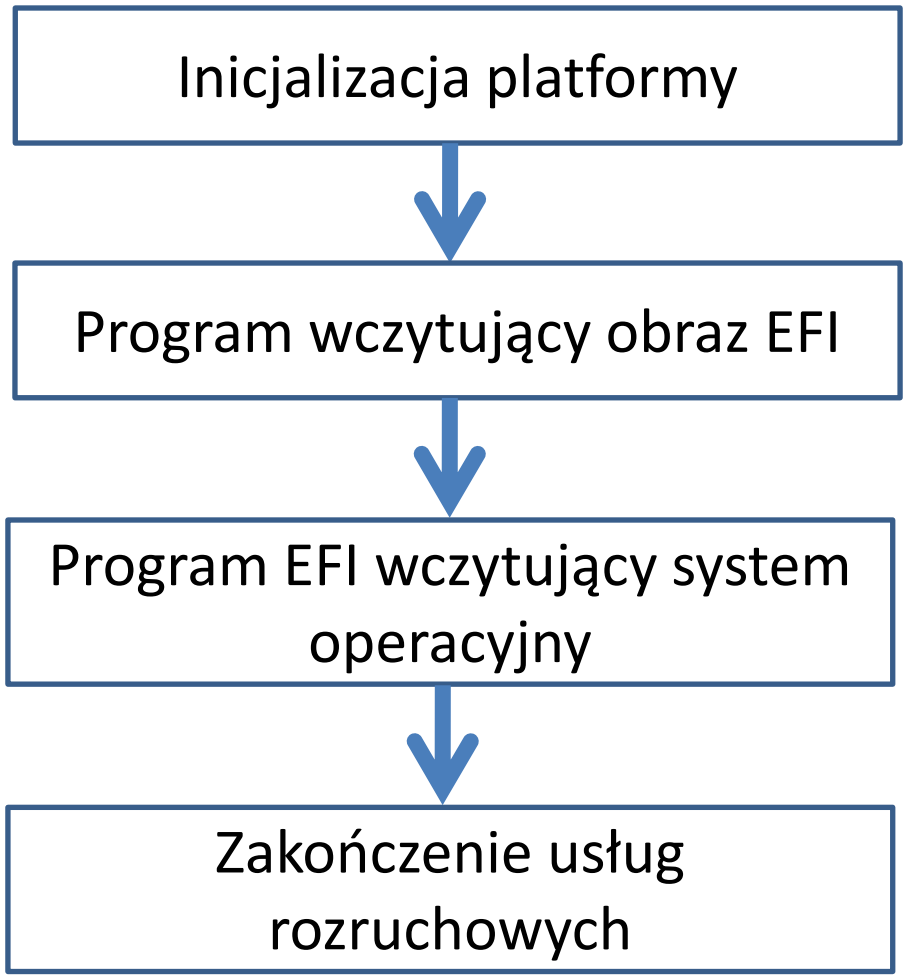
- Wczytanie sterowników sprzętu i oprogramowania używanego przez EFI

