INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Tato inovace předmětu Analýza dat je spolufinancována Evropským sociálním fondem a Státním rozpočtem ČR, projekt č. CZ.1.07/2.2.00/28.0014, "Interdisciplinární vzdělávání v ICT s jazykovou kompetencí".

Digitální analýza Cisco směrovačů a přepínačů 1

Analýza dat

Bc. Filip Pávek

Ústav informatiky
Filozoficko-přírodovědecká fakulta
Slezská univerzita v Opavě

filippavek@gmail.com

2012

Obsah prezentace

Co nového se naučíme a na jaké otázky odpovíme?

- Principy forenzní analýzy, co ke zkoumání musíme vědět a jak se zachovat při vzniklém incidentu?
- Zmíníme možnosti připojení na router (console, SSH, ...
- Připomeneme, která z metod vyžaduje extra konfiguraci a která funguje defaultně.
- Řekneme si, jaká hesla potřebujeme znát pro přihlášení na zařízení. Co když hesla neznáme? Jaké jsou postupy a jak tyto postupy ovlivní nestálá data v zařízení.
- Popíšeme si práci s programy, které budeme při zkoumání používat.
- Všechno budeme v průběhu výkladu prakticky testovat!

Obecné otázky

Znáte odpovědi na následující otázky?

- Proč myslíte, že jsou směrovače (přepínače) zajímávé jako cíl (mezikrok) útoků?
- Jak zareagovat na bezpečnostní incident (např. ztráta podnikových dat)?
- Co znamená Incident Response Plan? K čemu slouží a co v něm najdete? ... Pokud ho najdete :-).
- Co myslíte, že obnáší forenzní analýza aktivních prvků v síti? Jaké jsou kladeny požadavky na znalce?

Bezpečnostní incident a kroky, které by měli následovat

- Incident Response Plan (Plán odezvy na incident). Je v ogranizaci vytvořen? Kdo může řešit vyvstalý incident? Obecně, vede naše kroky při řešení bezpečnostního incidentu.
- Zkoumání provádí fundovaný specialista. Hluboké znalosti v HW a SW technologiích, orientace v moderních bezpečnostních incidentech. Důležitou roli hraje výměna informací mezi znalci.
- Pozor, řešení incidentu, sběr dat ze zasažených zařízení musí být prováděn trénovaným odborníkem.
- Důkazní materiál musí pro ográny činné v trestním řízení splňovat určité požadavky (dokumentace, integrita dat, časová osa, . . .). Chyby ve fázi sběru dat (např. neprůkazná dokumentace) mohou vést k tomu, že výsledky nelze použít.
- V průběhu zkoumání zapište do dokumentace každy krok který děláte a kdy ho děláte.

Bezpečnostní incident a kroky, které by měli následovat

Co musíme vědět než můžeme začít zkoumat?

- Jaká je síťová topologie, jaké jsou aktivní prvky v síti,
- (HP, Cisco, Juniper), jaká verze OS (např. IOSu),
- existuje záloha konfiguračních souborů, nastavené metody přístupu, jaká zařízení jsou zasažena,
- získat hesla nutná k přihlášeni na zařízení,
- existuje lokální nebo vzdálený přistup k zařízením,
- nastala před incidentem neočekávaná údálost (výpadek proudu, technický problém, pohyb cizích osob u zařízení,. . .)
- jak se projevil incident, incident již zkončil nebo stále trvá,
- porada s administračnim týmem, vytvoření plánu pro sběr nestálých a stálých dat,
- perfektní vedení dokumentace (včetně seznamu osob podílející se na zkoumání zařízení).

Možnosti připojení na směrovač a přepínač

Znáte odpovědi na následující otázky?

- Jaké znáte metody připojení na router?
- Jaké jsou výhody a nevýhody jednotlivých metod?
- Jaký HW ke každé metodě připojení potřebujete?
- Je třeba specifická konfigurace pro připojení?
- Umíte všechny metody připojení nastavit?

Znáte odpovědi na následující otázky?

- Na jaká hesla můžete při přihlášení na směrovač narazit?
- Lze hesla obejít aniž by došlo ke ztrátě nestálých dat?

Console port

- Port určený primárně ke konfiguraci zařízení (management).
- Rollover kabel - propojení mezi PC a portem console na směrovači. Zpravidla plochý a modré barvy

Možnosti připojení na směrovač a přepínač

- V laboratoři používáte RJ-45/DB-9 (console port do seriálového portu na PC). Adaptér serial/USB pro laptop.
- Pod portem je na směrovači modný popisek.
- Níže „vychytávka“, která urychlí sběr dat. Ideální nastavit na line odkud zkoumáme. Odstraní –More– a vypíše celý výpis bez ohledu na jeho délku.

```
Router(config)#line console 0
Router(config-line)#lenght 0
----------------------------
Router# terminal lenght 0
```

Auxiliary (AUX) port

- Primárně slouží pro vzdálenou konfiguraci - připojení modemu.
- Lze použít i ke konfiguraci lokální (nevypisuje na rozdíl od console systémová hlášení).
- Pod portem je na směrovači černý popisek.

Možnosti připojení na směrovač a přepínač

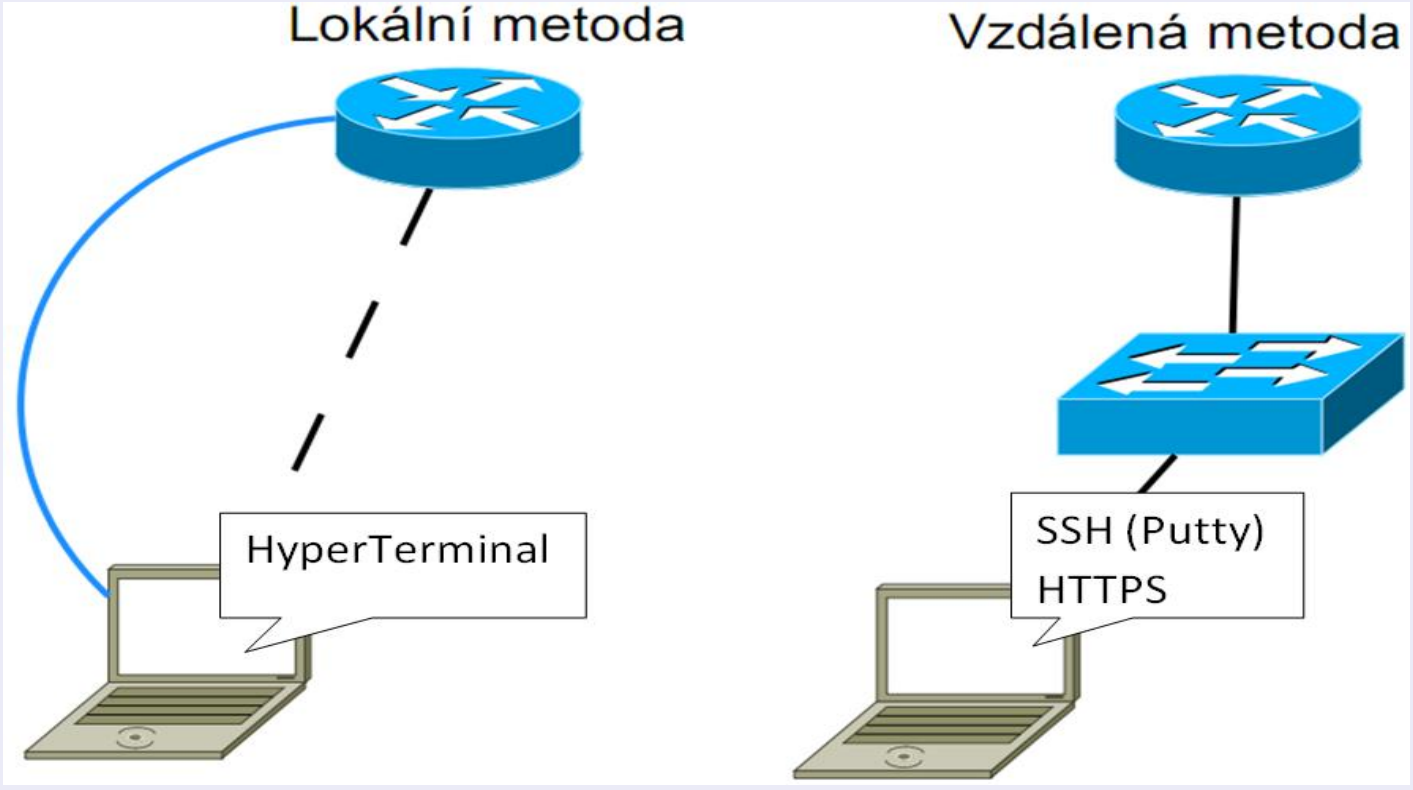
Telnet

- Metoda vzdáleného přístupu - nepoužívat.
- TCP/23 - velmi starý protokol.
- Obsah je posílán jako plain text - snadný odposlech při vzdálené konfiguraci čehokoli (síťové prvky, servery, . . .).
- Telnet musí být nakonfigurován. Jak se konfiguruje? Přístup lze omezit na konkrétní PC(s) (access-class).

SSH - Secure Shell

- Metoda vzdáleného přístupu. Nepodporují všechny verze IOS.
- TCP/22 - náhrada za Telnet. Obsah při přenosu šifrován.
- SSH musí být nakonfigurovaný. Jak se konfiguruje? Přístup lze omezit na konkrétní PC(s) (access-class).

