NÚKIB

# Zajištění dat pro forenzní analýzu

# Obsah

# Pro koho je tento manuál určen

Manuál slouží IT administrátorům jako návod k vytvoření:

- bitové kopie fyzického pevného disku osobního počítače či jednoduchého serveru,
- bitové kopie operační paměti spuštěného fyzického osobního počítače či jednoduchého serveru,
- kopie virtuálního stroje,
- zálohy provozních a síťových logů při podezření na napadení systému.

Z důvodu co nejširšího využití byl zvolen postup s využitím nativních nástrojů OS Windows, free nástroj FTK Imager, Linux a linuxová forenzní distribuce CAINE, ale zkušený uživatel může použít libovolný jiný nástroj (např. jinou linuxovou distribuci, nástroje dcfldd, LiME apod.).
Pro vytváření kontrolního součtu předávaných souborů byl z důvodu rychlosti a širokého použití ve forenzních nástrojích zvolen hashovací algoritmus MD5. Tento kontrolní součet slouží ke kontrole správného přenosu dat.

# Zajištění dat z fyzického stroje

## *Vypnutý stroj*

### Interní úložiště je možné vyjmout

#### Co si předem připravit

Pokud budete předávat celý fyzický stroj nebo úložiště, není třeba nic připravovat předem.
V případě vytváření bitové kopie vyjmutého úložiště si připravte následující:

1. **Externí USB pevný disk** s dostatečně velkou kapacitou (cca 1,5násobek celkové kapacity interních úložišť), datovou propustností (min. USB 3.x) a vhodným souborovým systémem (NTFS, exFAT). Na tento **externí USB pevný disk** budete ukládat zajištěná data k analýze.
2. Software pro vytvoření bitové kopie vnitřního datového úložiště (dále v návodu je
3. popisován postup pomocí **FTK Imager Lite**[1].
4. Nově nainstalovaný technologický počítač s operačním systémem Windows.
5. Odpovídající HW USB redukci k připojení napadeného disku k technologickému počítači (např. adapter SATA2USB).
6. Softwarový blokátor nechtěného zápisu, např. **USB Flash Drives Control**[2].
7. V případě zajišťování bitové kopie šifrovaných úložišť si připravte jejich obnovovací klíče.

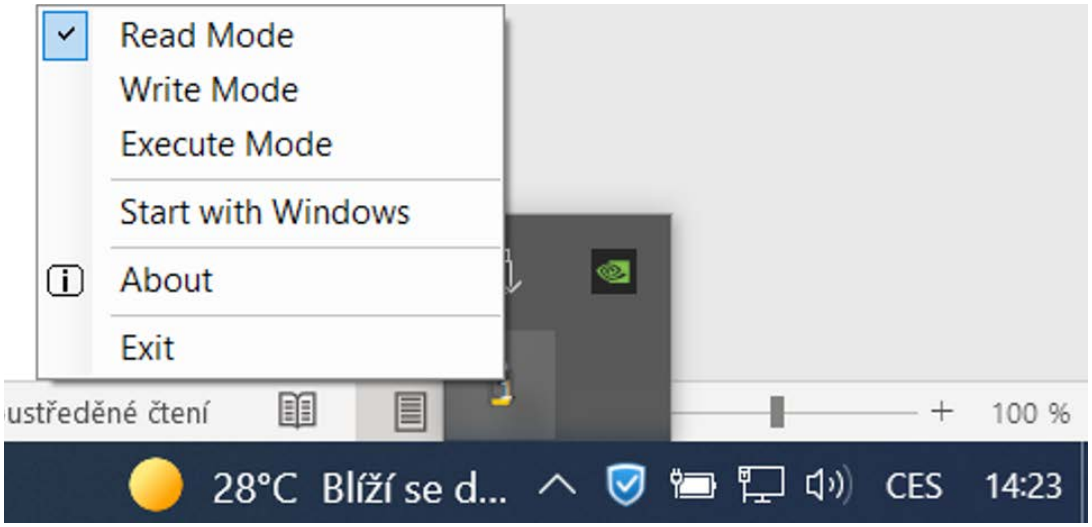
[1] https://www.exterro.com/ftk-imager

[2] https://binisoft.org/usbc.php

## Vlastní postup

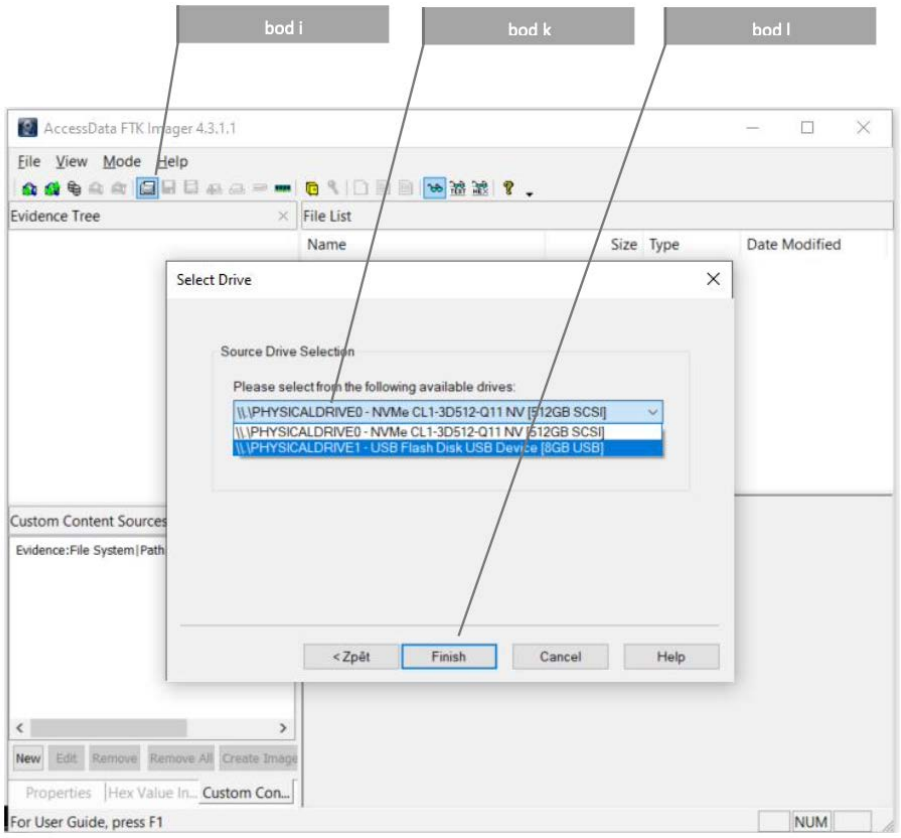
1. Stroj nezapínejte!
2. Vyjměte celé interní úložiště (všechny disky).
3. Kontaktujte pracovníky vládního CERT k dohodnutí předání úložiště (viz poslední stránka tohoto návodu).
4. Pouze pro zkušené uživatele: vytvořte bitovou kopii tohoto úložiště **na externí USB pevný disk** následujícím postupem:

   a. připravte si jiný čistý nebo nově nainstalovaný počítač s OS Windows,
   b. nainstalujte do něj SW **FTK Imager Lite**,
   c. nainstalujte do něj SW **USB Flash Drives Control**,
   d. připojte **externí USB pevný disk** pro uložení zajištěných dat,
   e. vytvořte cílovou složku na **externím USB pevném disku** a správně ji pojmenujte (viz poslední stránka tohoto návodu),
   f. zapněte na stavové liště programu **USB Flash Drives Control** mód Read,

