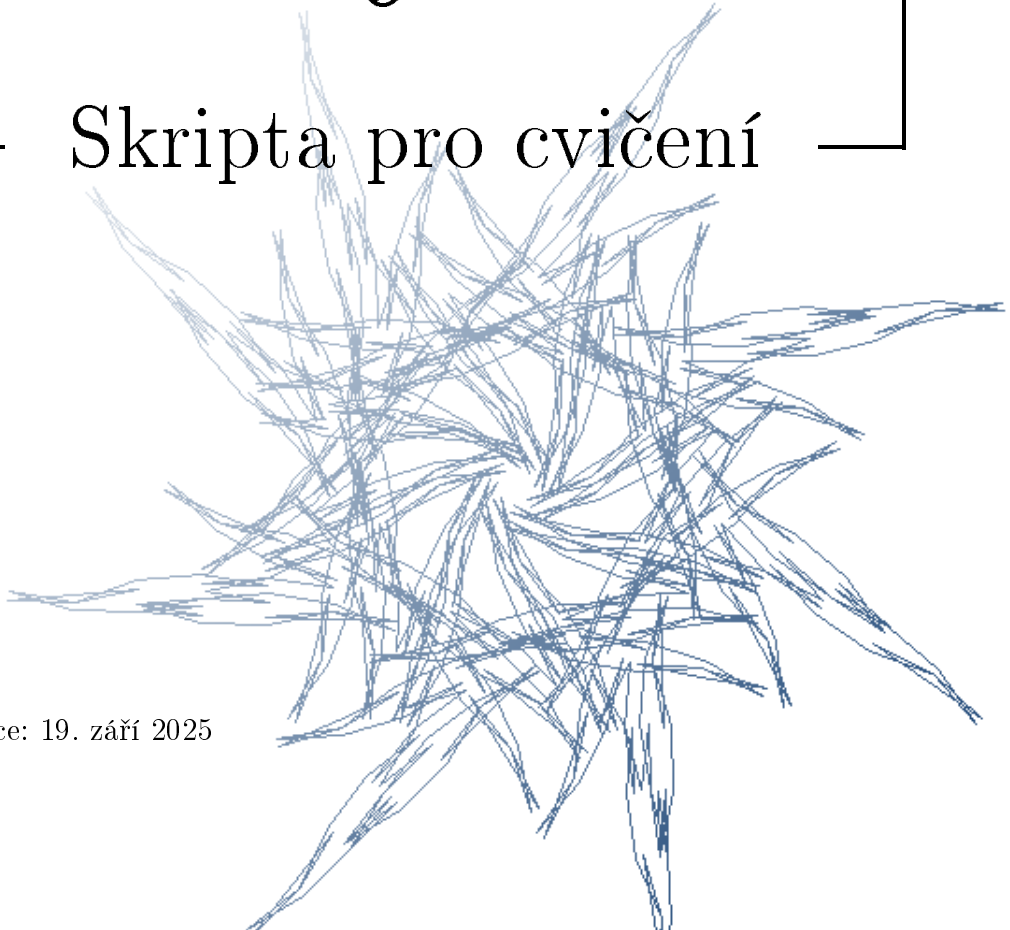
SLEZSKÁ
UNIVERZITA
FILOZOFICKO-
PŘÍRODOVĚDECKÁ
FAKULTA V OPAVĚ
ÚSTAV INFORMATIKY

Šárka Vavrečková

Operační systémy I

Skripta pro cvičení



Opava
Poslední aktualizace: 19. září 2025

Anotace: Tento dokument je určen pro studenty předmětu týkajícího se operačních systémů na Slezské univerzitě v Opavě (předmět Operační systémy I), v zimním semestru. Zabýváme se postupně operačními systémy Windows a Linux, konkrétně tématy:

- úvod do správy daného operačního systému (nástroje v grafickém režimu),
- průzkum struktury souborů se zaměřením na důležité systémové soubory,
- v případě Windows také práce s registrem Windows,
- úvod do práce v textovém režimu.

Součástí výuky jsou také obecná témata týkající se obou systémů: bezpečnost a licence.

Operační systémy I

Skripta pro cvičení

RNDr. Šárka Vavrečková, Ph.D.

Dostupné na: http://vavreckova.zam.slu.cz/pos.html

Ústav informatiky
Filozoficko-přírodovědecká fakulta v Opavě
Slezská univerzita v Opavě
Bezručovo nám. 13, Opava

Sázeno v systému LaTeX

Předmluva

Co najdeme v těchto skriptech

 *Rychlý náhled:* Cílem výuky v tomto předmětu je nacvičit si základy ovládání operačních systémů Windows a Linux, mnohá témata se týkají také systému Apple MacOS. Získáme orientaci ve verzích a edicích, resp. distribucích daného operačního systému, prozkoumáme strukturu souborů a naučíme se správě v grafickém režimu. Pak se zaměříme na základní postupy v textovém režimu.

Po tématech specifických pro jednotlivé operační systémy se budeme zabývat tématy obecnějšími: získáme přehled o licencích a základech zabezpečení.

Skripta se mohou zdát značně rozsáhlá. Důvodem je zařazení mnoha ukázkových (řešených) příkladů a motivačních (neřešených) úkolů, které mají pomoci při pochopení a osvojení si učiva, a také velké množství ilustračních obrázků. U některých příkazů jsou uvedeny také jejich obvyklé výstupy, také z důvodu často nedostatečných přístupových oprávnění studentů v učebnách.

Některé oblasti jsou také „navíc“ (jsou označeny ikonami fialové barvy), ty nejsou probírány a ani se neobjeví na testech – jejich úkolem je motivovat k dalšímu samostatnému studiu nebo pomáhat v budoucnu při získávání dalších informací dle potřeby v zaměstnání.

Značení

Ve skriptech se používají následující barevné ikony:

-  *Rychlý náhled* (skript, kapitoly), ve kterém se dozvíme, o čem to bude.
-  *Klíčová slova* kapitoly.
-  *Cíle studia* pro kapitolu nám řeknou, co nového se v dané kapitole naučíme.
-  Nové *pojmy*, značení apod. jsou označeny modrým symbolem, který vidíme zde vlevo. Tuto ikonu (stejně jako následující) najdeme na začátku odstavce, ve kterém je nový pojem zaváděn.
-  Konkrétní *postupy a nástroje* (příkazy, programy, soubory, skripty), způsoby řešení různých situací, do kterých se může administrátor dostat, syntaxe příkazů atd. jsou značeny také modrou ikonou.

-  Některé části textu jsou označeny fialovou ikonou, což znamená, že jde o *nepovinné úseky*, které nejsou probírány (většinou; studenti si je mohou podle zájmu vyžádat nebo sami prostudovat). Jejich účelem je dobrovolné rozšíření znalostí studentů o pokročilá témata, na která obvykle při výuce nezbývá moc času.
-  Žlutou ikonou jsou označeny odkazy, na kterých lze získat *další informace* o tématu. Nejčastěji u této ikony najdeme webové odkazy na stránky, kde se dané tématice jejich autoři věnují podrobněji.
-  Červená je ikona pro *upozornění* a poznámky.

Pokud je množství textu patřícího k určité ikoně větší, je celý blok ohraničen prostředím s ikonami na začátku i konci, například pro definování nového pojmu:

 **Definice**

V takovém prostředí definujeme pojem či vysvětlujeme sice relativně známý, ale komplexní pojem s více významy či vlastnostmi.

Podobně může vypadat prostředí pro delší postup nebo delší poznámku či více odkazů na další informace. Mohou být použita také jiná prostředí:

 **Příklad**

Takto vypadá prostředí s příkladem, obvykle nějakého postupu. Příklady jsou obvykle komentovány, aby byl jasný postup jejich řešení.

 **Úkol**

Otázky a úkoly, náměty na vyzkoušení, které se doporučuje při procvičování učiva provádět, jsou uzavřeny v tomto prostředí. Pokud je v prostředí více úkolů, jsou číslovány.

 Na konci každé kapitoly najdete odstavec se souhrnem kapitoly.

Jak probíhají testy

Na zápočtových testech z předmětů týkajících se operačních systémů lze používat počítač, a to nápovědu a nástroje běžně dostupné ve standardní instalaci daného operačního systému, ale bez přístupu na Internet. Nejsou dovoleny dokumenty vlastní ani cizí výroby, které nejsou součástí standardní instalace, nelze používat internetový prohlížeč ani jiný způsob přístupu na externí zdroje informací. Taktéž nástroje umělé inteligence nejsou povoleny, a to ani v případě, že v některém operačním systému je některý AI agent nainstalován.

Na stránkách předmětu je k dispozici orientační seznam otázek a úkolů, které se mohou objevit na testu, ovšem v testu se mohou objevit mírné odlišnosti (například v názvech zpracovávaných souborů či adresářů, jiné přepínače příkazů, apod.).

Obsah

Část 1

Windows

Kapitola 1

Jdeme od základů

Už na základní a střední škole nebo v domácnosti či různých kurzech se dnes uživatelé běžně učí základní postupy v systému Windows, tedy určitý stupeň počítačové gramotnosti v této oblasti operačních systémů se bude předpokládat i v tomto předmětu. Ty nejzákladnější dovednosti zde pouze připomeneme (na písemce obvykle slouží jako „snadný zdroj bodů“), na další se podíváme trochu podrobněji.

Rychlý náhled: V této kapitole najdete základní přehled systému Windows a jeho verzí, vysvětlení některých základních pojmů jako je jádro systému, a také seznam běžných klávesových zkratek. Budeme se zabývat základními postupy, seznámíme se s umístěními užitečných nástrojů v grafickém rozhraní, také se zaměříme na verze Windows a instalaci tohoto systému.

Klíčová slova: Windows, kontextové menu, nástroj Nastavení, Ovládací panely, Správa počítače, MS konzola, soubor, složka, adresář, speciální složka, jádro, zástupce, klávesová zkratka, verze, build, platforma, edice, Plug&Play, HotPlug, ReadyBoost, Superfetch, widget, ISO, Media Creation Tool, dism, Rufus.

Cíle studia: Po prostudování této kapitoly získáte základní přehled v systému Windows, zvládnete práci se soubory a složkami, budete umět nadefinovat různé druhy zástupců (souborů, webových stránek, procedur v knihovnách apod.), získáte přehled v běžných klávesových zkratkách. Také se budete se orientovat ve verzích a různých variantách systému Windows a zvládnete instalaci tohoto systému včetně jednoduché úpravy instalačního obrazu.

1.1 Kde hledat potřebné nástroje

V grafickém prostředí Windows najdeme většinu nástrojů na těchto místech:

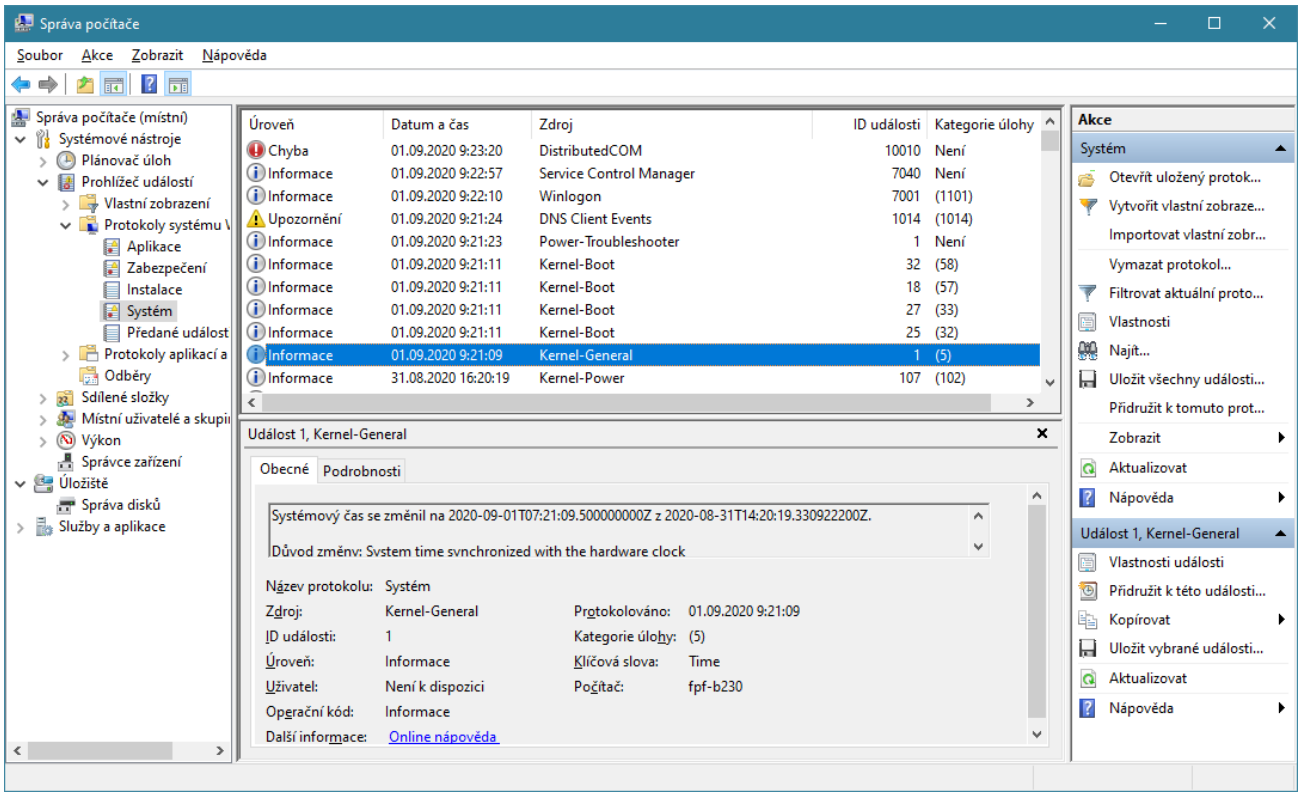
- *kontextové menu různých prvků* (pravým tlačítkem myši na daný prvek) – často to bývá nejrychlejší cesta, své kontextové menu mají ikony na ploše, ikony v *System Tray* (*Oznamovací oblasti* v pravé části *Hlavního panelu*), samotný *Hlavní panel*, tlačítko *Start*, atd.,
- Ve Windows 8/10/11 je hlavním správním centrem aplikace *Nastavení* (najdeme ji v nabídce *Start* podle verze vlevo nebo vpravo dole nebo mezi „připnutými“, ikona „ozubeného kola“ ⚙),

- *Ovládací panely* dostupné buď přes *Start* ⇨ *Systém Windows*, nebo spustíme program `control.exe` (přes nabídku *Start*, nebo tam zadáme „Ovládací panely“); najdeme zde především progamy přímo nazývané „ovládací panel“, jsou to soubory s příponou CPL,
- *Nástroje Windows* v nabídce *Start* (podobně jako různé programy), obsah se liší podle verze Windows,
- klávesové zkratky, případně zadáme příkaz pro spuštění nástroje (i nástroje s grafickým rozhraním se dají spustit zadáním příkazu).

Ve Windows je někdy složité najít ten správný nástroj, i proto, že Microsoft je v různých verzích přesouvá a přejmenovává. Takže někdy musíme volit postup pokus–omyl.

Některé nástroje jsou přístupné z několika míst (například některé nástroje z *Ovládacích panelů*, jiné nemají žádné grafické rozhraní a lze je používat pouze v *Příkazovém řádku* nebo spuštěním přes *Start* ⇨ *Spustit*. Spuštění vyhledáváním názvu nástroje v nabídce *Start* může být poslední možností, jak dotyčný nástroj najít, ale dostaneme se do problémů například v jiné jazykové variantě nebo sice ve stejné, ale dotyčný nástroj byl v té verzi přejmenován…

Správa počítače je *MS konzola*, tedy nástroj se standardizovaným grafickým rozhraním, který v sobě sdružuje jiné jednodušší nástroje. Podobných konzol existuje mnoho, vlastně jsou to všechny nástroje spouštěné ze souborů s příponou MSC. Všechny mají podobné grafické rozhraní.