- Pokud existuje možnost fyzického přístupu k zařízení, je přímé propojení mezi Laptopem a směrovačem přes consolový port nejlepší variantou. U vzdáleného přístupu používat vždy zabezpečené protokoly (nikdy Telnet).



Jaká hesla musíme znát chcete-li se připojit na zařízení?

Heslo na consoly

Již můžeme udělat zavěr, která z metod přístupu na směrovač je nejbezpečnější a zároveň neinvazivní k forenznímu získání dat. Další bodem je si uvědomit, na jaká hesla na směrovači narazíme.

Neduhy reálného provozu

- Může se to zdát neuvěřitelné, ale popis konfigurace a zabezpečení směrovače, jako i celé topologie v mnoha podnicích chybí úplně, je zastaralá nebo existuje, ale v době incidentu jí nikdo nenajde.
- Na pozicích správců menších firem nejsou vždy fundovaní experti.
- Mnoho hraničních směrovačů, které jsou připojeny do Internetu není zabezpečena vůbec nebo zpravidla jen defaultním heslem od výrobce.

- Stejná sitauce je i s aktviními prvky uvnitř LAN - zpravidla defaultní heslo (Admin - Admin).
- Zkuste vyhledat defaultní hesla pro zařízení která spravujete - např. http://www.phenoelit-us.org/dpl/dpl.html.
- Uroveň zabezepečení počítačových sítí je někdy katastrofální a odpovídá roku „1989“.

Co když heslo k přistupu na zařízení nemáme?

- Password recovery postupy - dle výrobce a řady produktu.
- Uvědomte si, že při password recovery dojde k restartování zařízení a všechna nestálá data z RAM paměti budou nenávratně smazána. Čímž můžete příjít o důležitá data dokreslující celý incident.

Hesla

Heslo na consoly

- Při přihlášení - slouží pro vstup do user-exec modu.
- Jak se nakonfiguruje?

Heslo na vstup do priviledge-exec (enable) režimu

- Slouží pro přechod s user-exec modu pro priviledge-exec modu (tzv. enable password).
- Enable password (plain text), enable secret (md5 hash).
- Jak se nakonfiguruje?.

Co řeší a kdy se používá #service password encryption?

- Účel - převede hesla (VTY, console, enable password, BGP neighbor) do nečitelné podoby v konfiguračním souboru.
- Cisco Password Cracker, Caine & Abel.

Pracovní režimy

>User-exec mode (uživatelský režim)

- Ihned po přihlášení. Omezený rozsah příkazů.
- Nezapomeňte: pokud útočník změnil heslo do privilegovaného režimu ale nikoli heslo pro přihlášení, lze tento režim dle verze IOSu použít pro sběr dat.
- Zjistě jaké příkazy IOS v uživatelském režimu podporuje. ? Pozor, na zařízení nic předem neotestovaného nezkoušejte. Vaše příkazy ovlivňují historii naposledy použitých příkazů!

#Priviledge-exec mode(privilegovaný režim)

- Používaný k monitoringu. Příkazy typu #**show**, #**copy**.

Programy používané při forenzní analýze

Úvodní informace

- V této části si představíme nástroje, které budeme při zkoumaní na cvičeních v laboratoři používat.
- Jde o nástroje sloužící ke vzdálenému připojení a použitelné jako síťová uložiště.
- Všechny nástroje jsou volně dostupné ke stažení.
- Zmíněné nástroje byly otestovány pod OS Windows XP a Windows 7. Samozřejmě existují Linuxové alternativy a budou zmíněny. Nutné pouze ověřit u terminálu vlastnost „zachytávání textu“.

Emulátory terminálu

Základní charakteristika

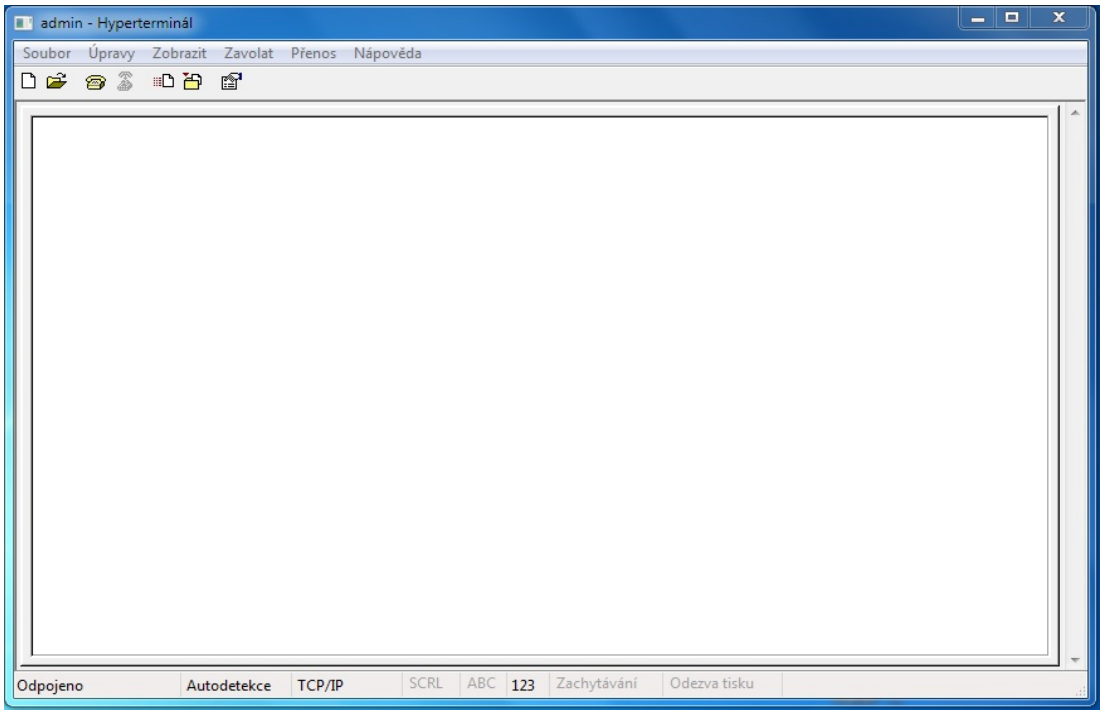
- Anglický známý jako „terminal emulator“.
- Umožně vzájemnou spolupráci mezi různýmim typy systémů, které by spolu normálně nefungovaly.
- Emulator použijeme ke vzádálenému připojení na směrovač pomocí protokolu SSH, Telnet nebo sériové asynchroní linky.
- Existují emulátory terminálů pod OS Windows i Linux.
- V tomto bloku se seznámíme s ovládáním HyperTerminálu a Putty. V dalších částech semestru ještě s emulátorem Cygwin.

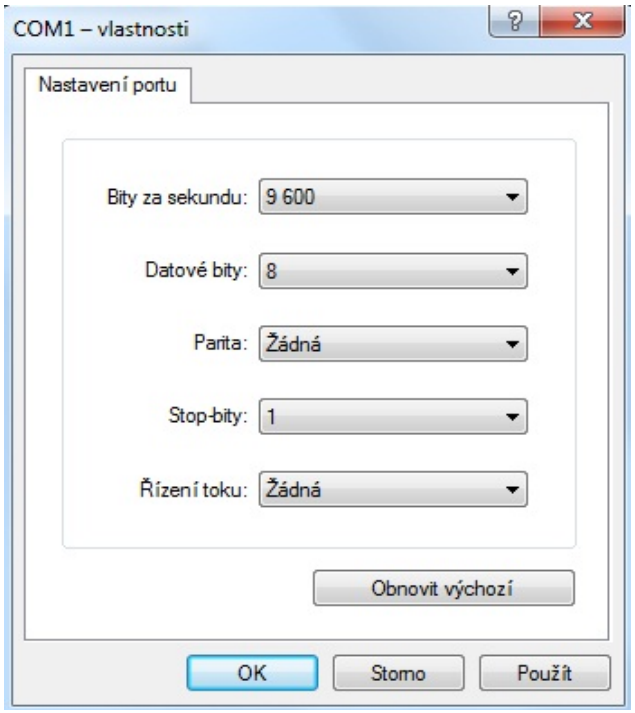
HyperTerminal

HyperTerminal

- Emulátor terminálu pro OS Windows.
- Od Windows Vista včetně není HyperTerminal součástí.
- Doporučuji mít HyperTerminal připravený na USB flash disku a nespoléhat na typ OS Windows (viz. LAB).
- Pokud zkoumání provádíte pod OS Windows XP, najdete HyperTerminal následovně: Start → Příslušenství → Komunikace → Hyperterminal (ikona telefonu).
- HyperTerminal budeme používat k vytvoření seriálového asynchroního spoje se směrovačem.