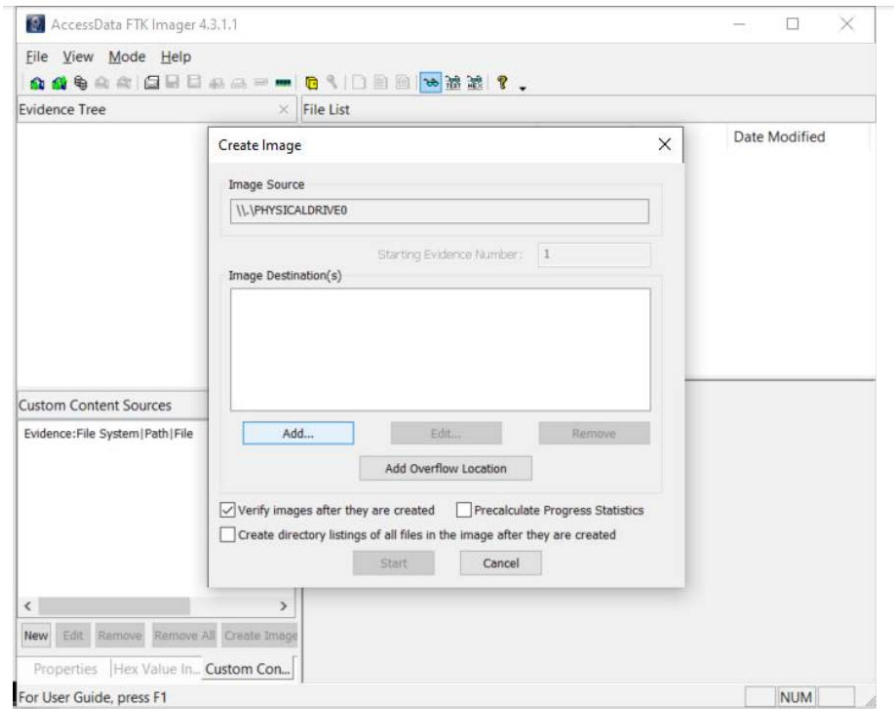



   g. připojte k počítači vyjmuté úložiště přes odpovídající adaptér (nejčastěji SATA2USB),
   h. spusťte program **FTK Imager Lite** s administrátorským oprávněním,
   i. v programu **FTK Imager Lite** vyberte záložku „Create Disk Image“,
   j. jako „Source“ vyberte „Physical Drive“,
   k. vyberte správné zdrojové úložiště (to, ze kterého chceme získat bitovou kopii),

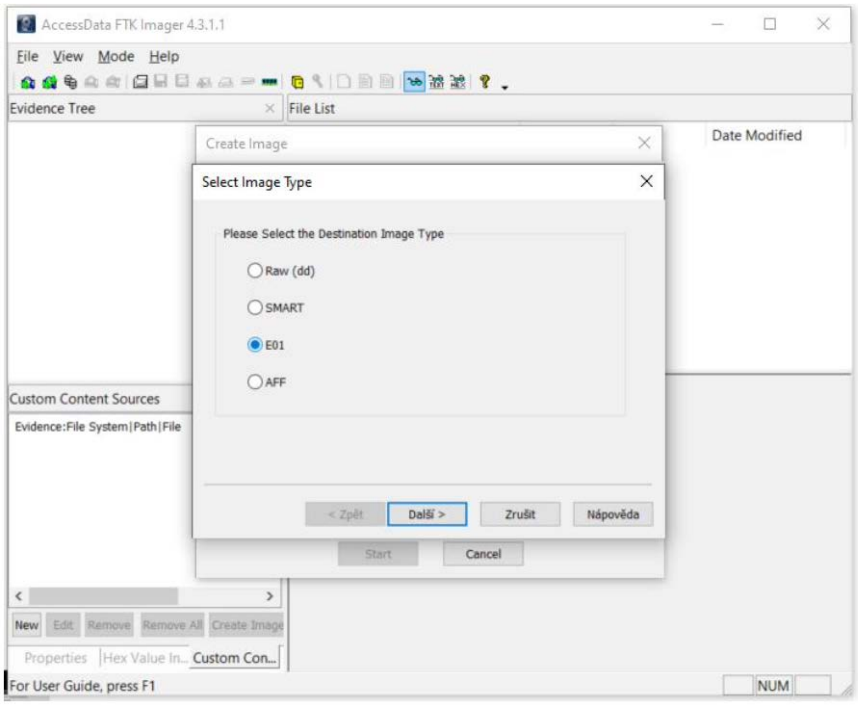
l. stiskněte „Finish“,



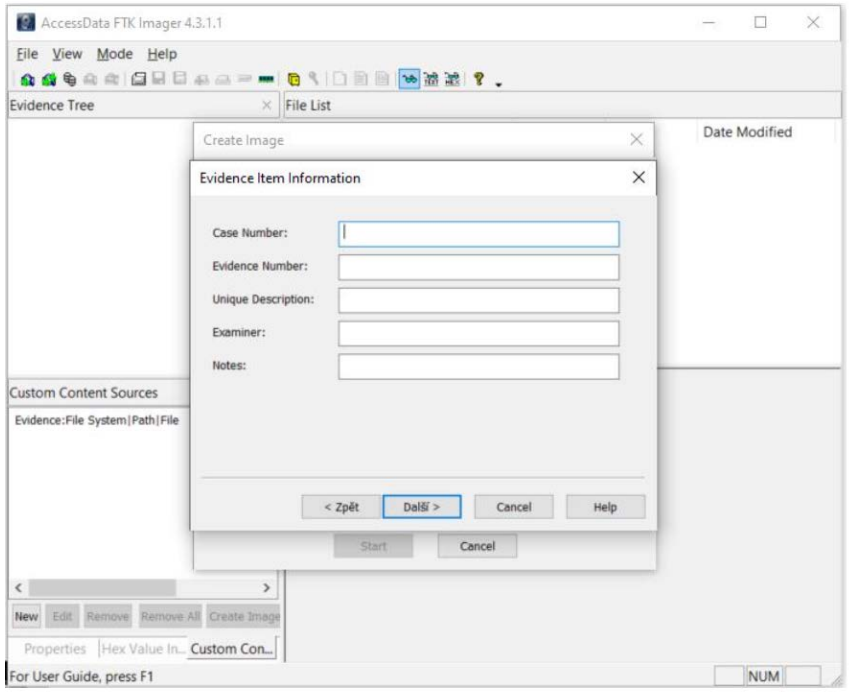

m. v okně „Image Destination(s)“ zvolte tlačítko „Add“,



n. v okně „Select Image Type“ vyberte jako typ „E01“,

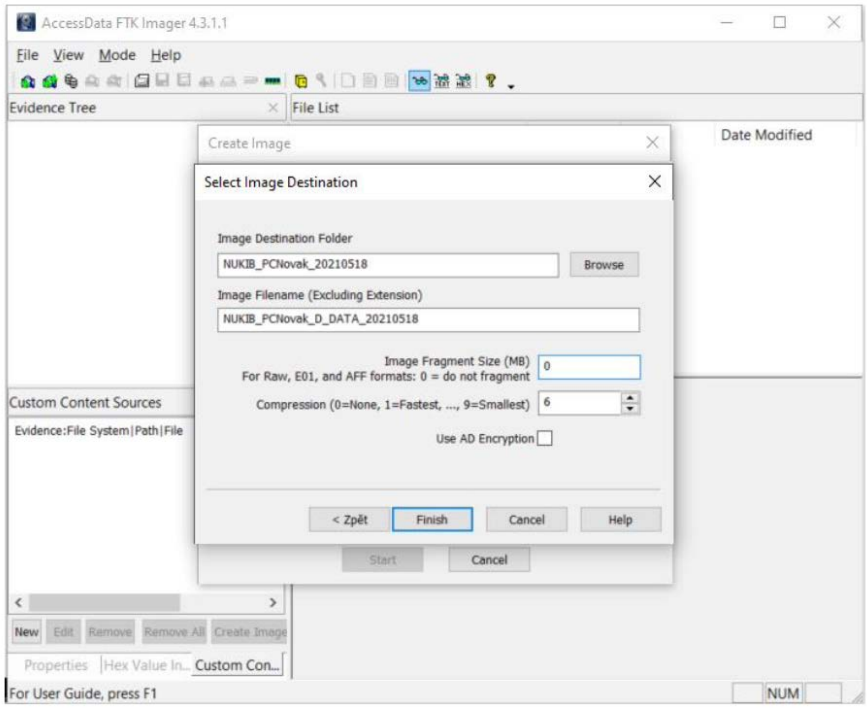



o. vyplňte políčko „Examiner“ v tabulce „Evidence Item Information“ svým jménem, ostatní pole můžete ponechat prázdná,