Obrázek 1.1: Konzola *Správa počítače* ve Windows 10 – Prohlížeč událostí, systémový protokol

Na obrázku 1.1 vidíme konzolu *Správa počítače* ve Windows 10 (ve verzi 11 vypadá stejně), konkrétně máme vlevo vybránu položku *Systémové nástroje* ⇨ *Prohlížeč událostí* ⇨ *Protokoly systému Windows* ⇨ *Systém*, a díváme se na první zaznamenanou událost ze dne 1. 9. 2020 – informace o synchronizaci času přes počítačovou síť.

Tuto konzolu můžeme spustit buď přes *Start* ⇨ *Vše* ⇨ *Nástroje Windows*, anebo také tak, že v kontextovém menu ikony *Tento počítač* (resp. *Počítač*) zvolíme *Spravovat* (Manage). Nejrychlejší způsob spuštění je klepnout pravým tlačítkem myši na ikonu *Tento počítač* na ploše a v kontextovém menu vybrat *Zobrazit další možnosti* ⇨ *Spravovat*.

Další způsob otevření konzoly *Správa počítače* je v nabídce Start napsat název spustitelného souboru pro tento nástroj, tedy `compmgmt.msc` (pozor, včetně přípony), nebo „Správa počítače“.

Poznámka

Pokud na ploše nemáte ikonu Tento počítač nebo Počítač, pak ji na plochu dostanete následovně:

- klepneme pravým tlačítkem na plochu a vybereme *Přizpůsobit*, nebo v nástroji Nastavení najdeme *Přizpůsobení*,
- vlevo klepneme na *Motivy*, na obrazovce *Motivů* je položka *Nastavení ikon na ploše*.

Úkol

Projděte si důkladně celý systém, zkoušejte pravé tlačítko myši a kontextové menu, věnujte pozornost položkám typu *Přizpůsobit*, *Pokročilé nastavení*, *Upřesnit nastavení* či podobně pojmenované, pozor – často bývají tak malým písmem, že je člověk často až přehlédne.

1.2 Co už bychom měli znát

1.2.1 Orientace v prostředí Windows

Windows v každé verzi obsahují *Pracovní plochu*. Předpokládá se, že každý student bude umět v té verzi Windows, kterou běžně používá:

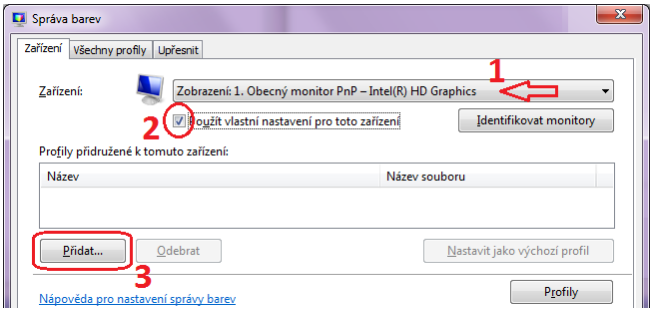
- nastavit obrázek na pozadí pracovní plochy, skrýt či zobrazit základní ikony plochy (Počítač, Koš, Síť apod.),
- nastavit motiv prostředí (což neznamená jen obrázek na pozadí), nastavit spořič obrazovky,
- nastavit rozlišení obrazovky,
- nastavit vlastnosti monitoru jako je obnovovací frekvence, barevná hloubka (většinou se volí mezi True Color a High Color), apod., případně pokud máme víc monitorů, i jejich přizpůsobení (nápověda: je to vlastnost zobrazení, můžete použít pravé tlačítko na ploše),
- nastavit velikost písma v popiscích ikon (pro případ, že máme nastaveno tak vysoké rozlišení, že je písmo z běžné vzdálenosti nečitelné) – je to vlastnost obrazovky pro usnadnění přístupu, hledejte v *Nastavení*,
- konfigurovat využívání koše, například určovat, na kterých oddílech disku koš bude nebo ne,
- sejmout obrazovku klávesou na klávesnici, sejmout aktivní okno, výsledek se uloží do schránky či souboru (klávesové zkratky najdete dál v této kapitole).

Důležitým konceptem je: pokud chci pracovat s určitou komponentou, která má vizuální podobu, použiju pravé tlačítko myši. Většinou se zobrazí kontextové menu, ve kterém bude položka pojmenovaná *Vlastnosti*, *Přizpůsobit* nebo podobně.

Postup

ICM (Image Color Management) je systém správy barev, který slouží k vyladění barevného výstupu na obrazovkách, tiskárnách apod. Na některých zařízeních je barevný výstup víceméně v pořádku, jindy je třeba podání barev trochu pozměnit, třeba načtením souboru s barevným profilem pro dané zařízení. Soubory s příponou .ICM jsou buď dodávány se zařízením (třeba na CD přidaném k monitoru) nebo jsou dostupné na webu výrobce.

Pokud máme soubor .ICM, musíme se dostat k nástroji *Správa barev*.



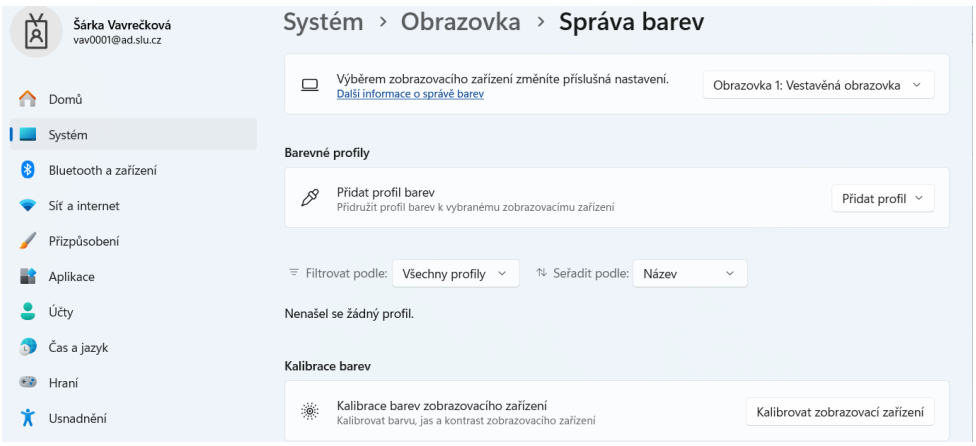
Obrázek 1.2: Správa barev

Ve Windows 10 klepneme pravým tlačítkem myši na plochu a zvolíme *Nastavení zobrazení*, najdeme odkaz *Upřesňující nastavení zobrazení*, *Zobrazit vlastnosti...*, záložka *Správa barev*. Pokud chceme pracovat s ICM profily pro tiskárny, pak v Nastavení zvolíme *Zařízení*, pak *Tiskárny a skenery*, klepneme na příslušnou tiskárnu, tlačítko *Spravovat*, *Vlastnosti tiskárny*, záložka *Správa barev*, tlačítko *Správa barev*. V okně, které se objeví (jako na obrázku 1.2), zvolíme zařízení (na obrázku monitor), zaškrtneme volbu *Použít vlastní nastavení pro toto zařízení* a pak přes tlačítko *Přidat* najdeme soubor s profilem.

Ve Windows 11 klepneme pravým tlačítkem myši na plochu a zvolíme *Nastavení obrazovky* (nebo v nástroji *Nastavení* zvolíme *Systém* ⇨ *Obrazovka*), v sekci o barvě a jasu je odkaz *Profil barev*. Nahoře vybereme zařízení, pro které chceme načíst nový profil, níže pak máme možnost načíst soubor (u obrazovky musíme určit, jestli se má jednat o SDR nebo HDR profil).

Profilů může být k dispozici více, takže pokud po použití jednoho není výsledek zrovna ideální, postupujeme metodou pokus–omyl (postupně zkoušíme různé profily). Bohužel ne vždy se dostaneme k žádanému cíli, pokud je zařízení špatně nakalibrováno (pak nezbývá než se pustit do kalibrace).

Určitě jste si všimli, že existuje ještě další možnost vylepšení podání barev na obrazovce: *kalibrace barev*. Velice jednoduše se k této funkci dá dostat ve Windows 11, kde ji najdeme na stejném místě jako správu barevných profilů.



Obrázek 1.3: Správa barev a kalibrace obrazovky ve Windows 11

Další součástí grafického rozhraní je *Hlavní panel*. Většinou se nachází u spodního okraje obrazovky a obsahuje tyto části (s určitými odlišnostmi mezi verzemi Windows):

- tlačítko *Start*,
- panel aplikací (s ikonami připnutých či spuštěných aplikací),
- *Oznamovací oblast* na pravé straně panelu s menšími aktivními ikonami a časem/datem.

Co by už každý student měl umět:

- konfigurovat nabídku *Start* (například co vše se má v nabídce Start zobrazovat a jak má vypadat): u starších verzí jsme použili kontextové menu tlačítka Start, ve Windows 11 musíme rozbalit nabídku a vyvolat kontextové menu na její ploše,
- změnit datum a čas, změnit časové pásmo,
- zajistit, aby se *Hlavní panel* automaticky schovával,
- změnit umístění *Hlavního panelu* na obrazovce, případně ve Windows 11 zvládnout změnu zarovnání obsahu Hlavního panelu z vystředěného na levé,
- určit, jak mají vypadat ikony aplikací na panelu aplikací (například zda se mají u ikon aplikací zobrazovat názvy aplikací, jestli se mají slučovat okna různých instancí téže aplikace, pokud to daná verze umožňuje),
- určit, které ikony budou za jakých okolností zobrazeny v *Oznamovací oblasti*,
- v případě, že máme připojeno více zobrazovacích zařízení v režimu Rozšíření (tj. na každé obrazovce něco jiného), jak bude vypadat panel na různých obrazovkách (například jestli na panelu určité obrazovky mají být vždy ikony všech spuštěných aplikací, nebo jen těch, co mají okno na dané obrazovce).

Obvykle si vystačíme s pravým tlačítkem myši na Hlavním panelu nebo jeho příslušné části.

Úkol

Prozkoumejte různé cesty ke konfiguraci toho, co se nachází na *Hlavním panelu*. Uvědomte si, že pokud chcete zobrazit kontextové menu *Hlavního panelu*, potřebujete na něm trochu volného místa. Používejte pravé tlačítko myši.

1.2.2 Adresář, složka, knihovna

Soubory jsou na discích organizovány v *adresářích* s možností rekurze, tedy adresář může obsahovat kromě souborů i další adresáře. Ve Windows používáme obecnější pojem – *složka*. Složka může být

- klasický *adresář*, tedy kontejner, do kterého ukládáme soubory či jiné složky,
- speciální složka.

Speciální složka je složka s definovaným *vlastním rozhraním*, které umožňuje lépe pracovat s prostředky v složce uloženými (například složka *Tiskárny* dává uživateli možnost přidat novou tiskárnu, v grafickém rozhraní je tato funkce reprezentována objektem v této složce s názvem *Přidat tiskárnu*, překonfigurováno je taky menu složky). Takže speciální složku můžeme považovat za takovou složku, která primárně slouží jako rozhraní k něčemu dalšímu.

Speciální složky jsou například *Tento počítač*, *Tiskárny*, *Ovládací panely*, *Plocha*, *Dokumenty*, *Oblíbené*. Tedy ne každá složka je adresářem, ale každý adresář je složkou. Speciální složky nemusejí

nutně sloužit k ukládání dat nebo programů (proč taky do složky *Tiskárny* umísťovat třeba obrázky?), ale k některému speciálnímu účelu, často bývají obrazem jiných existujících složek poskytujícím více možností, nastavení nebo jiný typ přístupu.

Zvláštním typem speciálních složek jsou od verze Vista *virtuální složky*. Má to být řešení problémů s kompatibilitou starších programů. Pokud se program pokouší zapsat data do složky, ke které nemá povolen přístup, je přesměrován (bez svého „vědomí“) do stejnojmenné složky nacházející se v profilu uživatele (například pro složku `Program Files` to bude `Users\%userprofile%\AppData\Local\VirtualStore\Program Files`).
Jde o virtualizaci přístupu ke složkám, která se týká pouze aplikací programovaných pro použití v operačním systému s benevolentnějšími oprávněními přístupu.

1.2.3 Jak na soubory

Přímo k souborům můžeme přistupovat různými způsoby:

1. spustíme *Průzkumníka*,
2. použijeme jiného správce souborů (souborového manažera), například *FreeCommander*, *Total Commander*,...,
3. použijeme Příkazový řádek (touto možností se budeme zabývat později).

Průzkumníka lze spustit více různými způsoby:

1. najdeme ho mezi aplikacemi v nabídce *Start*,
2. *Start* ⇨ *Spustit*, napíšeme `explorer` (dejte pozor, ať omylem nespustíte Internet explorer, který může být na prvním místě mezi nalezenými),
3. myší poklepeme na kteroukoliv složku nebo třeba ikonu *Tento počítač*,
4. myší zobrazíme kontextové menu kterékoliv složky či ikony *Tento počítač*, položka *Prozkoumat*,
5. použijeme klávesovou zkratku ⊞+E.

V levém okně *Průzkumníka* lze pracovat samozřejmě myší, ale můžeme používat také klávesnici. Používáme hlavně klávesy ↓ a ↑, Page ↑ a Page ↓, pro rozbalování a sbalování položek stromu klávesy ← a →.

V pravém okně *Průzkumníka* si volíme vhodný způsob zobrazení – velké či malé ikony, seznam apod., pro tento účel bychom měli najít ikonu *Zobrazení*.

Za účelem kopírování složek a souborů někdy potřebujeme označit najednou více položek v pravém okně. Máme více možností:

1. chceme označit všechny položky: Ctrl+A nebo najdeme položku v menu,
2. souvislý blok položek: stiskneme Shift ⇑, a dále
   - s použitím klávesnice: ↓, ↑, Page ↑, Page ↓, Home, ...
   - s použitím myši: ťukneme na počáteční „krajní“ položku, pak na poslední,
3. souvislý blok položek můžeme označit také jednoduše tažením myší se stisknutým levým tlačítkem,
4. nesouvislý (více bloků): stiskneme Ctrl a dále
   - s použitím klávesnice: klávesami ↓, ↑, Page ↑ a dalšími klávesami se pohybujeme, mezerníkem ( ) označujeme,
   - s použitím myši: ťukáme na ty položky, které chceme vybrat.

Pokud myší přetahujeme položky mezi složkami, používáme službu systému *drag&drop* (táhni a pusť). Možnými akcemi jsou kopírování, přesun a vytvoření zástupce. Implicitní akce:

- *přesun* pro přetahování objektů v rámci jednoho logického disku (oddílu),
- *kopírování* pro přetahování objektů mezi různými logickými disky (např. přetahujeme soubor z oddílu `C:` na oddíl `D:`),
- *vytvoření zástupce* pro přetahování programu (např. s příponou EXE) kamkoliv.

Pokud přetahujeme více souborů, obvykle je zvoleno kopírování. Pokud nám implicitní akce nevyhovuje, máme možnost vybrat si takto:

- při přetahování nedržíme levé, ale pravé tlačítko myši,
- po upuštění se zobrazí kontextová nabídka s možnostmi *Kopírovat*, *Přesunout*, ...

Takto můžeme kopírovat soubor nebo jiný objekt do té složky, ve které byl původně (tj. vytvořit kopii na stejném místě): chytneme položku pravým tlačítkem myši, o kousek posuneme (v tomtéž okně) a v menu zvolíme *Kopírovat*. Vytvoří se soubor *Kopie* ... Pro tento účel lze také použít třeba klávesové zkratky Ctrl+C a Ctrl+V.

Pro mazání bez použití *Koše* (tj. bez možnosti obnovení z *Koše*) je klávesová zkratka Shift+Del. Pokud si dodatečně uvědomíme, že toto být smazáno nemělo, je obnovení souboru těžší – dá se použít například nástroj Recuva.

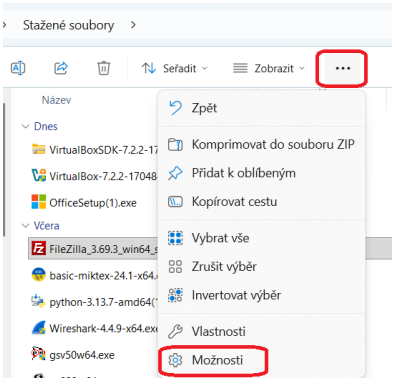
Obsah kontextového menu bývá u různých typů objektů (textový soubor, spustitelný soubor, složka, klíč registru,...) odlišný. Navíc pokud v kontextovém menu (čehokoliv) hledaná položka není (to nám provádějí hlavně Windows 11), použijeme položku *Zobrazit další možnosti*, kde je trochu jiná nabídka funkcí pro daný objekt.