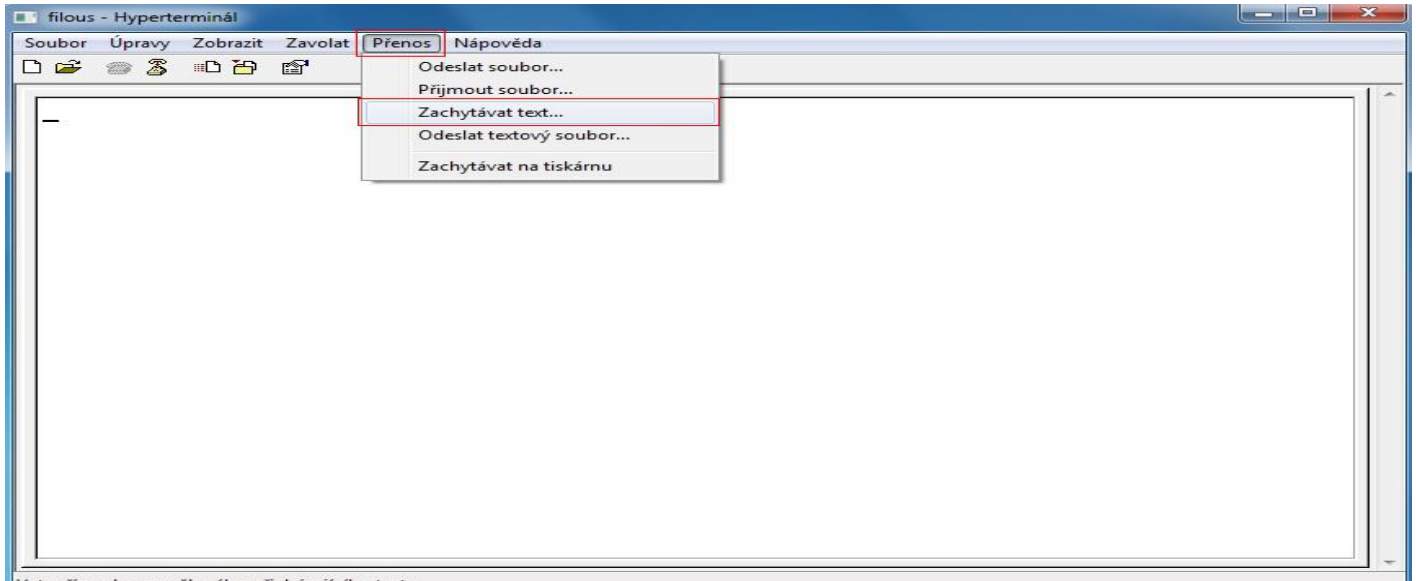
Nastavení HyperTerminalu k připojení na směrovač





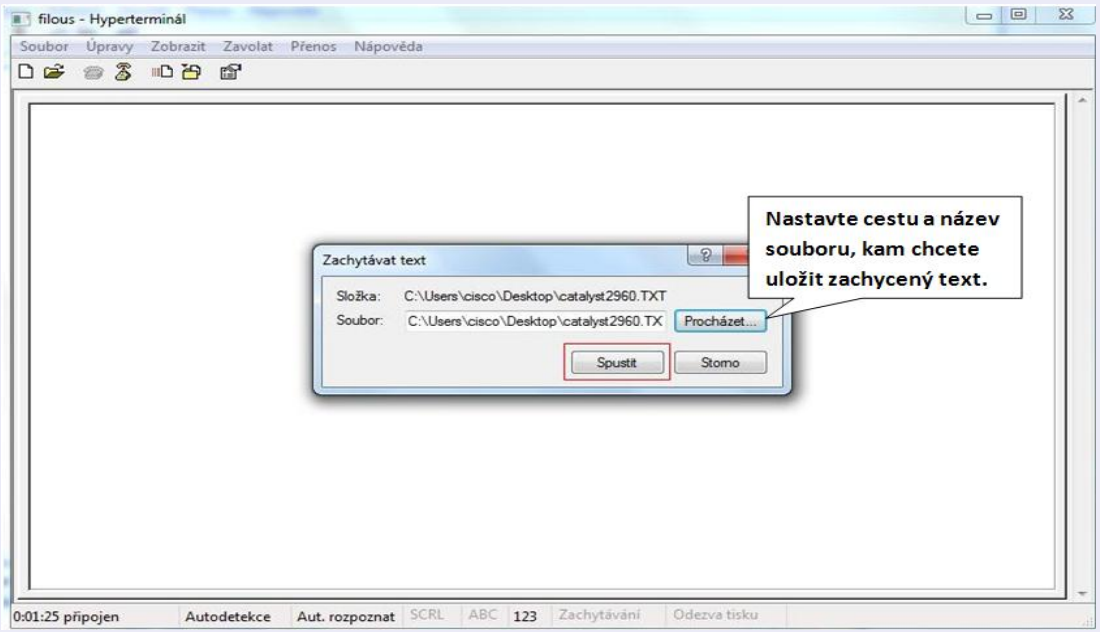
HyperTerminal a jeho využití při forenzní analýze

- HyperTerminal se spustí s pozadím nenasvědčujím žádnou aktivitu a vyžaduje od uživatele stisk tlačítka **Enter**.
- Při forenzním zkoumání využijeme silnou vlastnost HyperTerminalu - „Zachytávání textu..“ Před stiskem tlačítka **Enter** nastavte: **Přenos** → **Zachytávání textu..**
- Po stisku tlačítka **Zachytávání textu..** Vás aplikace vyzve k nastavení cesty a názvu souboru, kam bude dump uložený. Až poté stikneme tlačítko **Enter** a můžeme zahajít zkoumaní.

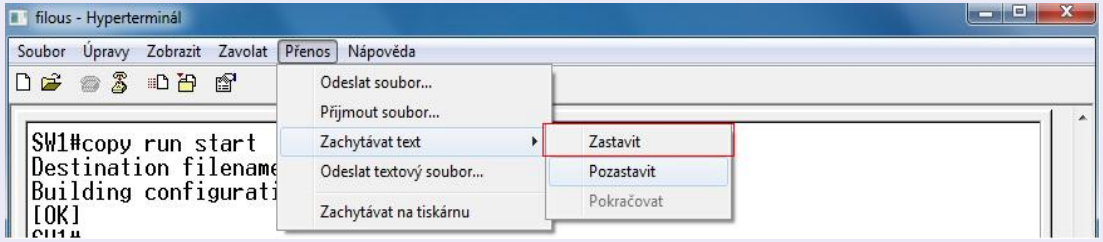


- Nezapomeňte: při forenzním zkoumání se klade velký důraz na doložení veškerých vašich činností ve zkoumaném systému. Musí být jasně průkazné, že Vaše zkoumaní nijak neovlivnilo a nezměnilo chování systému. Tedy, nedošlo k poškození nebo změně potencionálních důkazy.

Nastavení cesty a názvu souboru výsledného dumpu



Ukončení operace zachytávání textu



- Ukončit zachytávání textu: **Přenos** → **Zachytávání textu..** → **Zastavit**.
- Veškerá Vaše činnost je zachycena v textovém souboru.

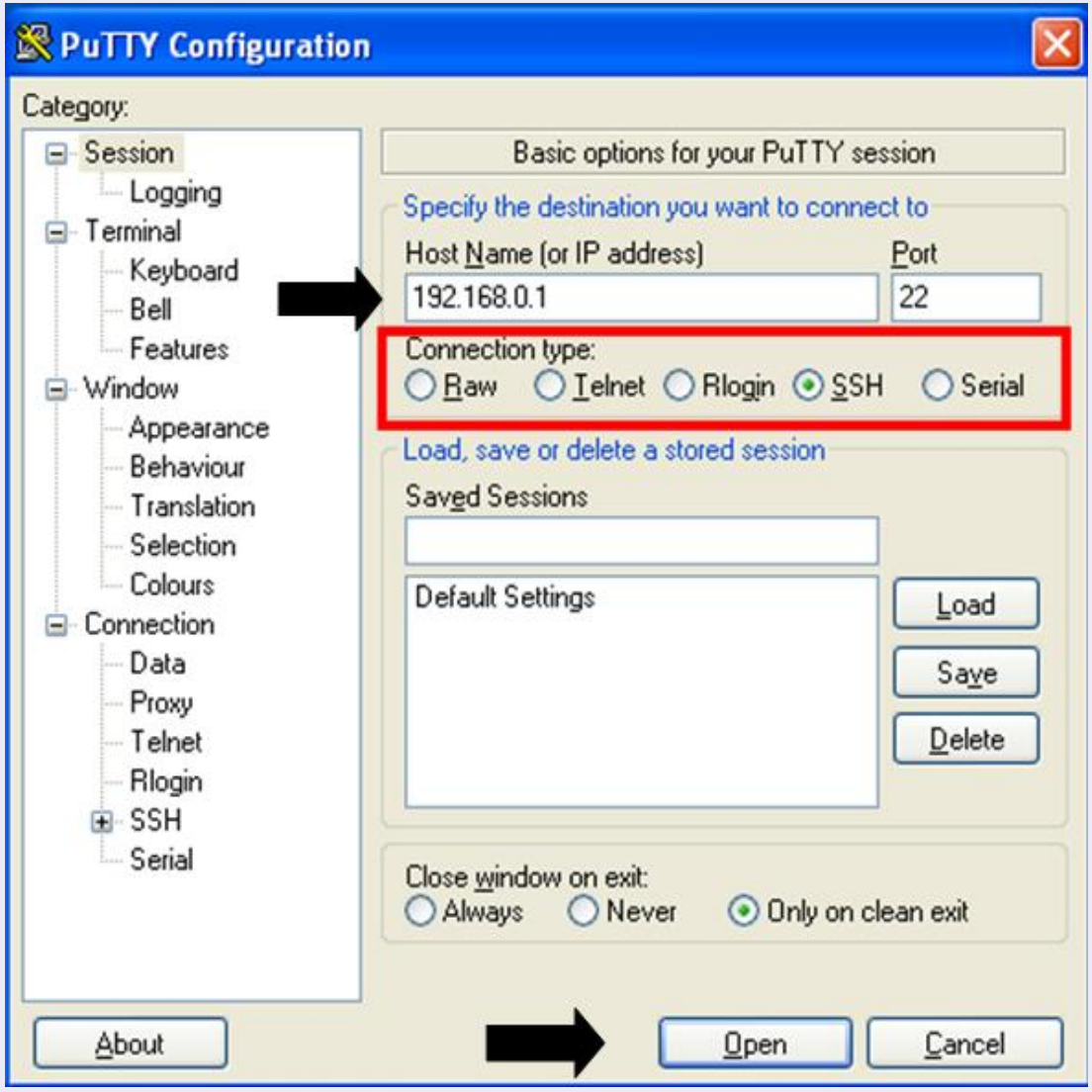
Putty

Putty

- Uvolněný pod licencí MIT (svobodný software).
- Umožňuje vzdálené připojení protokolem Telnet i SSH a lokální připojení přes consoly.
- Je dostupný pro OS Windows i Linux.
- Doporučuji mít tohoto klienta na USB flash disku.
- Pozor, jistě víte, že primární systémová hlášení (logy) se vypisují na consoly. Pokud chceme vidět výpisy ve vzdálené session (př. po připojení přes Telnet či SSH) aktivujeme je příkazem: #terminal monitor.
- Logy lze směrovat na consoly, buffer, vzdálenou session nebo na Syslog server. Logy hrají důležitou roli při FA (viz. níže).

