Prezentacja emulatora QEMU
Zajęcia SO
08.11.2006

Czym jest QEMU...?

QEMU to emulator procesora:

- osiągający bardzo dobrą szybkość emulacji
- udostępniony jako otwarte oprogramowanie

Do czego może się przydać..?

QEMU pozwala na:

- uruchomienie procesów Linuksa skompilowanych na innym typie procesora niż lokalny - tryb **User Mode Emulation** (tylko Linux jak system gospodarza):
  - sprawdzenie wyników działania cross-kompilatorów oraz cross-debugerów,
  - uruchamianie Wine Windows API

Do czego może się przydać..?

QEMU pozwala na:

- emulację pełnego komputera, przeważnie PC - wraz z procesorem, jak i urządzeniami peryferyjnymi – tryb **Full System Emulation**:
  - uruchomić kolejny system operacyjny
  - debugować kod systemowy - wirtualna maszyna może być łatwo zatrzymana, a jej stan skontrolowany, zapisany lub wznowiony.

Czemu QEMU jest taki szybki?

- używa dynamicznej translacji
- posiada tzw. translation cache o rozmiarze 16MB
- potrafi emulować MMU (jednostka zarządzania pamięcia) gościa za pomocą MMU gospodarza (wersja “qemu-fast”)

Czy szybki oznacza naprawdę szybki?

Testy ze strony:
http://fabrice.bellard.free.fr/qemu/benchmarks.html
wskazują, że na architekturze x86 osiąga on:

- ok. 25% prędkości natywnej przy operacjach na liczbach całkowitych
- ok. 10% przy operacjach na liczbach zmiennoprzecinkowych

ale... w porównaniu do innych emulatorów:

- ok. 1,2 razy szybszy od Valgrinda
- ok. 65 razy szybszy od Bochsa (ciekawostka: QEMU używa BIOS-u PC z projektu Bochsa)

ale... w porównaniu do wirtualizatorów np.

- ok. 3-4 razy wolniejszy od VMWare, Virtual PC :(

Ale może być jeszcze szybszy...!

QEMU Accelerator (kqemu):

- narzędzie zwiększające szybkość emulacji komputera PC na innym komputerze PC z architekturą procesora x86
  QEMU bez kqemu –> 10-20% prędkości natywnej
  QEMU + kqemu –> 50-100% prędkości natywnej

- umożliwia na wykonywanie większości instrukcji kodu działającej aplikacji bezpośrednio na procesorze gospodarza

- przeznaczony na razie wyłącznie dla systemów: Linux 2.4 i Linux 2,6 oraz Windows 2000/XP (eksperymentalnie)

- darmowy, jednak jego źródła nie są dostępne

Inne zalety..

- wsparcie w trybie pełnej emulacji m.in dla PC (procesor x86 lub x86_64), PreP i Power Mac (procesor PowerPC) oraz Sun4m (procesor 32-bit Sparc) i kilka innych,
- wsparcie w trybie użytkownika dla architektur procesorów: x86, PowerPC, ARM, MIPS czy Sparc32/64,
- możliwość emulacji wielu urządzeń
- wspiera wychwytywanie wyjątków
- wiele formatów obrazów dysków twardych np. qcow, vpc, wmdk
- wirtualny procesor „jest” biblioteką (libqemu), która może być wykorzystana w innych projektach (przykład w qemu/tests/qruncom.c)

Wady..

- niekompletne wsparcie dla MS Windows w roli gospodarza
- niekompletne wsparcie dla mniej popularnych architektur procesorów (a nawet dla procesora SPARC niektóre atomowe instruckje nie są jeszcze poprawnie zainplementowane)
- występują pewne ograniczenia w emulacji procesora x86:
  - brak obsługi rozkazów x86-64
  - brak obługi PC syscall (wywołań systemowych związanych z komunikacją międzyprocesowa) – dotyczy również SPARC
  - nie tłumaczy instrukcji SSE/MMX (jeszcze)

Instalacja – na przykładzie Windows

QEMU nie trzeba instalować, wystarczy pobrać archiwum zip ze strony http://www.h7.dion.ne.jp/~qemu-win/ i je rozpakować.

W archiwum znajduje się m.in:

- testowo-demonstracyjny obraz linuxa (linux.img) bazujący na Red-Hat,
- plik ReadMe ;)

Przewodnik instalacji QEMU pod Linux

- http://kidsquid.com/cgi-bin/moin.cgi/QuickStartGuide

Uruchomienie

Wydawać polecenia QEMU będziemy przy użyciu konsoli:

Uruchomienie testowo-demonstacyjnego obrazu linuxa:

```
$ qemu.exe -L . -hda linux.img
```

gdzie

`-L` – lokalizacja biosu (plik bios.bin)