Jestliže víme, že to, co hledáme, je až za „zobrazením dalších možností“, můžeme mezikrok trochu urychlit: pokud předem stiskneme (a držíme) klávesu Shift ⇧ a pak zobrazíme kontextové menu, objeví se rovnou tato druhá fáze.

Pokud potřebujeme provádět nastavení s vyššími oprávněními, pak dotyčný nástroj musíme spustit s těmito oprávněními. Najdeme ikonu nástroje (případně využijeme funkci hledání v nabídce *Start* a napíšeme název nástroje), zobrazíme kontextové menu a zvolíme *Spustit jako správce*. Takže opravdu není nutné přihlašovat se jako administrátor.

1.2.4 Možnosti složky

V menu *Průzkumníka* je nejdůležitější položkou *Možnosti*. Ve Windows 10 je najdeme na kartě *Zobrazení*, tlačítko *Možnosti* (případně v *Ovládacích panelech*), ve Windows 11 jdeme přes „tečky“, jak je znázorněno na obrázku 1.4.



Obrázek 1.4: Cesta k Možnostem složky ve Windows 11

Zde nastavujeme vlastnosti zobrazení složek platné pro první dva typy správců souborů uvedené na začátku této kapitoly, a také pro některé ostatní aplikace. Podíváme se, co všechno lze nastavit, soustředíme se na záložku *Zobrazení* – v různých verzích se liší.

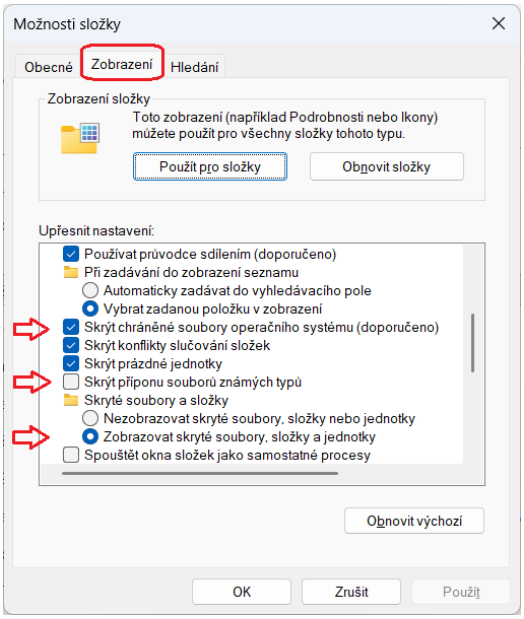
Přímo na panelu nástrojů v Průzkumníkovi (ve Windows 10 na záložce *Zobrazení*, ve Windows 11 přes tlačítko *Zobrazení*) najdeme zatrhávací pole pro zobrazování přípon souborů a skrytých souborů, ale přes *Možnosti* se dostaneme i k dalším užitečným nastavením. Na

obrázku jsou malými šipkami zvýrazněna nastavení zobrazování přípon souborů, skrytých souborů a také *chráněných souborů operačního systému*. Pod pojmem „chráněný soubor“ si můžeme představit systémové soubory samotných Windows.

Skryté a chráněné soubory budeme potřebovat viditelné (nastavení bude platit i v jiných aplikacích pro práci se soubory, nejen přímo v Průzkumníkovi), protože v následující kapitole se budeme probírat celým souborovým systémem.

Volbu *Skrýt přípony souborů známých typů* nedoporučujeme mít zaškrtnutou, protože některé viry toho využívají a například posílají e-mailem v přílohách soubory s dvojitou příponou, jako je třeba `obrázek.gif.exe`. Nepozorného uživatele to může zmást a zlákat k otevření takového potenciálně rizikového souboru.

V okně *Možnosti složky* najdeme i několik tlačítek. Tlačítko *Použít pro složky* stiskneme, pokud chceme, aby se zvolené nastavení pro aktuální složku (po jeho potvrzení tlačítkem *Použít*) použilo pro všechny složky, tlačítko *Obnovit složky* použijeme, pokud chceme obnovit nastavení určené při instalaci operačního systému.



Obrázek 1.5: Možnosti složky ve Windows 11

Soubory nemusíme jen otevírat. Pro každý typ souboru (určený příponou) může existovat více různých *akcí* – například otevřít, editovat, tisknout, přehrát, archivovat, atd., objevují se pak v kontextovém menu souborů s danou příponou. Některé akce jsou předem vytvořené, ale můžeme si vytvořit vlastní a přiřadit této akci jakýkoliv program pro její provedení.

Akce se konfigurují a vytvářejí v registru (s postupem se seznámíme v kapitole o registru). Alespoň akci otevření souboru lze ovlivnit tak, že v kontextovém menu souboru zvolíme *Otevřít v programu* ⇨ *Zvolit jinou aplikaci*.

Úkoly

1. Zapněte si zobrazování chráněných souborů operačního systému, skrytých souborů a systémových složek, a také přípon souborů známých typů. To budeme potřebovat i pro mnohé úkoly z následujících částí těchto skript.
2. Projděte si všechny volby na záložkách okna nástroje *Možnosti složky* – jestli se vám nebude ještě něco „hodit“.
3. Všimli jste si, že v dlouhém seznamu souborů lze „vyhledávat psaním“? Vyzkoušejte například v *Průzkumníku* v některém velmi dlouhém seznamu složek a souborů.

1.3 Přihlášení a odhlášení, Secure Attention Sequence

Při přihlášení je zároveň načten *profil uživatele*, tedy například obsah složky `Dokumenty`, veškerá nastavení uživatelského prostředí a další.

Přihlašovat se dá nejen pomocí hesla, ve Windows postupně přibývají další možnosti (otisk prstu, obrázkové heslo, PIN, rozpoznávání obličeje apod.), novější možnosti se souhrnně označují jako funkce *Windows Hello*, tato funkce se konfiguruje přes *Nastavení* ⇨ *Účty* ⇨ *Možnosti přihlášení*. Některé z těchto možností nejsou považovány za neprůstřelné, ale záleží na okolnostech a hardwaru. Například rozpoznávání obličeje se sice build od buldu zlepšuje, ale pořád není až takový problém ji obelstít.

Poznámka

Někdy se může stát, že při zobrazení Úvodní obrazovky nereaguje myš, a tedy nemůžeme klepnout myší na uživatele. Na vině bývá obvykle některá aktualizace, naštěstí po restartování systému bývá většinou všechno v pořádku. Klávesnice však bude fungovat i v takovém případě, tedy se například můžeme klávesou ⇆ přesouvat mezi objekty na obrazovce a klávesou Enter potvrzovat výběr.

V takové situaci se může hodit, když je na Úvodní obrazovce tlačítko pro vypnutí a restart. Ve skutečnosti můžeme použít i hardwarové tlačítko pro vypnutí (nebo pro restart, jestli je máme).

Pokud počítač není vypnutý, není nikdo přihlášen a není zobrazena přihlašovací obrazovka, zobrazíme ji klávesovou zkratkou Ctrl+Alt+Del. Tutéž klávesovou zkratku můžeme použít i kdykoliv během činnosti systému, pak se zobrazí speciální obrazovka nabízející možnost přepnutí uživatele, odhlášení, uzamknutí či spuštění *Správce úloh*. Dá se také nastavit, aby při každém přihlašování bylo nutné použít tuto zkratku.

Sekvence kláves Ctrl+Alt+Del se nazývá *zabezpečená sekvence upozornění* (Secure Attention Sequence, SAS). Tuto sekvenci nemůže zachytit žádná aplikace běžící v uživatelském režimu, jedná se o ochranu proti možnosti získání hesla programy zachytávajícími klávesy.

Pokud zamrzne Úvodní obrazovka (chceme se přihlásit, ale nejde to, systém odmítá přejít na přihlašovací obrazovku), může také pomoci SAS sekvence, protože je systémem zpracovávána jinak než jiné vstupy.

Postup

Když chceme počítač vypnout, restartovat, odhlásit se nebo přepnout na jiného uživatele, můžeme samozřejmě použít běžnou „myšovou“ cestu (podle verze Windows, třeba přes tlačítko *Start*). Pokud ale vidíme pracovní plochu, existuje rychlejší cesta – klepneme myší na pracovní plochu (aby se stala aktivním objektem) a stiskneme Alt+F4. Kdyby bylo aktivním objektem některé okno, uzavřelo by se. Pokud je ale aktivním objektem pracovní plocha, zobrazí se běžný dialog, ve kterém můžeme zvolit vypnutí, restart, odhlášení apod.

Úkoly

1. Na svém počítači zjistěte, jaké možnosti podporuje ve funkci Windows Hello.
2. Vyzkoušejte sekvenci SAS (zabezpečenou sekvenci upozornění) za běžného provozu.
3. Vyzkoušejte poslední uvedený postup – použití klávesové zkratky Alt+F4.

1.4 Jádro operačního systému

Nejdůležitejší částí operačního systému je jeho jádro, tento pojem zde budeme při popisu operačních systémů hodně používat.

Jádro je souhrn základních funkcí systému, jako je přístup k prostředkům výpočetního systému včetně pamětí a procesoru, správa souborů apod. Jádro zajišťuje běh procesů v systému a přiděluje jim prostředky. Právě struktura a naprogramování jádra má zásadní vliv na bezpečnost, stabilitu a obecně funkčnost celého systému.

Ostatní části operačního systému obvykle při své činnosti pouze využívají *služeb jádra*. Služby jádra bývají (ve všech operačních systémech, nejen Windows) implementovány jako funkce v dynamicky linkované knihovně, která slouží jako „překladatel“ mezi procesy a jádrem. V případě Windows s jádrem NT jde především o knihovnu `NTDLL.DLL`, která tvoří *nedokumentované rozhraní*. Aplikace většinou nevyužívají přímo funkce této knihovny, ale spíše zprostředkovaně přes funkce knihoven tvořících *dokumentované rozhraní* (`user32.dll`, `gdi32.dll`, `advapi32.dll` a další).

O operačních systémech, knihovnách a různých binárních souborech říkáme, že jsou 32bitové, 64bitové apod. 32bitový systém je takový systém, ve kterém zabírá *adresa místa v paměti*, třeba adresa některé proměnné, 32 bitů (tj. 4 B). Od této hodnoty se odvíjí také množství paměti zabrané ukazatelem (pointerem, tento datový typ známe z programování, obsahuje adresu místa v paměti a „odkazuje“ na toto místo) a souvisejících datových typů včetně integer. Pointery obsahují adresu místa, na které odkazují, tedy vícebitový systém používá větší rozsah adres a může také využít větší operační paměť, velikost tohoto typu má zásadní vliv na vlastnosti operačního systému (například hovoříme o tom, že knihovny jsou třeba 64bitové, tedy používají 64bitové adresy).

Podobně s jinými označeními – u 16bitového systému se adresa musí vměstnat do 16 bitů (například Windows do verze 3.x), u 8bitového systému (MS-DOS) jsou adresy pouze 8bitové, u 64bitového systému (dnes běžné varianty u Windows i jiných operačních systémů) jde o 64 bitů.

V 32bitovém systému je možné adresovat $2^{32} = 4\,294\,967\,296$ B = 4 GB operační paměti.

Navíc rozlišujeme 32- nebo 64bitové instrukční sady pro procesory. V základních instrukčních sadách jsou instrukce například pro práci s čísly a řetězci, pamětí, místy na disku, z nich se pak skládají příkazy, které známe z programovacích jazyků. 64bitový operační systém používá 64bitovou instrukční sadu. Mezi 32- a 64bitovou instrukční sadou je rozdíl v tom, s jakými adresami dokážou příslušné instrukce pracovat, ale ve skutečnosti jsou rozdíly mnohem větší.

Pokud máme procesor s podporou 64bitových instrukcí (což je dnes naprostá většina), je lepší instalovat 64bitové Windows, ale 32bitové taky budou fungovat. Naopak to neplatí: když procesor nepodporuje 64bitové instrukce, lze instalovat jen 32bitový systém. Dalším kritériem pro rozhodnutí je velikost operační paměti. Pokud máme jen 4 GB nebo méně, nemá moc smysl instalovat 64bitový systém, protože pak dynamicky linkované knihovny (ať už na disku nebo v operační paměti) budou zabírat zbytečně mnoho místa – obsahují obvykle velmi mnoho adres. Nicméně, běžné edice Windows 10 se již používají jen v 64bitové variantě.

Poznámka

V systému najdeme mnoho souborů, i knihoven, u nichž je součástí názvu číslo 32, včetně 64bitových verzí Windows. Při přechodu z 16 na 32 bitů Microsoft začal v záchvatu nadšení takto některé soubory pojmenovávat, a nikdo si neuvědomil, že v budoucnu se zřejmě bude přecházet na 64bitové adresy. Pře-

jmenovávání souborů by bylo zbytečně náročné (názvy těch souborů jsou často i součástí programového kódu), tak prostě v názvech zůstalo číslo 32.

1.5 Zástupci

Na ploše, ale i v téměř kterékoliv složce si můžeme vytvořit zástupce některého objektu. Zástupce slouží jako zkratka pro často používané objekty, navíc umožňuje definovat různé operace, které se mají provést při přístupu na objekt. Jde vlastně o pouhý odkaz na existující objekt, je to malý soubor, ve kterém je uložena cesta k odkazovanému objektu, název zástupce a další informace. Zástupce najdeme na mnoha místech grafického rozhraní Windows, například na ploše, v nabídce *Start* nebo na *Panelu snadného spuštění*.

Zástupci jsou ve skutečnosti soubory s příponou LNK, která se standardně nezobrazuje (zobrazování lze nastavit v registru).

 Jak vytvoříme zástupce na ploše (a vlastně kdekoliv jinde): Na ploše (nebo v některé jiné složce) kontextové menu, *Nový* ⇨ *Zástupce*.

 *Zástupce souboru nebo složky* vytvoříme tak, že v příkazovém řádku zástupce zadáme cestu k souboru. Může jít o zástupce jakéhokoliv souboru nebo složky včetně spustitelných souborů. Zadáváme buď ručně (je třeba napsat absolutní cestu, například `C:\windows\notepad.exe` pro Poznámkový blok), nebo vkopírujeme či vybereme myší.

 *U zástupce internetové stránky* do příkazového řádku napíšeme internetovou adresu, a to včetně protokolu (například http://www.google.com). Lze použít jak protokol http, tak i další (například ftp).

 *Zástupce e-mailové adresy* funguje, pokud máme nadefinováno přiřazení určitého poštovního klienta (Outlook, Outlook Express, Thunderbird, Pegas, Eudora, ...), do příkazového řádku zástupce napíšeme `mailto:...@...` (samozřejmě doplníme konkrétní adresu).