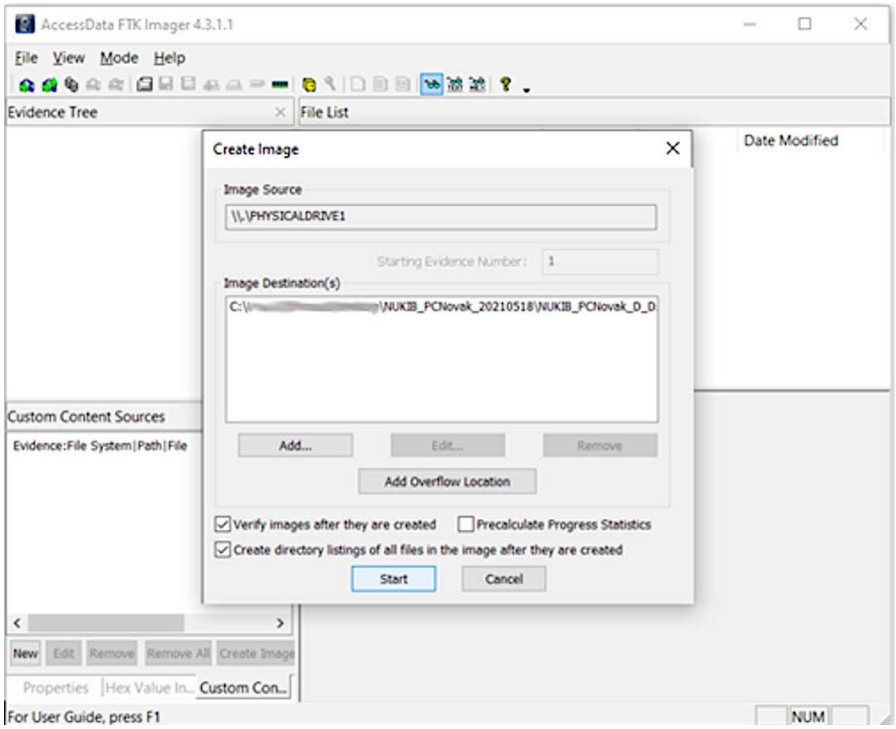


p. v okně „Select Image Destination“ vyberte cílovou složku na externím USB pevném disku a správně pojmenujte název bitové kopie (viz poslední stránka tohoto návodu),

q. v poli „Image Fragment Size“ zvolte 0 (Do Not Fragment) a stiskněte „Finish“,




r. zatrhněte volby „Verify Images…“ a „Create Directory Listings…“ a stiskněte „Start“,




s. body i až r opakujte pro každý zapojený interní disk (např. pro 4 samostatné disky zapojené v RAID poli vytvořte 4 samostatné bitové kopie).

## Interní úložiště není možné vyjmout

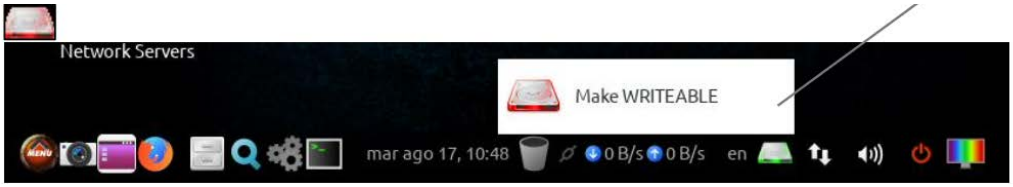
1. Kontaktuje pracovníky vládního CERT k dohodnutí dalšího postupu, nebo
2. Pouze pro zkušené uživatele: vytvořte bitovou kopii tohoto úložiště na **externí USB pevný disk** následujícím postupem:

### Co si předem připravit

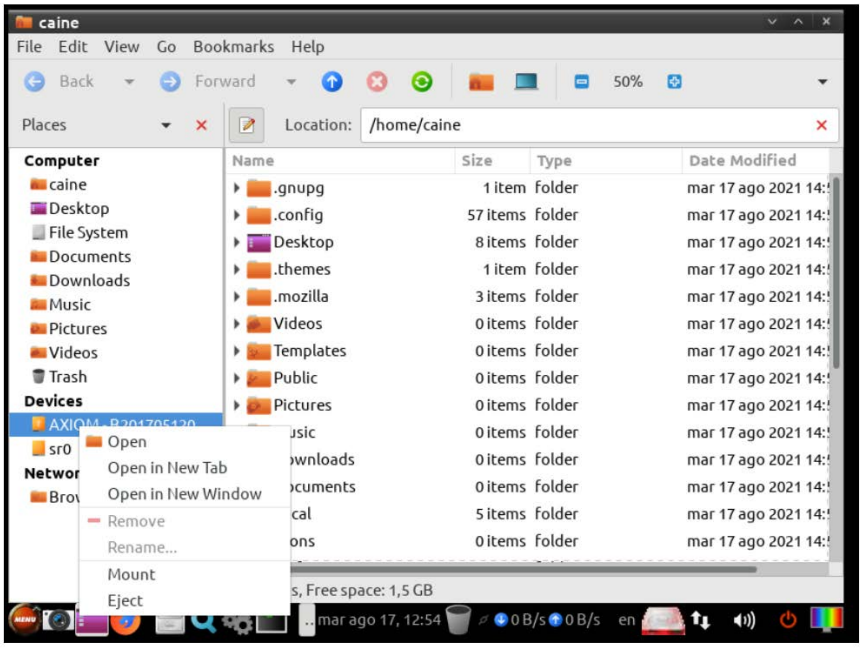
1. **Externí USB pevný disk** s dostatečně velkou kapacitou (cca 1,5násobek celkové kapacity interních úložišť), datovou propustností (min. USB 3.x) a vhodným souborovým systémem (NTFS, exFAT), na tento externí USB pevný disk budete ukládat zajištěná data k analýze.
2. Bootovací LIVE linux distribuci **CAINE**[3] pro forenzní zajištění dat na USB flash disku.
3. V případě zajišťování bitové kopie šifrovaných úložišť si připravte jejich obnovovací klíče.

### Vlastní postup

1. Vložte bootovací CAINE USB flash disk, zapněte počítač a vstupte do BIOSu.
2. V BIOSu zapněte bootování z USB flash disku a vypněte SecureBoot.
3. Nabootujte napadený stroj pomocí LIVE linux distribuce **CAINE**.
4. Přepněte režim na RW (kliknutím pravým tlačítkem na zelenou ikonu, ikona zčervená).



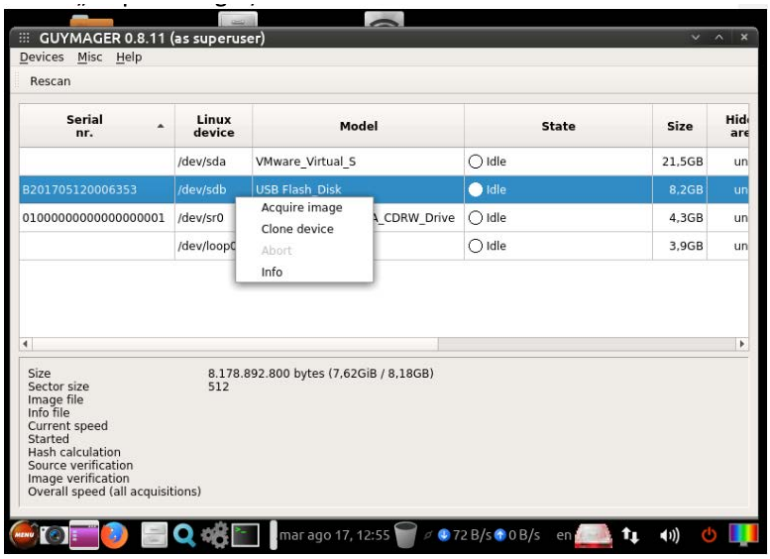

5. Připojte **externí USB pevný disk** v režimu RW.



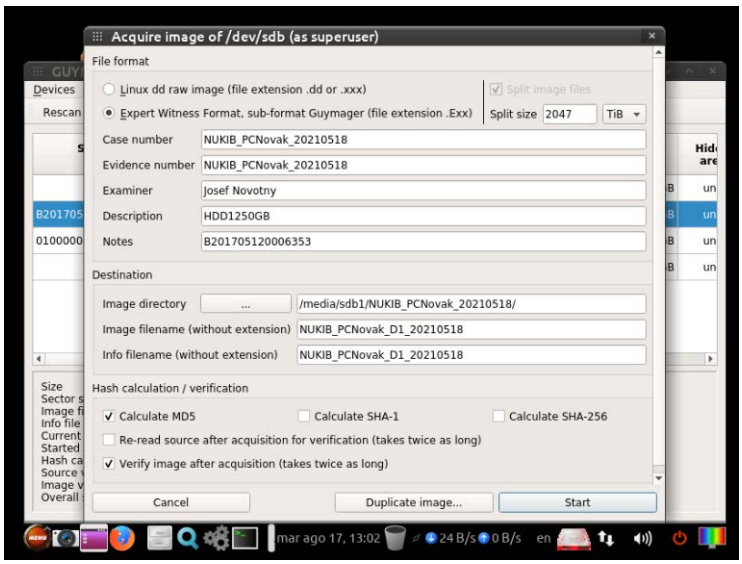

[3] https://www.caine-live.net/

6. Vytvořte cílovou složku na externím USB pevném disku a správně ji pojmenujte (viz poslední stránka tohoto návodu).
7. Spusťte z plochy nástroj **GUYMAGER** a vytvořte bitovou kopii vnitřního úložiště (každý interní disk samostatně) a uložte ji na **externí USB pevný disk** do cílové složky:

