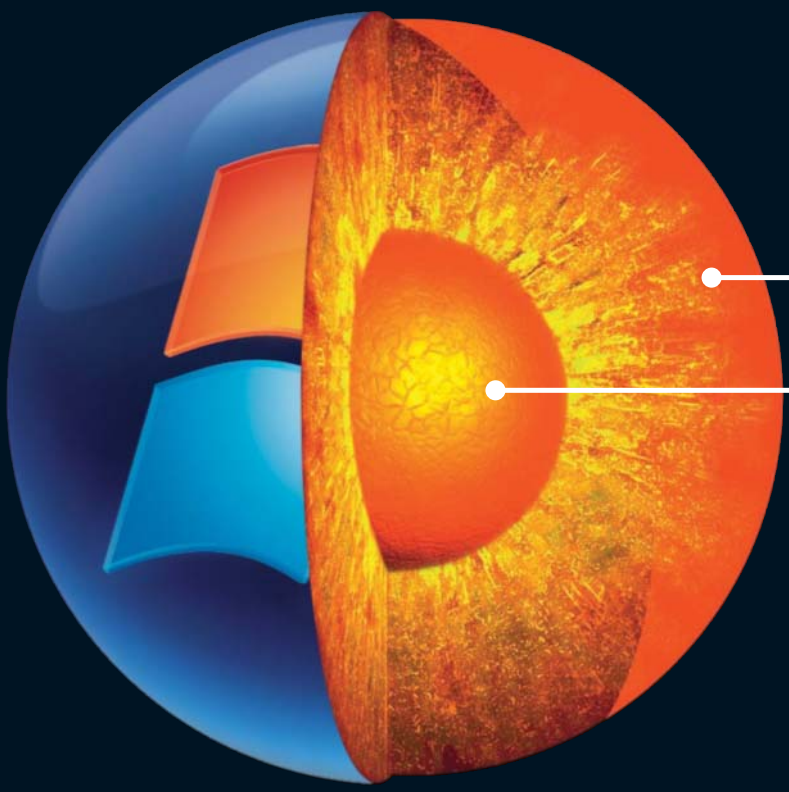
Speciální mise: Cesta do jádra Windows

Chip se rozhodl podniknout cestu až do srdce Windows, tedy tam, kam se běžný uživatel většinou nedostane. Právě v jádře systému lze vyřešit potíže s ovladači. Vydejte se na tuto výpravu s námi.

Markus Hermannsdorfer, Vratislav Klega, vratislav.klega@chip.cz



Co leží pod desktopem?

Pod vnější vrstvou Windows (user mod) fungují ovladače jako tektonické desky. Když jsou s nimi potíže, vyvolají zemětřesení, které se projeví i na povrchu.

Musíme dovnitř

Abychom mohli desky opravit, musíme se vydat až k samotnému zdroji problémů – do jádra Windows. A jak poznáte, že je nejvyšší čas vyrazit? Když Windows zobrazují modré obrazovky.

V tomto článku najdete

Začalo to docela nevinně. „Můžete mi pomoci? Můj USB port přestal fungovat," zněla prosba jednoho z našich čtenářů. „Samozřejmě," odpověděli jsme. To jsme ještě netušili, jaké dobrodružství nás čeká: cesta přímo do srdce Windows. Jen tam je totiž možné řešit velké problémy operačního systému.

Nechcete se k nám přidat? Výsledkem bude rychlejší počítač a stabilnější běh systému – jak XP, tak Visty. Cesta je navíc snazší, než se může zdát. Veškeré nástroje, které budeme pro „provrtání se do jádra" potřebovat, jsou buď přímou součástí operačního systému, nebo je naleznete na Chip DVD. Po tomto dobrodružství se stanete znalcem jádra Windows a modré obrazovky, kterých jste se dosud báli, budou pro vás zdrojem důležitých informací.

TEST OVLADAČŮ

Dobrodružství začíná

Nejprve je třeba podívat se na „zemský povrch", tedy na samotný počítač. Uživatel instaloval nejrůznější USB gadgety a různé hardwarové komponenty. Právě při instalování nového zařízení hrozí s největší pravděpodobností zemětřesení. Zapnuli jsme tedy počítač. Ten se začal spouštět a ještě předtím, než jsme se dostali do Windows, nastal pád s modrou obrazovkou. Usměv na tváři nám rázem ztuhl.