 *Zástupce procedury dynamické knihovny:* Dynamické (vlastně dynamicky linkované, linkované za chodu programu v případě potřeby) knihovny jsou zásobárny procedur, funkcí a různých objektů, které mohou používat programy, a touto metodou se k nim můžeme přímo dostat (není nutné jít přes kód). K vyvolání dané procedury ze zvolené knihovny používáme ve Windows program *rundll32.exe*. Do příkazové řádky zástupce napíšeme

`rundll32.exe ⟨knihovna⟩,⟨procedura⟩ ⟨parametry⟩` (případně s celou cestou, soubor `rundll32.exe` bývá ve složce `%WINDIR%\system32`). Zatímco v názvech souborů se ve Windows obvykle nerozlišují malá a velká písmena, u názvu procedury je důležité přepsat řetězec i s ohledem na malá a velká písmena. Několik příkladů:

`rundll32.exe shell32.dll,Control_RunDLL` – po poklepání na zástupce se zobrazí *Ovládací panely*,

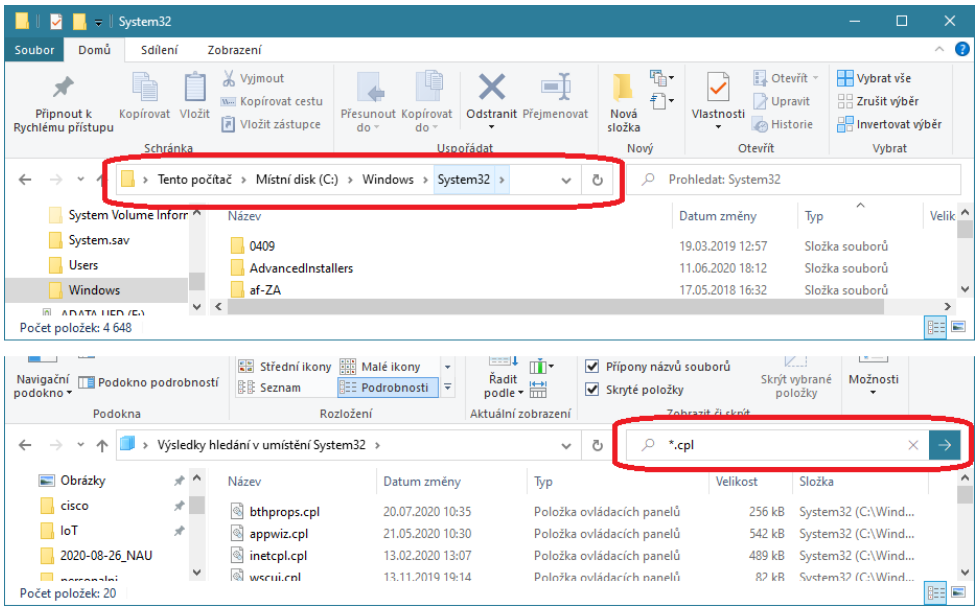
`rundll32.exe user32.dll,LockWorkStation` – vytvoříme ikonu pro zamknutí počítače (pokud musíme od počítače odběhnout, odemknout lze heslem uživatele); jsou i jiné možnosti, jak počítač softwarově zamknout, toto řešení má výhodu v tom, že se jedná o program, který lze spustit automaticky například po určité době nečinnosti počítače (odskočím do vedlejší kanceláře s tím, že tam jenom něco donesu, a nakonec se zdržím déle).

 Seznam dalších zajímavých příkladů využití zástupce procedury dynamické knihovny najdeme v příloze A.1 (strana 39).

Zástupce nástroje Windows: Nástroje Windows jsou často také spustitelnými programy, i když mohou mít jinou příponu než EXE nebo COM. Můžeme se setkat například s příponami CPL (nástroje z *Ovládacích panelů*, je to zkratka z Control Panel – tyto nástroje se nazývají *ovládací panely*) a MSC (konzolové nástroje s unifikovaným grafickým rozhraním, zkratka z Microsoft Console), například:

- `desk.cpl` je nástroj pro konfiguraci pracovní plochy,
- `sysdm.cpl` jsou *Vlastnosti systému*,
- `perfmon.msc` je nástroj pro sledování výkonu systému,
- `diskmgmt.msc` je nástroj pro práci s disky,
- `compmgmt.msc` je nám známá konzola Správa počítače.

Některé nástroje mají příponu EXE, například soubor `control.exe` spouští *Ovládací panely*, `msconfig.exe` spouští nástroj pro konfiguraci systému. Všechny tyto soubory můžeme napsat do příkazové řádky zástupce, a tedy vytvořit si např. na ploše zástupce tohoto nástroje, nebo spustit přes *Příkazový řádek Windows* či v menu *Start*.



Obrázek 1.6: Vyhledání všech .CPL souborů ve složce System32 (Windows 10)

Úkoly

1. Na pracovní ploše vytvořte zástupce některého ze souborů z disku C:, dále zástupce některé webové adresy (například https://is.slu.cz).
2. Vytvořte na pracovní ploše zástupce procedury dynamické knihovny takového, že po poklepání na něj se počítač zamkne (využijte výše uvedený příklad).
3. Vyhledejte všechny soubory s příponou CPL ve složce System32. Pokud nevíte, jak na to, na obrázku 1.6 na straně 13 je návod (ve Windows 11 je to stejné).

   Některý z nalezených nástrojů vyberte, na pracovní ploše k němu vytvořte zástupce a přes tohoto zástupce nástroj spusťte.

1.6 Klávesové zkratky

Při práci v systému se nám mohou hodit některé klávesové zkratky, které dokážou hodně zrychlit práci (pokud ovšem je člověk zná zpaměti). V následujících čtyřech tabulkách je celá řada užitečných klávesových zkratek, které můžeme používat.

Tabulka 1.1: Některé klávesové zkratky pro Plochu, obrazovky a nabídku Start

Klávesy	Význam
⊞	Otevření nabídky *Start*.
Ctrl+Esc	Totéž, hodí se, když přestane fungovat tlačítko ⊞ .
⊞+D	Zobrazení plochy.
⊞+M	Minimalizace oken. Není úplně totéž jako předchozí, srovnejte například situaci, kdy jsou zobrazeny *Možnosti složky*. Obnovení původního stavu: ⊞+Shift+M
⊞+L	Zamknutí počítače.
⊞+R	Totéž jako *Start* ⇨ *Spustit*, otevře se dialog *Spustit program*.
Alt +poklepání	Při poklepání myší při stisknutém Alt na objektu (ikona na ploše, soubor, apod.) získáme vlastnosti (jako když v kontextovém menu najdeme *Vlastnosti*).
⊞+P	Pokud je připojeno více obrazovek (příp. projektor), zobrazí panel s možností výběru posílání obrazu na displeje (duplikace vs. každý displej jiný obraz)
⊞+Shift + →	Pokud máme připojeno více obrazovek (druhý monitor, projektor apod.), přesuneme aktuální otevřené okno na následující zařízení (← na předchozí).

Tabulka 1.2: Klávesové zkratky pro snímání obsahu obrazovky

Klávesy	Význam
PrtScr	Spustí aplikaci *Výstřižky*.
Ctrl+PrtScr	Vytvoří snímek obrazovky, uloží ho do schránky.
Alt+PrtScr	Vytvoří snímek aktivního okna, uloží ho do schránky.
⊞+PrtScr	Vytvoří snímek aktivního okna, uloží ho do souboru s příponou .PNG do profilu uživatele, složka `Obrázky\Screenshots`.

Tabulka 1.3: Klávesové zkratky pro virtuální plochy

Klávesy	Význam
⊞+Ctrl + D	Vytvoří novou virtuální plochu.
⊞+Ctrl + F4	Uzavře virtuální plochu.
⊞+Ctrl + →	Přesuneme se na následující virtuální plochu (← na předchozí).

Tabulka 1.4: Některé klávesové zkratky pro aplikace, okna, nástroje

Klávesy	Význam
Ctrl+Shift+Esc	Rychlé spuštění *Správce úloh*.
Alt+Tab	Přepínání mezi spuštěnými úlohami (držíme Alt a ťukáme na Tab).
⊞+Tab	Funkce Flip 3D, ve Windows 10 a 11 zobrazí náhledy otevřených oken.
F10 nebo Alt	Aktivace menu aplikace (v některých aplikacích funguje jedno, v jiných druhé).
Alt+F4	Zavření aktivního okna (příp. ukončení aplikace). Může být použito i na objekt *Plocha*, důsledkem je vypnutí systému.
Levý Alt+Shift	Přepínání mezi českou a anglickou klávesnicí (pokud jsou obě povoleny).
⊞+E	Spuštění *Průzkumníka*.
⊞+i	Ve Windows 10 a vyšších se spustí nástroj Nastavení (v angličtině Immersive Panel).
⊞+X	Seznam některých nástrojů. Totéž jako pravým tlačítkem myši na Start.
Ctrl+L	(v Adobe Readeru) Přepnutí do celoobrazovkového režimu, vhodné pro prezentace (zpět: klávesa Esc).
Shift+Del	Odstraníme vybrané položky tak, aby se nedostaly do Koše.

Další informace

Na webu najdeme mnoho stránek s přehledy klávesových zkratek, například na:
https://wintip.cz/455-klavesove-zkratky-pro-windows-10

Vlastní klávesovou zkratku si můžeme nadefinovat například pomocí zástupce. Když vytvoříme zástupce jakéhokoliv objektu, můžeme v jeho vlastnostech (v kontextovém menu položka *Vlastnosti*) určit klávesovou zkratku, po jejímž použití je tento objekt vyvolán. Tento postup můžeme použít na téměř kterýkoliv objekt, nejen programy, jen se doporučuje dávat pozor, aby klávesová zkratka ještě nebyla definována pro jinou operaci (je dobré volit zkratky typu Ctrl+Alt+...).

Úkoly

1. Vyzkoušejte klávesové zkratky uvedené v tabulkách 1.1 až 1.4, pokud máte možnost.
2. V nápovědě zjistěte, jak lze změnit klávesové zkratky pro přepínání národních prostředí.
3. Vytvořte na ploše zástupce některé internetové adresy podle vlastního výběru a přiřaďte jí vlastní klávesovou zkratku (například Ctrl+Alt+N) – přesuňte kurzor do daného okna a stiskněte zvolenou klávesovou zkratku. Potvrďte a vyzkoušejte (plocha by měla být aktivním oknem).

1.7 Verze Windows

Předchůdcem Windows byl operační systém MS-DOS, který předinstalovávala na své produkty společnost IBM. Poslední samostatně distribuovaný MS-DOS má číslo verze 6.22, jako grafická nástavba se používaly MS-Windows do verze 3.11, to ale ještě nebyl operační systém, pouze jeho nástavba.

Operační systémy MS Windows dělíme do dvou skupin, které se liší především vnitřní strukturou; vizuálně a vybavením jsou si poměrně podobné. První skupina, vývojově starší, přejímá jádro ze systému MS-DOS a je vlastně jeho pokračováním s přidáním grafického rozhraní (a jistými vylepšeními jádra), například Windows 95 měly v sobě jako jádro MS-DOS 7.0. Druhá, typu NT („New Technology“), byla již od začátku konstruována především s ohledem na bezpečnost a možnost použití v síti. V tabulce 1.5 jsou na stejném řádku systémy podobně vypadající a z přibližně stejné doby.

Tabulka 1.5: Druhy operačních systémů typu MS Windows

Řada s DOS jádrem	Řada s NT jádrem	NT Server
[MS-DOS (+ MS Windows do verze 3.x)]	MS Windows NT verze 3.x	Windows NT Server 3.x
MS Windows 95, 95 OSR2, 98, 98 SE	MS Windows NT 4.x	Windows NT Server 4.0
MS Windows ME	MS Windows 2000	Windows 2000 Server
–	MS Windows XP	Windows Server 2003
–	MS Windows Vista	Windows Server 2008
–	MS Windows 7	Windows Server 2008 R2
–	MS Windows 8, 8.1	Windows Server 2012 (R2)
–	MS Windows 10	Windows Server 2016, 2019, 2022
–	MS Windows 11	Windows Server 2025

1.7.1 Verze, build, platforma

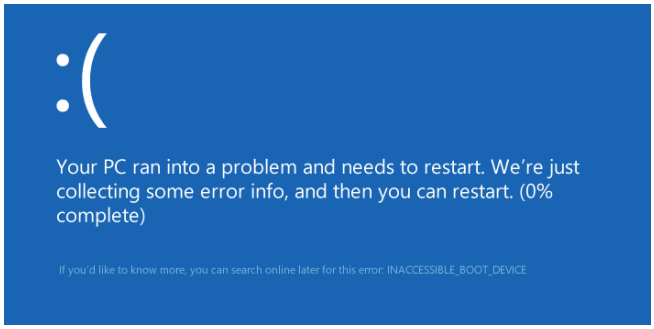
V tabulce 1.5 vidíme různé *verze Windows* ve starším slova smyslu. Liší se z pohledu uživatele zejména vizuálně (tlačítko Start i s jeho nabídkou, dlaždice,...), také ve vybavenosti různými nástroji a funkcemi, v tom, kde co najdeme a jak se to ovládá. Další rozdíly jsou však „pod kapotou“, tedy ve struktuře jádra, ve způsobu komunikace mezi procesy a v tom, jak procesy komunikují s jádrem.

Uživatelé zaznamenali změny především v grafickém rozhraní, z nichž některé se dají chápat spíše jako downgrade, například hlavní panel již není možné přesouvat. Vycentrované ikony na hlavním panelu si spousta uživatelů přenastavila na „desítkové“ umístění vlevo, hlavně proto, že především tlačítko Start prostě očekáváme v levém rohu.

Na druhou stranu, kromě grafických změn například konečně zmizely zmínky o disketě.

Celkově začal být znát tlak Microsoftu na přesun uživatelů „do cloudu“, konkrétněji na *One Drive*, objevilo se přihlášení účtem Microsoft.

Ve Windows 8 se oproti předchozím změnila dokonce i „Blue Screen of Death“ (s tou se setkáme, když jádro přestane fungovat tak, jak má) – viz obrázek 1.7, tato podoba zůstala do současnosti. Ve Windows 10 se přidal QR kód s odkazem na další informace o hlášené chybě.



Obrázek 1.7: Obrazovka BSOD ve Windows 8

Kontroverze působí zejména hardwarové nároky Windows 11, především nutnost mít čip TPM ve verzi min. 2.0, a také nutnost mít novější procesor, i kdyby starší procesor byl dostatečně výkonný.

Ve Windows 10 a 11 již pod pojmem *verze* často rozumíme to, co bychom dříve nazvali aktualizační balíček či service pack. Například v roce 2023 oba tyto systémy přešly na verzi 23H2, v roce 2024 přišla verze 24H2, ale jen pro Windows 11.

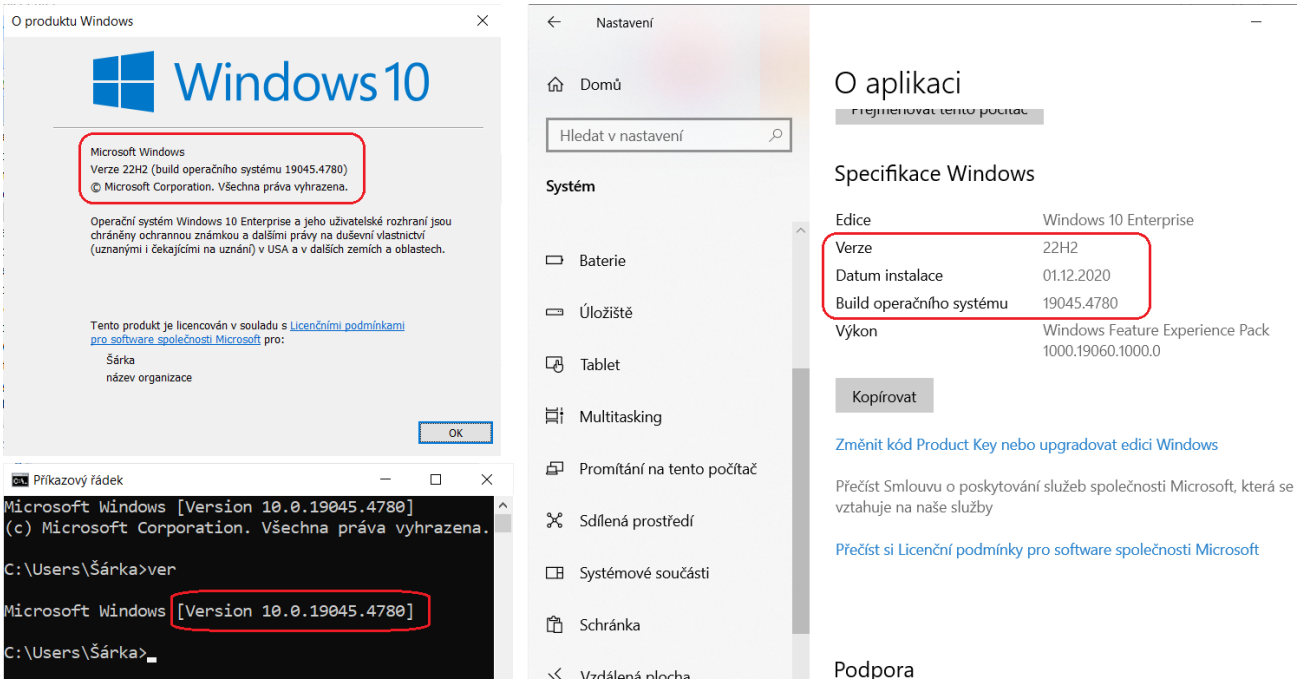
Ve Windows 10 a 11 máme také něco jako podverze, kterým říkáme *build* (sestavení).