   a. zvolte správný zdrojový disk a pravým tlačítkem vyberte volbu „Acquire Image“,




   b. vyplňte tabulku dle následujícího vzoru, do „Split Size“ zadejte hodnotu vyšší, než je objem úložiště tak, aby nedošlo k rozdělení bitové kopie na více částí,




   c. jako „Image Directory“ zvolte vytvořenou cílovou složku na **externím USB pevném disku**,
   d. stiskněte tlačítko „Start“,
   e. body a až c opakujte pro všechny interní fyzické disky.

# *Zapnutý stroj*

## S operačním systémem Windows

### Co si předem připravit

1. **Externí USB pevný disk** s dostatečně velkou kapacitou (cca 1,5násobek celkové kapacity interních úložišť), datovou propustností (min. USB 3.x) a vhodným souborovým systémem (NTFS, exFAT), na tento externí USB pevný disk budete ukládat zajištěná data k analýze.
2. Software pro vytvoření bitové kopie vnitřního datového úložiště a operační paměti **FTK Imager Lite**[4] uložený na **externím USB pevném disku**.
3. Pokud je to možné, odpojte stroj od datové sítě a zajistěte u něj co nejnižší možnou míru ukládání dat na vnitřní úložiště po celou dobu zajišťování dat.

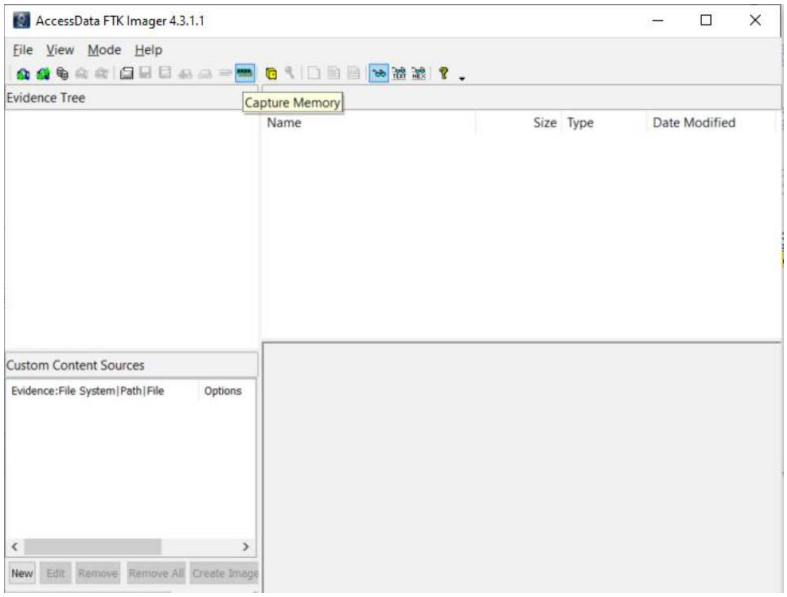
### Vlastní postup

### Zajištění kopie operační paměti

1. Vytvořte cílovou složku na **externím USB pevném disku** a správně ji pojmenujte (viz poslední stránka tohoto návodu),zjistěte verzi OS a build a uložte je do textového souboru do cílové složky, např. pomocí příkazové řádky:

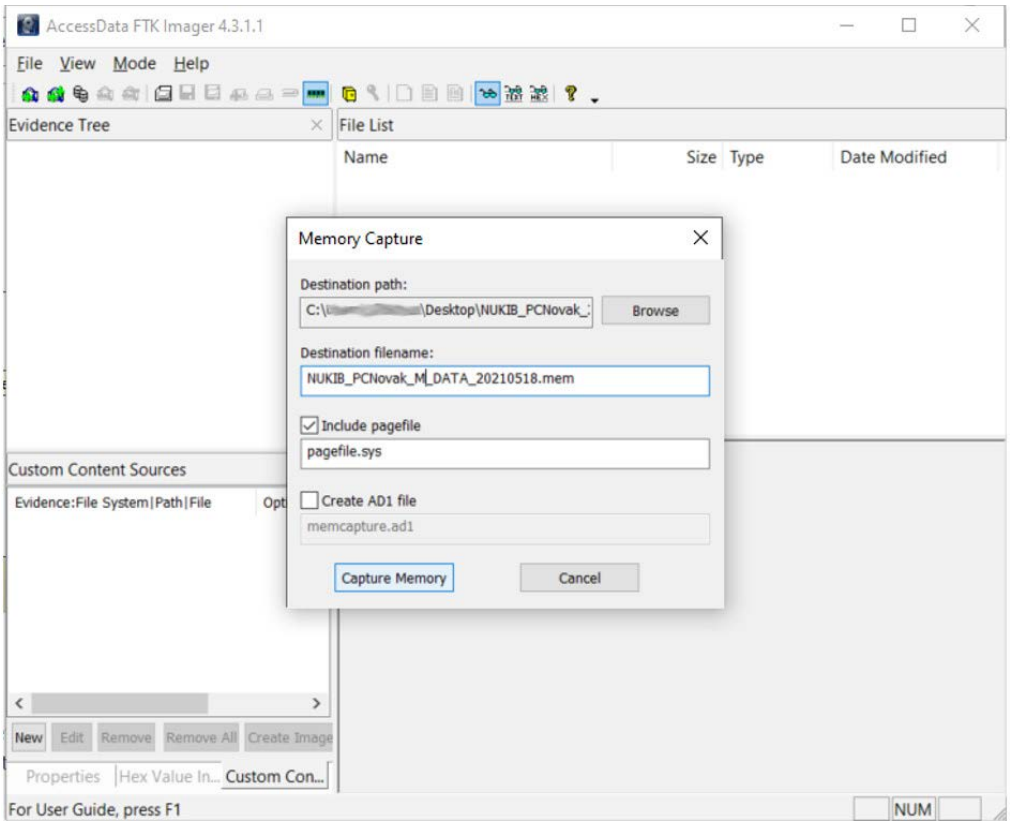
`WIN+R` → `cmd` → nastavte se do cílové složky pomocí příkazu `cd` → `systeminfo > system.txt`

2. Nástroj **FTK Imager Lite** zkopírujte na **externí USB pevný disk** (nikdy nic nekopírujte na interní zajišťované úložiště!) a spusťte ho s administrátorským oprávněním.
3. Zvolte File → Capture Memory.




[4] https://www.exterro.com/ftk-imager

4. Jako cílovou složku zvolte složku na **externím USB pevném disku.**
5. Jako „filename“ správně pojmenujte název bitové kopie (viz poslední stránka tohoto návodu).
6. Zaškrtněte políčko „Include pagefile“.