Putty

Putty - výběr typu a nastavení připojení

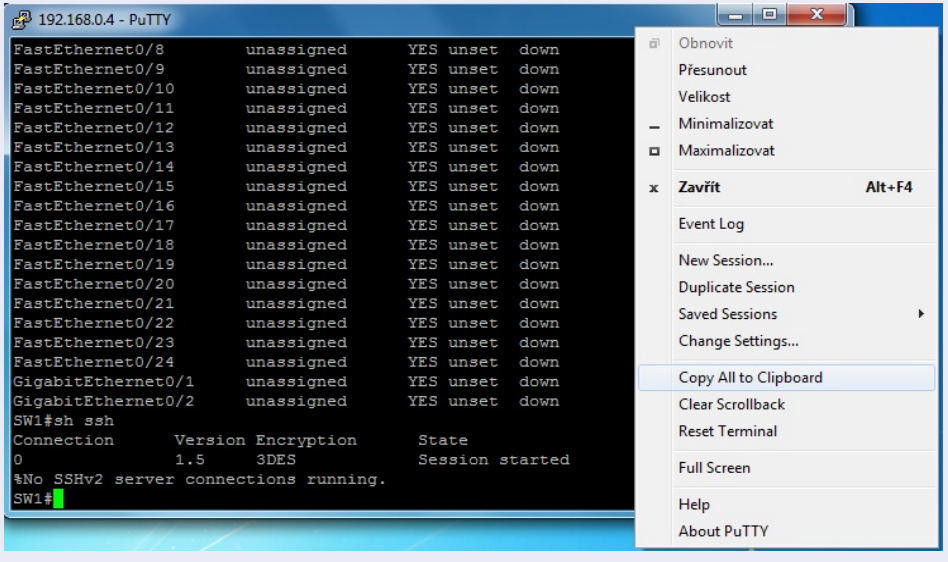


Client Putty při forenzní analýze

Putty

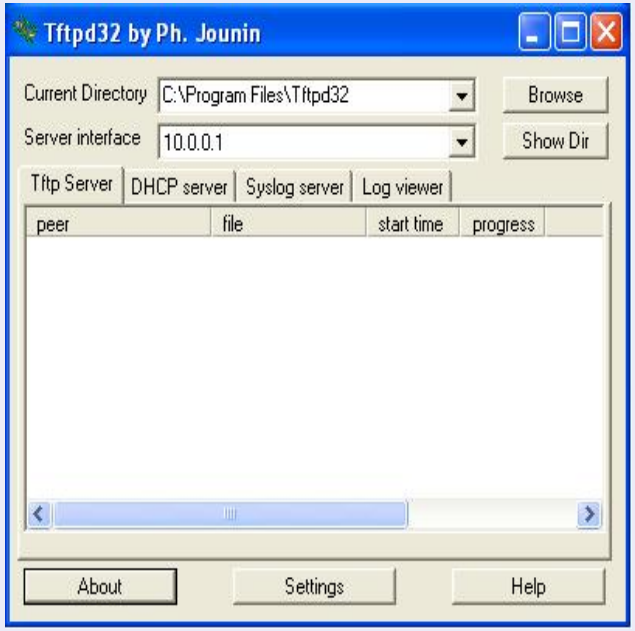
- Neumožňuje zachytávání textu jako předchozí HyperTerminal. To lze řešit např. snímky obrazovky (PrtSc) nebo fotoaparátem (pozor na správné nastavení data a hodin).
- Nelze použít z kontextové nabídky **Copy All to Clipboard**. Při výpisech dochází k přepisu schránky.

Putty - použití schránky k zachycení textu



Tftpd32

- Open source aplikace obsahující TFTP server/client a DNS, DHCP,SNTP, Syslog server.
- TFTP využívá protokolu UDP/69 - není šifrován.
- TFTP server se při správě aktivních prvků v síti výborně hodí k záloze a nahrávání konfiguračních souborů (IOSu).
- Lepší variantou je použití protokolu FTP TCP/20,21 (dále).



Tftpd32 - TFTP server při forenzní analýze

- Stejně jako při běžné práci, použijeme TFTP server jako síťové uložiště, kam zkopírujeme konfigurační soubory, IOS, ...
- Výstupy z #show příkazů, lze při sběru dat ze směrovače přesměrovávat na TFTP server a ukládat do souboru .txt.
- Pozor: není optimální každý příkaz ručně napsat a výstup přesměrovat na TFTP server. Problém jsou časné překlepy. Čím méně příkazů použijeme při zkoumání tím více omezíme změny na systému. Ukážeme si sofistikovanější přístup.

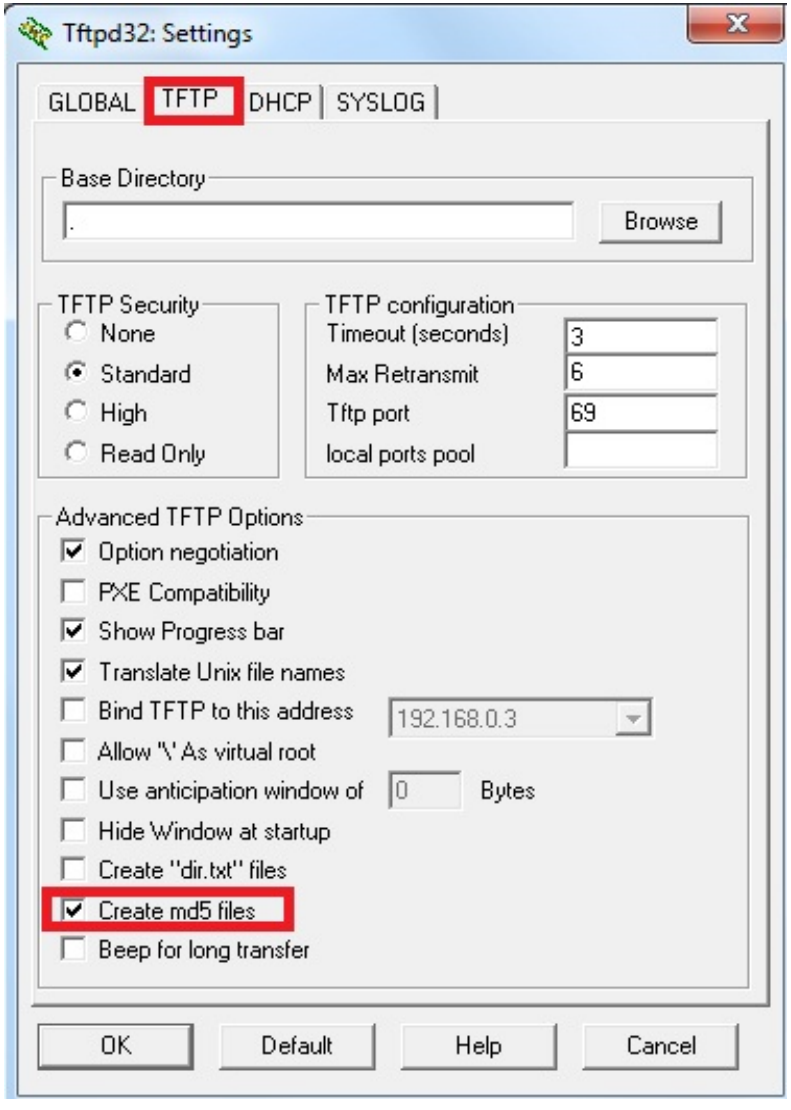
```
Router#show running-config | redirect tftp://192.168.0.2/run.txt
```

- IPv4 adresa určuje adresu TFTP serveru (cil), následuje adresářová struktůra. Pokud ukládáme do roota, pak pouze název souboru (pokud neexistuje, bude vytvořen).
- Úspěšný přenos souborů na server je vyjádřen !.

Tftpd32 - TFTP server při forenzní analýze

Integrita dat

- Při vytváření kopií ze všech souborů na směrovači (config, IOS, . . .) je velmi nutné prokázat, že nedošlo při vytváření nebo přenosu kopie ke změně dat.
- Zaručení integrity dat pomocí hashovacích funkcí (MD5, SHA-1, SHA-2).
- Znáte historický vývoj, použití a úroveň zabezpečení hash?
- Tftpd32 lze nastavit tak, aby byl při přenosu souboru vypočítal kontrolní součet.



