

Práce s disky a ISO soubory

Vytváření, připojování, virtuální mechaniky

Šárka Vavrečková

Ústav informatiky, FPF SU Opava

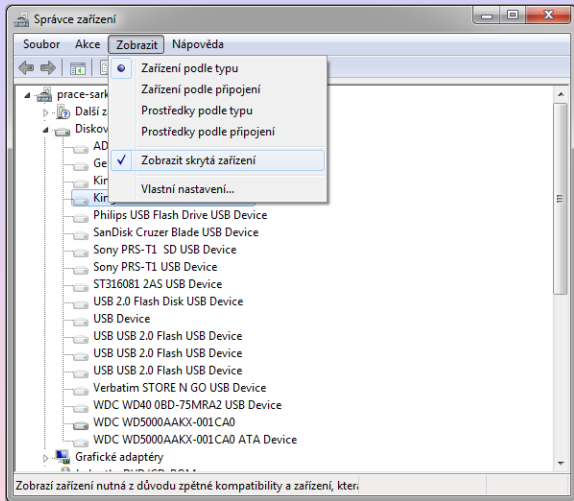
sarka.vavreckova@fpf.slu.cz

Poslední aktualizace: 8. října 2014

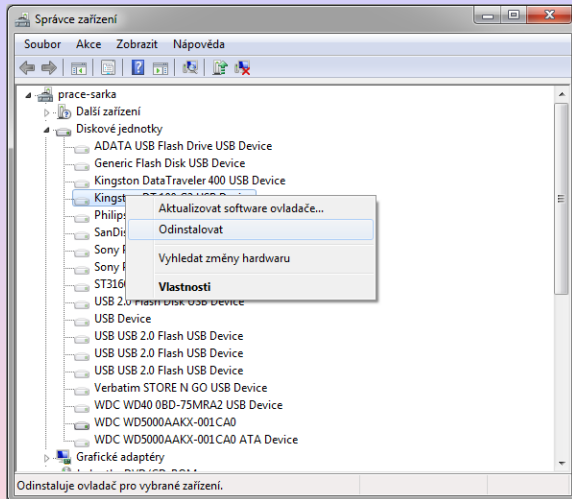
Jak zobrazit všechna zařízení

- ve Správci zařízení se nezobrazují všechna zařízení
- která ne: poškozená a právě nepřipojená
- občas potřebujeme zobrazit všechna
- jedno z mnoha využití: odstranění „chaosu“ v evidenci USB flash disků, které kdy byly k počítači připojeny
- jedno z mnoha využití: odstranění některých problémů s ovladači USB flash disků

The screenshot shows the Windows 7 'System' control panel window. The left sidebar has 'Úpravit nastavení systému' (Change system settings) circled in red, with an arrow pointing to the 'Úpravit nastavení systému' link in the main content area. Below this, the 'Proměnné prostředí' (Environment variables) window is open. In the 'System variables for current user' section, the 'devmgr_show_nonpresent_devices' variable is highlighted. A red circle is around the 'Nová...' (New...) button at the bottom of the window, with an arrow pointing to it.



Zobrazení všech zařízení



Změna způsobu připojení disku

Automatické připojení

- účel: abychom omylem nepozměnili data na disku
- jak na to:
 - spustíme Příkazový řádek s oprávněními správce
klepneme na Start, vyhledáme `cmd`, na ně pravým tlačítkem myši
 - zakážeme automatické připojování nových svazků
`mountvol /N`
 - až tuto vlastnost nebudeme potřebovat, znovu automatické připojování povolíme:
`mountvol /E`
- moc nefunguje, Windows si výměnné disky stejně připojují dle vlastního rozmaru

Změna způsobu připojení disku

Offline (nemá písmenko)

- účel: abychom se dostali k disku na nižší úrovni
- jak na to:
 - spustíme Příkazový řádek s oprávněními správce
klepneme na Start, vyhledáme `cmd`, na ně pravým tlačítkem myši
 - spustíme programové prostředí Diskpart
`diskpart`
 - tam zvolený (bohužel už připojený) disk vybereme a označíme *offline* (viz dále)
 - konec práce s Diskpartem: příkaz `exit`
- k čemu je to dobré: můžeme vytvořit ISO obraz disku
- kdybychom to neudělali: vytvoření ISO obrazu by zkrachovalo

```
DISKPART> list disk
```