7. Vytvořte bitovou kopii operační paměti stisknutím tlačítka „Capture Memory“.
8. Vytvořte kontrolní sumu typu MD5 pro vytvořený soubor a uložte ho do textového souboru suma[X[5]].md5 do cílové složky - v OS Windows např. v příkazovém řádku příkazem:

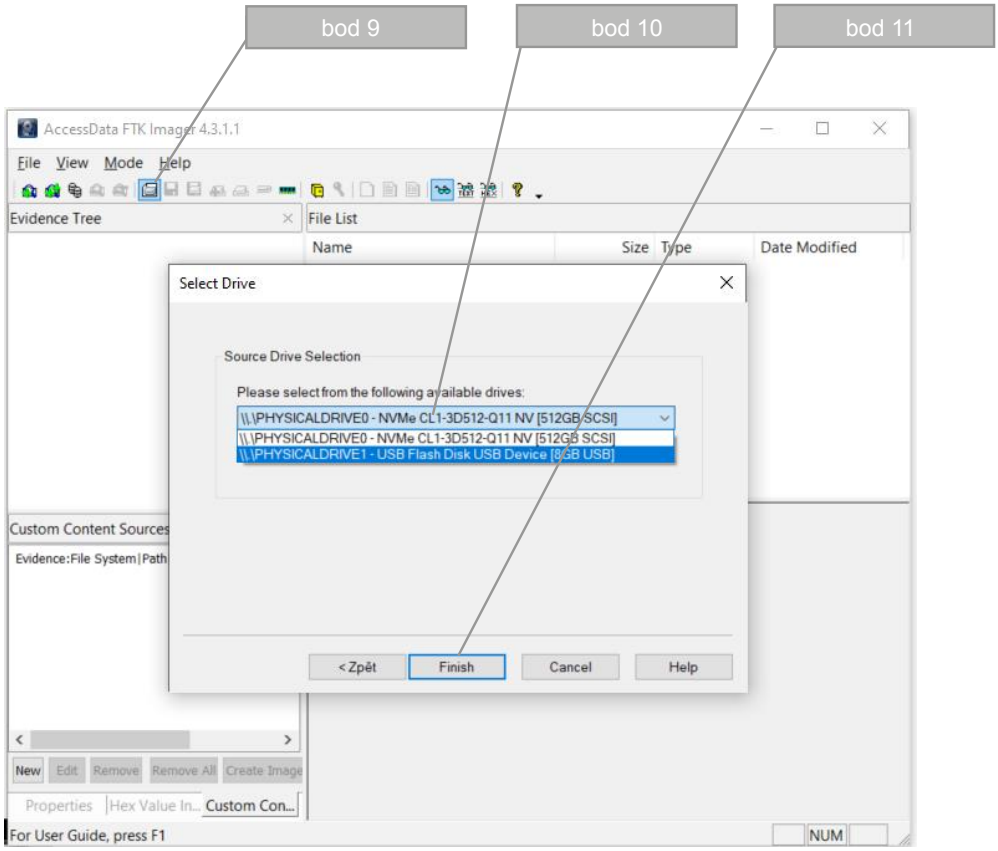
```
certutil -hashfile NUKIB_PCNovak_M_DATA_20210518.mem MD5 >
sumaNUKIB_PCNovak_M_DATA_20210518.md5
```

## Zajištění bitové kopie interního úložiště:

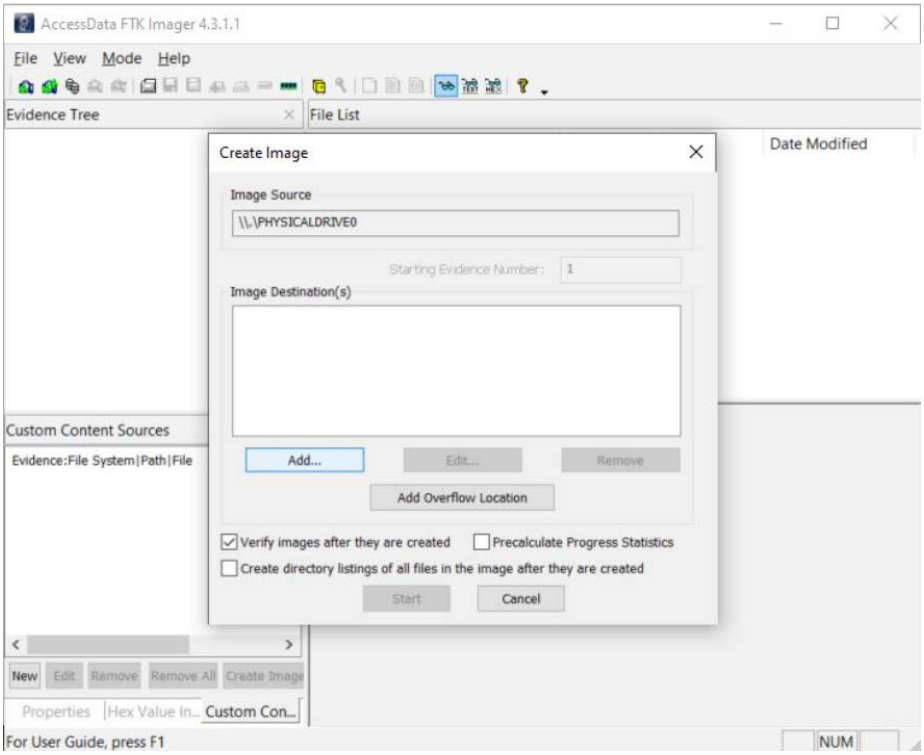
9. V programu FTK Imager Lite vyberte záložku „Create Disk Image“, jako „Source“ vyberte „Physical Drive“, v případě zajišťování dat z RAID nebo LVM polí vyberte „Logical Drive“.
10. Vyberte správné interní úložiště (to, ze kterého chceme získat bitovou kopii).

[5] X nahraďte odpovídajícím názvem kopie operační paměti či pevného disku

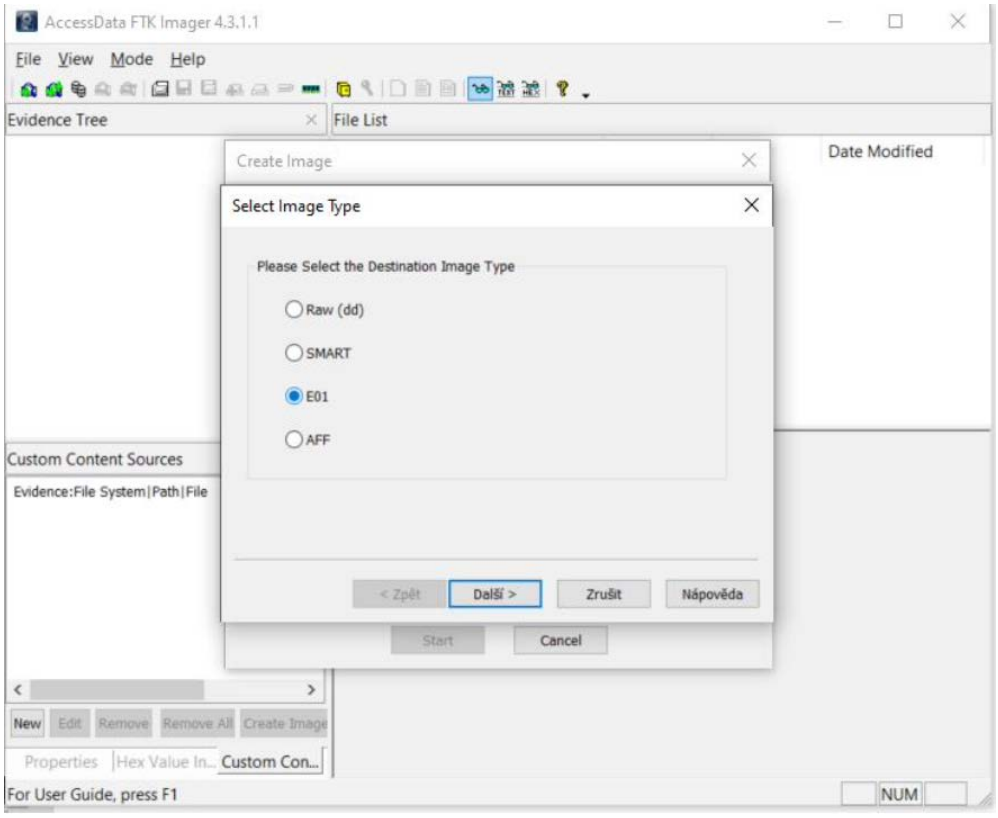
11. Stiskněte „Finish“.