Wczytanie systemu operacyjnego



- Wczytanie systemu operacyjnego współpracującego z EFI

Uruchomienie systemu operacyjnego



- Przekazanie dalszych czynności startowych do systemu operacyjnego

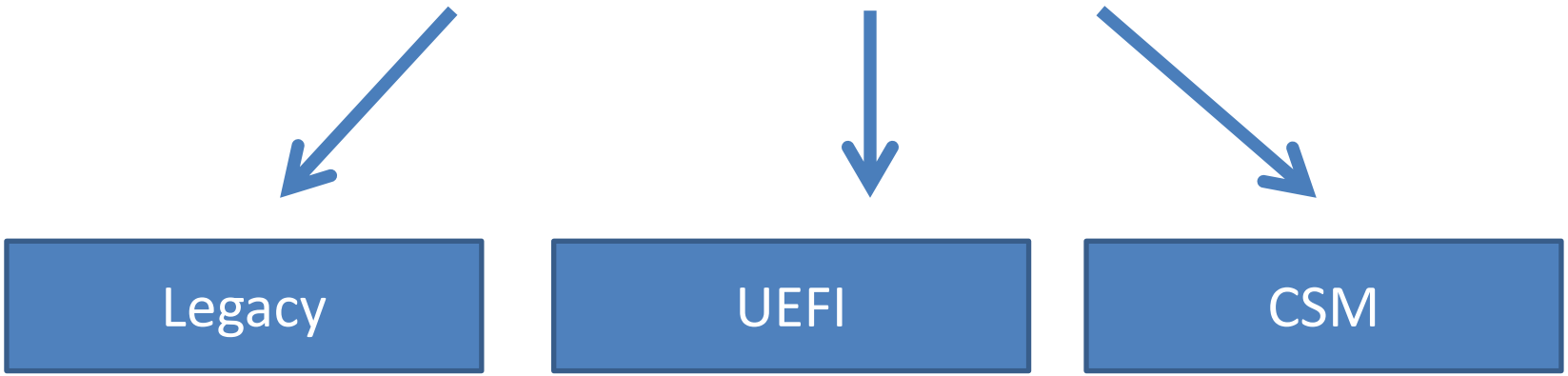
Start z EFI

- EFI ma własny menedżer rozruchu systemu operacyjnego, z którym zintegrowane są bootmenedżery zainstalowanych systemów.
- EFI posiada sobie na dysku twardym małą (100–250 MB) partycję sformatowaną w FAT 32 – *Extensible Firmware Interface System Partition* (w skrócie ESP).
- EFI bootuje tylko z medium sformatowanego w FAT 32.
  - Wyjątkiem jest nośnik DVD
- Na Partycji EFI znajdują się sterowniki sprzętowe, z których może korzystać również uruchomiony system operacyjny. Na przykład Windows 7 i 8 zapisują cały *Hardware Abstraction Layer* na Partycji EFI.

Emulacja BIOSu w EFI

- EFI ma możliwość emulacji BIOSu dla systemów operacyjnych wymagających go do pracy.
- Realizuje to funkcja Compatibility Support Module (CSM)
  - CSM można aktywować w UEFI, aby potem wgrać na przykład 32-bitową wersję Windows 7 albo XP.
- CSM umożliwia realizację funkcji BIOSu przez EFI.

Tryby bootowania UEFI



Legacy

- Rezygnacja z UEFI
- Korzystanie ze starszych funkcji BIOSu
- Przydatne do wcześniejszych wersji systemów operacyjnych (Windows Vista i wcześniejsze)