Postup

Není od věci poznat, kterou verzi máme, u Windows 10 a 11 taky který build, případně jestli je náš procesor 64bitový apod. Některé informace máme v nástroji *Systém* v *Ovládacích panelech*, resp. *Nastavení* ⇨ *Systém* ⇨ *O systému* či *O aplikaci*.

Vcelku podrobnou informaci získáme také následovně: spustíme příkazový řádek (například tak, že klepneme na tlačítko Start a zadáme `cmd`), napíšeme `winver`.

Na obrázku 1.8 vidíme tři možnosti, jak zjistit údaje o verzi a buildu Windows 10.



Obrázek 1.8: Tři možnosti zjištění verze Windows 10: okno po použití příkazu `winver`, příkaz `ver` a nástroj *Nastavení*

Poznámka

Verze 9 byla přeskočena – údajně proto, že Microsoft chce zdůraznit velikost skoku od starší verze. O skutečných důvodech se hodně spekuluje, například pod číslem 9 bývají někdy chápány systémy Windows 9x (tj. 95 a 98) a automatické rozpoznání operačního systému by to mohlo poplést.

Možná je to jinak: nejvážnější konkurent Microsoftu, Apple, nabízí systém OS X, kde písmeno „X“ znamená číslo 10. Apple svého času prohlásil, že u „X“ (tedy verze 10) zůstane už napořád, Microsoft také prohlásil, že verze 10 je konečná a budou následovat pouze její aktualizace (přesněji: Windows as a Service). Nezní to podobně? Podobně možná uvažuje i Apple, protože od pojmenování OS X přechází k názvu MacOS.

Úkol

Zjistěte co nejpodrobnější informace o svém systému (verze, build, typ systému apod.).

Další informace

Pokud budete z nějakého důvodu potřebovat dokumentaci MSDN ke starším verzím Windows, najdete ji na https://docs.microsoft.com/en-us/previous-versions/windows/

Platforma určuje, na jakém hardwaru má daný systém běžet. Rozlišujeme desktopovou platformu (dále ji dělíme na 32bitovou a 64bitovou), dále mobilní (pro mobilní telefony, tablety apod.), IoT (Internet věcí, například pro chytré hodinky nebo Raspberry Pi), zvlášť může být také Xbox.

Ve starších verzích se rozlišovaly pouze 32bitové a 64bitové systémy, zcela zvlášť byla mobilní platforma pro chytré telefony. Ve Windows 8 přišel Microsoft s platformou Windows RT pro procesory ARM (typicky pro tablety).

Platforma je důležitá pro běh aplikací, protože určuje, jaký typ instrukcí lze na ní provozovat. Víme, že se odlišují 32bitové a 64bitové aplikace, jejich kód je jiný. Taktéž kód pro procesory ARM má jinou strukturu. Pokud chceme na systému provozovat aplikace patřící do jiné platformy, záleží, jestli procesor tyto „cizí“ instrukce zvládá přímo nebo zda operační systém nabízí emulační vrstvu, nebo jestli si s nimi neporadí vůbec.

Jak bylo dříve uvedeno, Windows 8 byl průkopníkem v přidávání platforem. Existovaly tyto hardwarové varianty:

- *Instalace 32bitového systému* se automaticky spustí z instalačního DVD při instalaci na 32bitovém hardwaru, v systému jsme schopni spouštět běžné 32bitové aplikace a dále „Windows Store Apps“ (původně myšlené jako mobilní).
- *Instalace 64bitového systému* se automaticky spouští na 64bitovém hardwaru, v systému fungují 32bitové a 64bitové aplikace a „Windows Store Apps“.
- Windows RT je edice pro procesory ARM (typicky pro tablety), zde je možné spouštět pouze „Windows Store Apps“. Tato varianta byla distribuována pouze předinstalovaná na zařízeních.

Ve Windows 10 a vyšších také existují hardwarové varianty pro různé platformy, ale Microsoft se rozhodl je (většinou) distribuovat na společném instalačním médiu, přičemž během instalace se do systému nakopíruje ta varianta, která odpovídá cílové platformě.

1.7.2 Edice

Zatímco verze a build souvisí s časem vydání a platforma s hardwarem, edice určuje, jak moc bude systém vybavený funkcemi (a taky jak bude drahý). U různých verzí se setkáváme s odlišným rozdělením do edicí.

Tabulka 1.6: Přehled edic ve starších verzích Windows

Použití \ verze	Windows Vista	Windows 7	Windows 8
Rozvojové trhy	Starter	Home Basic	Windows 8
Nenáročné použití – domácnost	Home Basic	Starter	Windows 8
Domácnosti (lepší)	Home Premium	Home Premium	Windows 8
Firmy	Business	Professional	Windows 8 Pro
Velké společnosti	Enterprise	Enterprise	Windows 8 Enterprise
Max. vybavení	Ultimate	Ultimate	–

Zatímco produkty z jiných edic mají vždy svůj vlastní produktový klíč, u hromadné licence mají všechny instalace tentýž produktový klíč.

Edice Windows 10 jsou následující:

Home je základní varianta pro domácnosti, obdoba základních Windows 8.

Pro je edice pro malé a střední firmy. Má navíc některé funkce související s řízením přístupu a zabezpečením, možnost práce v doméně apod.

Enterprise je určena pro velké společnosti. Oproti edici Pro má navíc další funkce související s řízením přístupu a zabezpečením, především směrem k hromadné správě.

Education odpovídá edici Enterprise, ale neobsahuje Cortanu a je více zaměřena na vzdělávání. Licence je finančně zvýhodněna.

Mobile je edice pro malá mobilní zařízení. Microsoft zde přišel s funkcí Continuum. Také existuje edice *Mobile Enterprise* pro mobilní zařízení zaměstnanců velkých společností.

IoT Core je edice obsahující pouze jádro a jeho API, neobsahuje grafické rozhraní. Je určena pro IoT zařízení (Internet of Things), včetně známého Raspberry Pi.

Ve Windows 11 existuje základní edice Home pro domácnosti, dále edice Professional (resp. Pro) určená pro firmy, Enterprise pro velké společnosti, Education pro školství, dále varianty s přídomkem IoT pro Internet věcí, a také varianty s přídomkem LTSC (například Enterprise LTSC) s prodlouženou dobou platnosti licence. Přídomek „N“ znamená verzi bez multimediálních nástrojů. Existují i další speciální edice, ale toho chaosu nám už stačilo.

1.7.3 Typické vlastnosti

Už od začátku byla ve Windows implementována možnost běhu více procesů zároveň. Pojem *multitasking* označuje vlastnost systému, kdy může být spuštěno více procesů zároveň (na procesoru se střídají obvykle v tak krátkých intervalech, že působí dojmem opravdového paralelismu), ale navíc tyto procesy mohou stanoveným způsobem spolupracovat (třeba si předávat data, komunikovat, sdílet

data či kód). Ovšem také jsou procesy navzájem chráněny – neměla by nastat situace, kdy jeden proces zasahuje do prostoru jiného procesu, pokud nejde o vyjednané sdílení.

První verze Windows (do 3.11) používaly *kooperativní multitasking* (procesy spolupracovaly se systémem na svém střídání na procesoru); od Windows 95 v DOS řadě, resp. v celé NT řadě se používá *preemptivní multitasking* (střídání procesů je transparentní, procesy o něm „neví“, nespolupracují na něm).

Postupně se objevila vlastnost *Plug&Play* – usnadnění instalace a konfigurace hardwaru. Většinou nemusíme systému ručně „sdělovat“, že jsme něco nového připojili, není nutná hardwarová konfigurace komponenty (nastavování komunikačních kanálů, ruční přepojování pinů na komponentě apod.), systém sám pozná, co je třeba udělat a případně si vyžádá ovladač. Pozor, neznamená to, že ovladač není potřeba dodat. Někdy to není nutné, protože systém může použít generický (obecný) ovladač pro daný typ komponenty (například USB flash disk), nebo už ovladač je v systému obsažen, ale někdy musíme ovladač dodat.

Nepleťte si tuto vlastnost s *HotPlug*. HotPlug zařízení lze připojovat za běhu systému (tj. tato vlastnost přichází „ke slovu“ nejen při instalaci nového zařízení, ale kdykoliv ho použijeme), není nutné systém vypínat a znovu zapínat. USB Flash disky splňují obě vlastnosti (zjednodušená instalace a lze je připojovat za běhu), kdežto například většina rozšiřujících karet do sběrnice PCI Express je pouze Plug&Play a nikoliv HotPlug.

ReadyBoost umožňuje použít USB flash disk nebo paměťovou kartu jako mezipaměť (cache) při přenosu mezi operační pamětí a pevným diskem. Flash zařízení jsou při čtení výrazně rychlejší než pevný disk, účelem je tedy zrychlit načítání dat z disku. ReadyBoost lze nastavit po prvním vložení flash disku do USB rozhraní v okně *Přehrát automaticky*, a pak ve vlastnostech připojeného disku.

Pokud máme místo pevného disku SSD, který je také flash pamětí, ReadyBoost nemá smysl. Podobně když používáme hybridní disk, nemá ReadyBoost s „externím“ USB flash diskem smysl (hybridní disky v sobě obsahují flash čip, viz níže ReadyDrive).

V použité flash paměti se pro tato data vytvoří soubor `ReadyBoost.sfcache` o velikosti max. 4 GB (i na médiu s větší kapacitou), který je komprimovaný a šifrovaný (mohou v něm být i citlivá data). Protože tato mezipaměť může kdykoliv zmizet (USB flash disk lze kdykoliv vyjmout), jde vždy o kopii dat, která jsou také buď v operační paměti nebo na pevném disku.

Superfetch (ve Windows XP se jmenovala Prefetch, Superfetch je jejím nástupcem) je funkce, jejímž účelem je zrychlit spouštění aplikací. Každá aplikace potřebuje mít v paměti načteny určité soubory (dynamicky linkované knihovny, ale i další). Superfetch sleduje, které soubory si jednotlivé aplikace načítají do paměti, a dále se pokouší převídat potřeby těchto aplikací v budoucnu. Mělo by to fungovat tak, že při dalších spouštěních aplikace jsou už tyto soubory předem v paměti načteny. Důsledkem je, že aplikace se mohou rychleji dostat do provozuschopného stavu, protože při svém spouštění nemusejí tolik dat načítat z disku.

Superfetch může zrychlit práci v systému, pokud používáme klasický pevný disk. Jestliže však máme data na SSD, je spíše kontraproduktivní, protože flash paměť v SSD je poměrně rychlá.

Widgety nebo jejich obdoba se u různých verzí Windows střídavě objevují a mizí, ve Windows 11 se tedy zase objevily. Na hlavním panelu je pro ně speciální ikona. Ve skutečnosti jde o specifické webové stránky, které se po klepnutí otevírají vždy v prohlížeči Edge (jiný nelze nastavit).

Microsoft se veze s módní vlnou umělé inteligence. Stal se spoluvlastníkem ve společnosti OpenAI a produkt této společnosti propaguje jako webovou aplikaci *Copilot* (https://copilot.microsoft.com/), ve svém prohlížeči Edge jako doplněk, a v poslední době také jako integrální součást Windows 11.

1.8 Instalace Windows 11 a upgrade z předchozí verze

U (momentálně) nejnovější verze Windows, stejně jako v případě Windows 10, je možné si zdarma stáhnout instalační obraz systému. Platí se až za licenci, tedy konkrétně produktový klíč, kterým systém aktivujeme.

Instalační obraz Windows 11 stáhneme na následující adrese:
https://www.microsoft.com/cs-cz/software-download/windows11
Nebo se jednoduše zeptáme některého internetového vyhledávače, třeba: windows 11 download, jedna z prvních nalezených adres bude pravděpodobně ta správná.

Na zobrazené webové stránce jsou tři části:

1. Pomocník s instalací Windows 11, tuto část použijeme, jestli chceme instalovat Windows 11 na stejné zařízení, na kterém si tuto stránku prohlížíme,
2. Vytvoření instalačního média systému Windows 11, což znamená použití nástroje Media Creation Tool pro vytvoření instalačního USB flash disku nebo DVD, to se hodí, pokud budeme instalovat na jiném zařízení, než kde zrovna pracujeme,
3. Stažení bitové kopie instalačního disku, tuto možnost použijeme, když chceme jen stáhnout ISO obraz.

U každé z těchto možností najdeme krátký popis, dále odkaz na podrobnější informace („Než spustíte...“/„Než zahájíte stahování...“), ve vlastním zájmu si tyto informace nejdřív přečteme. Určitě bychom si měli být předem jistí, zda zařízení, na které chceme Windows 11 nainstalovat, splňuje minimální požadavky, i o nich je ve zmíněných informacích psáno.

První a druhá možnost spočívají ve spuštění průvodce. Liší se hlavně v tom, že v druhém případě musíme mít k dispozici příslušné datové médium (USB flash disk nebo prázdné zapisovatelné DVD, u obojího s kapacitou nejméně 8 GB).

Zajímavá je třetí možnost. Výše je zmíněno, že první způsob (použití Pomocníka) je vhodný, pokud chceme instalovat na totéž zařízení, na kterém zrovna pracujeme, ale někdy potřebujeme předem upravit instalační obraz systému (přidat aplikace, upravit průběh instalačního procesu, zrušit nutnost používání pouze online účtů, atd.), v takovém případě na zobrazené webové stránce přejdeme ke třetí možnosti.

Pokud si tedy stáhneme ISO obraz Windows 11 a chceme ho upravit, můžeme k tomu použít nástroj `dism`, ale není to zrovna uživatelsky přívětivý produkt. Nicméně jestliže potřebujeme provést složitější úpravy (přidání ovladačů, úprava jazykových sad apod.), nic jiného nám nezbývá.

Jednodušší možností je využití nástroje *Rufus*[1], ve kterém jen zvolíme instalační médium (obvykle prázdný USB flash disk), navedeme program ke staženému ISO souboru, jako souborový systém navolíme NTFS (pozor, pokud je tam FAT32, musíme změnit), a po potvrzení se v dalším dialogu Rufu zeptá, co konkrétně chceme změnit. První možností je odstranění požadavku na velikost RAM, Secure Boot a čip TPM 2.0, ale tato možnost už dnes není použitelná, protože novější buildy Windows 11 se na takto upraveném systému odmítají aktualizovat.

[1] Rufus je dostupný na adrese https://rufus.ie/cs/.

Poznámka

Produktový klíč k aktivaci Windows je možné zadat už během instalace, nebo kdykoliv později v nástroji *Nastavení* ⇨ *Systém* ⇨ *Aktivace*. Někteří doporučují nechat zadání klíče až po aktivaci, při zadání během instalace někdy nebývá správně rozpoznána edice.

Po nainstalování Windows nastává velmi důležitá fáze: úpravy konfigurace systému, instalace aktualizací (včetně nejméně jednoho restartu) a nainstalování potřebných aplikací.

Úkol

Pokud máte možnost, vyzkoušejte si buď Media Creation Tool nebo stažení instalačního obrazu Windows.

Souhrn kapitoly 1

Účelem této kapitoly bylo zejména alespoň trochu vyrovnat počáteční rozdíly ve znalostech a zkušenostech studentů přicházejících z různých středních škol. Podívali jsme se na nejběžnější místa, ve kterých mají Windows „rozstrkané“ různé nástroje na nastavení funkcí systému, podívali jsme se na Hlavní panel, nabídku Start, přiblížili jsme si pojem jádra operačního systému a zabezečené sekvence upozornění (SAS), také jsme si vyzkoušeli vytvoření různých druhů zástupců, naučlili jsme se nejběžnější klávesové zkratky a prošli jsme si pojmy související s verzemi Windows. Také jsme se naučli zjistit si verzi a build svých Windows a nainstalovat Windows 11.

Kapitola 2

Průzkum struktury souborů

Rychlý náhled: V této kapitole se pustíme do průzkumu struktury složek a souborů. Projdeme si všechna důležitá místa v celé struktuře a také se naučíme získat informace ke konkrétnímu „podezřelému“ souboru.

Klíčová slova: Soubor, přípona, složka, adresář, System32, nedostupné složky

Cíle studia: Po prostudování této kapitoly získáte přehled v souborové struktuře především na systémovém disku, na kterém je nainstalován systém Windows. Budete umět najít nejdůležitější systémové soubory a složky, včetně umístění registru, spustitelných souborů a knihoven.