Tftpd32 - TFTP server při forenzní analýze

Integrita dat

- Pokud vybereme možnost vytvořit MD5 soubor - bude v adresáři kam zkopírujete soubor vytvořený i další textový soubor, který obsahuje samotný kontrolní součet.
- Ale pozor, jak víme, že kontrolní součet skutečně odpovídá origiálnímu souboru? Nevíme!
- Pro každý originální soubor ve směrovači vypočítáme kontrolní součet a následně po přenesení do cílového uložiště znovu opakujeme tento postup i pro kopii. Pokud se hodnoty neshodují, pak proces opakujeme.
- Neprokázání zajištění integrity dat při vytváření obrazu může vést k nepoužitelnosti výsledků zkoumaní v soudním řízení!

Výpočet kontrolního součtu na směrovači

```
Router#verify /md5 <název_souboru>
```

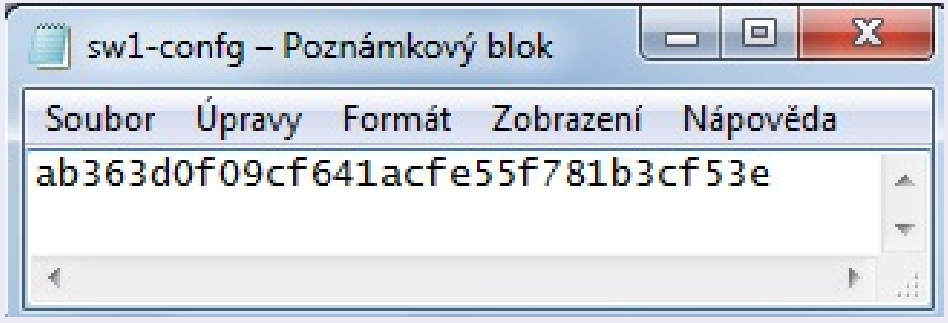
Tftpd32 - TFTP server při forenzní analýze

Výpočet kontrolního součtu originálního soboru na směrovači

```
SW1#verify /md5 startup-config
.Done!
verify /md5 (nvram:startup-config) = ab363d0f09cf641acfe55f781b3cf53e


SW1#copy sta
SW1#copy startup-config tf
SW1#copy startup-config tftp:
Address or name of remote host []? 192.168.0.3
Destination filename [sw1-confg]?
!!
1641 bytes copied in 0.025 secs (65640 bytes/sec)
```

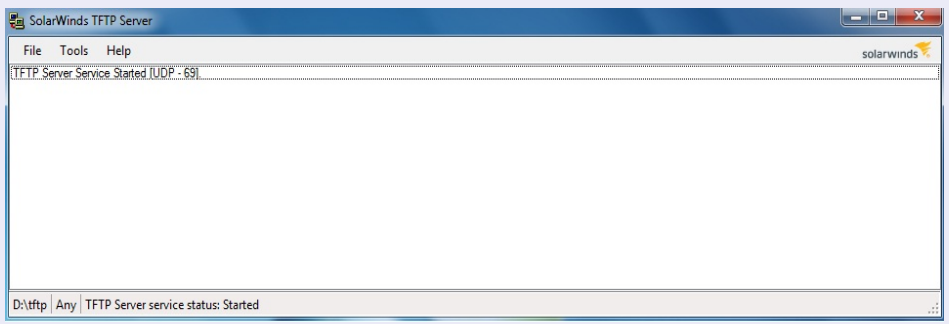
Ověření kontrolního součtu souboru po přenosu na PC znalce



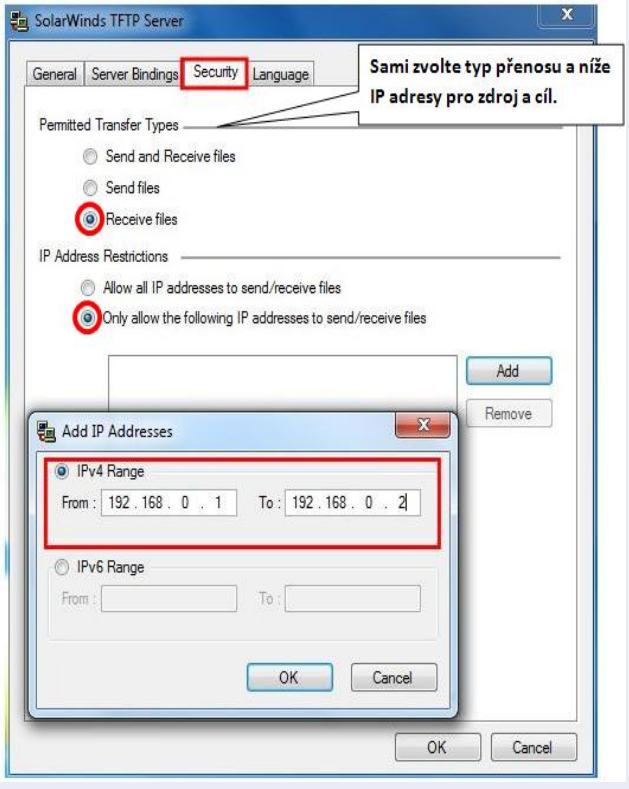
SolarWinds - TFTP server při forenzní analýze

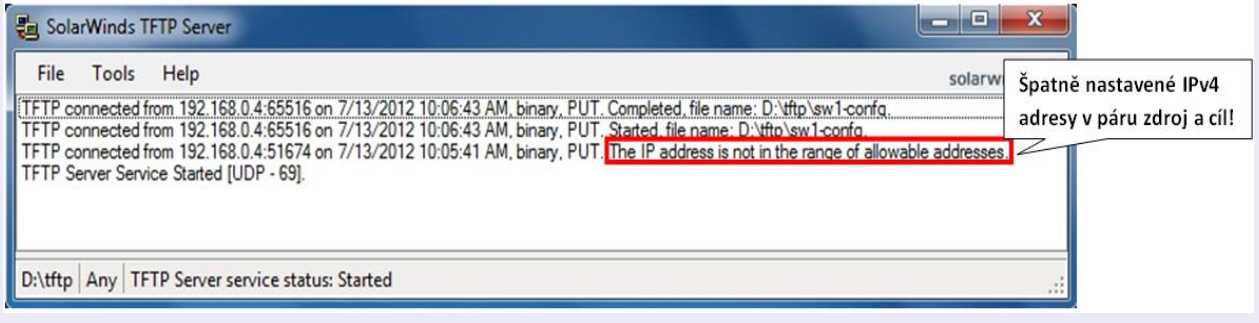
- Zajímavá alternativa vzhledem k předchozímu nástroji.
- Uvolněn pod licencí freeware. Na oficiálních stránkách vyžaduje registraci (http://www.solarwinds.com/downloads/).
- Zvyšuje bezpečnost přenášených dat mezi směrovačem (zdroj) a PC (cil) znalce autorizací IP adres.
- Nepočítá z přenášených souborů kontrolní součet.

SolarWinds TFTP server - nastavení autorizace dvojic.



SolarWinds - TFTP server při forenzní analýze





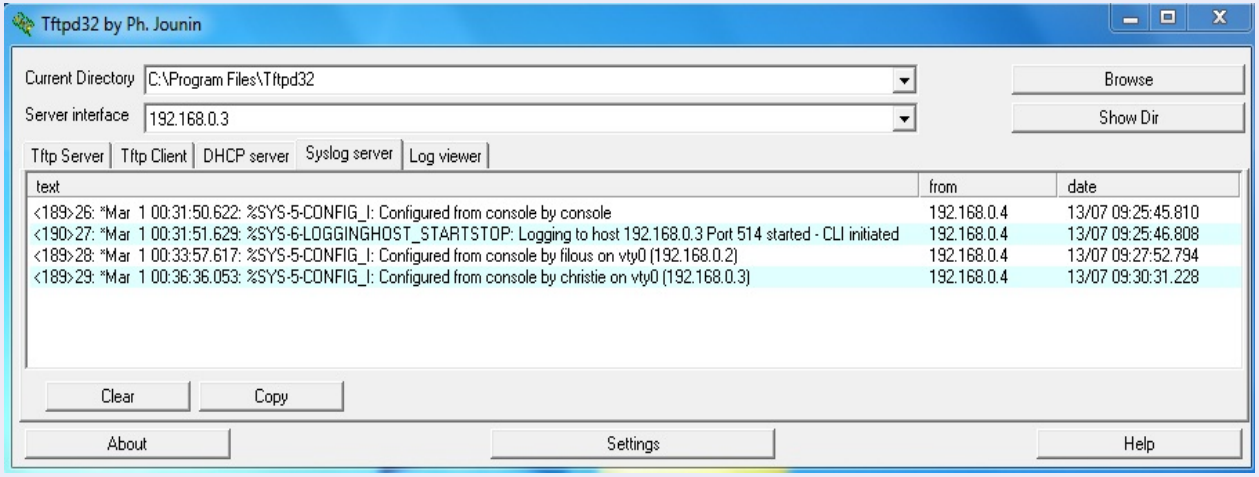
Tftpd32 - Syslog server

Syslog server

- Logy jsou defaultně vypisovány na konzoly, lze nastavit jejich přesměrování do bufferu nebo až na 16 syslog serverů.
- Poskytuje hlavní síťové uložiště pro všechny aktivní prvky.
- Logovány mohou být různé události jako přihlášení (kdo, z jaké IP adresy, datum, čas a kdy se odhlásil), varování o pokusech přihlášení (překročený počet pokusů), konfigurace zařízení, ...
- Lze konfigurovat úroveň 0–7 (nižší číslo značí vyšší důležitost).
- Server syslog zprávy zpracovává a client zprávy generuje (aktivní prvky sítě, servery, ...) a posílá na server.
- Syslog zpráva v sobě obsahuje čas/datum, úrověň závažnosti (0–7) a text.