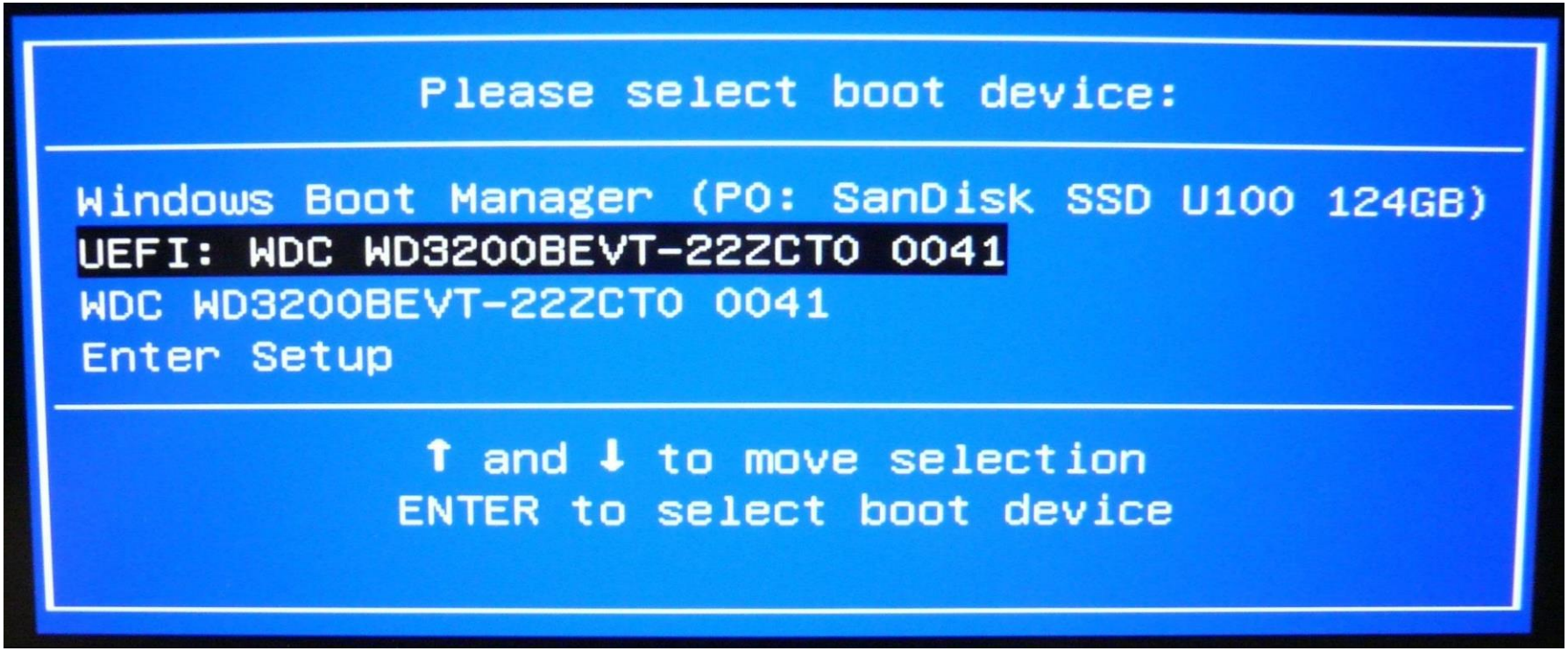
UEFI

- Wykorzystujemy wszystkie funkcje UEFI
- Zalecane dla współczesnych wersji systemów operacyjnych (Windows 7 i nowsze)