V textu používáme pojem systémový disk. *Systémový disk* je ten disk, na kterém máme nainstalovaný operační systém. Většinou to bývá disk `C:`, ale může být jiný, třeba `D:`.

Pokud při práci se soubory a složkami používáme *Průzkumníka*, k jednotlivým diskům se dostaneme přes speciální složku `Tento počítač` nebo `Počítač` (podle verze Windows).

Poznámka

Některé z uvedených složek a souborů jsou skryté nebo chráněné (nebo obojí), proto pokud chceme prozkoumat opravdu vše, měli bychom zapnout zobrazení skrytých a chráněných souborů a složek (postup je v kap. 1.2.4 na straně 8).

2.1 Přípony souborů

Ve Windows se už v prvních verzích přípony souborů používají pro odlišení typu jejich obsahu. Setkáváme se zejména s těmito příponami:

- EXE, COM – spustitelné binární soubory (programy),
- BAT, CMD, PS1 – spustitelné textové soubory (skripty) pro Příkazový řádek, grafické rozhraní, PowerShell; obsah si můžeme prohlédnout v textovém editoru, poklepáním myší se spustí,
- CPL, MSC – nástroje pro konfiguraci různých nastavení systému, jde o binární soubory (CPL jsou ovládací panely, MSC jsou konzoly s unifikovaným grafickým rozhraním),

- DLL – dynamicky linkované knihovny obsahující funkce a objekty používané systémem a aplikacemi, komunikační rozhraní mezi spuštěnými procesy a jádrem je tvořeno především těmito knihovnami (ale některé knihovny neslouží jako rozhraní), můžeme je brát jako zásobu předpřipravených funkcí a objektů (včetně prvků grafického rozhraní) procesům k dispozici,
- FON, TTF, OTF – dynamicky linkované knihovny s definicí fontů,
- NLS – dynamicky linkované knihovny s podporou různých znakových sad národních abeced (National Language Support); zde je určeno, jaké znakové sady lze pro daný jazyk použít, jaká rozložení klávesnice existují, jak se má v daném jazyce zobrazovat datum, čas, měna, čísla s desetinnou tečkou/čárkou, atd.,
- MUI – soubor s podporou některého jazyka (třeba češtiny nebo němčiny) pro některou součást uživatelského rozhraní či aplikaci – Multilingual User Interface (například kombinace přípon .CPL.MUI znamená podporu jazyka pro daný ovládací panel); zjednodušeně jde o řetězce v daném jazyce, které se v rozhraní aplikace mají zobrazit na určitých místech,
- SYS – většinou ovladače (hardwarových zařízení, ale i softwarové), až na výjimky (`config.sys`, `pagefile.sys` apod.),
- HLP, CHM, hxs, hxt, H1S, H1T – soubory s nápovědou v různých verzích Windows, některé jsou komprimované, binární, jiné ve formě XML, většinou nemá smysl je přímo prohlížet,
- INI – textové soubory s konfigurací (nastavením) systému nebo některé aplikace,
- INF – textové informační soubory, většinou pro ovladače, také může jít o šablony zabezpečení – podle jejich umístění, obecně obsahují informace nutné k řízení či provádění přístupu k prostředkům,
- REG – textové soubory, do kterých je exportována jedna nebo více větví registru, mají podobný formát jako INI a INF soubory,
- LOG – textové soubory zachycující průběh různých akcí nebo sledování prostředků,
- BLG – protokoly, binární obdoba LOG souborů (je v nich zachyceno sledování prostředků), jejich vytvoření a používání si ukážeme později,
- EVT, EVTX – protokoly událostí (EVT jsou binární, EVTX textové ve formátu XML), slouží ke sledování událostí, práci s těmito protokoly si ukážeme také později,
- LNK – soubory zástupců (čehokoliv – jiných souborů, adresářů, WWW adres, atd.), tato přípona se obvykle nezobrazuje, jsou to binární soubory,
- PIF – binární soubory, obdoba zástupců pro staré DOS programy, obsahují informaci o způsobu spuštění takového programu v prostředí (okně) Windows (přidělená paměť, použité písmo, přístupová oprávnění, atd.), k těmto nastavením se dostaneme v kontextovém menu, položka *Vlastnosti*,
- MSI, MSP – instalační balíčky aplikací (MicroSoft Installer), resp. opravné balíčky.

To rozhodně není vyčerpávající výčet, s některými dalšími se setkáme v průběhu výuky.

Úkol

Soubor `c:\Windows\notepad.exe` je spustitelným souborem aplikace Poznámkový blok. Existuje také soubor `c:\Windows\cs-CZ\notepad.exe.mui` obsahující textové řetězce pro provoz aplikace v českém jazyce, a v jiných podadresářích obdobný soubor pro jiné jazyky. Najděte .MUI soubor pro svůj jazyk a otevřete (můžete použít samotný Poznámkový blok nebo třeba PSPad, pokud máte nainstalovaný).

Jde sice o binární soubory, ale díky tomu, že obsahují řetězce, pro nás nejsou až tak nečitelné. Všimněte si záhlaví na začátku souboru, a také zápatí na konci souboru.

Další informace

Na https://file.org/sitemap.html je přehled nejrůznějších přípon souborů. Stačí zvolit první písmeno a případně se ve výpisu posunout na některou další stranu.

Soubory s příponou INI, INF, REG a některými dalšími příponami mají pevně danou strukturu, pro jejíž vytvoření a zpracování existují funkce jak v programovém rozhraní v knihovnách Windows, tak i v mnohých programovacích nástrojích, proto jsou především INI soubory využívány mnoha aplikacemi pro uložení konfigurace místo registru.

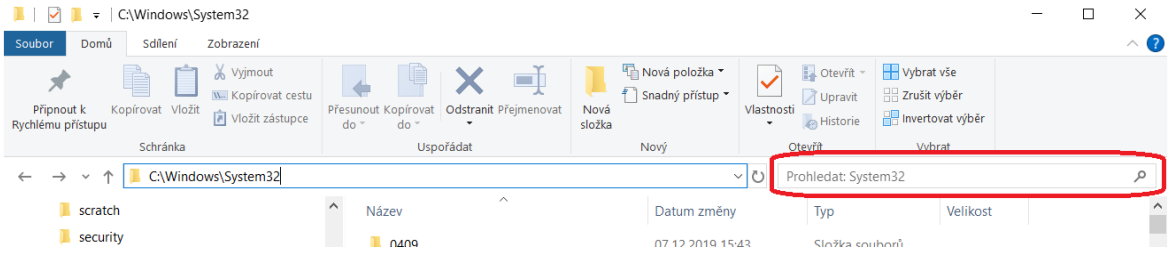
Tato struktura je založena na členění souboru na *sekce*. Každá sekce začíná názvem sekce v hranatých závorkách, následuje seznam položek pro tuto sekci. Tyto položky jsou ve tvaru vlastnost=hodnota. Například pokud máme instalován program *Total Commander*, existuje soubor `wincmd.ini` ve složce `Windows` začínající řádky

```
[Configuration]
InstallDir=C:\Program Files\totalcmd
languageini=wcmd_cz.lng
...
```

Jak vidíme, první sekce se nazývá Configuration, první položka této sekce nám říká, jak se nazývá složka, do které je program nainstalován, druhá pak určuje soubor s jazykovým nastavením.

Úkoly

1. V Průzkumníkovi přejděte do `c:\Windows\System32`. Najděte pole pro hledání, pro Windows 10 je ukázáno na následujícím obrázku (ve Windows 11 je to podobné, ale to už víme z předchozí kapitoly):



   Do pole pro hledání zadejte řetězec `*.ini` nebo `.ini` (bez hvězdičky, můžete vyzkoušet obojí). Měly by se vyfiltrovat všechny soubory s příponou INI v systémovém adresáři a jeho podadresářích. Najděte soubor `winrm.ini` a otevřete ho (poklepáním nebo přes kontextové menu). Všimněte si struktury tohoto souboru, a také obsahu. Mnohé z řetězců jsou ve skutečnosti texty pro chybová hlášení, účelem je tyto řetězce reprezentovat „proměnnou“, která je na začátku řádku. Oproti .MUI souborům sice .INI soubory nezvládají složitější hierarchii položek ani pokročilejší parametry pro překlad, ale pro tyto účely postačí.
2. Přejděte do `c:\Program Files`. Použijte tentýž postup – vyfiltrujte si soubory s příponou .INI. Všimněte si, kolik aplikací si část své konfigurace ukládá do tohoto typu souborů.

3. Následně se přesuňte do `c:\Windows\Inf`. Všimněte si, že zde najdeme hodně dvojic souborů – podobně pojmenovaný soubor má příponu .INF a druhý .PNF. První z nich je čitelný v textovém editoru, druhý je komprimovaný. Zaměříme se na soubory .INF. Některý si vyberte, například `monitor.inf` nebo `keyboard.inf` (všimněte si, že se dá vyhledávat psaním). Poklepáním soubor otevřete a prohlédněte si ho.
4. Mnoho prohlížečů podporuje funkci drag&drop. Pokud máte otevřený Poznámkový blok (který tuto funkci taky umí), stačí sebrat myší soubor, který v něm chceme otevřít, a přetáhnout ho do okna aplikace. Vyzkoušejte to na některém .INF souboru.
5. Na ploše vytvořte zástupce některého programu (EXE souboru) podle vlastního výběru. Pak zobrazte vlastnosti tohoto zástupce. Pak změňte ikonu zástupce.
6. Nechte si vypsat všechny soubory s příponou SYS a zjistěte, ve které složce se jich nachází nejvíc.
7. Zjistěte, zda je na ploše soubor `desktop.ini` (může být skrytý). Pokud ano, prohlédněte si obsah.

V některých případech si sami můžeme určit, jakou ikonou bude určitý objekt označen. Jde to například u zástupců, a pokud je zapnuto *Vlastní nastavení složky* (v *Možnostech složky*), tak i u složek. Ikonu můžeme určit ve *Vlastnostech* objektu (v kontextovém menu). Ikony najdeme v různých dynamicky linkovaných knihovnách, ale také v EXE souborech.

Pokud jsou u složky nastaveny některé funkce související s *Vlastním nastavením*, pak se v této složce objeví soubor `desktop.ini`. Je to textový konfigurační soubor, ve kterém je možné také definovat vlastnosti zobrazení složky.

2.2  Nedostupné složky ve Windows od verze Vista

V této a několika dalších sekcích budeme probírat také složky, které jsou od verze Vista uživatelům nedostupné (například `Documents and Settings` nebo některé podsložky ve složce `Users`). Ve většině případů je vlastníkem těchto složek systémový účet (*System*), ke kterému se nelze běžným způsobem přihlásit (běží pod ním mnohé systémové procesy) a přístupová oprávnění jsou nastavena velmi striktně (uživatelům včetně administrátorů je zakázán přístup do složky včetně jejího prohlížení).

Pokud se na takovou složku podíváme oklikou přes jiný operační systém (například když máme nainstalováno více operačních systémů a nabootujeme do Linuxu, anebo použijeme tzv. LiveDVD – více v druhé polovině semestru), zjistíme, že je takováto složka prázdná, neobsahuje ani skryté soubory.

Není zcela jisté, proč se Microsoft rozhodl tyto složky takto (téměř) absolutně znepřístupnit (zřejmě kvůli některým typům zvědavých uživatelů), ale vysvětlení samozřejmě existuje. Fyzicky se totiž jedná o takzvané *symbolické odkazy* (junction). O možnosti existence symbolických odkazů u NTFS se moc neví (my se jimi budeme zabývat v navazujícím předmětu), ale existují a lze si vytvářet také vlastní (pro tyto účely existuje například program `junction` od společnosti Sysinternals).

Existují také jiné nedostupné složky, které nejsou symbolickými odkazy. Se symbolickými odkazy logicky nemá smysl cokoliv dělat, ale pokud se opravdu jedná o běžnou složku vlastněnou systémovým účtem (nebo běžným uživatelem, který je „odlišný od naší osoby“), může administrátor převzít její vlastnictví (ve vlastnostech složky na záložce *Zabezpečení* přes další tlačítka – podrobněji v Operačních systémech) a pak nastavit přístupová oprávnění tak, jak mu vyhovují.

2.3 Složky pro uživatele a aplikace

Složka `Users` (kdysi `Documents and Settings`) na systémovém disku slouží ve Windows řady NT do verze XP k ukládání *profilů uživatelů*. Profil je souhrn lokálních nastavení (platných pro konkrétního uživatele) a osobních dat, tedy vše, co se týká jediného konkrétního uživatele. Ve Windows od Visty výše máme složku `Users`, ale také existuje složka `Documents and Settings`, ovšem je to jen link na `Users` (navíc ve vlastnictví uživatele System a pro běžné uživatele nefunkční).

`Users` má podsložky pojmenované stejně jako přihlašovací jména jednotlivých uživatelů, zde tedy najdeme data a nastavení konkrétního uživatele (to znamená, že v těchto podsložkách jsou uloženy *profily uživatelů*). Dále tu najdeme skrytou složku `Default` nebo `Default User` obsahující implicitní nastavení, která se použijí při vytváření nového profilu. Může být přítomna složka `Veřejné`: cokoliv do ní umístíme, je přístupné všem uživatelům na daném stroji, je určena ke sdílení dat mezi těmito uživateli.

U aplikace může její konfigurace platit buď pro všechny uživatele společně, nebo bude mít každý uživatel možnost si aplikaci nastavit po svém (nebo jde obojí). Nastavení platná zvlášť pro jednotlivé uživatele jsou uložena v profilech těchto uživatelů ve složce `Users\uživatel\Appdata`, kdežto společná nastavení se ukládají do `ProgramData` na systémovém oddílu (viz dále).

Ve složkách s profily najdeme například složku Plocha s obsahem plochy daného uživatele. Také je tam složka `AppData` nebo `Data Aplikací` – zde mohou aplikace ukládat nastavení specifická pro konkrétního uživatele, má tři podsložky:

- `Local` – data aplikací pro konkrétního uživatele, která se při přenosu profilu uživatele na jiný počítač (nebo na server) nemají přenášet, tedy jsou spojena s tímto počítačem a jeho lokálním systémem, například cache, historie,...
- `LocalLow` – podobně jako předchozí, ale navíc přístup k těmto datům je chráněný (např. data webového prohlížeče běžícího v chráněném režimu – „integrity level“ je nastaveno na „low“),
- `Roaming` – data aplikací pro konkrétního uživatele, která lze při přenosu profilu uživatele na jiný počítač bez problémů zkopírovat, v jiném systému budou také platná,

například

- `...\Roaming\Microsoft\Windows\SendTo` obsahuje linky v položce menu *Odeslat*,
- `...\Roaming\Microsoft\Windows\Start Menu` je uživatelská část položek v nabídce *Start*,
- `...\Local\VirtualStore` slouží jako virtuální úložiště pro starší aplikace zastupující některé systémové složky, které byly funkční jen do Windows XP,

Ve složce `Local` je také složka `Temp` pro dočasné soubory různých aplikací, který je dobré občas promazávat.

Postup

Funkce *SendTo* (*Odeslat do*) funguje celkem jednoduše. Pokud chceme například přidat do kontextového menu *Odeslat do* položku pro některou aplikaci, musíme postupovat takto:

- najdeme složku `.../AppData/Roaming/Microsoft/Windows/SendTo`,
- umístíme sem zástupce vybraného programu (například přitáhneme ikonu programu myší při držení jejího pravého tlačítka, nebo zvolíme *Nový* ⇨ *Zástupce* a zapíšeme třeba `notepad.exe`).

Na stejném místě jako `SendTo` jsou i další složky, například `Šablony` (`Templates`). Tam by měly být šablony dokumentů, které se použijí při využití položky *Nový* v kontextovém menu. Ovšem pokud bychom chtěli do tohoto menu přidat další šablonu, nestačí do této složky přidat příslušný soubor, ale je třeba provést změnu v registru. Na to se podíváme v kapitole o registru Windows.

V profilech uživatelů najdeme také soubor `NTUSER.DAT` obsahující část registru platnou pro daného uživatele. Je to binární soubor, nemůžeme ho prohlížet přímo, ale používáme aplikaci *Editor registru* (`regedit.exe`), se kterou se seznámíme v kapitole **??** o registru.