`-hda` – obraz dysku twardego

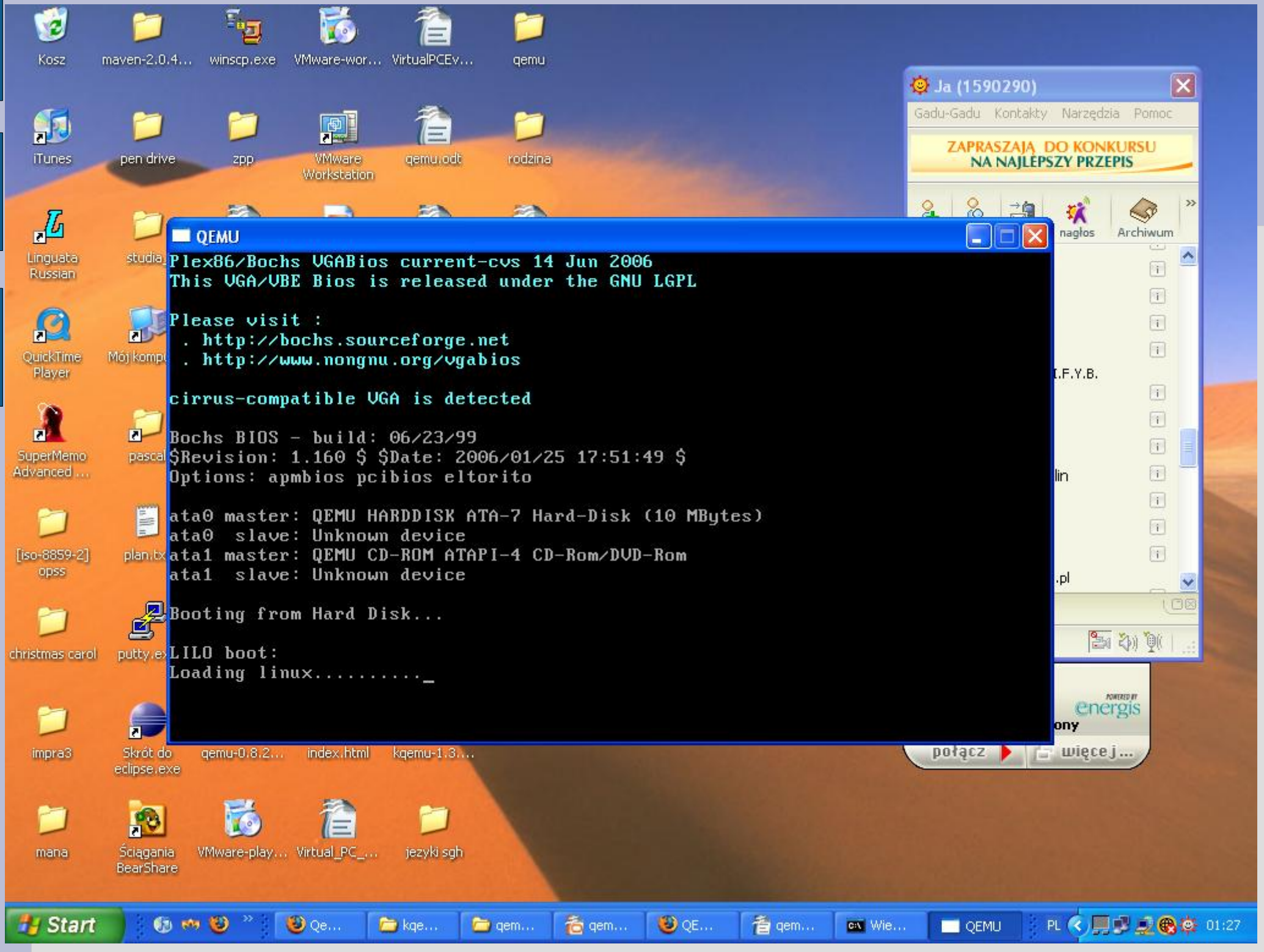
Listę możliwych parametrów wyświetla polecenie:

```
$ qemu.exe
```

Przydatne skróty klawiszowe:

`Ctrl+Alt` – przełączenie myszki z QEMU na Windows

`Ctrl+Alt+f` – włączenie/wyłaczenie trybu pełnego okna


QEMU
Plex86/Bochs VGABios current-cvs 14 Jun 2006
This VGA/VBE Bios is released under the GNU LGPL
Please visit :
. http://bochs.sourceforge.net
. http://www.nongnu.org/vgabios
cirrus-compatible VGA is detected
Bochs BIOS - build: 06/23/99
$Revision: 1.160 $ $Date: 2006/01/25 17:51:49 $
Options: apmbios pcibios eltorito
ata0 master: QEMU HARDDISK ATA-7 Hard-Disk (10 MBytes)
ata0 slave: Unknown device
ata1 master: QEMU CD-ROM ATAPI-4 CD-Rom/DVD-Rom
ata1 slave: Unknown device
Booting from Hard Disk...
LILO boot:
Loading linux.....
Ja (1590290)
Gadu-Gadu Kontakty Narzędzia Pomoc
ZAPRASZAJĄ DO KONKURSU
NA NAJLEPSZY PRZEPIS
nagłos
Archiwum
połącz
więcej...
Start
QEMU
PL
01:27

Instalacja SO – tworzenie dysku

- Można wykorzystać dodatkowe narzędzia QEMU Manager http://kidsquid.com/cgi-bin/moin.cgi/QEMU_Manager lub QEMUMenu http://kidsquid.com/cgi-bin/moin.cgi/QEMUMenu dla ułatwienia instalacji systemów i dalszego użytkowania.