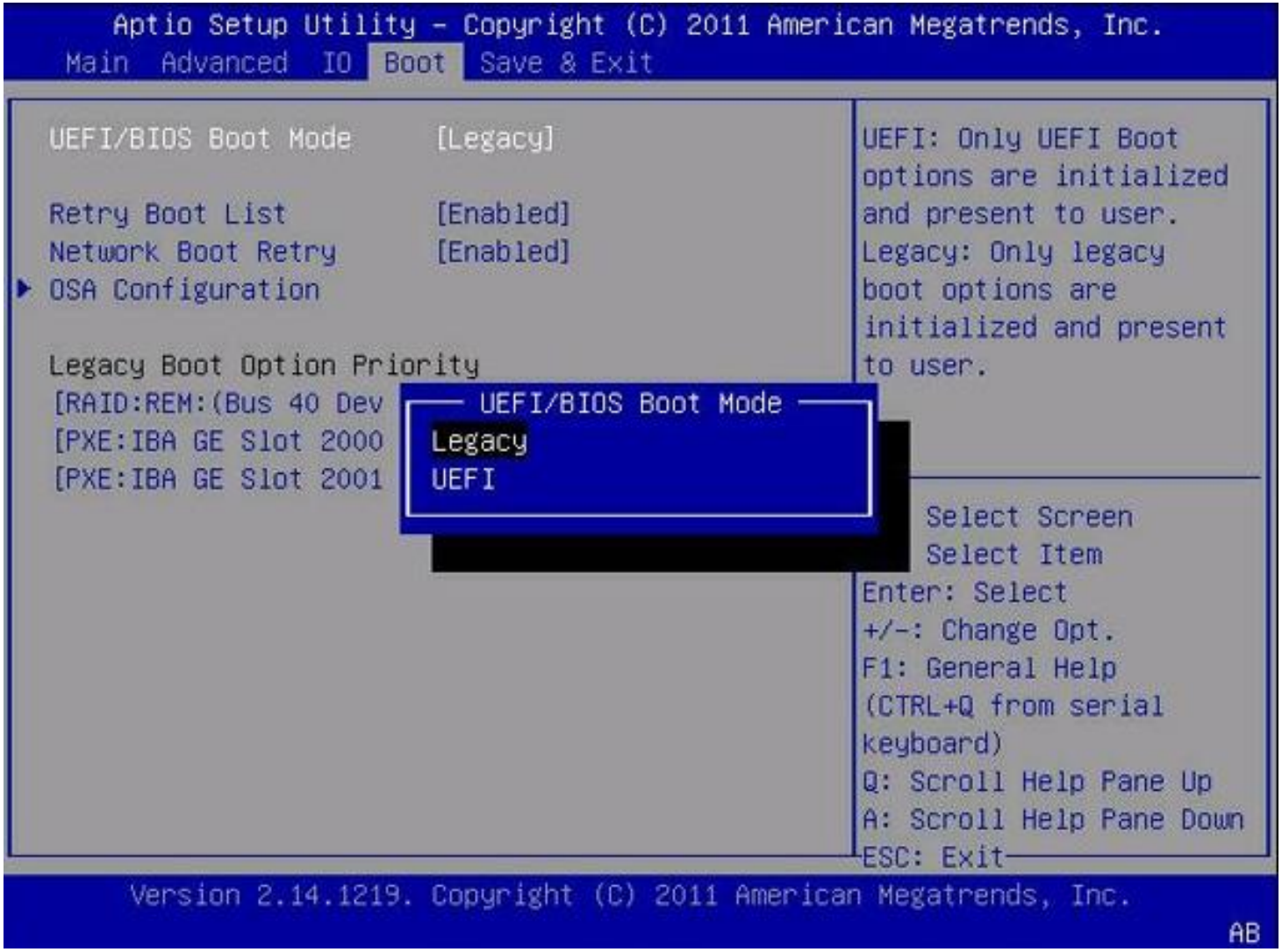
CSM

- Emulacja tradycyjnego BIOSu w UEFI
- Korzystanie ze starszych funkcji BIOSu
- Przydatne jakiś starszy komponent komputera nie obsługuje UEFI

Bootowanie UEFI



Bootowanie UEFI



EFI SHELL

EFI Shell

- EFI Shell to dodatkowa powłoka na BIOS.
- Jest to miniaturowy system operacyjny, który pozwala wydawać proste komendy tekstowe w wierszu poleceń.
  - Cd – zmiana katalogów
  - Map – lista napędów w systemie
- Można nimi sterować uruchomieniem komputera lub uruchamiać pewne aplikacje skryptowe.
- EFI Shell jest instalowane na partycji EFI system (oznaczonej jako EF00), sformatowanej w systemie VFAT i nazwanej shellx64.efi (dla systemów 64-bitowych).
- EFI Shell może być dostępne bezpośrednio z menu BIOSa.

EFI Shell


REPUBLIC OF GAMERS
Advanced Mode
Exit
Extreme Tweaker
Main
Advanced
Monitor
Boot
Tool
Exit
Load Optimized Defaults
Load Safe Defaults
Save Changes & Reset
Discard Changes & Exit
WARNING
Not Found
Ok
ASUS EZ Mode
Launch EFI Shell from filesystem device
Attempts to Launch EFI Shell application (Shellx64.efi) from one of the available filesystem devices
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Shortcut
F5: Optimized Defaults
F6: ASUS Ratio Boost
F10: Save ESC: Exit
F12: Print Screen
ASUS
Version 2.14.1219. Copyright (C) 2012 American Megatrends, Inc.