Správce zařízení: Náš první krok byl jasný – odpojili jsme USB zařízení, o kterém jsme se domnívali, že je pravděpodobným zdrojem problémů. Správná trefa. Bez nehody jsme se dostali až do Windows. Nyní jsme se mohli propracovat až ke Správci zařízení, který nám prozradil všechny informace o hardwaru a problémových ovladačích. Žlutý vykřičník u řady produktů nám prozradil, kde leží zakopaný

Chybové kódy Správce zařízení v XP

Nastane-li u hardwaru nebo ovladače nějaký problém, Správce zařízení u něj nakreslí varovný symbol – otazník nebo vykřičník. Pokud poté kliknete pravým tlačítkem myši na tuto nekorektně pracující položku a zvolíte vlastnosti, zobrazí Správce zařízení podrobné informace. V rámečku Stav zařízení se pak nachází kód chyby. Pro porozumění těmto kódům se stačí podívat do vedlejší tabulky. Kromě vysvětlení nabízíme i krátký návod na řešení problému. Další informace získáte na webové stránce **http://support.microsoft.com/kb/310123/cz**.

Chybový kód	Problém	Řešení
Kód 1	Není nainstalován ovladač, problém s konfigurací.	Aktualizace ovladače.
Kód 3	Chybný ovladač nebo málo operační paměti.	Nahrazení ovladače, rozšíření RAM.
Kód 10	Chybí záznam v registrech.	Aktualizace ovladače.
Kód 12	Dvě zařízení používají stejné prostředky.	Jedno zařízení deaktivovat.
Kód 14	Zařízení čeká na reset počítače.	Restartovat počítač.
Kód 16	Zařízení je poškozené nebo chybně nakonfigurované.	Test na UPnP, ruční konfigurace.
Kód 18	Poškozený ovladač.	Nová instalace ovladače.
Kód 19	Pro zařízení je nainstalováno více ovladačů, nebo je ovladač poškozený.	Nová instalace zařízení.
Kód 21	Odinstalování zařízení není dokončeno.	Restartovat počítač.
Kód 22	Zařízení je zakázáno uživatelem.	Povolit zařízení.
Kód 24	Chyba hardwaru nebo ovladače.	Nová instalace ovladače nebo odstranění hardwaru.
Kód 28	Ovladače nejsou nainstalovány.	Nainstalovat ovladače.
Kód 29	Zařízení je zakázáno v BIOS.	Povolit v BIOS.
Kód 31	Systém nemůže načíst ovladače.	Aktualizace ovladače.
Kód 32	Ovladač byl zakázán v registrech.	Aktualizace nebo nová instalace ovladače.
Kód 33	Chyba hardwaru.	Výměna hardwaru nebo jeho oprava.
Kód 34	Zařízení je třeba nastavit ručně.	Pomocí jumperů na zařízení proveďte konfiguraci.
Kód 35	BIOS neumí rozpoznat toto zařízení.	Aktualizace BIOS.
Kód 36	Chybné nastavení přerušení (IRQ) v BIOS.	Konfigurace přerušení v BIOS ručně.
Kód 37	Ovladač vrátil chybu „DriverEntry“.	Ovladač odinstalovat a znovu nainstalovat.
Kód 38	V RAM je stará verze ovladače, nový nelze zavést.	Restartovat počítač.
Kód 39	Systém nenašel ovladač.	Nová instalace ovladače.
Kód 40	Chybný záznam v registrech.	Ovladač odinstalovat a znovu nainstalovat.
Kód 41	Ovladač zaveden, ale hardware není připraven.	Hardware buď není plug and play, nebo je špatně nakonfigurovaný.
Kód 42	Na sběrnici jsou dvě identická (duplikátní) zařízení.	Restartovat počítač nebo odstranit duplikátní hardware.
Kód 43	Ovladač ohlásil chybu zařízení.	Záleží na příčině, vyžádat si u výrobce opravený ovladač.
Kód 44	Program nebo služba vyřadily ovladač.	Restartovat počítač.
Kód 45	Chybný ovladač, nebo není zařízení připojeno.	Ovladač opravit, nebo připojit zařízení.
Kód 46	Operační systém se vypíná.	Hardware bude funkční po příštím spuštění.
Kód 47	Zařízení již bylo odebráno a je nachystáno k vyjmutí.	Funkční bude po příštím připojení.
Kód 48	Chybný ovladač.	Nainstalovat správný ovladač.
Kód 49	Do registrů již není možné přidat další hardware.	Vyčistit a defragmentovat registry.