- Pierwszy krok to utworzenie pustego obrazu dysku dla nowego systemu

```
$ qemu-img.exe create -f qcow hda.img 4G
```

- Ogólna składnia polecenia:

```
create [-e] [-b base_image] [-f fmt] filename [size],
```

gdzie

`-b base_image` – obraz dysku wzorca,

`-f fmt` – format dysku, qcow, raw – bez konkretnego formatu, vpc (kompatybilny z Virtual PC), vmdk (kompatybilny z VMWare 3 i 4)

`size` – ograniczenie górne rozmiaru, dysk “przyrostowy”

`-e` – czy obraz dysku ma być zaszyfrowany (tylko dla qcow).

Instalacja SO

Możliwość instalacji nowego systemu z

- płyty CD:

```
$ qemu.exe -L . -cdrom "\\.\D:" -hda hda.img -m 256 -boot d
```

- obrazu instalacyjnego systemu

```
$ qemu.exe -L . -cdrom my_os_install.iso -hda hda.img -m 256
  -boot d
```

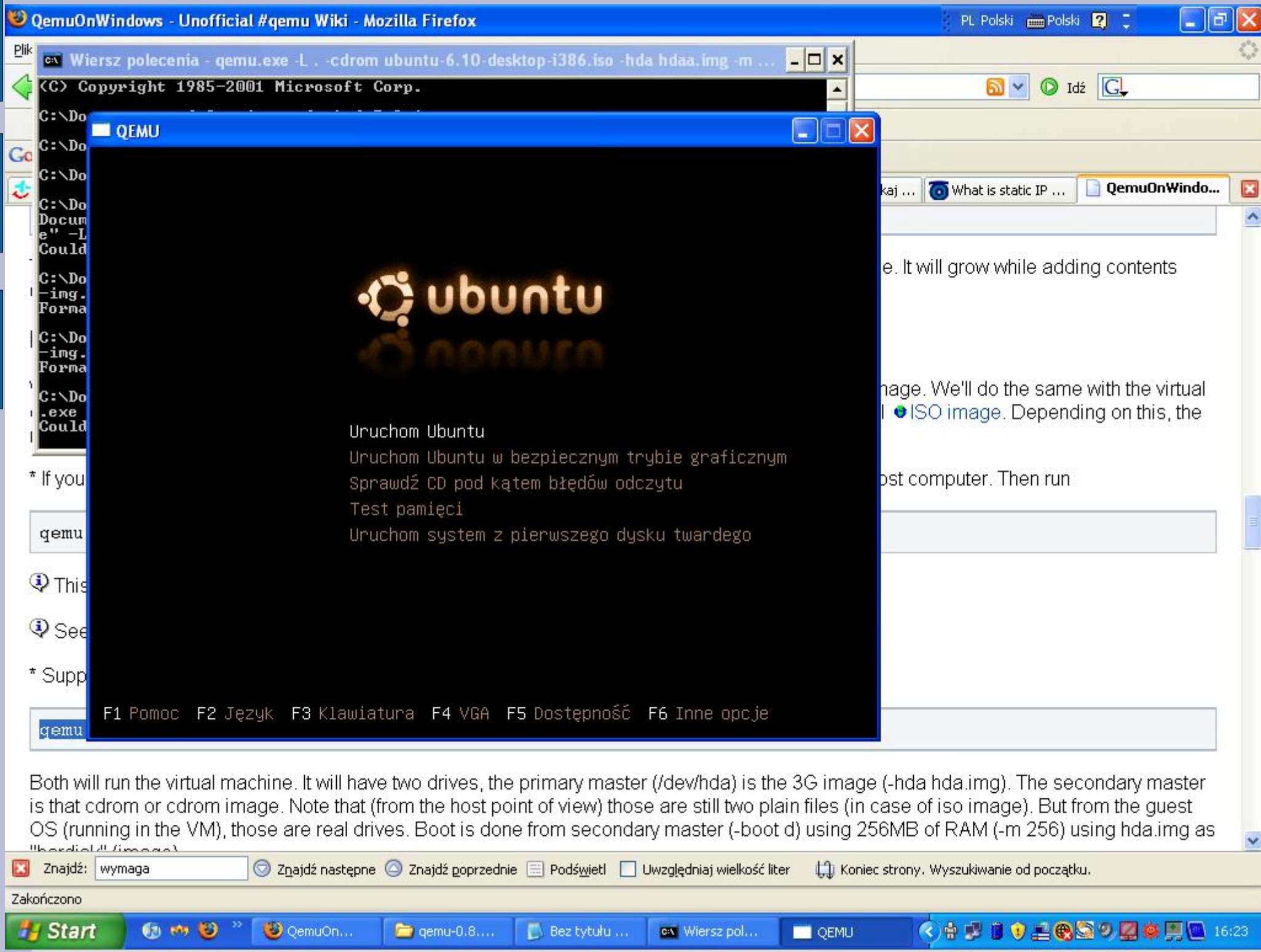
gdzie,

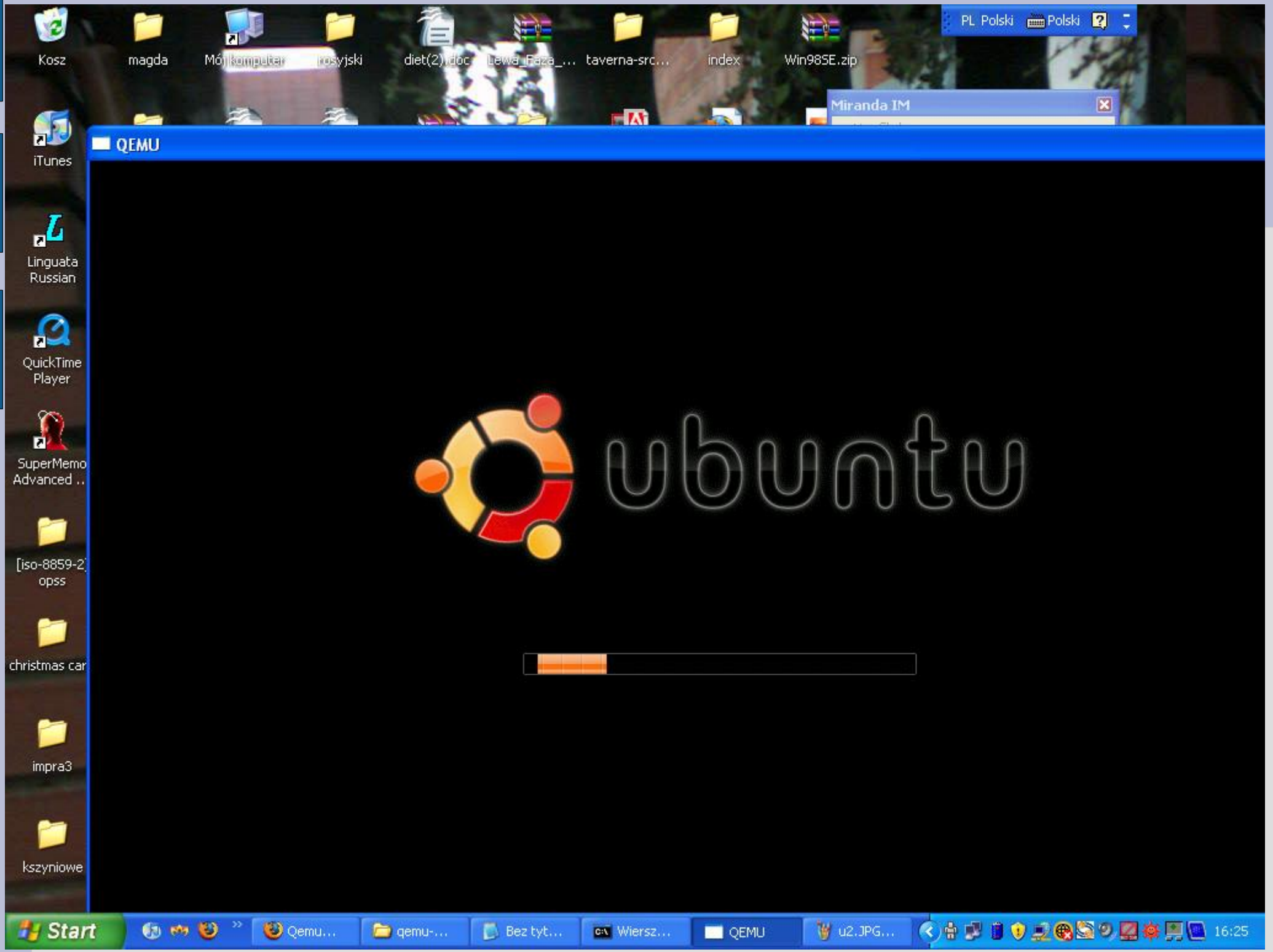
`-cdrom` – stacja dysków CD (z “ i \\), bądź nazwa pliku z obrazem,