EFI Shell

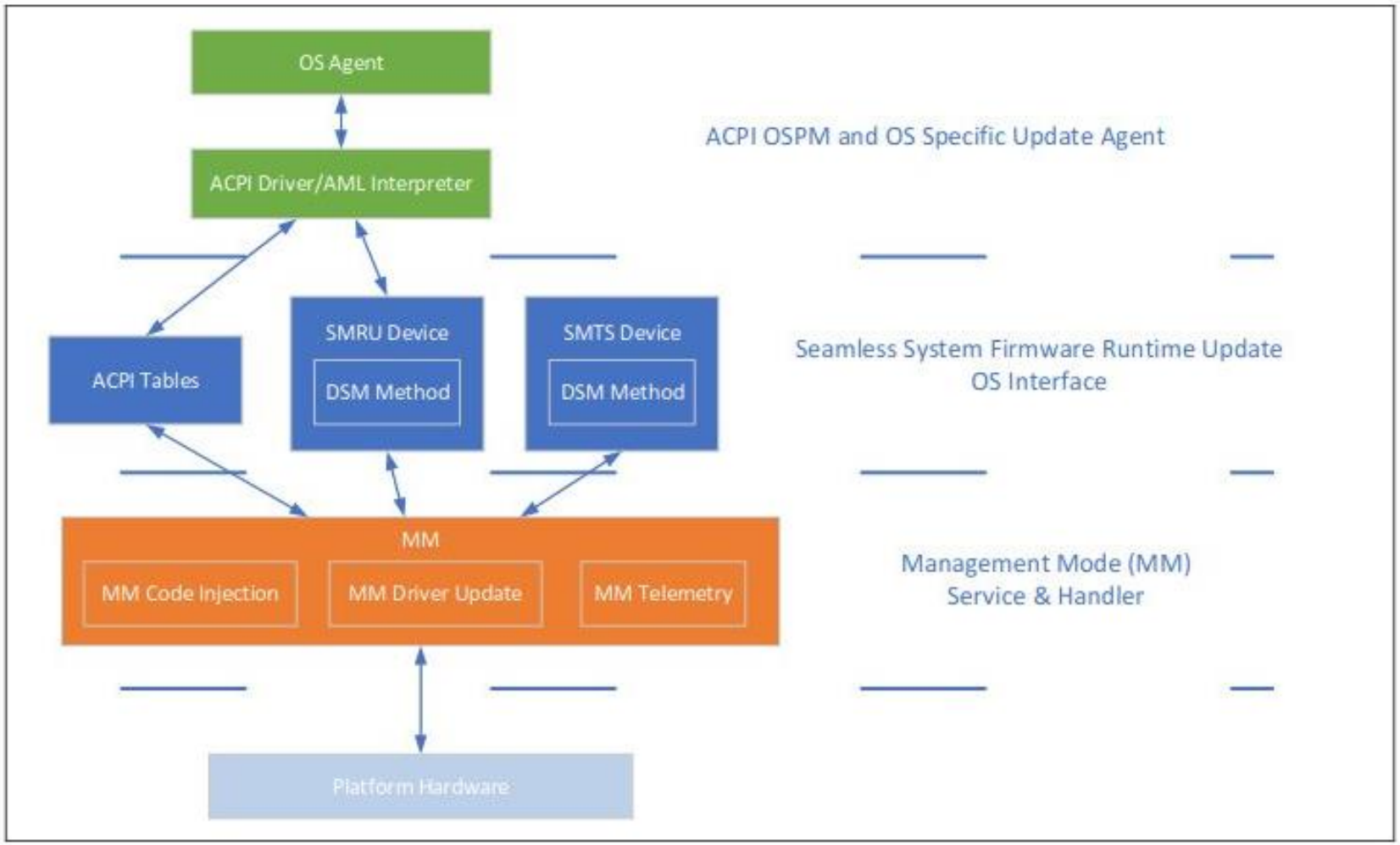

Shell> fs0:
fs0:\> cd EFI\BOOT
fs0:\EFI\BOOT> ls
Directory of: fs0:\EFI\BOOT
07/13/09 09:20a <DIR> 0 .
07/13/09 09:20a <DIR> 0 ..
07/13/09 04:19p 438,784 BOOTX64.EFI
1 File(s) 438,784 bytes
2 Dir(s)
fs0:\EFI\BOOT> BOOTX64.EFI
UEFI Interactive Shell v2.1
EDK II
UEFI v2.40 (EDK II, 0x00010000)
Mapping table
BLK0: Alias(s):
PciRoot(0x0)/Pci(0x1,0x1)/Ata(0x0)
BLK1: Alias(s):
PciRoot(0x0)/Pci(0xD,0x0)/Sata(0x0,0x0,0x0)
Press ESC in 1 seconds to skip startup.nsh or any other key to continue.
Shell>