Na Chip DVD

Bez náležitého vybavení by cesta do jádra nebyla úspěšná. Veškerý potřebný software naleznete na Chip DVD.

Driver Magician Lite
Práce s ovladači

DriverMax
Hledání a aktualizace ovladačů

UPnP-Test
Testuje plug and play zařízení

PowerStrip
Zpřístupní nové funkce

cFOS
Optimalizuje ADSL

DFX pro Winamp
Plug-in pro lepší kvalitu zvuku

The Driver Packs Base
Komfortní stahování ovladačů

pes. Pro detailní prozkoumání problému jsme správce zavřeli a znovu jsme připojili zařízení.

Nyní zpět do Správce zařízení – varovný symbol se nyní nachází u zařízení „Kořenový rozbočovač USB“. Nezbývá než kliknout pravým tlačítkem myši a zvolit *Vlastnosti*. Windows jen suše konstatují: „Zařízení nebylo nalezeno nebo nepracuje správně, případně nemá nainstalovány všechny ovladače (Kód 24).“ To nám opravdu pomůže – prakticky to může být cokoliv!

Typická chyba USB zařízení, která nemají dostatečné množství elektrického proudu. Jeden pohled do záložky napájení však prozrazuje, že zařízení požaduje proud 500 miliampér a že kořenový rozbočovač ho je schopen dodávat.

Sigverif: Nyní zkusíme překontrolovat ovladače USB, přesvědčilo nás velké množství varovných symbolů ve Správci zařízení. Proto mačkáme *Start* | *Spustit* a zadáváme příkaz

```
sigverif
```

Jedná se o nástroj integrovaný ve Windows, který vypisuje všechny nepodepsané ovladače. Je-li ovladač podepsaný, byl zkontrolován ve „Windows Hardware Quality Labs“ a není nebezpečný ani pro srdce Windows, ani pro žádné další orgány operačního systému. Po spuštění jsme klikli na Upřesnit a zvolili jsme *Vyhledat další soubory, které nejsou digitálně podepsané.*

Aby nástroj vyhledával jen ovladače, omezili jsme hledání jen na složku C:\Windows\System32\Drivers. Poté stačí kliknout na *OK* a spustit prohledávání. Po chvíli se zobrazí seznam nepodepsaných ovladačů. Pro podrobnější informace lze kliknout na položky *Zavřít* | *Upřesnit* | *Protokolování* | *Zobrazit protokol.* Zobrazí se soubor SIGVERIF.TXT, který obsahuje podrobné informace.

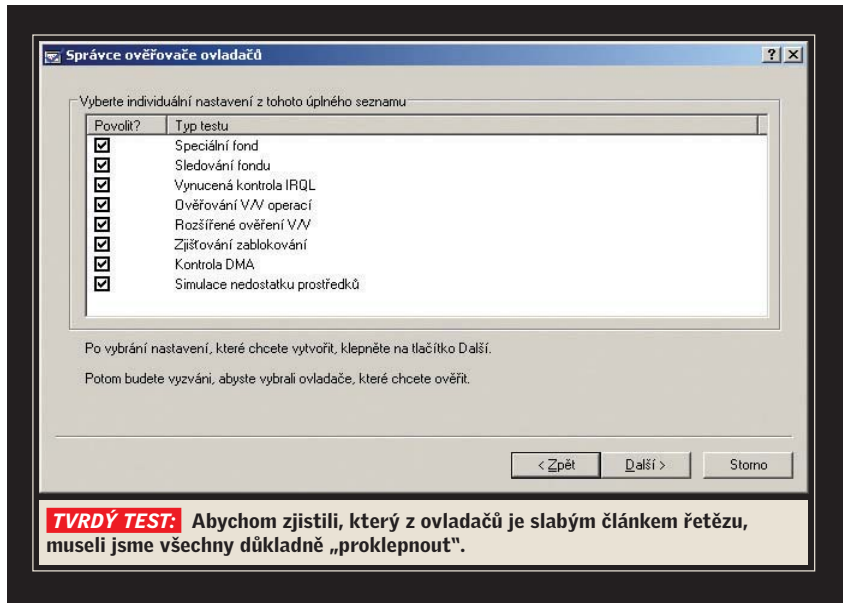
Verifier: Nyní přistoupíme k hledání černé ovce. Abychom ověřili, který ovladač je chybný, necháme všechny nepodepsané ovladače projít zátěžovým testem. To lze →