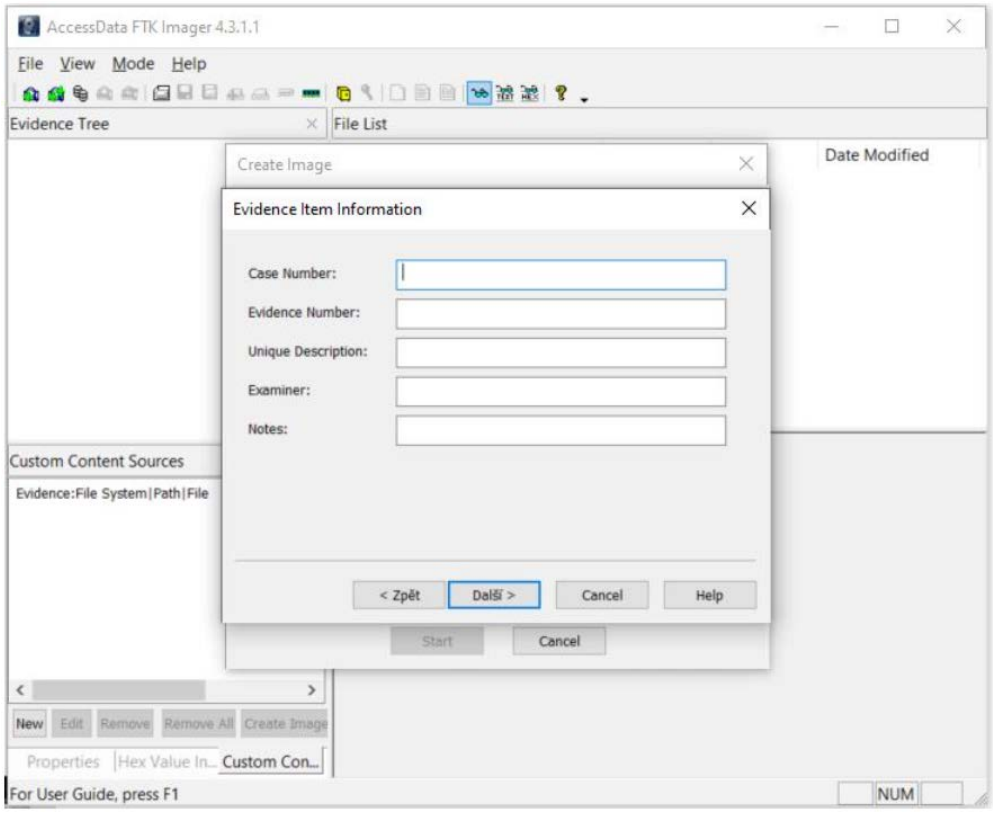

12. V okně „Image Destination(s)“ zvolte tlačítko „Add“.



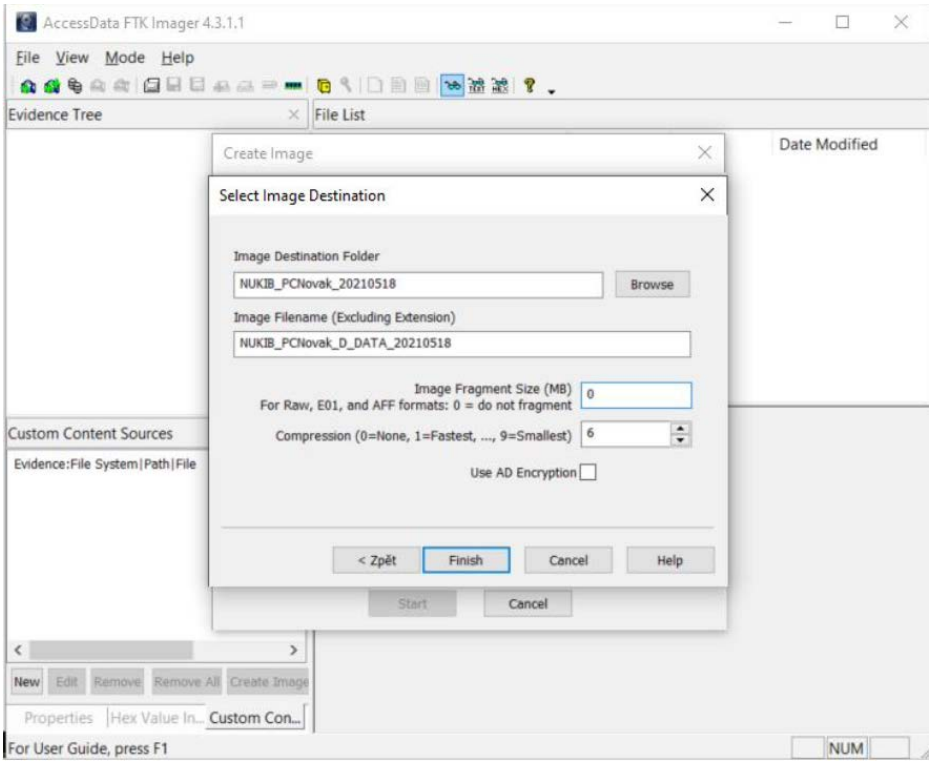
13. V okně „Select Image Type“ vyberte jako typ „E01“.



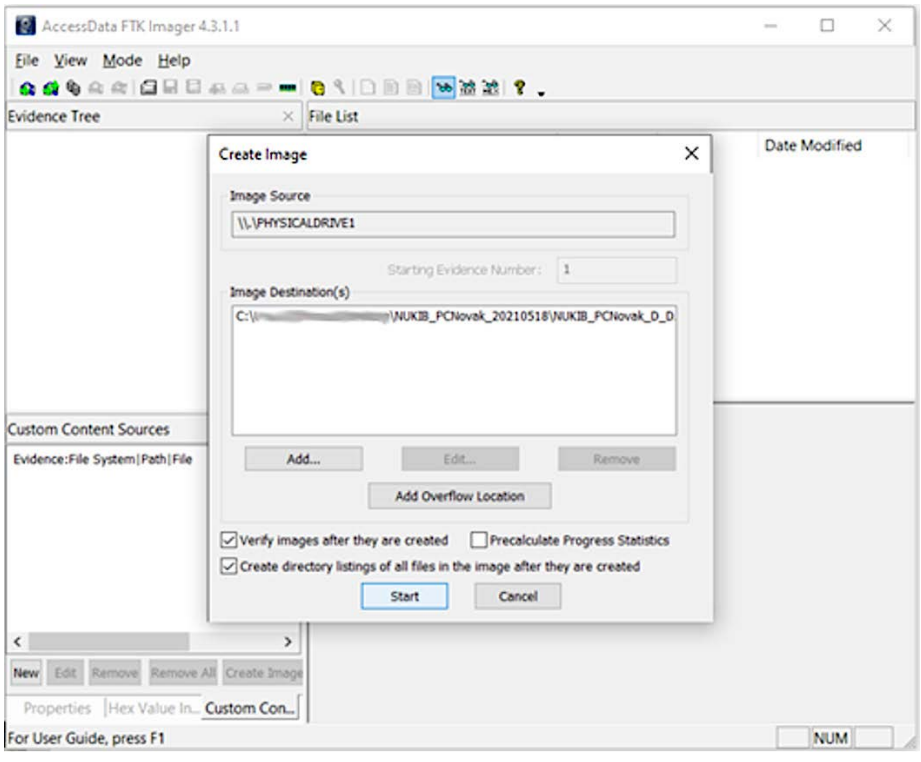

14. Vyplňte pole „Examiner“ v tabulce „Evidence Item Information“ svým jménem, ostatní pole můžete ponechat prázdná.



15. V okně „Select Image Destination“ vyberte cílovou složku na externím USB pevném disku a správně pojmenujte název bitové kopie (viz poslední stránka tohoto návodu).
16. V poli „Image Fragment Size“ zvolte 0 (Do Not Fragment), pole „Compression“ ponechte v defaultním stavu a stiskněte „Finish“.