Disk ###	Stav	Velikost	Volné	Dyn	Gpt
-----	-----	-----	-----	---	---
Disk 0	Online	465 GB	1024 KB		
Disk 1	Online	29 GB	0 B		
Disk 2	Online	37 GB	6144 KB		


```
DISKPART> list disk
```

Disk ###	Stav	Velikost	Volné	Dyn	Gpt
-----	-----	-----	-----	---	---
Disk 0	Online	465 GB	1024 KB		
Disk 1	Online	29 GB	0 B		
Disk 2	Online	37 GB	6144 KB		

```
DISKPART> select disk 2
```

Nyní je vybrán disk 2.

```
DISKPART> offline disk
```

Program DiskPart úspěšně převedl vybraný disk do offline režimu.

```
DISKPART> offline disk
```

Program DiskPart úspěšně převedl vybraný disk do offline režimu.

```
DISKPART> list disk
```

Disk ###	Stav	Velikost	Volné	Dyn	Gpt
-----	-----	-----	-----	---	---
Disk 0	Online	465 GB	1024 KB		
Disk 1	Online	29 GB	0 B		
* Disk 2	Offline	37 GB	6144 KB		

Změna způsobu připojení disku

Pouze pro čtení

- účel: abychom při práci s diskem omylem něco nepřepsali
- jak na to:
 - spustíme Příkazový řádek s oprávněními správce
 - spustíme programové prostředí Diskpart
 - tam zvolený (bohužel už připojený) disk vybereme a změníme jeho atributy

```
select disk xxxxx
attributes disk set readonly
```
 - konec práce s Diskpartem: příkaz exit
- problém: ve skutečnosti jsme zablokovali jen změnu *vlastností* oddílů, tj. musíme nastavit readonly spíše u oddílů disku

Změna způsobu připojení disku

Pouze pro čtení

- `diskpart`
- `list disk`
- `select disk xxxx`
- `list volumes`
- `select volume xxxx`
- `attr volume set readonly`
- až nebudeme potřebovat: `attr volume clear readonly`

Jak v diskpartu volat o pomoc:

- `help`
- `help attr`
- `help attr volume`

Změna způsobu připojení disku

Odpojení svazku

- svazek se dá odpojit i pomocí nástroje `fsutil`
- jak na to:
 - spustíme Příkazový řádek s oprávněními správce
 - zadáme (zde například pro oddíl připojený jako F:)
`fsutil volume dismount f:`
 - funguje pouze na místní disky, ne na výměnná média

Nápověda k `fsutil`:

```
fsutil ?
```

```
fsutil volume ?
```

```
atd.
```

- podmínka „pouze pro místní disky“ je paradoxní, výměnná média lze bohužel odpojit jen myší

Jak zjistit informace o svazku

Je to výměnné nebo místní (fixed) médium? A další informace

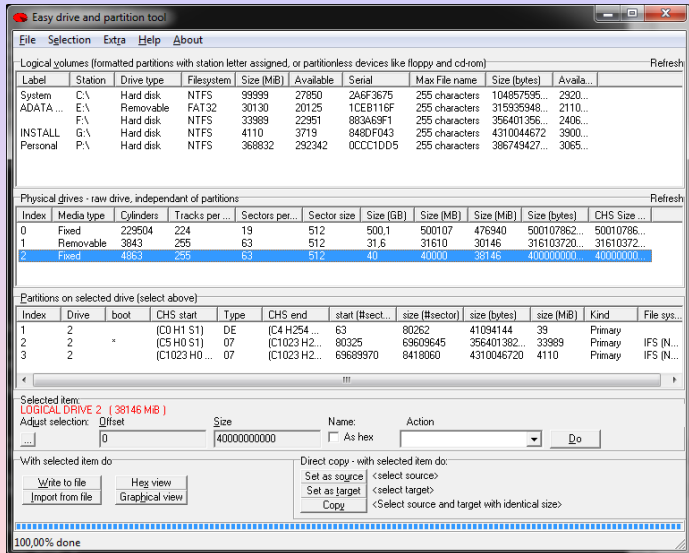
- `fsutil fsinfo drivetype f:`
- `fsutil fsinfo volumeinfo f:`