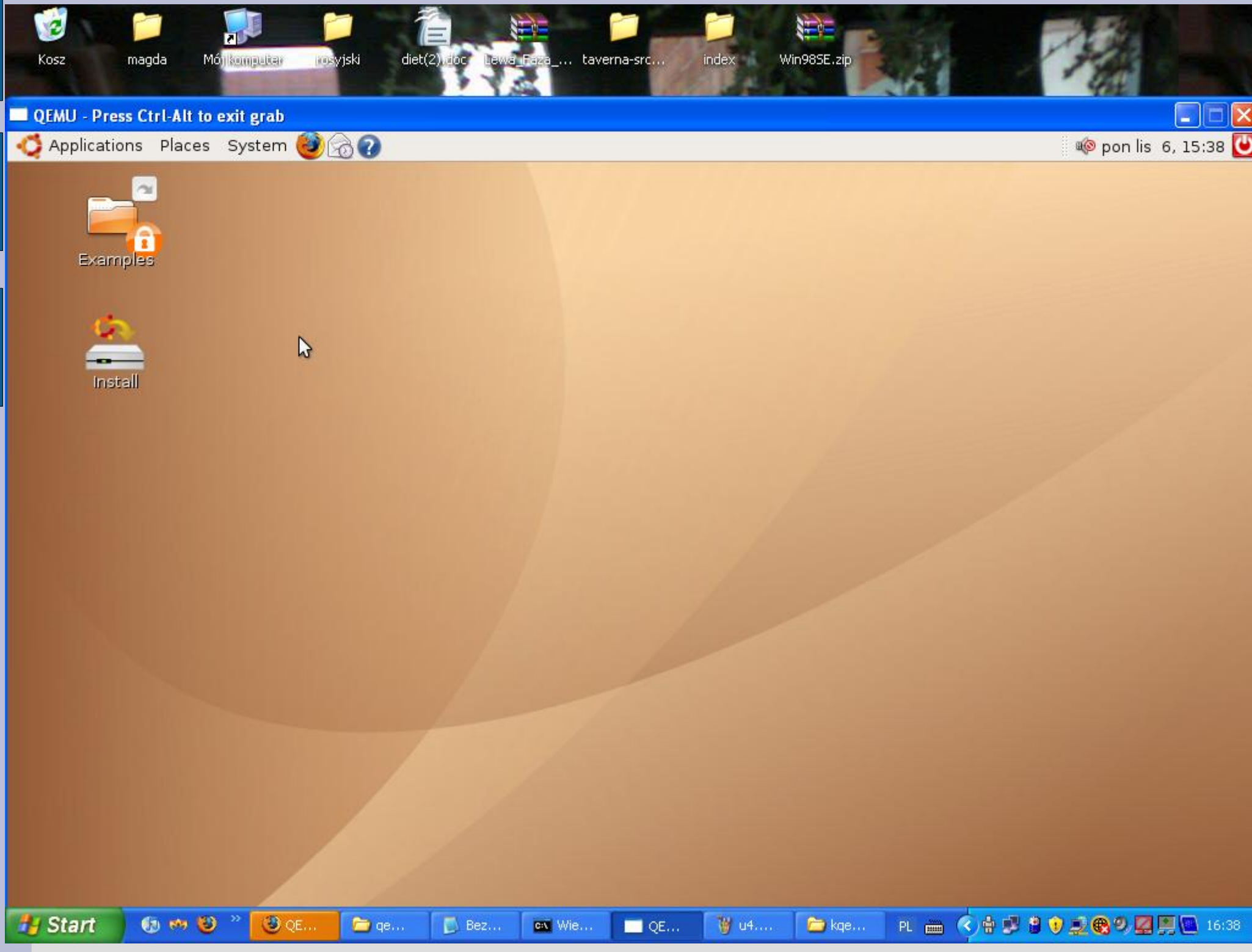
`-hda` – przygotowany wcześniej obraz dysku twardego,

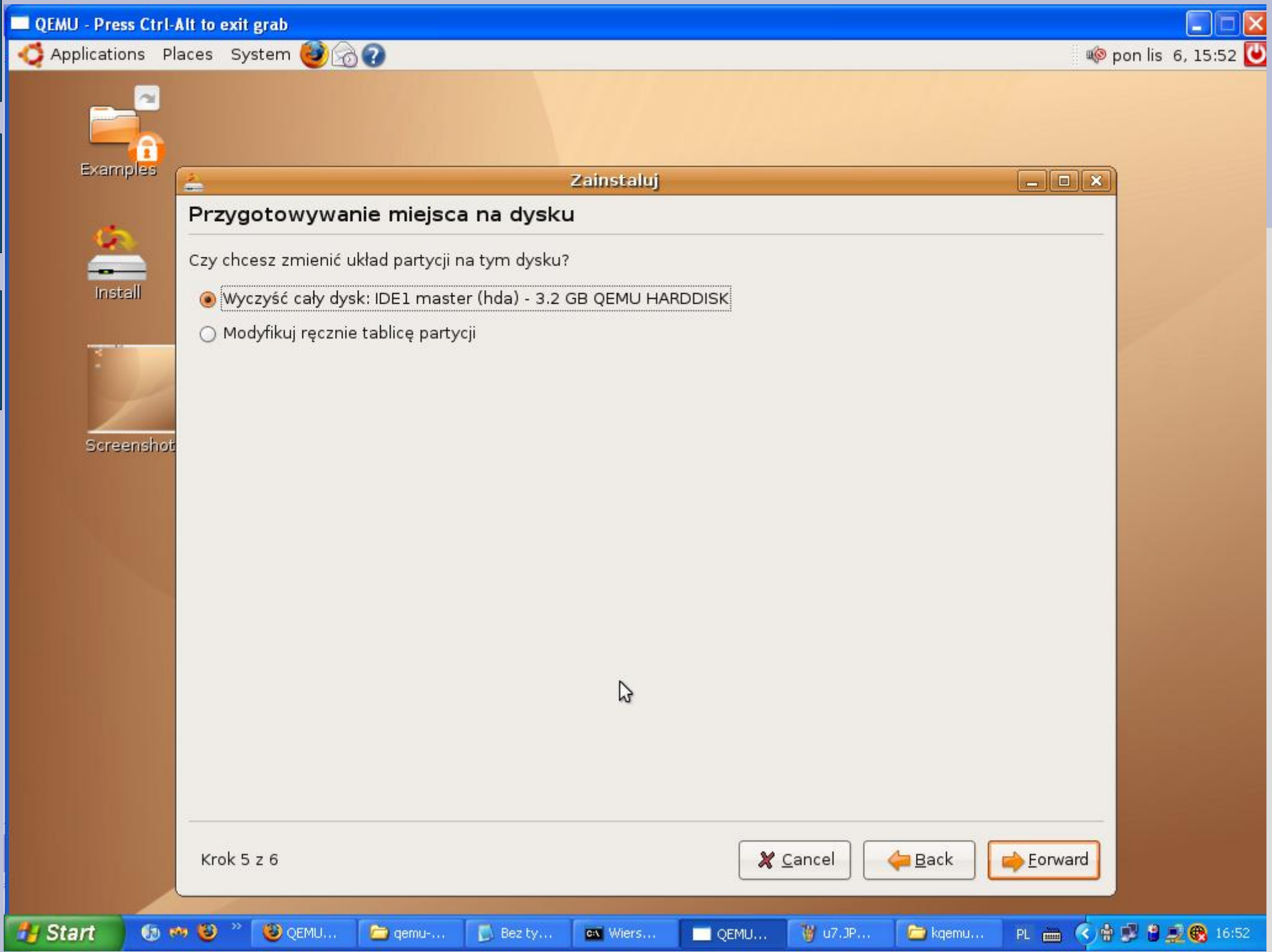
`-m` - ilość MB przydzielonej pamięci RAM na potrzeby instalacji