PFRUT

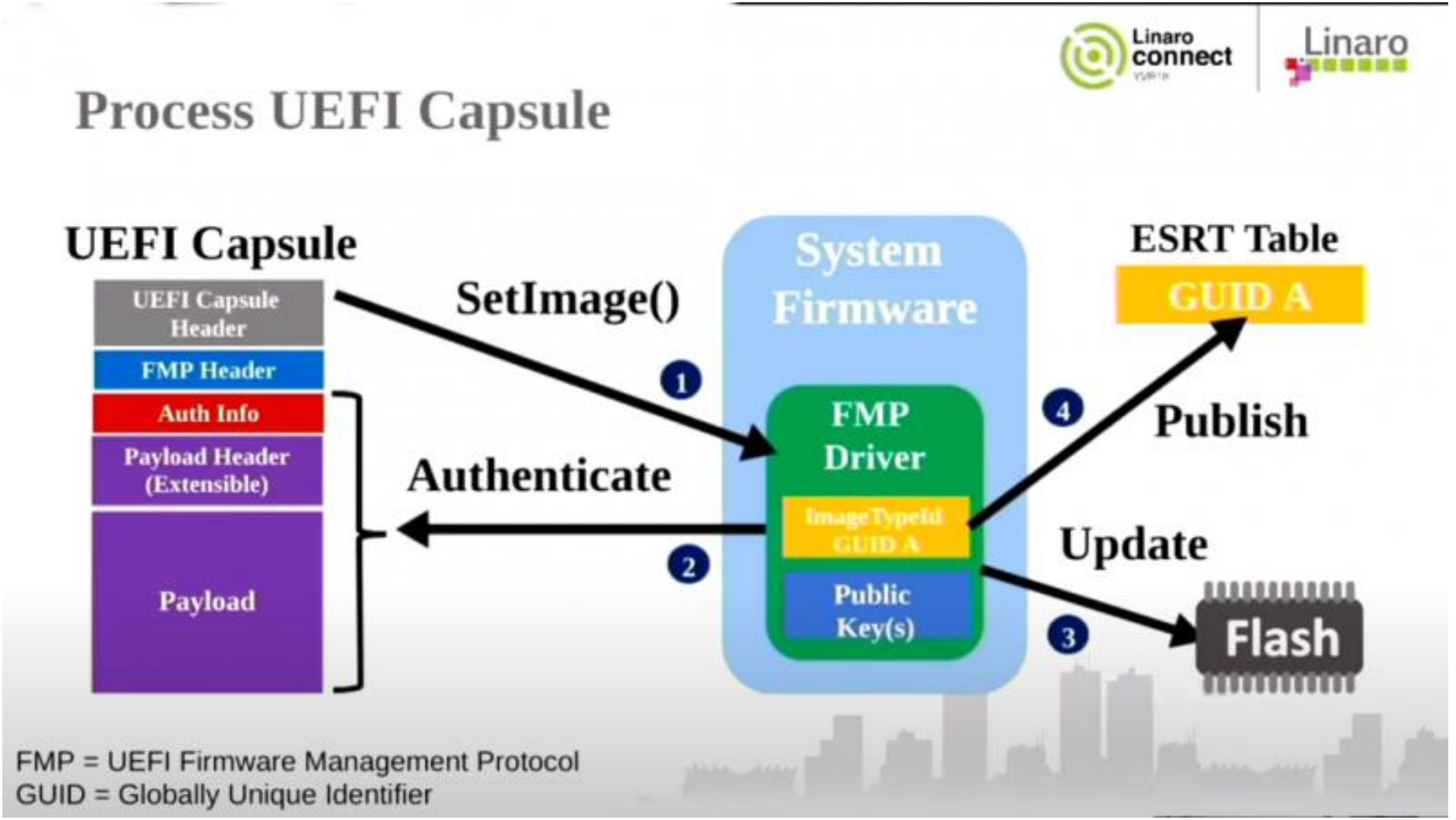
PFRUT

- PFRUT to skrót od „Platform Firmware Runtime and Telemetry”.
- PFRUT to wersja Linuksa (wersja 5.17), która ma umożliwić systemowi operacyjnemu uaktualnienie UEFI bez restartu systemu.
- Rozwiązanie jest przydatne w rozwiązaniach serwerowych, gdzie występują wysokie wymagania co do ciągłości pracy.

Schemat PFRUT



PFRUT


Linaro connect
Linaro
Process UEFI Capsule
UEFI Capsule
UEFI Capsule Header
FMP Header
Auth Info
Payload Header (Extensible)
Payload
SetImage()
1
Authenticate
2
System Firmware
FMP Driver
ImageTypeId GUID A
Public Key(s)
ESRT Table
GUID A
4
Publish
Update
3
Flash
FMP = UEFI Firmware Management Protocol
GUID = Globally Unique Identifier

Pytania powtórkowe

1. Co to jest BIOS?
2. Ilu bitowy jest BIOS?
3. Ile zajmuje pamięci RAM?
4. Gdzie na płycie głównej znajduje się BIOS?
5. Jakie są zadania BIOSu?
6. Omów właściwości pamięci CMOS w której ukrywa się BIOS.
7. Jak wyczyścić ustawienia BIOSU?
8. Co to jest shadowing?
9. Omów poszczególne kroki realizowane przez BIOS w trakcie uruchamiania komputera.
10. Co to są testy POST?