Jak vytvořit obraz disku

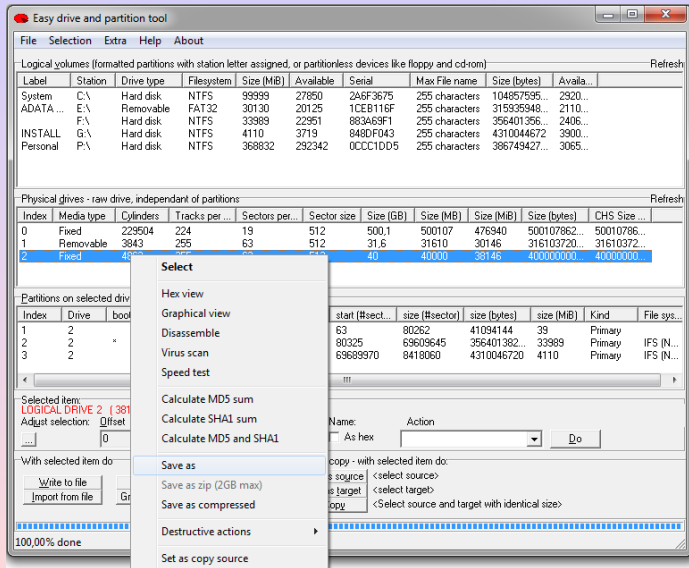
DuBaron Disk Image

- freeware, dostupné na <http://www.dubaron.com/diskimage/>
- zpřístupní všechny fyzicky připojené disky (i offline), jejich oddíly, vlastnosti
- umožní vytvořit ISO a jiné obrazy disku a oddílů, také uložit komprimované
- vytvoří kontrolní součty (MD5, SHA1)
- grafický i hexadecimální náhled disku