→ provést velmi jednoduše: stačí zvolit *Start* | *Spustit* a zadat příkaz

```
verifier
```

Pro nejvyšší přesnost je nutné zvolit položku *Vytvořit uživatelská nastavení (pro vývojáře kódu)* | *Vybrat individuální nastavení z úplného seznamu*. Zde je k dispozici osm různých scénářů testování ovládačů, jako je třeba „Simulace nedostatku prostředků". Pro otestování skutečně všech částí ovladače je nutné zaškrtnout všech osm voleb. V dalším kroku vybereme položku *Automaticky vybrat nepodepsané ovladače* a klikneme na tlačítko *Další*. Ale ouha – nepodepsaných ovladačů je nějak málo, přesněji mnohem méně, než kolik jsme našli v předchozím kroku pomocí nástroje sigverify. To nám ale nevadí. Vrátíme se o krok zpět a zvolíme příkaz *Vybrat ovladače ze seznamu*.

Pomocí logu, který vytvořil sigverify, během chvilky vytvoříme seznam ovladačů, které je třeba zkontrolovat. Poté už stačí restartovat počítač a testování ovladačů může začít. Teď teprve začíná to opravdové dobrodružství.



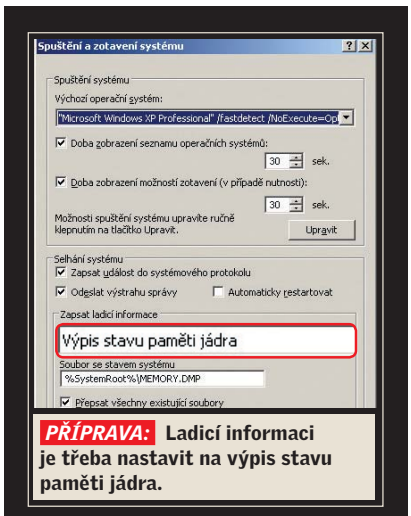
TVRDÝ TEST: **Abychom zjistili, který z ovladačů je slabým článkem řetězu, museli jsme všechny důkladně „proklepnout".**

HLEDÁNÍ CHYBNÉHO OVLADAČE

Cesta k jádru

Připojujeme zařízení a spouštíme PC – opět se zobrazuje modrá obrazovka s hlášením „STOP: 0x0000000A IRQ_OR_LESS_EQUAL". Profesionálové samozřejmě hned vidí, že problém je v ovladači. Ale ve kterém? A proč? To může prozradit jen jádro Windows. To komunikuje s uživatelem právě pomocí modrých obrazovek.

Je třeba ponořit se na samé dno Windows. K tomu je ovšem nutné znovu se dostat do Windows. Pomocí klávesy [F8] spustíme systém ve stavu nouze a zadáme příkaz, který ukončí zátěžový test:



PŘÍPRAVA: **Ladicí informaci je třeba nastavit na výpis stavu paměti jádra.**

```
verifier /reset
```

Když je test ukončen, nastartují Windows zase normálně.

Nyní to bude o něco těžší. Uživatelé Windows totiž mají přístup jen k aplikacím – k jádru se tedy nemohou dostat. Z tohoto důvodu je téměř nemožné, aby uživatel vyvolal pád jádra. Jiné je to s ovladači. Ty běží v kernel modu a s jádrem přímo komunikují. Pokud dva různé ovladače v jednom okamžiku přistupují ke stejným prostředkům počítače v jádře, dojde ke konfliktu. Jádro samotné poté hlásí uživateli konflikt prostřednictvím známé hlášky „IRQ_OR_LESS_EQUAL".