`Program Files` je složka, do které se obvykle instalují aplikace. Od Windows Vista je tato složka chráněna stejně jako systémová, bez oprávnění správce sem nic nenainstalujeme.

Někdy bývá problém s fungováním aplikací, které byly instalovány s oprávněním správce, ale běží s oprávněním běžného uživatele (pokud se pokoušejí do tohoto prostoru zapisovat, například do konfiguračních souborů). Aplikace naprogramovaná pro novější verze Windows by již kromě instalace neměla do této složky nic zapisovat, od toho existují další složky jak systémové, tak i v profilech uživatelů.

V 64bitových systémech najdeme kromě `Program Files` také `Program Files(x86)`. Pokud instalujeme 64bitovou aplikaci, nainstaluje se do složky `Program Files` (najdeme tam také složky, ve které je nainstalováno .NET Framework a některé důležité předkompilované .NET knihovny – assemblies), kdežto 32bitová aplikace se nainstaluje do složky `Program Files(x86)` (aplikace tuto složku „vidí“ jako `Program Files`, opět jde o virtualizaci).

Na systémovém disku je také složka `ProgramData`. Zatímco do `Program Files` by aplikace měly ukládat své „statické“ soubory, které se po dokončení instalace už nemění, složka `ProgramData` je určena pro „dynamické“ a datové soubory, u kterých se počítá s alespoň občasnými změnami za provozu.

Úkoly

1. Prohlédněte si složku se svým profilem. Najděte umístění pro dočasné soubory a podívejte se, jestli nepotřebuje promazat. Aplikace mohou umísťovat dočasné soubory i mimo „oficiální“ úložiště.
2. Otevřete složku obsahující položky nabídky *Start* a porovnejte ji přímo s nabídkou *Start*.
3. Ve složce `SendTo` ve svém profilu (najděte podle používané verze Windows) vytvořte zástupce programu `notepad.exe`, pojmenujte například *Poznámkový blok*. Pak zobrazte kontextové menu jakéhokoliv textového souboru (s příponou TXT, INI, INF nebo jinou) a vyzkoušejte položku *Odeslat* ⇨ *Poznámkový blok*.
4. Prozkoumejte složky `Program Files` a případně `Program Files(x86)`. Pokud máte 64bitový systém, můžete tak zjistit, které aplikace máte v 64bitové nebo 32bitové verzi.

2.4 Hlavní složky a soubory Windows

2.4.1 Složky na systémovém disku

Kromě výše zmíněných `Program Files`, `ProgramData`, `Users` apod. zde máme také tyto složky:

`PerfLogs` – obvyklé místo pro uložení BLG a LOG souborů, pokud ovšem máme logování zapnuto. BLG soubory jsou produktem sledování výkonu systému (performance logs – můžeme si určit například sledování vytížení procesoru, využití paměti apod.). Od verze Vista je tato složka dostupná pouze administrátorovi.

`System Volume Information` – tuto složku běžně neotevře ani administrátor, ukládají se zde například *body obnovy* (o nich se budeme učit v kapitole **??**, na straně **??**). V bodech obnovy se ukládá také záloha registru; Když je registr poškozen (škodlivým softwarem, neodborným zásahem, špatně napsaným programem, chybou na disku), obnovuje se právě odtud.

Tato složka může být ve skutečnosti na každém oddílu nebo třeba i paměťovém médiu typu USB flash disk takovém, kde jsme nevypnuli funkci Obnovení systému.

`Windows` – nejdůležitější složka, jejíž název je uložen v systémové proměnné `WINDIR`, obvykle se jmenuje `Windows`, `WinNT`, `Win32`. Dá se říct, že v této složce je nainstalován operační systém a jeho nástroje.

2.4.2 Soubory na systémovém disku

Přímo v kořenovém adresáři systémového disku najdeme několik důležitých souborů:

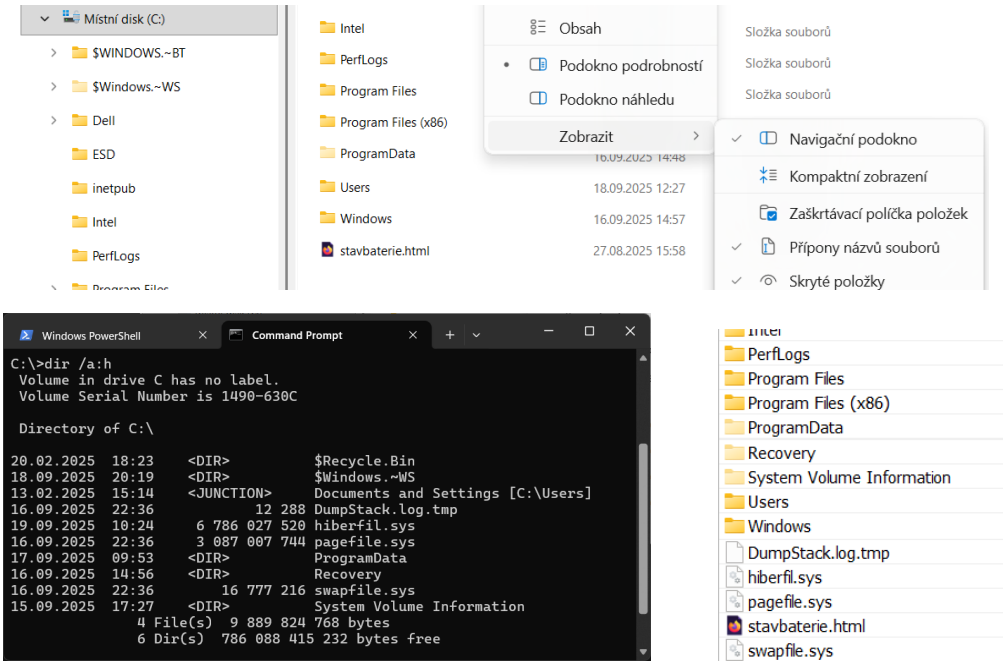
`pagefile.sys` – stránkovací soubor systému (virtuální paměť). Sem se ukládá to, co potřebujeme mít v operační paměti, ale nevejde se do fyzické operační paměti. Je to vlastně „nástavba“ paměťových modulů. Využití tohoto souboru nastavujeme v nástroji *Systém*, záložka *Upřesnit*, část *Výkon*.

`swapfile.sys` – toto je obdoba souboru `pagefile.sys` pro „univerzální“ aplikace z App Storu. Bývá obvykle menší (typicky 250 MB) a systém s ním zachází trochu jiným způsobem.

`hiberfil.sys` – do tohoto souboru se ukládá celý obsah operační paměti při přechodu do režimu hibernace. Je zde pouze tehdy, když je zapnuta podpora tohoto režimu, jinak tento soubor nenajdeme.

Postup

Ve Windows 11 se Microsoft rozhodl mást své uživatele ještě víc než v předchozích verzích. Některé skryté soubory totiž v Průzkumníkovi neuvidíte ani v případě, že si nastavíte zobrazování skrytých souborů.



Obrázek 2.1: Srovnání zobrazených skrytých souborů na C: (nahoře Průzkumník, dole levo Příkazový řádek, vpravo FreeCommander)

Přesto se k nim dá dostat, a to buď v Příkazovém řádku (na to se podíváme později) nebo v některém z alternativních správců souborů, jak vidíme na obrázku 2.1.

2.4.3 Podsložky ve složce `Windows`

Složka `Windows` má důležité podsložky:

`Boot` – podrobnosti o průběhu bootování budeme brát v jiném předmětu, zatím nám stačí vědět, že v této složce najdeme některé soubory, které se při načítání Windows používají.

`Cursors, Fonts, Media` – v první uvedené složce jsou soubory s kurzory, v druhé jsou uloženy soubory s fonty (písmem), v třetí najdeme většinou systémové zvuky (WAV soubory).

`ImmersiveControlPanel` – umístění pro spustitelný soubor `SystemSettings.exe`, který představuje nástroj *Nastavení*, a další související soubory. Ale pozor: *Nastavení* se spouští s využitím určitých parametrů, a bez jejich zadání se „nic nestane“.

`Inf` – informační soubory definující obvykle ovladače (instalační a konfigurační informace pro ovladače). Pokud se má intalovat ovladač nějakého zařízení, systém bude vyžadovat nejdřív soubor .INF, ve kterém si najde vše důležité pro instalaci samotného ovladače.

`Logs, LiveKernelReports, debug` – složky pro nejrůznější druhy logů, další jsou přímo v adresáři `Windows`.

`Microsoft.NET` – soubory rozhraní .NET Framework. To je sada knihoven (framework, běhové prostředí), díky kterému lze provozovat .NET aplikace.

`Prefetch` – Windows zde ukládají soubory související s nejčastěji spouštěnými aplikacemi (v názvech souborů můžeme poznat příslušnou aplikaci), které využívá funkce Superfetch (o té jsme se už dozvěděli na straně 20). Pokud je těchto souborů příliš mnoho, systém to spíše zpomaluje, navíc Superfetch není úplně praktická, pokud máme data uložená na SSD. Obsah této složky můžeme průběžně promazávat, systém si soubory postupně vytvoří znovu.

Tato složka neexistuje, pokud nemáme nastavenu optimalizaci spouštění aplikací. Je zde také soubor pro optimalizaci spuštění samotných Windows, a to `Layout.ini`.

`Resources` – soubory témat (motivů); v podsložkách `Themes` a `Ease of Access Themes` jsou soubory, kterými se přímo spustí nastavení motivu (pozor).

`ServiceProfiles` – podobně jako má každý uživatel svůj profil v `Users`, existují také profily účtů služeb LocalService a NetworkService, jsou uloženy zde.

`System32` – obsahuje dynamicky linkované knihovny (většinou zde jsou knihovny systému), ovladače, ovládací prvky ActiveX (OCX soubory, vlastně jde také o dynamické knihovny) a systémové aplikace. Je hodně rozsáhlý, proto se mu budeme věnovat v samostatné sekci.

`SystemApps` – prostor pro „nové“ systémové aplikace jako je Cortana, MS Edge, zamykací obrazovka, MS Feedback, Centrum akcí, nastavení pro rodinu apod. Obsah je hůře čitelný a spustitelné soubory nelze odtud přímo spouštět. Jak je u Microsoftu obvyklé: pokrokem ke zhoršení přístupnosti.

`SysWoW64` –zde je nainstalován podsystém pro spouštění 32bitových aplikací v 64bitovém systému (Windows32 on Windows64)

`Tasks` – naplánované úlohy (takové, které nenaplánoval přímo systém nebo hlavní aplikace). Například zde může být úloha pro pravidelnou kontrolu existence aktualizací pro některou aplikaci. Dalším úložištěm pro naplánované úlohy je adresář `.../Windows/System32/Tasks`.

`WinSxS` – zde najdeme knihovny existující ve více verzích (některé aplikace vyžadují konkrétní verzi určité dll knihovny, tedy pokud je nutné mít více verzí, jsou zde a přístup k nim je virtualizován), podrobnosti v příštím semestru.

`Web` – navzdory názvu zde jsou především tapety na plochu.

Poznámka

Možná už jste zjistili, že pokud místo Průzkumníka používáte alternativní prohlížeč souborů, některé položky se vůbec nezobrazují, třebaže máte zapnuto zobrazení chráněných i skrytých souborů.

Prvním důvodem může být to, že váš program je 32bitový. Souborový systém NTFS, který ve Windows slouží k evidenci souborů a jako přístupové rozhraní k paměťovým médiím, je totiž 64bitový, a Windows jednoduše odmítají přístup 32bitovým aplikacím do některých míst souborového systému, třeba i jen pro výpis položek. Proto nezbývá než použít Průzkumníka nebo jinou 64bitovou aplikaci.

Ovšem ve Windows 11 nám jsou některé soubory ukryty přesto, že použijeme Průzkumníka, na to už jsme narazili dříve.

2.4.4 Soubory ve složce `Windows`

V průběhu vývoje verzí se složka `Windows` stala značně chaotickou, ale ve vyšších verzích zde začal Microsoft dělat trochu pořádek (například tapety na plochu shrnul do vlastní složky, podobně dočasné soubory). Nicméně pořád tam najdeme soubory, které „není kam dát“, včetně některých logů.

Podíváme se na několik nejdůležitějších:

`explorer.exe` – první instance tohoto programu (tj. proces vzniklý prvním spuštěním) představuje grafické rozhraní Windows, každá další instance je *Průzkumník Windows*.

`hh.exe` – aplikace pro zobrazení souborů nápovědy ve Windows od verze 2000 (včetně XP), jako parametr je třeba uvést soubor nápovědy, který chceme zobrazit (s příponou CHM).

`HelpPane.exe` – aplikace pro zobrazení souborů nápovědy od verze Vista, spouští se obvykle s parametrem `-Embadding`.

`winhlp32.exe` – pro zobrazování souborů nápovědy v ještě starším formátu.

`notepad.exe` – spustitelný soubor Poznámkového bloku.

`regedit.exe` – základní program pro editaci registru. Jeho používání není zcela bez rizika, budeme se jím zabývat v kapitole **??** od strany **??**.

`system.ini, win.ini` (případně další INI soubory) – konfigurační soubory pro zpětnou kompatibilitu (kdybychom náhodou chtěli spouštět 16bitové aplikace).

Úkol

Projděte si umístění všech souborů a složek ve `c:\Windows` zde popisovaných.

2.5 Složka `System32` – základ systému Windows

Ve složce `System32` je uložena většina instalace Windows. Je zde ještě více různých typů souborů než ve složce `Windows`, najdeme tu především dynamické knihovny, spustitelné soubory (nejrůznější příkazy

a nástroje, ale také hry dodávané se systémem), některé softwarové ovladače (`ansi.sys`, `country.sys`, `himem.sys` apod.), pomocné datové soubory (binární i textové), spořiče obrazovky a další.

2.5.1 Podsložky ve složce `System32`

Nejdůležitější podsložky jsou:

`Boot` – vše potřebné pro start systému (především soubory `winload.exe` a `winresume.exe` pro start vypnutého, resp. hibernovaného systému). Pozor, o patro výš je stejně pojmenovaná složka, ale s jiným obsahem.

`config` – soubory se systémovou částí registru. Od verze Vista se do této složky nedostaneme bez administrátorských oprávnění, v 64bitovém systému vám nepomohou ani ta, pokud přistupujete přes 32bitovou aplikaci.

`Dism` – soubory nástroje DISM (Deployment image Servicing and Management), tento nástroj se používá na různé opravy instalace Windows a pokročilou správu, včetně chyb aktualizačního systému.

`drivers` – instalované ovladače. Zajímavý je také podadresář `etc` obsahující soubory s názvy hodně podobnými názvům souborů v UNIXových systémech v adresáři `/etc`.

`DriverStore` – od verze Vista se zde ukládají ovladače a související soubory. Najdeme zde několik podsložek, v jedné z nich – `FileRepository` – je uložena většina souborů SYS s ovladači, ke každému INF soubor. Pokud zde najdeme jen INF soubor, pak dotyčný ovladač není přímo nainstalován.

`GroupPolicy` – složka na skripty a různá nastavení související s nástrojem *Zásady skupiny* (budeme probírat později).

`Licenses` – plné znění EULA licence (v RTF souboru).

`LogFiles` – různé log soubory, obvykle binární.

`oobe` – je zkratka z Out-of Box Experience, obecně znamená takové zprovoznění produktu (třeba operačního systému), které je maximálně uživatelsky zjednodušeno (průvodce, který si sem tam od uživatele vyžádá nějakou informaci), dnes se tento princip používá při instalaci prakticky jakéhokoliv operačního systému. Zde najdeme soubory nástroje OOBE pro Windows, včetně jazykových nastavení.

`Spool` – konfigurační soubory pro tisk, ale také dočasné soubory související s výstupem, například tiskové položky po dobu, než jsou zpracovány. V podsložce `drivers\color` najdeme ICM soubory s barevnými profily pro zobrazovací zařízení.

`Tasks` – další úložiště pro naplánované úlohy systému a aplikací.

`Wbem` (zkratka z Web-Based Enterprise Management) – WBEM je souhrn technologií pro správu systému přes web. Jeho implementace pro Windows se nazývá *WMI* (Windows Management Instrumentation). Ve složce `Wbem` tedy najdeme soubory potřebné k provozu WMI. K této problematice se dostaneme v dalším semestru.