- Z hlediska forenzní analýzy a bezpečnostní poliky obecně, jsou logy důležitým zdrojem informací. Logy dokumentují i činnost znalce na zařízení.
- Níže můžete vidět základní kroky konfigurace Syslog klienta a použití aplikace Tftpd32 v roli Syslog serveru.

```
Router(config)#logging host <ip_address>
Router(config)#logging trap <0-7>
Router(config)#logging source-interface <typ/port>
Router(config)#logging on
```



FTP server

- FTP server představuje bezpečnější variantu síťového uložiště než je tomu v případě TFTP serveru.
- FTP využívá spolehlivých služeb TCP/20,21
- Na FTP serveru musí být vytvořeny uživatelé.
- V logu na serveru je vidět, který uživatel, z jaké IP adresy, čas/datum se na server připojil, přenesl data a spojení ukončil.
- Nevýhoda oproti TFTP serveru spočívá v nutné dodatečné konfiguraci na zařízení (username/pass pro FTP přenos).
- Autentizace zvyšuje bezpečnost potencionálních důkazů ve fázi sběru dat, kdy jsou data kopírována ze zařízení na server. Pozor, nezapomeňte, že username/heslo i samotný obsah jsou přenášeny v plain textu.
- Není tedy problém komunikace odposlechnout (viz. níže). Existují i zabezpečené verze FTP client/server.

- Můžeme použít např. freeware CesarFTP server.
- Stránky programu: http://www.aclogic.com/index.html.

Zachycení průběhu navázání spojení mezi FTP client/server

No.	Time	Source	Destination	Protocol	Info
48	1.015632s	172.16.0.1	172.16.0.2	TCP	35249 > ftp [SYN] Seq=0 Win=4128 Len=0 MSS=1460
49	0.000060s	172.16.0.2	172.16.0.1	TCP	ftp > 35249 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=14
50	0.085916s	172.16.0.1	172.16.0.2	TCP	35249 > ftp [ACK] Seq=1 Ack=1 Win=4128 Len=0
51	0.001179s	172.16.0.2	172.16.0.1	FTP	Response: 220 CesarFTP 0.99g Server Welcome !
52	0.032008s	172.16.0.1	172.16.0.2	FTP	Request: USER filous
53	0.121056s	172.16.0.2	172.16.0.1	TCP	ftp > 35249 [ACK] Seq=38 Ack=14 Win=17507 Len=0
54	0.302797s	172.16.0.2	172.16.0.1	FTP	Response: 331 User login OK, waiting for password
55	0.009716s	172.16.0.1	172.16.0.2	FTP	Request: PASS cisco
56	0.196294s	172.16.0.2	172.16.0.1	TCP	ftp > 35249 [ACK] Seq=79 Ack=26 Win=17495 Len=0
57	0.297647s	172.16.0.2	172.16.0.1	FTP	Response: 230 User password OK, CesarFTP server ready

Vytvoření uživatele pro FTP na směrovači. Níže příkaz pro kopírování konfiguračního souboru na FTP server

```
Router(config)#ip ftp username <username>
Router(config)#ip ftp password <password>

Router#copy startup-config ftp://<ip_server>
```

Forensic CaseNotes

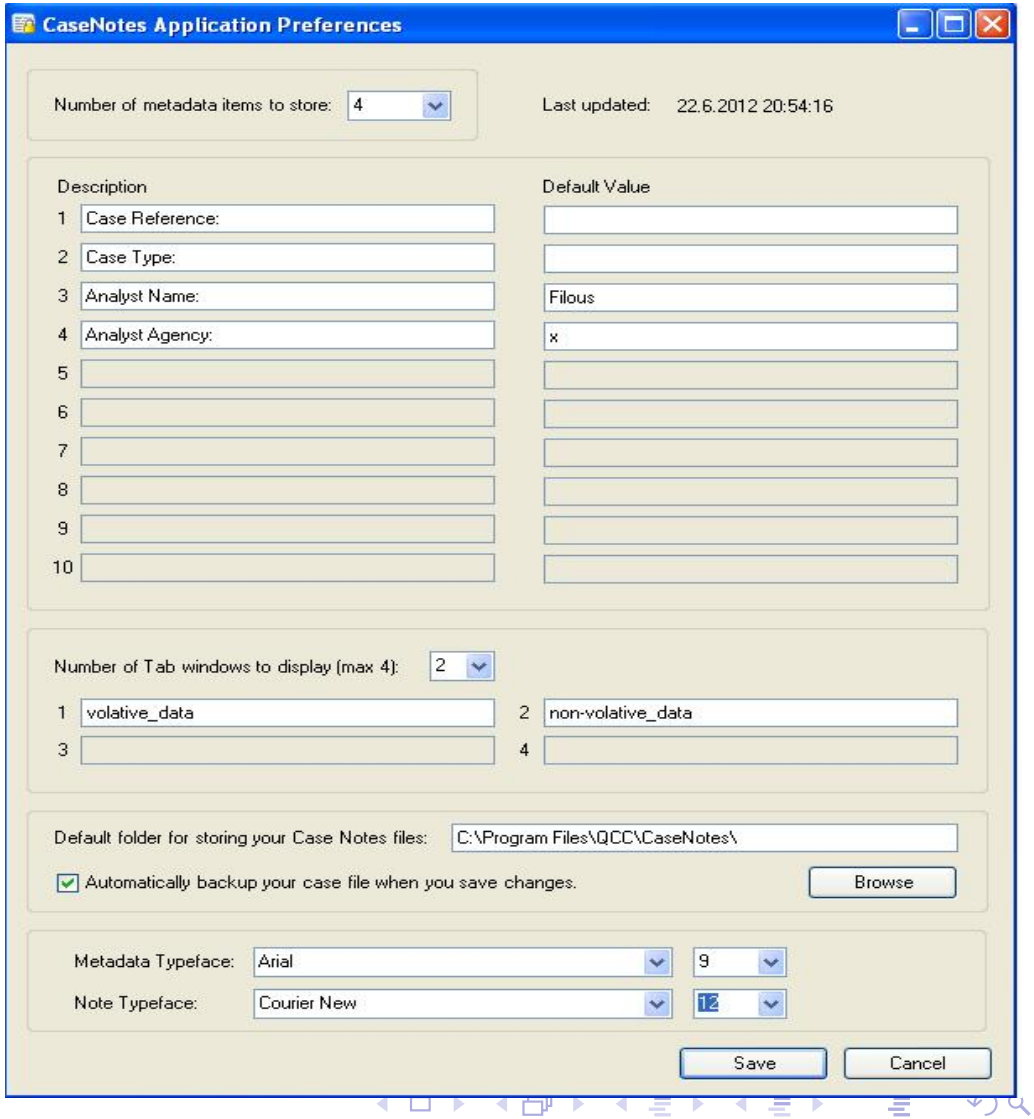
- Stejně, jak je důležité zkoumání je i důležitá dokumentace.
- Prostředky k dokumentaci zmiňuji v následující části .ppt.
- Seznámíme s nástrojem používaným k dokumentaci.

Základní charakteristika nástroje Forensic CaseNotes

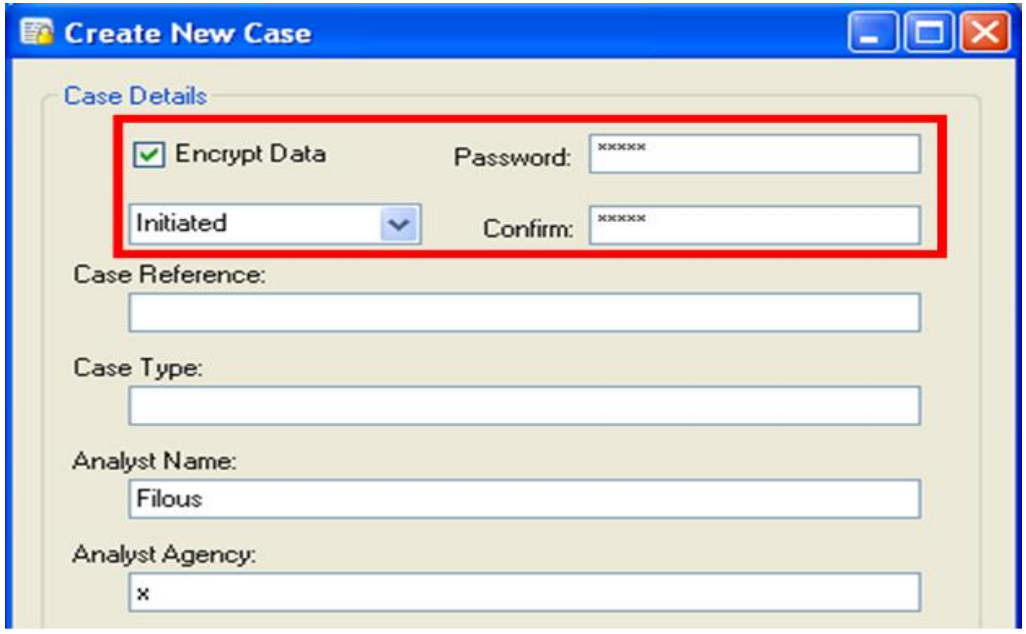
- Informace o nástroji a možnost stažení:
  http://qccis.com/resources/forensic-tools/casenotes-lite/.
- Nástroj je zdarma!
- Při vytvoření nového případu, umožňuje nastavit různá metadata a záložky k případu.
- Všechny vstupy, které vložíte jsou označeny, časem/datumem, kontrolním součtem MD5 (tím se stávají poznámky hodnověrnými a nelze do nich zasahovat).
- Program je podporován OS Windows XP–Windows 7.