Díky tomu můžeme vidět do jádra hned při jeho práci a takřka jej i vyfotografovat. K tomu však nesmí obraz jádra hned zmizet. Zvolíme nabídku *Ovládací panely* | *Systém* | *Upřesnit*, v rámečku Spuštění a zotavení systému klikneme na volbu *Nastavení* a deaktivujeme zaškrtnutí u položky *Automaticky restartovat*. V části Zapsat ladicí informace zvolíme položku *Výpis stavu paměti jádra*. Všechna okna potvrdíme kliknutím na tlačítko *OK*.

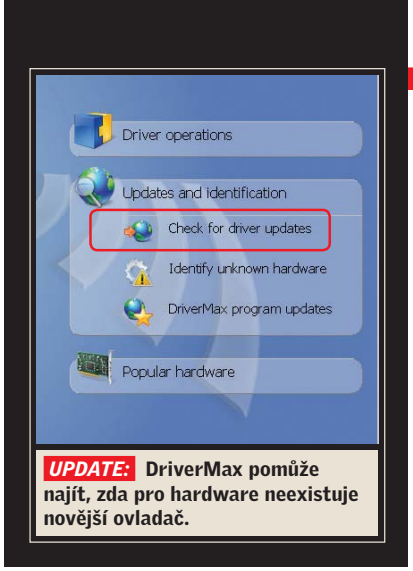
Jelikož jsme ovladač odchytili in flagranti, tedy přesněji při kolizi, znovu vyskočila modrá obrazovka. Tentokrát je však něco jinak – při havárii se vytvořil obraz jádra, který nám pomůže odhalit, proč se modrá obrazovka zobrazila.

Dříve než se pokusíme identifikovat škodlivý ovladač, je třeba provést dvě důležité věci. Nejprve vypneme verifier z prostředí nouzového stavu systému. Aby nebyl obraz jádra přepsán, v okně Spuštění a zotavení systému opět zvolíme ladicí informace do modu „Omezený výpis stavu paměti". Po nastartování Windows začne lov na defektní ovladač.

Aby bylo možné pohodlně číst vytvořený logovací soubor, potřebujeme nástroj „Debugging Tools for Windows". Nástroj se nachází na Chip DVD, soubor má necelých 17 MB. Instalace je automatická, po jejím dokončení zvolíme *Start* | *Všechny programy* | *Debugging Tools for Windows* | *WinDbg*. K tomu, abychom správně interpretovali obraz uloženého jádra, bude nutné využít Symbol Server, který pomůže provést analýzu vytvořeného logu. V programu WinDbg zvolíme *File* | *Symbol file path* a do zobrazeného okna zadáme příkaz

```
SRV*C:\Symbols*http://msdl.microsoft.com/download/symbols
```

Nyní v programu zvolíme *File* | *Open Crash Dump* a otevřeme soubor, který byl vytvořen po pádu systému. Nazývá se MEMORY.DMP a nachází se ve složce C:\Windows. Při otevření položí program otázku „Save information for workspace?". Klikneme na *Yes*. Otevře se okno „Command". Do něj se začnou načítat informace ze souboru. Načtení však nějakou dobu trvá, můžeme čekat i minutu. Poté můžeme začít studovat výpis. Ze všeho nejzajímavější je řádka „Probably caused by :". Za ní je napsáno, co způsobilo havárii systému. Je-li důvodem pádu soubor, který má koncovku .SYS, pak se jedná o hardwarový ovladač. Čísla v šestnáctkové soustavě, která se nachází v části Bugcheck, také →



UPDATE: **DriverMax pomůže najít, zda pro hardware neexistuje novější ovladač.**

→ poznáváme. Jsou to ta samá čísla, která se zobrazují na modré obrazovce za hláškou „STOP:“.

Jelikož nám WinDbg stále ještě neprozradil, o jaký ovladač se jedná, zkusíme použít příkaz

```
!analyze -v
```

Jeho pomocí lze totiž zjistit další podrobnosti. Pokud objeví nějakou známou chybu, vypíše k ní i detaily. Například k chybě „IRQ_OR_LESS_EQUAL“ vypíše podrobné chybové hlášení, bohužel pouze v anglickém jazyce. Stačí najít část „STACK_TEXT“. Přímo zde se nachází jméno a také adresa funkce jádra, která byla vyvolána těsně před pádem, a která je tedy s největší pravděpodobností odpovědná za zhroucení systému. Funkci jádra bezpečně poznáme tak, že začíná na „nt!“. Tento pád se vyskytuje právě tehdy, když ovladač koliduje s nějakou službou ve Windows.