`WindowsPowerShell` – zde je nainstalován Windows PowerShell, jeho moduly a nápověda, zde také můžeme zjistit jeho verzi.

`winevt` – logy, které lze procházet v *Prohlížeči událostí* (probereme v další kapitole). Jsou to hlavně soubory s příponou EVT nebo EVTX.

2.5.2 Soubory ve složce `System32`

Ve složce `System32` je obrovské množství souborů. Jsou to většinou dynamicky linkované knihovny (s různými příponami, nejen DLL) a spustitelné soubory (EXE, MSC a další).

Nejdřív se podíváme na několik souborů, které (samozřejmě i s dalšími) tvoří základní strukturu Windows. Na obrázku 2.2 najdeme jednoduché schéma naznačující vztahy mezi těmito soubory a jejich zařazení do struktury systému.

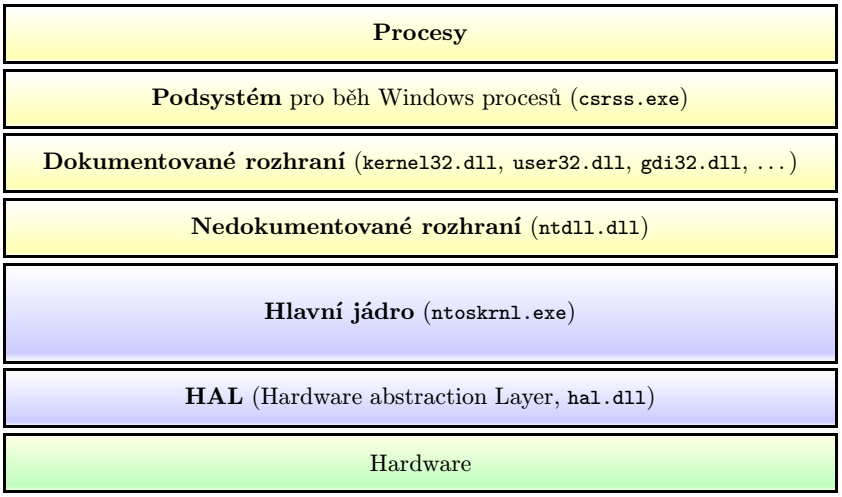
`hal.dll` – knihovna obsahující funkce pro vrstvu abstrakce hardware (HAL = Hardware Abstraction Layer) – část jádra přímo přistupující k hardwaru.

`ntoskrnl.exe` – hlavní soubor jádra, exekutiva (řídí jádro a tedy i celý operační systém). Je to část jádra nezávislá na hardwaru.

`kernel32.dll, user32.dll, gdi32.dll` a další – knihovny přístupné procesům, umožňují komunikovat s jádrem (součást tzv. dokumentovaného rozhraní jádra).

`ntdll.dll` – rozhraní mezi procesy běžícími v uživatelském režimu a procesy běžícími v chráněném režimu (tzv. nedokumentované rozhraní jádra). Procesy tuto knihovnu obvykle nepoužívají přímo, ale přes dokumentované rozhraní.

`csrss.exe` – program pro podsystém Win32 (v 64bitových Windows prostě podsystém Windows), přes něj se spouštějí (téměř) všechny Win procesy včetně systémových.



Obrázek 2.2: Zjednodušená struktura Windows, modré vrstvy tvoří jádro operačního systému, žluté uživatelský režim

Ale jsou zde i další důležité soubory, například:

`svchost.exe` – hostitel služeb, některé služby běží právě v tomto programu.

`cleanmgr.exe` – jednoduchý nástroj na mazání nepotřebných souborů.

`cmd.exe` – *Příkazový řádek* (přes ten můžeme zadávat příkazy).

`colorcpl.exe` – nástroj pro práci s ICM profily, které jsou zmíněny dříve, také je zde soubor `dccw.exe` (Display Color Calibration) pro kalibraci displeje.

`control.exe` – *Ovládací panely*.

`curl.exe` – program pro transfer souborů po síti (je ve Windows od verze 10), nápovědu získáme příkazem `curl -h`.

`services.exe` – řadič služeb, zajišťuje běh služeb systému a komunikaci s nimi. V tomto souboru je modul *SCM* (Service Control Manager), který má právě na starosti řízení služeb a jejich komunikaci.

`services.msc` – přes tuto konzolu s grafickým rozhraním můžeme pracovat se službami.

`shutdown.exe` – program pro vypínání, příp. restartování Windows. Popis přepínačů pro tento program (vypnutí, restart, vzdálené vypnutí, ...) je v nápovědě. Efektivně se dá použít například pro zástupce na plochu.

`taskmgr.exe` – *Správce úloh*.

`winlogon.exe` – program pro proces přihlašování uživatelů.

Najdeme zde hodně spustitelných souborů, které používáme jako příkazy v Příkazovém řádku, ale i nástroje s grafickým rozhraním spouštěné „myšovým způsobem“, například `calc.exe` (kalkulačka) nebo grafické konzoly (soubory s příponou .MSC).

Úkoly

1. Ve složce `c:\Windows\System32` si vyfiltrujte všechny soubory s příponou .EXE a pak soubory s příponou .MSC. Jak vidíte, těchto souborů je hodně – buď přímo v dané složce, nebo v jejích podsložkách.
2. Přejděte do složky `c:\Windows\System32\drivers\etc`. Prohlédněte si obsah souborů `hosts`, `networks` a `services`. Tyto soubory jsou textové, jen nemají příponu, tedy je můžete otevřít třeba tak, že si předem otevřete Příkazový řádek a do jeho okna přetáhnete ikonu příslušného souboru myší.

2.6 Lustrace souboru

Pokud jsme našli soubor s příponou, kterou neznáme, můžeme ji prověřit například na https://fileinfo.com/. Zadáme hledanou příponu a dozvíme se, k čemu takové soubory slouží.

Může se stát, že narazíme na soubor (většinou program), o kterém si nejsme jisti, zda je v pořádku. Málokdo má o souborech v systémových složkách tak dokonalý přehled, aby dokázal rozpoznat drobnosti v názvech (třeba záměna jednoho písmene) a umístění souborů nebo v jiných parametrech indikujících přítomnost škodlivého softwaru.

Existují možnosti, jak si ověřit správnost názvu a umístění souboru – většinou stačí zaúkolovat Google, dále se můžeme přímo obrátit na specializované weby, například:

- https://www.processlibrary.com/ (v menu pak Process Directory)
- https://www.fileinspect.com/
- https://www.file.net/

Všímáme si vždy správného umístění procesu (většinou „file path“ nebo „common path“) a informace, zda nejde o škodlivý software. Na některých z uvedených stránek najdeme také stručnou charakteristiku programu.

Úkoly

1. Projděte si umístění všech souborů a složek zde popisovaných. Vyzkoušejte programy `control.exe`, `services.msc`, `taskmgr.exe` (poklepáním spusťte).
2. Zjistěte, k čemu slouží soubory s příponami DRV, CAT, PSD1, ETL.
3. U následujících souborů zjistěte, zda nejde o škodlivý software:

   - `fixmapi.exe`
   - `psapi.dll`
   - `alg.exe`
   - `isass.exe`
   - `lsass.exe`
   - `svhost.exe`
   - `svchost.exe`
   - `rundll32.exe`
   - `rundlg32.dll`
   - `csrrs.exe`
   - `csrss.exe`
   - `csrsc.exe`

Postup

Na výše uvedených webech lze o souborech zjistit mnohé, také tam obvykle najdeme kontrolní součet (hash) posuzovaného souboru. Abychom měli s čím porovnat, je dobré vědět, jak si vygenerovat kontrolní součet u souboru, který máme na disku (a potenciálně mu nedůvěřujeme, tedy chceme kontrolní součet porovnat s tím uvedeným na webu). Vygenerování kontrolního součtu si ukážeme na malém textovém souboru umístěném ve vlastním profilu, abychom zbytečně neriskovali v systémových oblastech.

- Spusťte Příkazový řádek (klepněte na tlačítko *Start*, napíšete `cmd` a klepnete na Enter).
- Zadejte tento příkaz:

  ```
  echo nejaky text > pokus.txt
  ```

  Ve svém profilu byste teď měli mít soubor `pokus.txt`, což si můžete ověřit buď tak, že se tam podíváte v Průzkumníku či jiném správci souborů, nebo zde na Příkazovém řádku zadáte

  ```
  dir pokus.txt
  ```

  (vypíše se informace o tom, že tam takový soubor je, včetně jeho vlastností).
- Zadejte příkaz, kterým vygenerujete kontrolní součet pomocí algoritmu MD5:

  ```
  certutil -hashfile pokus.txt md5
  ```

  Pokud místo `md5` zadáme `sha1`, vygeneruje se kontrolní součet podle algoritmu SHA1, pokud použijeme řetězec `sha256`, dostaneme hash podle algoritmu SHA verze 2 s délkou klíče 256.
- V PowerShellu je podobný nástroj. Spusťte PowerShell (klepněte na *Start* a napište `powershell`, potvrďte). Zadejte tento příkaz:

  ```
  get-filehash pokus.txt -algorithm md5
  ```

  Měl by se vypsat stejný řetězec, jaký jsme dřív získali pro hash MD5 v Příkazovém řádku. Místo `md5` můžeme zadat také `sha1`, `sha256` a některé další algoritmy.

Souhrn kapitoly 2

V této kapitole jsme se zabývali souborovou strukturou ve Windows. Osvětlili jsme si význam nejběžnějších přípon (především systémových) souborů a pak jsme postupně procházeli nejdůležitější složky a soubory v kořenovém adresáři systémového diskového oddílu a ve složkách `Windows` a `Windows\System32`. Podívali jsme se na formát některých typů souborů, a také vztahy mezi některými soubory tvořícími páteř struktury systému. Na konci kapitoly jsme se zaměřili na lustraci „podezřelých“ souborů.

Část 2

Linux

Část 3

Bezpečnost

Přílohy

Příloha A

Seznamy

A.1 Příklady pro využití mechanismu *RunDll*

Následují příklady použití programu `rundll32.exe`. Pokud se rozhodnete některé z příkladů vyzkoušet, nejdřív si ověřte, že víte, „co to udělá“, a zda je příklad vhodný pro vaši verzi Windows. V názvech souborů obvykle není nutné dodržovat velikost písmen, ale v názvech funkcí v knihovnách a také v řetězcích parametrů je nutné přepsat velká a malá písmena přesně podle příkladu, jinak bude výsledkem pouze chybové hlášení.

`rundll32.exe shell32.dll,Control_RunDLL`

spustí nástroj *Ovládací panely* (totéž jako `control.exe`)

`rundll32 shell32.dll,Control_RunDLL main.cpl @0`

zobrazí okno s nastavením vlastností myši (první záložka)

`rundll32 shell32.dll,Control_RunDLL main.cpl @0,0`

totéž jako předchozí příkaz, jen jsme navíc zadali, že se má zobrazit první záložka (indexovaná číslem 0)

`rundll32 shell32.dll,Control_RunDLL main.cpl @0,1`

totéž, ale zobrazí se druhá záložka v nástroji pro nastavení myši (indexovaná číslem 1), atd. pro další čísla záložek

`rundll32 shell32.dll,Control_RunDLL main.cpl @1`

zobrazí nástroj pro nastavení klávesnice (první záložka, další záložky můžeme určit stejně jako v předchozích příkazech)

`RunDll32.exe shell32.dll,Control_RunDLL ncpa.cpl`

zobrazí nástroj *Síťová připojení*, ve kterém lze konfigurovat jednotlivá připojení do sítě a případně vytvářet nová (ve skutečnosti stačí zadat pouze `ncpa.cpl`, soubory ovládacích panelů jsou spustitelné samy o sobě)

`rundll32 shell32.dll,Control_RunDLL HotPlug.dll`

zobrazí okno *Bezpečně odebrat hardware*; získáme tak seznam právě připojených výměnných zařízení (třeba USB flash disky nebo CD) v jakékoliv běžné verzi Windows, ke kterému je ve Windows 7 jinak poněkud ztížený přístup (ikona, která do verze Vista sloužila právě k tomuto účelu, slouží pouze ve Windows 7 jen k synchronizaci)

`rundll32 shell32.dll,Control_RunDLL Sysdm.cpl,,3`

zobrazí nástroj *Vlastnosti systému*, a to poněkud překvapivě jeho třetí záložku (záložky jsou zde indexovány od 1, nikoliv od 0)

`RunDll32.exe shell32.dll,Options_RunDLL`

zobrazí se nástroj *Možnosti složky*

`RunDll32.exe shell32.dll,Options_RunDLL 1`

zobrazí se nástroj *Vlastnosti Hlavního panelu a nabídky Start*, všimněte si, že od předchozího příkazu se tento odlišuje pouze přidáním číselného parametru na konec

`RunDll32.exe shell32.dll,Options_RunDLL 2`

opět zdánlivě stejný příkaz, ale tentokrát zobrazí nástroj *Možnosti složky*, a to jeho třetí záložku s konfigurací vyhledávání (číslo na konci teď znamená číslo záložky, indexy jdou od 0); tento příkaz nefunguje ve Windows XP (tj. je použitelný až od Visty)

`rundll32 shell32.dll,SHHelpShortcuts_RunDLL Connect`

ve Windows XP spustí nástroj *Síťová připojení*, od verze Vista se spustí průvodce *Připojit síťovou jednotku*

`rundll32 shell32.dll,SHHelpShortcuts_RunDLL PrintersFolder`

otevře se okno se seznamem tiskáren (hodí se zvláště ve Windows 7, kde v *Ovládacích panelech* najdeme jen položku *Zobrazit zařízení a tiskárny*, jejíž spuštění může z důvodu drobných chyb na ovladačích zamrznout a k tiskárnám se nedostaneme)

`RunDll32.exe devmgr.dll DeviceManager_Execute`

spustí *Správce zařízení* (tj. můžeme se dostat k vlastnostem jednotlivých zařízení a případně přeinstalovat ovladač nebo odpojit zařízení)

`RunDll32.exe user32.dll,LockWorkStation`

uzamčení počítače (když potřebujeme na chvíli někam odběhnout)

`RunDll32.exe powrprof.dll,SetSuspendState`

uspání počítače – počítač je vpodstatě vypnutý, ale po běžném startu a případném výběru operačního systému se místo běžného bootování (nabíhání) Windows spustí „Obnovení činnosti systému Windows“, funguje jen tehdy, když příslušný operační systém tuto funkci podporuje a je zapnutá

`rundll32 Printui.dll,PrintUIEntry /?`

zobrazí se okno *Uživatelské rozhraní tiskárny*; jde o nápovědu modulu *PrintUI*, který lze použít k (vzdálené) správě tiskáren v místní síti nebo lokálně na počítači, lze zobrazovat konfiguraci, instalovat či odstraňovat tiskárnu, uložit nastavení nebo načíst zastavení ze souboru, pracovat s tiskovou frontou, atd.

`rundll32 Printui.dll,PrintUIEntry /e /n "Název tiskárny"`

zde využíváme informace z nápovědy zobrazené předchozím příkazem – chceme zobrazit předdefinovaná nastavení tisku pro tiskárnu, jejíž jméno jsme zadali v posledním parametru (všimněte si uvozovek, jsou nutné pro případ, že název obsahuje mezeru nebo některý znak, který není součástí anglické abecedy)

`rundll32.exe advapi32.dll,ProcessIdleTasks`

spuštěním tohoto příkazu se okamžitě (s vyšší prioritou) provedou všechny úlohy, které právě běží na pozadí; použijeme, pokud chceme delší dobu provozovat aplikaci, která bude potřebovat

vysoký výpočetní výkon a nechceme, aby se o něj musela při svém běhu dělit s indexováním, defragmentací a jinými podobnými úlohami běžícími na pozadí

`rundll32 winspool.drv,ConnectToPrinterDlg`

zobrazí se průvodce *Připojit k tiskárně* (rozumí se k síťové tiskárně v místní síti)

`RunDll32.exe InetCpl.cpl,ClearMyTracksByProcess 8`

promaže dočasné soubory vytvořené *Internet Explorerem*

Tento seznam rozhodně není úplný. Další příklady najdete na webu.