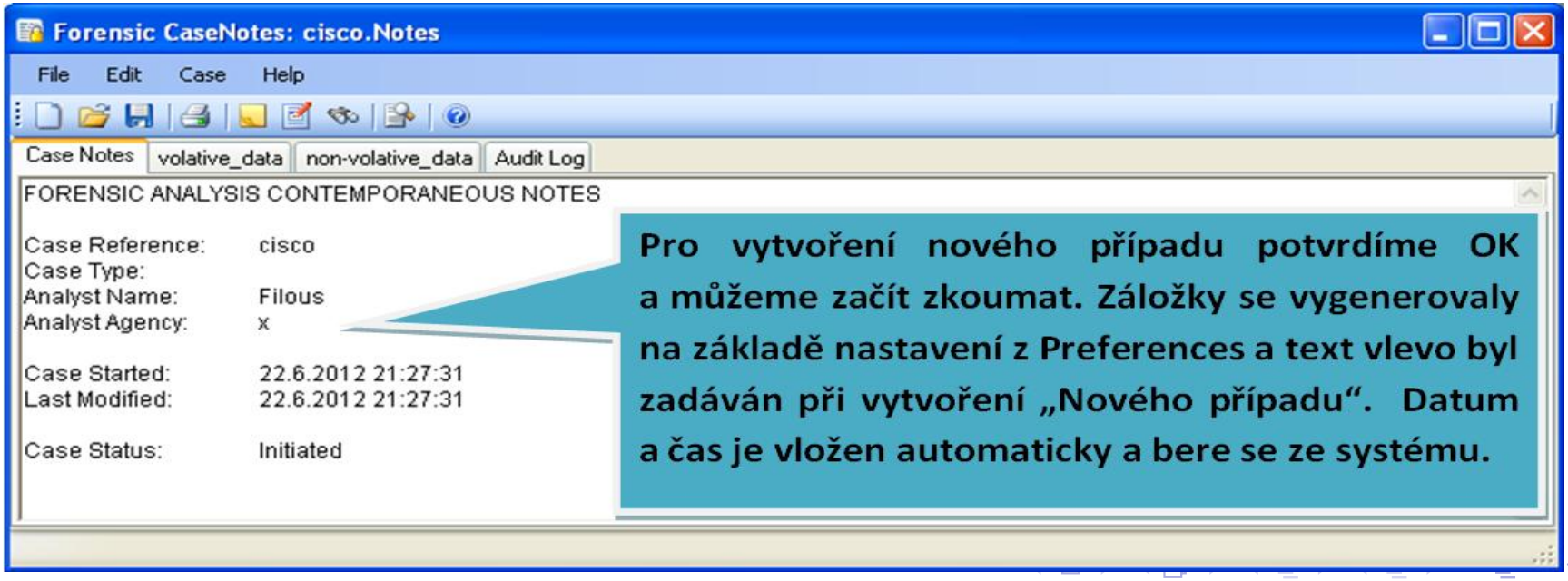
- Umožňuje pracovat na několika případech současně.
- Vytvořenou dokumentaci lze zašifrovat pomocí AES-512bit.

- Nainstalujte a spuste aplikaci.
- Nastavíme vlastností: **Case** → **Preferences**.
- Vyplníme obecné informace, navrhněte si označí záložek v případu (max. 4), místo uložení případu, styl písma.
- Tato konfigurace zůstane po zavření aplikace uložena. Pro jiné případy lze zase upravit.

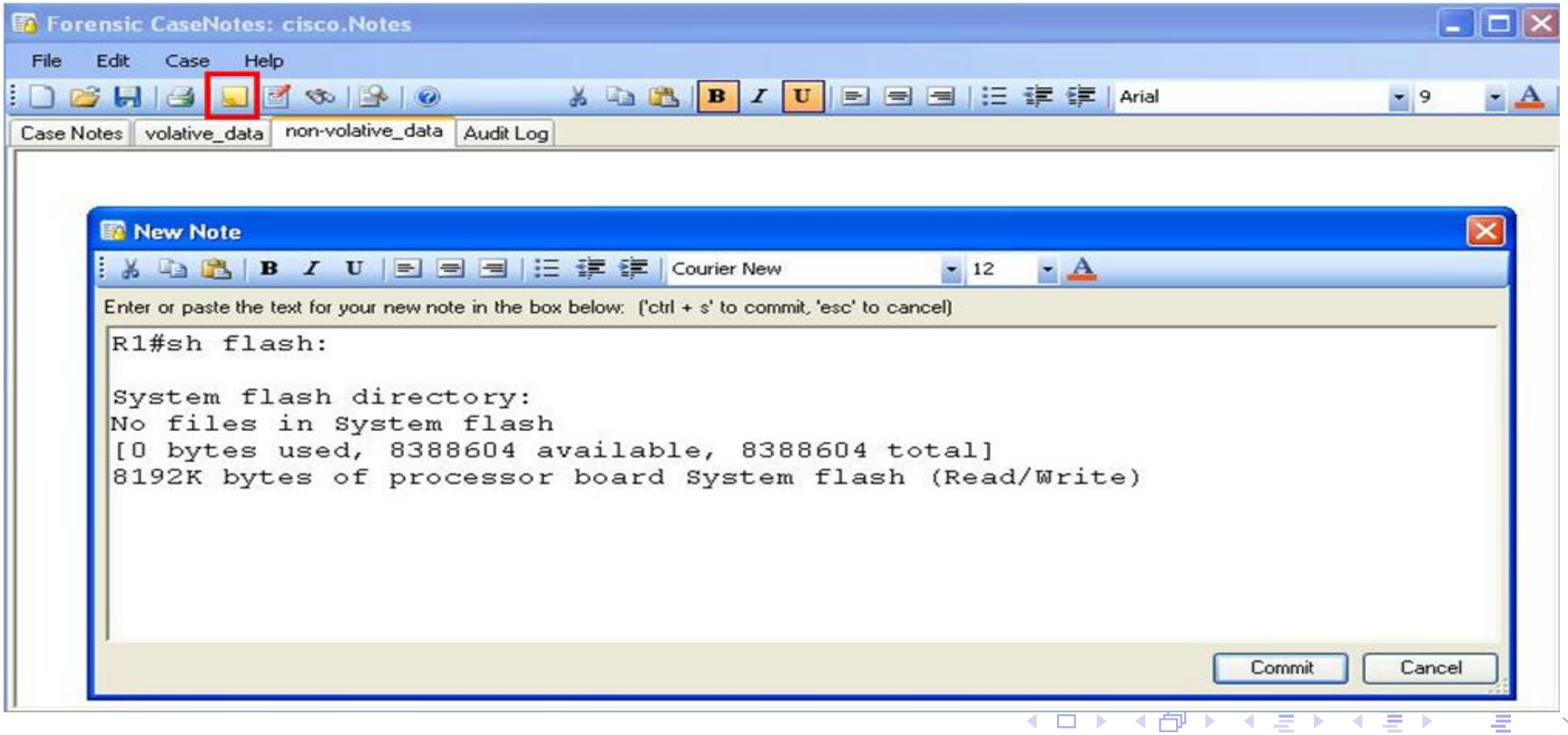


- Před zkoumáním vytvoříme „Nový případ“.
- **File** → **New** (obr. v pravo).
- Pro konkrétní případ můžeme nastavit zabezpečení v podobě šifrování (AES-512).