Zkoumání však opět nepřineslo žádnou odpověď, protože v bloku STACK_TEXT začínají všechny řádky na nt!.

Nic naplat, je nutné použít komando. Stačí zadat příkaz

```
!thread
```

Tím se zobrazí soubory, se kterými bylo pracováno během pádu. Konečně úspěšná trefa! WinDbg zobrazuje seznam, ze kterého kopírujeme šestnáctkové číslo a zadáváme příkaz, který vypadá takto:

```
!irp f8978ffc
```

Příkaz nám prozrazuje, že během pádu byl vyslán vstupně-výstupní požadavek (I/O Request Packet, IRP) na adresu „f8978ffc“. Dva ovladače, jejichž název je dole přímo uveden, zkoušely ve stejný okamžik přistupovat ke stejnému zařízení, což způsobilo konflikt a pád systému.

Hříšník je nalezen, nyní je čas vrátit se zpět do Windows a vše dát do pořádku.

AKTUALIZACE OVLADAČŮ

Zpět do Windows

Jakmile jsme zpět ve Windows, spouštíme DriverMax a hledáme ovladač, o kterém informoval WinDbg. V programu volíme položku *Updates and identification a Check for driver updates*. Program chvíli prozkoumává nainstalovaná

Tuning ovladačů: Výkon zdarma

Bez hardwarových konfliktů běží Windows rychle a stabilně. Jde to však ještě lépe. Pomocí freewarových nástrojů je možné výkon ještě navýšit.

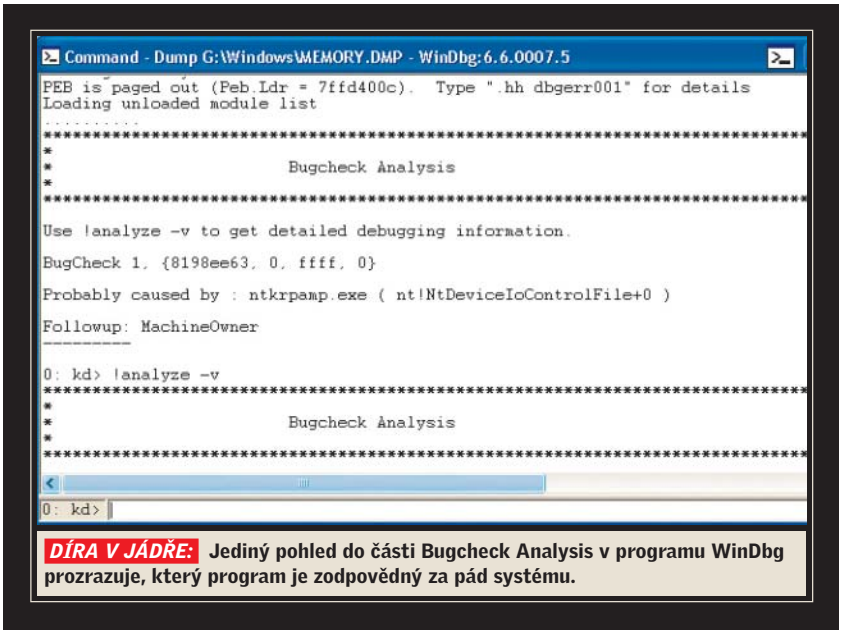
■ **Lepší grafika zdarma:** Profesionální 3D grafika je ve Windows zobrazována pomocí výkonných DirectX a Direct3D z dílny Microsoftu. Freeware naproti tomu používá bezplatnou alternativu v podobě OpenGL. Pomocí nástroje GLDirect **(www.scitechsoft.com)** můžete výkon DirectX využít, i když je používán bezplatný OpenGL, a tím naplno využít možnosti grafické karty. Na počítač se nainstalují nové ovladače GL-Direct, které přenos zajistí.

■ **Nalezení nových funkcí:** Vaše grafická karta toho umí mnohem více, než jste si mysleli. Často jsou však funkce zablokované a nejsou dostupné. Pomocí freewarového nástroje PowerStrip z Chip DVD můžete zjistit, které funkce jsou potlačeny a lze je aktivovat. Nevýhoda: Setkáte se s řadou odborných výrazů, jako je třeba „Force anisotropic filtering“. Co podobné funkce vaší kartě přinesou, to se dozvíte na Googlu.