11. Jak BIOS uruchamia system operacyjny?
12. Jakie firmy produkują BIOSy?
13. Jakie rodzaje użytkowników mogą występować w BIOSie?
14. Co to jest hasło uniwersalne (serwisowe)?
15. Jak skasować hasło BIOSu?
16. O czym mówią poszczególne elementy nazwy BIOSu?
17. Gdzie w rejestrze Windows znajdziemy dane konfiguracyjne BIOSu?
18. Jakie parametry konfiguracyjne zawiera BIOS?
19. Czy jest program BIOS setup?
20. Jakie informacje przekazują nam kody dźwiękowe?

Pytania powtórkowe

21. O czym informuje użytkownika karta sygnałowa POST?
22. Omów proces aktualizacji BIOSu?
23. Jak zidentyfikować BIOS w komputerze?
24. Jak działają wirusy atakujące BIOS?
25. Co to jest Hot Swapping?
26. Jak działają systemy ochrony BIOSu?
27. Dual BIOS
28. Quad BIOS
29. Die Hard BIOS
30. Co to jest OpenBIOS?
31. Co to jest LinuxBIOS?
32. Co to jest CoreBoot?
33. Co to jest AMI Core 8?
34. Cym jest EFI?
35. Omów poszczególne kroki realizowane przez EFI w trakcie uruchamiania komputera.
36. Jak EFI współpracuje z BIOSem?
37. Co to jest EFI Shell?
38. Jakie są tryby bootowania BIOSu?
39. Co to jest EFI Shell?