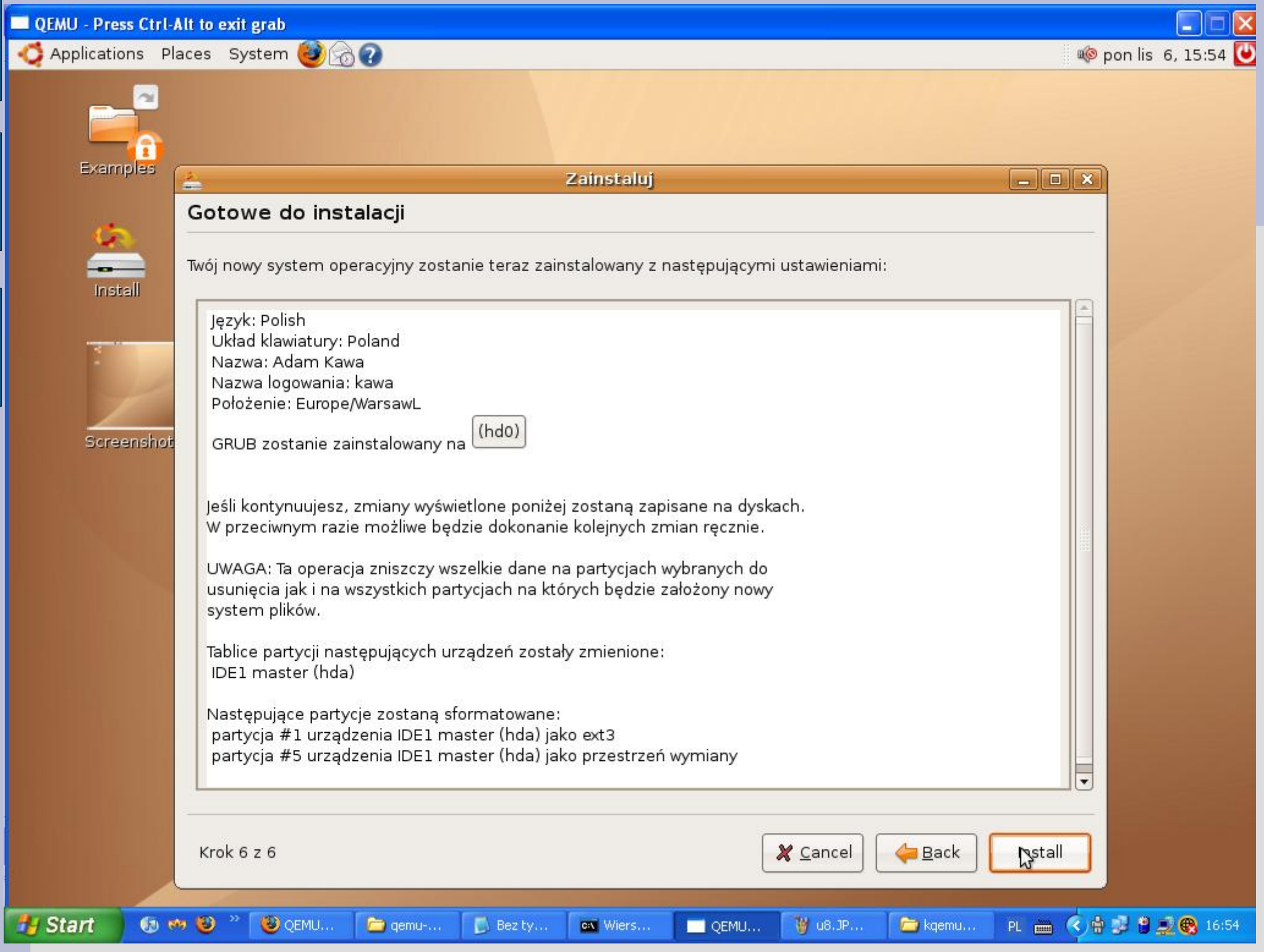
`-boot` – urządzenie bootujące

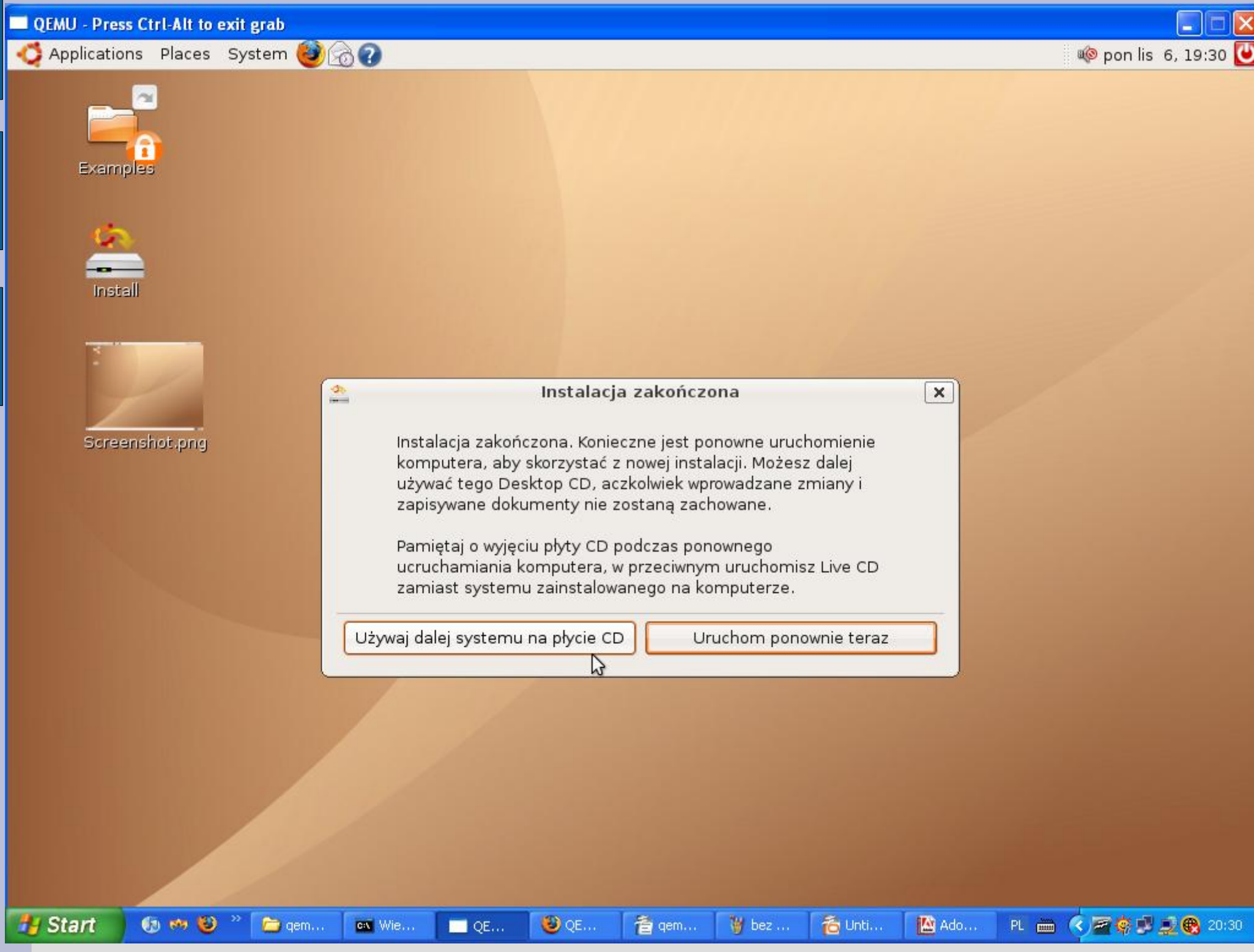

QemuOnWindows - Unofficial #qemu Wiki - Mozilla Firefox
Wiersz polecenia - qemu.exe -L . -cdrom ubuntu-6.10-desktop-i386.iso -hda hdaa.img -m ...
(C) Copyright 1985-2001 Microsoft Corp.
QEMU
ubuntu
Uruchom Ubuntu
Uruchom Ubuntu w bezpiecznym trybie graficznym
Sprawdź CD pod kątem błędów odczytu
Test pamięci
Uruchom system z pierwszego dysku twardego
F1 Pomoc F2 Język F3 Klawiatura F4 VGA F5 Dostępność F6 Inne opcje
ISO image. Depending on this, the
qemu
Both will run the virtual machine. It will have two drives, the primary master (/dev/hda) is the 3G image (-hda hda.img). The secondary master is that cdrom or cdrom image. Note that (from the host point of view) those are still two plain files (in case of iso image). But from the guest OS (running in the VM), those are real drives. Boot is done from secondary master (-boot d) using 256MB of RAM (-m 256) using hda.img as
Znajdź: wymaga
Znajdź następne
Znajdź poprzednie
Podświetl
Uwzględniaj wielkość liter
Koniec strony. Wyszukiwanie od początku.
Zakończono
Start
16:23