TUNING ZVUKU: **DXF se stará o vylepšení zvuku. Existuje jako plug-in do řady přehrávačů, takto vypadá jako rozšíření do Winampu.**

■ **Zrychlení ADSL:** Skutečně vysokorychlostní internet získáte, pokud standardní ovladač ve Windows nahradíte ovladačem speciálním. Profesionálové rádi sahají po bezplatném nástroji RASPPPOE **(www.raspppoe.com)**, který je sice výkonný, nenabízí však dostatečný komfort v ovládání. Mnohem luxusnější ovládání nabízí cFos-Speed **(www.cfos.de)**, jehož ukázkovou verzi naleznete na Chip DVD.

■ **Optimalizace zvuku:** Lepší zvuk získáte pomocí plug-inu DFX8-Plugin **(www.fxsound.com)**. Bezplatnou verzi pro Winamp naleznete na Chip DVD, další verze si musíte stáhnout ze stránek výrobce.



DÍRA V JÁDŘE: **Jediný pohled do části Bugcheck Analysis v programu WinDbg prozrazuje, který program je zodpovědný za pád systému.**

zařízení a zobrazuje webovou stránku, na které jsou vypsány všechny ovladače a také jejich možné aktualizace. A hleďme – ovladač pro USB není aktuální. Naštěstí DriverMax nabízí odkaz pro okamžité stažení nového ovladače. Klikáme tedy na symbol diskety pro stažení, avšak zobrazuje se chybová hláška „Driver download are NOT AVIABLE YET“. Zde pomůže už jen návštěva stránek výrobce hardwaru.

Druhý ovladač je speciální případ. DriverMax jej nedokázal rozpoznat a hardware pojmenoval jako „Identify unknown Hardware“. Pátrali jsme tedy na Googlu a ten nám prozradil, že ve skutečnosti se nejedná o žádnou hardwarovou komponentu, ale o kopírovací ochranu známou pod názvem Starforce. Je jasné, že ochrana nemohla být rozpoznána jako hardware. Pro tuto specialitku je nutné stáhnout nástroj SFUpdate ze stránky výrobce ochrany a nainstalovat nejnovější ovladač.

ZÁLOHA OVLADAČŮ

Cesta pokračuje

Zbývá ještě kousek, než dorazíme do cíle. DriverMax nabízí funkce, jejichž pomocí lze snadno zazálohovat ovladače. To má řadu výhod – až se příště setkáme s modrou obrazovkou, budeme mít k dispozici ovladače, o kterých budeme vědět, že jsou funkční. Nebo až přeinstalujeme systém, nebudeme muset navštěvovat stránky výrobců a postupně stahovat potřebné ovladače.

Spustíme DriverMax a zvolíme *Driver operations | Export Drivers*. Spustí se průvodce, který nám s procesem zálohování pomůže. Klikneme na *Next*. Program začne prohledávat nainstalovaný hardware a k němu dostupné ovladače. Po vyhledání klikneme na *Settings*. Zde zrušíme zatržení u položky *Show phantom device*. Vysvětlení: Jedná se o ovladače různých USB zařízení, která byla někdy do systému připojena, ale která nejsou již delší dobu používána. Je pravděpodobné, že už je tedy ani nemáme a že tyto ovladače nebudeme potřebovat. Poté klikneme na *OK* a na *Select all*. Tím označíme všechny ovladače nalezené v systému. Pokračujeme kliknutím na *Next*. Program nabídne, kam by mohl ovladače exportovat, je však možné zvolit jiné místo. Opět pokračujeme kliknutím na *Next*.

Nyní se spustí proces, který začne zálohovat ovladače. Podle počtu nainstalovaných hardwarových komponent to bude chvíli trvat. O dokončení nás program informuje a okno lze zavřít kliknutím na *Close*.

Nyní nesmíme zapomenout přikopírovat k ovladačům instalační soubor programu DriverMax (je na Chip DVD). Poté vše zazálohujeme na externí nosič, třeba na CD. Až budeme při instalaci Windows formátovat pevné disky, záloha na smazané partition by nám nebyla k ničemu.

Důležité je, že naše cesta do jádra Windows měla význam a mise byla úspěšná.

Markus Hermannsdorfer, Vratislav Klega