17. Zatrhněte volby „Verify images after they are created“ a „Create directory listings…“ a stiskněte tlačítko „Start“.



18. Body 9 až 18 opakujte pro každý zapojený interní disk (neplatí pro zajišťování dat z logických jednotek viz bod 11).

## *S operačním systémem Linux*

### Co si předem připravit

1. **Externí USB pevný disk** s dostatečně velkou kapacitou (cca 1,5násobek celkové kapacity interních úložišť), datovou propustností (min. USB 3.x) a vhodným souborovým systémem (NTFS, exFAT). Na tomto **externím USB pevném disku** budete předávat zajištěná data k analýze.
2. Software pro vytvoření bitové kopie operační paměti – portable nástroj **AVML for Linux**[6].
3. Pokud je to možné, odpojte stroj od datové sítě a zajistěte u něj co nejnižší možnou míru ukládání dat na vnitřní úložiště po celou dobu zajišťování dat.

### Vlastní postup

### Zajištění kopie operační paměti

Pro podporované distribuce[7] použijte nástroj **Microsoft AVML** for Linux, pro ostatní nástroj LiME[8].

1. Připojte externí **USB pevný disk** v režimu RW.
2. Spusťte příkazovou řádku.
3. Přesuňte se na root **externího USB pevného disku**.
4. Vytvořte v kořenovém adresáři na externím USB pevném disku složku AVML např.
   `mkdir AVML`
5. Přepněte se do této složky, např. cd AVML.
6. Z https://github.com/microsoft/avml stáhněte z nejnovějšího vydání (release) soubor s názvem avml a uložte ho do složky AVML na **externím USB pevném disku**.
7. Příkazem `sudo chmod 755 avml` změňte oprávnění k tomuto souboru.
8. Přesuňte se na root externího USB pevného disku.
9. Vytvořte cílovou složku na **externím USB pevném disku** a správně ji pojmenujte (viz poslední stránka tohoto návodu), např.
   `mkdir NUKIB_PCNovak_20210518`
10. Přesuňte se do nově vytvořené složky.
11. Zjistěte verzi distra a uložte ji do textového souboru do cílové složky, např.
    `cat /etc/*-release > distro.txt`
12. Zjistěte verzi Kernel a uložte ji do textové souboru do cílové složky, např.
    `uname -r > kernel.txt`

[6] https://github.com/microsoft/avml

[7] https://github.com/microsoft/avml/blob/main/README.md

[8] https://github.com/504ensicsLabs/Lime

13. Příkazem `sudo ../AVML/avml xxx.dmp`
    vytvořte na externím USB pevném disku v cílové složce soubor xxx.dmp s bitovou kopií operační paměti, kdy místo xxx dosaďte správný název (viz poslední stránka tohoto návodu), např. `sudo ../AVML/avml NUKIB_PCNovak_M_20210518.dmp`
14. Vytvořte kontrolní sumu typu MD5 pro vytvořený dmp soubor a uložte ji do textového souboru suma[X[5]].md5 do cílové složky, např.
    `md5sum NUKIB_PCNovak_M_20210518.dmp > sumaNUKIB_PCNovak_M_20210518.md5`

## Zajištění bitové kopie interního úložiště

15. Zjistěte informace o interním úložišti, např.
    `sudo fdisk -lu`
    a vyberte správný disk, v případě zajišťování dat z RAID nebo LVM polí vyberte správnou logickou jednotku,
16. Vytvořte bitovou kopii interního úložiště pomocí nativního nástroje dd a uložte ji do odpovídající cílové složky pod odpovídajícím jménem (viz poslední stránka tohoto návodu), např.
    `sudo dd if=/dev/sdx of=NUKIB_PCNovak_D1_20210518.dd conv=sync,noerror status=progress`
    kdy x nahraďte odpovídajícím označením zdrojového disku nebo logické jednotky,
17. Vytvořte kontrolní sumu typu MD5 pro vytvořený dd soubor a uložte ji do textového souboru suma[X[5]].md5 do cílové složky, např.
    `md5sum NUKIB_PCNovak_D1_20210518.dd > sumaNUKIB_PCNovak_D1_20210518.md5`
18. Body 14 až 16 opakujte pro každý zapojený interní disk (neplatí pro zajišťování dat z logických jednotek viz bod 15).

# Zajištění dat z virtuálního stroje

## *Vypnutý virtuální stroj*

### Co si předem připravit

1. **Externí USB pevný disk** s dostatečně velkou kapacitou (cca 1,5násobek celkové kapacity interních úložišť), datovou propustností (min. USB 3.x) a vhodným souborovým systémem (NTFS, exFAT), na tento **externí USB pevný disk** budete ukládat zajištěná data k analýze.
2. V případě šifrovaných úložišť si připravte jejich obnovovací klíče.

### Vlastní postup

1. Připojte **externí USB pevný disk** k hostitelskému počítači.
2. Vytvořte cílovou složku na **externím USB pevném disku** a správně ji pojmenujte (viz poslední stránka tohoto návodu).
3. Zabalte celou složku s virtuálním strojem (ujistěte se, že obsahuje kopii interního virtuálního disku) do jednoho zip archívu se správným názvem stroje (viz poslední stránka tohoto návodu) do cílové složky.
4. Vytvořte kontrolní součet typu MD5 vytvořeného zip archívu a uložte ho do textového souboru suma[X[5]].md5 na externí USB pevný disk do cílové složky v OS Windows např. v příkazovém řádku příkazem

```
certutil -hashfile sumaNUKIB_PCNovak_V_20210518. zip MD5 > sumaNUKIB_PCNovak_V_20210518.zip.md5
```

## *Zapnutý virtuální stroj*

### Co si předem připravit

1. **Externí USB pevný disk** s dostatečně velkou kapacitou (cca 1,5násobek celkové kapacity interních úložišť), datovou propustností (min. USB 3.x) a vhodným souborovým systémem (NTFS, exFAT), na tomto **externím USB pevném disku** budete předávat zajištěná data k analýze.
2. V případě šifrovaných úložišť si připravte jejich obnovovací klíče.

### Vlastní postup

1. Připojte **externí USB pevný disk** k hostitelskému počítači.
2. Vytvořte cílovou složku na **externím USB pevném disku** a správně ji pojmenujte (viz poslední stránka tohoto návodu).
3. Zvolte volbu Suspend a zabalte celou složku se suspended virtuálním strojem do jednoho zip archívu do cílové složky.

Pokud nelze virtuální stroj suspendovat, pak:

4. Vytvořte klon běžícího virtuálního stroje, u tohoto klonu zvolte volbu Suspend a zabalte celou složku se suspended virtuálním strojem do jednoho zip archívu do cílové složky.
5. Ujistěte se o zkopírování souboru s virtuální pamětí RAM a souboru s kopií interního virtuálního disku.
6. Zip archívu správně pojmenujte (viz poslední stránka tohoto návodu).
7. Vytvořte kontrolní součet typu MD5 vytvořeného zip archívu a uložte ho do textového. souboru suma[X[5]].md5 na **externí USB pevný disk** do cílové složky - v OS Windows např. v příkazovém řádku příkazem

   ```
   certutil -hashfile NUKIB_PCNovak_V_20210518.zip MD5 >
   sumaNUKIB_PCNovak_V_20210518.zip.md5
   ```

Pokud nejde virtuální stroj ani suspendovat, ani klonovat, pak postupujte obdobně jako u běžícího fyzického stroje.

# Zajištění dat z mobilních telefonů

## Vlastní postup

Zajištění dat z mobilních telefonů je vysoce specializovaná činnost, která se vymyká možnostem běžných IT administrátorů.

Z tohoto důvodu musí zajišťování provádět pracovník vládního CERTu a z vaší strany je pouze požadováno:

1. Telefon uvést do režimu Letadlo a vypnout.
2. Vyjmout SIM kartu (tu není potřeba předávat a je možné ji dále používat v jiném telefonu).
3. Telefon ve vypnutém stavu plně nabít.
4. Vypnutý telefon uložit do ochranného přepravního obalu, např. bublinkové obálky. Přístupové údaje – PIN, gesto, heslo – zašlete bezpečným způsobem (např. šifrovaně na kontaktní e-mailovou adresu uvedenou na poslední stránce).

Ve výjimečných případech mohou pracovníci vládního CERTu provést zajištění dat na místě, je ale třeba počítat s několikahodinovou akvizicí.