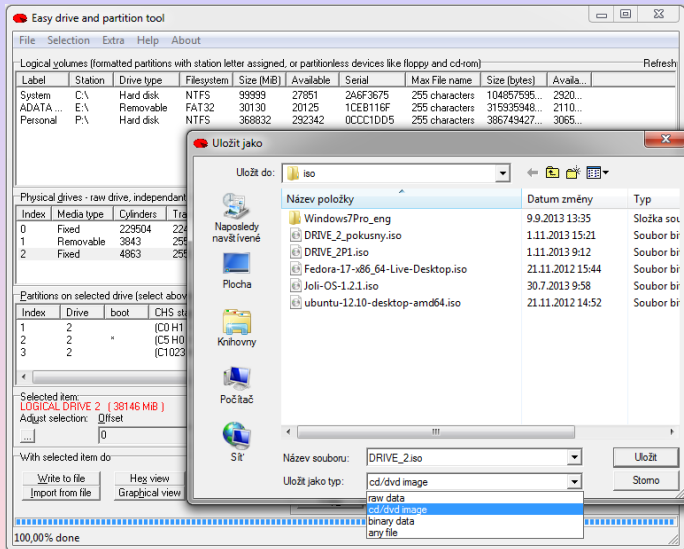
Vytvoření obrazu disku



Vytvoření obrazu disku



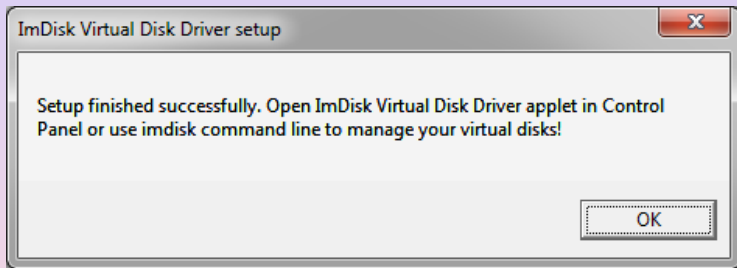
Vytvoření obrazu disku



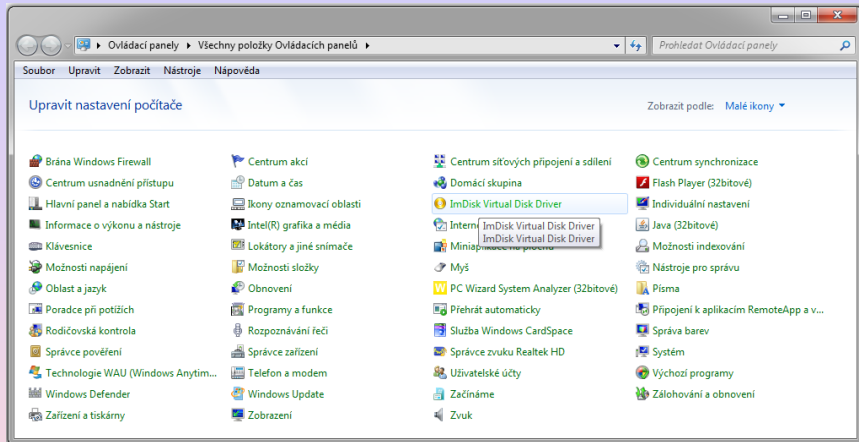
Připojení ISO obrazu disku

ImDisk

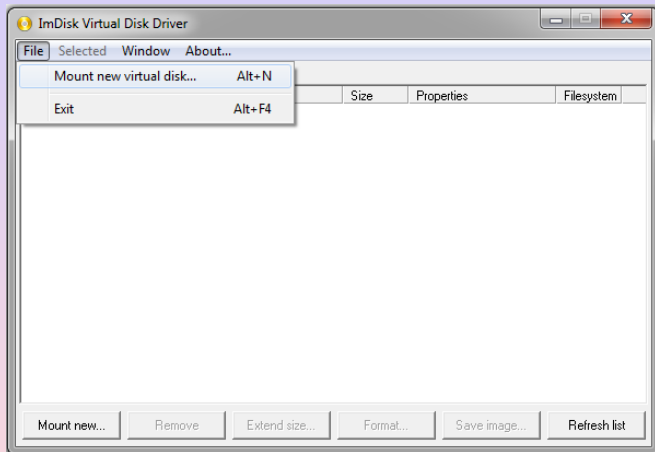
- freeware, dostupný na <http://www.ltr-data.se/opencode.html/#ImDisk>
- umožňuje pracovat s ISO obrazy tak, jako by šlo o běžná připojená datová média
- ovladač, který přidá do Ovládacích panelů ikonu (můžeme si vytvořit zástupce na ploše nebo připnout na Hlavní panel)
- umožňuje připojit obraz i jen pro čtení



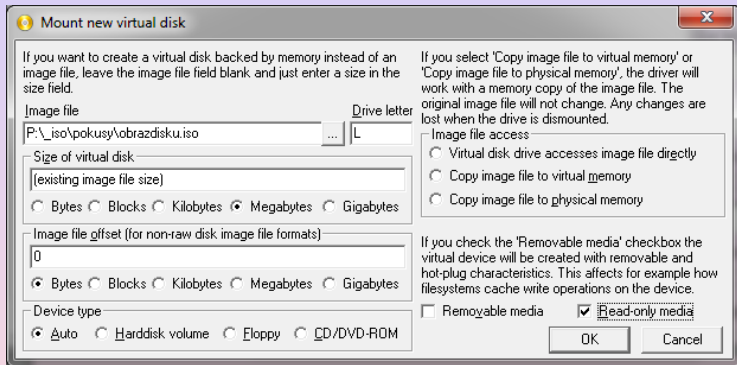
Připojení ISO obrazu disku



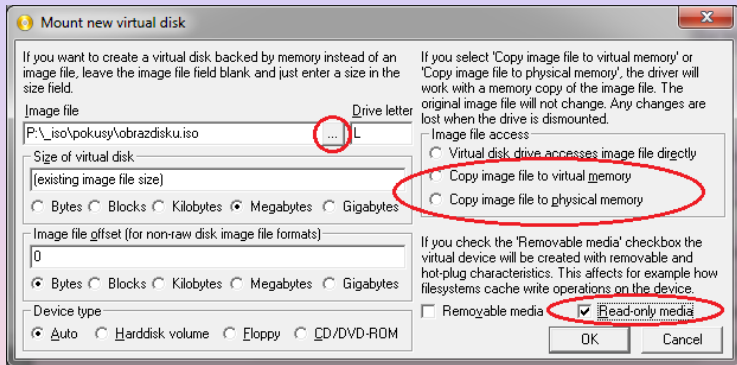
Připojení ISO obrazu disku



Připojení ISO obrazu disku



Připojení ISO obrazu disku



Linuxové distribuce

- většina „uživatelských“ distribucí Linuxu připojuje paměťová zařízení automaticky
- forenzní distribuce ne, některé Live distribuce taky ne
- konfigurace: viz nápovědu ke konkrétní distribuci, například pro Ubuntu:
<https://help.ubuntu.com/community/Mount/USB>
- obvykle se konfiguruje podle konkrétního grafického prostředí, může být také v `/etc/fstab`
- nejdřív vyzkoušet, jestli fungovalo, pak teprve používat „naostro“