Kosz
magda
Mój komputer
rosyjski
diet(2).doc
Lewa_Faza_...
taverna-src...
index
Win98SE.zip
PL Polski
Polski
Miranda IM
iTunes
Linguata Russian
QuickTime Player
SuperMemo Advanced ..
[iso-8859-2]
opss
christmas car
impra3
kszyniowe
QEMU
ubuntu
Start
Qemu...
qemu-...
Bez tyt...
Wiersz...
QEMU
u2.JPG...
16:25


Kosz
magda
Mój komputer
rosyjski
diet(2).doc
Lewa_Faza_...
taverna-src...
index
Win98SE.zip
QEMU - Press Ctrl-Alt to exit grab
Applications
Places
System
pon lis 6, 15:38
Examples
Install
Start
QE...
qe...
Bez...
Wie...
QE...
u4....
kqe...
PL
16:38


QEMU - Press Ctrl-Alt to exit grab
Applications
Places
System
pon lis 6, 15:52
Examples
Install
Screenshot
Zainstaluj
Przygotowywanie miejsca na dysku
Czy chcesz zmienić układ partycji na tym dysku?
Wyczyść cały dysk: IDE1 master (hda) - 3.2 GB QEMU HARDDISK
Modyfikuj ręcznie tablicę partycji
Krok 5 z 6
Cancel
Back
Forward
Start
QEMU...
qemu-...
Bez ty...
Wiers...
QEMU...
u7.JP...
kqemu...
PL
16:52


QEMU - Press Ctrl-Alt to exit grab
Applications Places System
pon lis 6, 15:54
Examples
Install
Screenshot
Zainstaluj
Gotowe do instalacji
Twój nowy system operacyjny zostanie teraz zainstalowany z następującymi ustawieniami:
Język: Polish
Układ klawiatury: Poland
Nazwa: Adam Kawa
Nazwa logowania: kawa
Położenie: Europe/WarsawL
GRUB zostanie zainstalowany na (hd0)
Jeśli kontynuujesz, zmiany wyświetlone poniżej zostaną zapisane na dyskach.
W przeciwnym razie możliwe będzie dokonanie kolejnych zmian ręcznie.
UWAGA: Ta operacja zniszczy wszelkie dane na partycjach wybranych do usunięcia jak i na wszystkich partycjach na których będzie założony nowy system plików.
Tablice partycji następujących urządzeń zostały zmienione:
IDE1 master (hda)
Następujące partycje zostaną sformatowane:
partycja #1 urządzenia IDE1 master (hda) jako ext3
partycja #5 urządzenia IDE1 master (hda) jako przestrzeń wymiany
Krok 6 z 6
Cancel
Back
Install
Start
QEMU...
qemu-...
Bez ty...
Wiers...
QEMU...
u8.JP...
kqemu...
PL
16:54


QEMU - Press Ctrl-Alt to exit grab
Applications
Places
System
pon lis 6, 19:30
Examples
Install
Screenshot.png
Instalacja zakończona
Instalacja zakończona. Konieczne jest ponowne uruchomienie komputera, aby skorzystać z nowej instalacji. Możesz dalej używać tego Desktop CD, aczkolwiek wprowadzane zmiany i zapisywane dokumenty nie zostaną zachowane.
Pamiętaj o wyjęciu płyty CD podczas ponownego ucruchamiania komputera, w przeciwnym uruchomisz Live CD zamiast systemu zainstalowanego na komputerze.
Używaj dalej systemu na płycie CD
Uruchom ponownie teraz
Start
PL
20:30

Po zainstalowaniu..

- Po instalacji, uruchamiamy wirtualny komputer poleceniem:
  ```
  $ qemu -L . -hda hda.img -m 256
  ```
- Chyba wszystko działa... choć wolno...

Kqemu – QEMU Accelerator Module

- Aby przyśpieszyć jego działanie 5-10krotnie wykorzystujemy darmowy akcelerator – kqemu (http://fabrice.bellard.free.fr/qemu/download.html)
- Instalacja kqemu pod Windows:
  - Zainstalowanie kqemu.inf (prawy przycisk myszy + zainstaluj)
- Uruchomienie usługi kqemu moduł poleceniem

```
$ net start kqemu
```

- Używanie (dodatkowe opcje):
  - `-kernel-kqemu` – uruchamia wraz z akceleratorem (nie można jednak zrobić tego w czasie instalacji Windows jako systemu gościa)
  - `-no-kqemu` – uruchamiamy bez akceleratora

```
$ qemu -L . -hda hda.img -m 256 -kernel-kqemu
```