# Zajištění síťových logů

Síťové logy většinou slouží jako podpůrný zdroj informací o proběhlém útoku/kompromitaci, případně jako záznam o neúspěšném pokusu o útok. Vychází se z předpokladu, že tyto logy nejsou zasaženy proběhlým útokem a jde tedy o nezávislou evidenci (na rozdíl od logů přímo z kompromitované stanice, které mohly být útočníkem pozměněny). Obvykle slouží jako doplňková data k zajištěnému obrazu disku/paměti napadeného stroje, které nám pomáhají udělat si komplexní představu o incidentu, potvrdit nebo vyvrátit pracovní hypotézy, doplnit detaily o proběhlé komunikaci (trvání, objem přenesených dat) a prověřit rozsah napadení.

Vzhledem k rozmanitosti používaných technologií a množství výrobců neexistuje univerzální definice potřebných záznamů ani jednotný postup, jak je vyexportovat. Budeme zde tedy popisovat spíše rozsah potřebných informací a obecné principy.

Nejčastěji jde o **přístupové záznamy** z dané serverové aplikace nebo předřazených systémů (proxy, WAF) nebo o **síťová data** ze síťových zařízení a síťové sondy (záznam PCAP, netflow a podobně).

Dle charakteru incidentu jsou potřeba některé z následujících typů logů:

## Přístupové záznamy:

- access.log + error.log z webserveru (pokud byl kompromitován samotný server, pak jsou relevantní pouze záznamy z nezávislého log-management systému!),
- WAF logy, PROXY logy, LoadBalancer logy apod. (tedy logy předřazených nástrojů, kterými komunikace pouze prošla),
- VPN logy,
- přístupové záznamy z e-mailového serveru,
- RDP, SSH autentizační logy,
- Citrix, VMware Horizon přístupové logy,
- a další obdobné typy dat.

## Síťová data:

- logy zachycující průběh komunikace přes vaši síťovou infrastrukturu, např:
  - data o proběhlé datové komunikaci
    - sFlow/NetFlow záznamy,
    - IPFIX data (pokud jsou k dispozici tak včetně L7 detailů),
    - logy z jiného network monitoring nástroje (flow-like logy i další),
    - PCAP v případě FPC monitoringu (často značný objem!),
    - pokud nedisponujete vlastním síťovým monitoringem, můžete se obrátit na vašeho ISP (obvykle flow záznamy uchovává) a požádat o export těchto dat. Současně jej prosím požádejte o poskytnutí součinnosti pro NÚKIB pro případné dotazy,

    - detekované události z vaší IDS/IPS sondy,
    - logy proběhlých i zahozených spojení z firewallu apod.,
    - DNS logy,
- podpůrné logy sloužící pro identifikaci komunikujících stran:
    - DHCP logy (pokud je využito).

I když tento výčet není úplný, přesto by měl pokrývat alespoň běžně se vyskytující zdroje síťových logů, na které byste rozhodně neměli zapomenout.

## Vlastní postup

- Provést export logů/dat pokrývající veškerou komunikaci za dané období (neomezovat se jen na jediný identifikovaný zdroj/cíl).
- Pro prvotní zevrubnou analýzu obecně preferujeme poskytnout nejméně 14 dní před první známkou incidentu a alespoň 14 dní po něm. Dle vektoru útoku a typu incidentu se uvedený časový rámec potřebný k prověření incidentu může významně lišit.
- Časové rozmezí i rozsah podezřelých cílů bude pravděpodobně upřesněn/rozšířen v průběhu vyšetřování incidentu, proto:
    - doporučujeme **provést externí zálohu všech starších logů**, u kterých hrozí jejich brzké nenávratné smazání (vlivem rotace logů, retence dat apod.) pro případ pozdějšího prověření předcházejících událostí na základě vyšetřování incidentu. To se týká i všech logů, které nejsou centrálně sbírány a hrozilo by jejich ztracení např. při výpadku napájení!

## Na co si dát pozor při exportu dat:

- **Jednoznačná identifikace** komunikujících stran – je v logu skutečná adresa protistrany? (pokud je v cestě NAT/Proxy, nejspíše bude potřeba dalších podpůrných logů).
- Zkontrolovat **čitelnost souborů** – zda opravdu obsahují to, co bylo očekáváno.
- Zkontrolovat časové značky – zda jsou synchronní napříč logy, jejich časovou zónu (Nejlépe ověřit na nějakém posledním záznamu, zda odpovídají realitě. Pokud tomu tak není, uvést zjištěnou odchylku v popisu dat.).
- CSV **včetně záhlaví** (obecně tedy data včetně popisu-významu jednotlivých položek).
- **Vyhnout se** nestandardním formátům (binární data, kopie databáze, šifrované zálohy apod.) a různým formám „copy&paste“ z GUI, exportům do PDF, „obrázkům“ apod.
- Veškeré **nejasnosti/důležité detaily zaznamenat** formou průvodního popisu dat (nejlépe do předávacího protokolu viz dále).

# Co přiložit k zajištěným datům

K zajištěným datům přiložte i vyplněný Předávací protokol, který zároveň uložte na **externí USB pevný disk**. Předávací protokol je k dispozici na stránkách NÚKIB a měl by obsahovat:

- Čas zajištění a osoba, která zajištění provedla (včetně kontaktu na tuto osobu).
- Nástroje použité k zajištění dat.
- Popis **externího USB pevného disku**, na kterém jsou bitové kopie předávány (výrobce, označení, kapacita, výr. číslo).
- Popis zdrojového fyzického či virtuálního stroje (název, určení, operační systém, build, kernel, velikost RAM, počet a velikost disků).
- IP adresy/rozsahy vašich systémů vyskytujících se v datech, jejich provozovaných služeb a jejich účelu (včetně jejich krátkého popisu).
- V případě RAID polí a svazků: konfiguraci pole, typ RAIDu, počet a popis jednotlivých disků.
- V případě šifrovaných úložišť obnovovací klíče.
- Pro každou vytvořenou bitovou kopii uveďte její kontrolní sumu typu MD5 (**FTK Imager Lite i GUYMAGER** vytváří tyto kontrolní sumy automaticky).
- Všechny samostatně předávané soubory (s výjimkou bitových kopií vytvořených pomocí sw. **FTK Imager Lite** či **Guymager** a přehledového souboru) zabalte do jednoho archívu ZIP a uveďte jeho název a kontrolní sumu typu MD5.
- Kontaktujte pracovníky vládního CERT k dohodnutí způsobu předání zajištěných dat pracovníkům NÚKIB.
- V případě fyzického předání vše vhodně zabalte (např. bublinková obálka, kartonová krabice apod.).

# Jak pojmenovat cílovou složku

Všechny soubory týkající se jednoho stroje ukládejte na **externí USB pevný disk** do jedné pracovní složky, kterou pojmenujte dle následujícího vzorce:

Organizace_Nazevstroje_DatumPorizeni, např. **NUKIB_PCNovak_20210518**

# Jak pojmenovat bitové kopie

- Pro názvy bitových kopií disků a pamětí použijte následující vzorec:
  Organizace_JmenoStroje_TypZdroje _UrceniDisku _DatumPorizeni
  - Organizace je název mateřské organizace,
  - JmenoStroje je název stanice,
  - TypZdroje je **M** pro bitovou kopii paměti, **D** pro bitovou kopii pevného disku, **V** pro bitovou kopii virtuálního disku,

- v případě **D** nebo **V**: UrceniDisku je funkce disku ve stroji (SWAP, SYSTEM, DATA apod.),
- DatumPorizeni je datum vytvoření bitové kopie.

Např.: **NUKIB_PCNovak_D1_DATA_20210518**

## Jak popsat externí disk

**Externí USB pevný disk** s předávanými daty popište (nalepte na něj identifikační štítek) dle následujícího vzorce:

- Organizace_NazevStroje1_NazevStroje2_..._DatumPorizeni,
  např. **NUKIB_PCNovak_PCNovotna_Dcserver_20210518**,
- kontaktní osoba pro vrácení disku.

## Co dělat, když si nevím rady

V případě, že:

- některé výše uvedené postupy nefungují nebo nemohou být použity,
- je potřeba zajistit data z jiných typů úložišť, cloudů apod.,
- si nejste úplně jisti zvoleným postupem,

konzultujte svůj další postup s pracovníky vládního CERTu.

## Kontakty:

- mail: cert.incident@nukib.cz
- telefon:
  - 541 110 777 (v pracovní době 7:00-15:30)
  - 725 502 878 (mimo pracovní dobu)