Jak na paměťová média v Linuxu

Čím je charakterizováno paměťové médium

- ❶ ovladač – modul jádra
- ❷ speciální soubor – k nízkoúrovňovému přístupu k zařízení
/dev/sda první pevný disk
/dev/sdb druhý pevný disk
/dev/sda1 první oddíl prvního pevného disku
/dev/sda2 druhý oddíl prvního pevného disku
/dev/sdb1 první oddíl druhého pevného disku
- ❸ bod připojení (adresář/složka) – k vysokoúrovňovému přístupu, mají pouze bloková zařízení
/media/nějakýnázev (obvykle)

Nástroje

Připojení disku či obrazu pouze pro čtení

- `mount -o ro /dev/sdb1` (příp. podle parametrů)
- `mount -o ro /cesta/nazevsouboru.iso` (příp. podle parametrů)

Vytvoření obrazu disku

- předně disk/oddíl *odpojíme!!!*
(například `umount /dev/sdb1`)
- `dd if=/dev/sdb1 of=/dev/sda1/nazevsouboru.iso`
- `dd if=/dev/sdb1
of=/media/externidisk/nazevsouboru.iso`
- další parametry – `bs` (velikost bloků, které se kopírují „najednou“), chování v případě výskytu chyby, apod.
- takto lze taky vytvářet obrazy optických médií
- můžeme taky vytvořit ISO obraz obsahující vybrané soubory z disku (program `mkisofs`)

Jiné použití dd:

chceme oddíl na disku přepsat náhodnými čísly

```
dd if=/dev/random of=/dev/sda1 bs=4k  
(4 k = 4 KB = 4096 B)
```

chceme oddíl na disku přepsat znaky s ascii kódem 0

```
dd if=/dev/zero of=/dev/sda1 bs=4k
```

Dá se použít na celý disk – of=/dev/sda

Vytvoření obrazu disku

Jiné možnosti

- **ddrescue**
 - užitečný hlavně v případě, že je zdroj poškozený (nejdřív do obrazu extrahuje všechna OK data, pak se postupně pokouší obnovit poškozená data)
- **dcfldd, dc3dd**
 - podobně jako dd, ale některé funkce navíc (záznam průběhu, vytvoření hashe, apod.)

Kontrola integrity

Program pro vytvoření kontrolního součtu MD5

vygenerování MD5 hashe a uložení do souboru:

- `md5sum /dev/sdb1 > kontrola.txt`
- `md5sum isoobraz.iso >> kontrola.txt`

Program pro vytvoření kontrolního součtu SHA-1 nebo SHA-2

- `sha1sum isoobraz.iso`
 - vygeneruje hash SHA-1 (160bitový)
- `sha256sum isoobraz.iso`
 - vygeneruje hash SHA-2 (256bitový, nepoužívanější varianta je 256 bitů, SHA-2 umožňuje i 224, 384, 512, atd. bitů)

Kontrola integrity

Kontrola MD5

- `cd /nejakyadresar` (přesun do adresáře se soubory)
- (jsou tam soubory `isoobraz.iso` a `isoobraz.iso.md5`)
- `md5sum -c isoobraz.iso.md5`

Kontrola SHA-1 a SHA-2

- `cd /nejakyadresar`
- (jsou tam soubory `isoobraz.iso` a `isoobraz.iso.sha1`)
- `sha1sum -c isoobraz.iso.sha1`
- `sha256sum -c isoobraz.iso.sha1`

Grafický nástroj: **gtkhash** (je třeba nainstalovat)

Mac OS X

- `cd /nejakyadresar`
- `shasum -a 256 isoobraz.iso`

nebo program HashTab

Přístup k oddílům s různými souborovými systémy

V Linuxu:

- ext2fs, ext3fs, ext4fs, RaiserFS
- XFS, JFS, atd.
- FAT, VFAT, NTFS, obvykle také exFAT
- HFS+
- UDF, ISO9660 (CDFS)
- ovladače dalších souborových systémů už v základu
- možnosti rozšíření