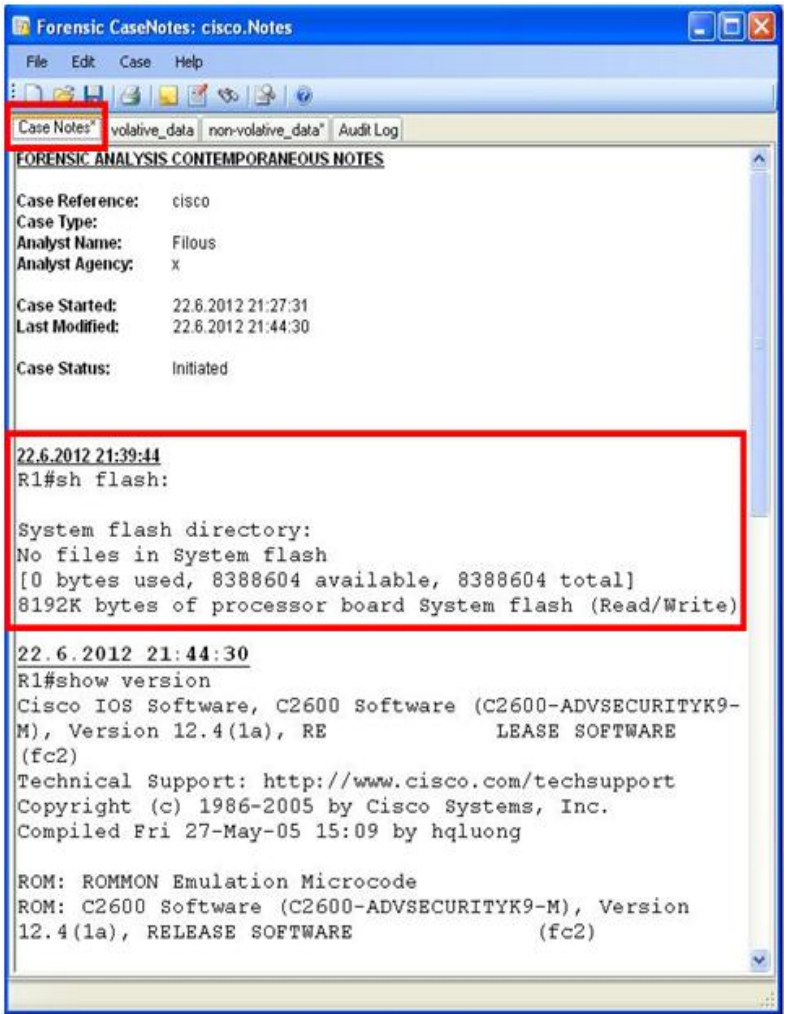


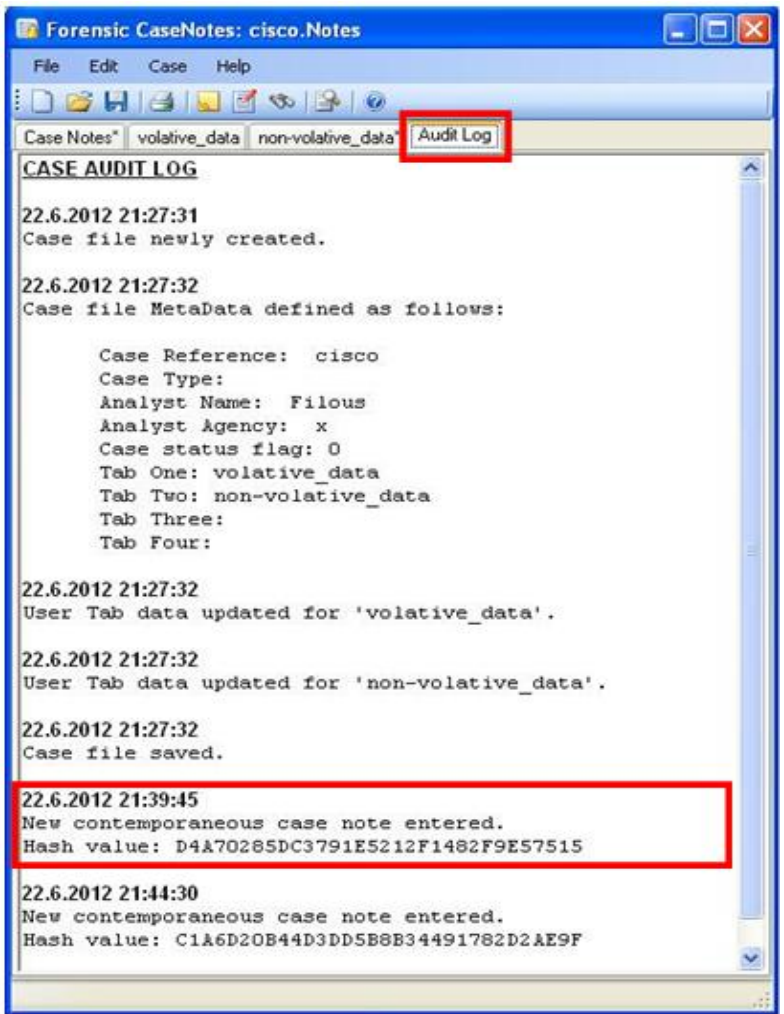


- Na obrázku níže je vidět postup vkládání nového příspěvku. Po kliknutí na „Commit“ již není možné příspěvek editovat.
- Je několik možností, jak vložit nový příspěvek během zkoumání. Použijeme klávesovou zkratku Ctrl + N, v panelu nástrojů klikneme na zvýrazněnou ikonu nebo **Case** → **Add a New Note**.

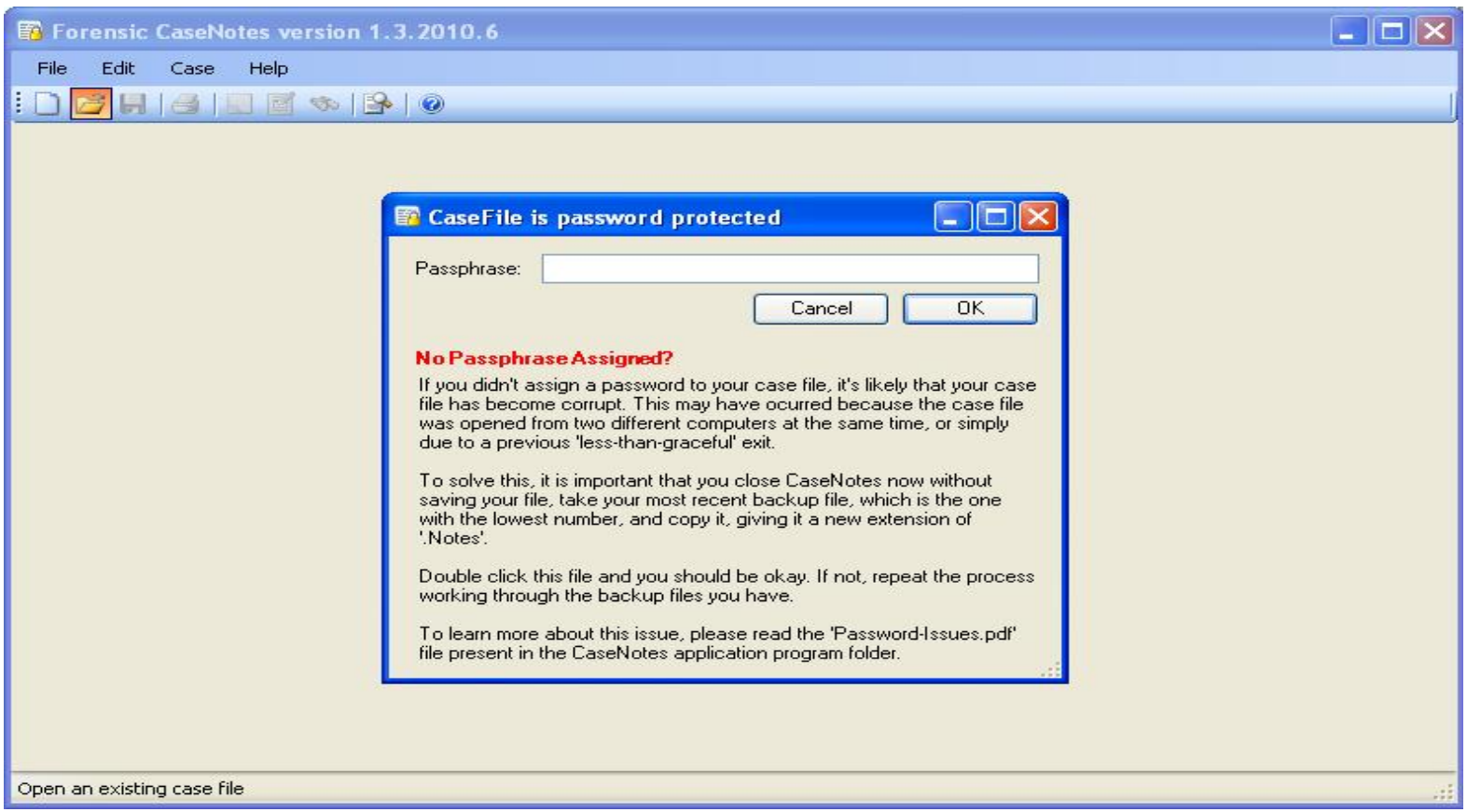


- Porovnejte obsah záložky **Case Notes** na obrázku vlevo a záložky **Audit Log** na obrázku v pravo.
- Vlevo vidíte v rámečku vložený výpis ze směrovače a vpravo vypočtený kontrolní součet k této poznámce.





- Postup pro zavření případu je: **File** → **Close**.
- V případě, že jste při vytváření „Nového případu“ zaškrtli možnost „šifrovat data“ a vyplnili jste heslo pak je nutné Vámi nastavené heslo zadat při otevírání případu (obr. níže).
- .



Integrita dat

- Pokud zvolíte TFTP (FTP) server nepodporující funkci MD5, jsou i jiné způsoby jak na stanice znalce tento kontolní součet pro soubory, diskové oddíly a celé disky provést.
- Live CD určená k forenznímu zkoumání digitálních zařízení obsahují mnoho grafických i textových programů k počítající hash funkce.
- Příklady programů na Forensic Live CD - Gtkhash, md5sum, MD5deep, WinMD5Sum, DHash a mnohé další.
- Další triviální možností je ověřit kontolní součet přímo v příkazové řádce Linuxu.
- Příklad je uveden níže pro hashovací funkci MD5 a SHA-1.

Výpočet kontrolního součtu souboru na PC znalce

```
root# md5sum <cesta/název_souboru>
root# sha1sum <cesta/název_souboru>
```

Děkuji za pozornost!