Přístup k oddílům s různými souborovými systémy

Ve Windows:

- FAT, VFAT, NTFS, ve vyšších verzích také exFAT
- UDF, ISO9660
- ext2fs: lze doinstalovat ovladač Ext2Fsd (<http://www.ext2fsd.com/>)
- HFS: Java aplikace HFS Explorer (<http://www.catacombae.org/hfsx.html>)
- horší možnosti rozšíření, nutno shánět ovladače souborových systémů

Skryté oblasti na disku

Host Protected Area (HPA)

- používají distributoři PC, běžný uživatel (ani v BIOSu) nemá do HPA přístup, ani tu oblast nevidí
- dá se tam dostat pomocí speciálních ATA příkazů (od verze ATA 4)
- program `hdparm` (pro Windows i Linux), volně dostupný
- program `MHDD` (bootovací, postavený na FreeDOS) umí HPA zviditelnit a pracovat s ním
- forenzní distribuce dto. (Sleuth Kit apod.)

HPA

Zjištění HPA v Linuxu

```
hdparm -N /dev/sdb
```

```
/dev/sdb:
```

```
max sectors = 78125000/78165360, HPA is enabled
```

Zrušení HPA v Linuxu

```
hdparm -N p78165360 /dev/sdb
```

```
(pozor, pro /dev/sdb destruktivní)
```

Skryté oblasti na disku

Device Configuration Overlay (DCO)

- taktéž určen pro skrytí dat, od verze ATA 6
- pokud je na HDD jen DCO, je to v podstatě podobný případ jako HPA
- problém: kombinace obou typů oblastí (na konci adres nejdřív HPA a pak DCO) – velice náročné vytvořit odpovídající nepozměněný obraz disku

DCO

Zjištění DCO v Linuxu

```
hdparm --dco-identify /dev/sdb
```

```
/dev/sdb:
```

```
DCO Revision: 0x0001
```

```
The following features can be selectively disabled via  
DCO:
```

```
Transfer modes:      .....
```

Zrušení DCO v Linuxu

```
hdparm --dco-restore /dev/sdb      (zobrazí se varovné hlášení)
```

```
hdparm --yes-i-know-what-i-am-doing --dco-restore /dev/sdb
```

Přístup k těmto oblastem

ATA příkazy

Proces s určitými oprávněními může komunikovat s ovladačem disku a posílat ATA příkazy

- sada ATA příkazů pro verzi ATA 8 (z roku 2006):
<http://www.t13.org/documents/uploadeddocuments/docs2006/d1699r3f-ata8-ac.pdf>
- API funkce `DeviceIoControl(...)`
- o ATA registrech a komunikaci s pevnými disky:
http://martin.lipinsky.cz/skola/pz/pz_08_ata-atapi-sata.pdf

Removable Media Bit (RMB)

Kdy je médium výměnné:

- optický (CD/DVD/Blu-Ray) disk je výměnné médium
- USB flash disk je výměnné médium
- externí disk připojovaný přes USB/eSATA/... není výměnné médium

Removable Media Bit (RMB)

Čím je to určeno:

- RMB bit ve vlastnostech firmwaru (nastaven na 1: výměnné médium), bit 7 prvního oktetu příkazu „SCSI Inquiry Data response“
- ovladač tento fakt zjistí od jádra žádostí *StorageDeviceProperty*
- týká se především paměťových zařízení připojovaných přes USB, která vnitřně komunikují SCSI příkazy
- změna hodnoty RMB bitu není zrovna bezpečná, navíc není řečeno, že to půjde (Lexar's BootIt)

Removable Media Bit (RMB)

V čem je problém

- Linux: v podstatě bez problémů
- Windows:
 - na výměnném médiu odmítají „vidět“ více než jeden oddíl
 - výměnné médium nelze označit offline ani připojit pouze pro čtení
 - když chceme vytvořit obraz, tak pouze konkrétního oddílu, nikoliv celého disku

```
http://msdn.microsoft.com/en-us/windows/hardware/gg487419.aspx
http://www.t10.org/
http://msdn.microsoft.com/en-gb/library/ff566971%28VS.85%29.aspx
http://ubuntuforums.org/showthread.php?t=1020293
```