ZAJIŠTĚNÍ DAT PRO FORENZNÍ ANALÝZU

Národní úřad pro kybernetickou a informační bezpečnost

Používejte externí úložiště pro spouštění nástrojů k akvizici dat i pro ukládání získaných souborů. Omezí se tak vykonané zápisy na interní úložiště a tím předejdete přepsání informace v nealokovaných blocích. Použijte vhodný souborový systém uložiště (FAT32 neumožňuje vytvářet soubory větší než 4 GB).

Společně se získanými soubory předávejte i následující informace:
- Seznam dokumentovaných uživatelů systému a jejich oprávnění
- Čas zajištění a hash všech souborů
- Nástroje použité k akvizici
- Identifikátory externího úložiště (výrobce, jméno svazku a jeho mapování v systému)

Pokud je počítač vypnutý, postupujte dle pokynů v sekci vypnutý počítač.

WINDOWS

FTK IMAGER
(http://marketing.accessdata.com/ftkimagerlite3.1.1)

Spusťte FTK Imager s právy administrátora.

1) Klikněte na ikonu "Capture Memory",
vyberte "Destination path",
zaškrtněte "Include pagefile",
klikněte na "Capture Memory"

2) Klikněte na ikonu "Add Evidence Item",
vyberte "Logical Drive", "Next",
vyberte systémový disk,
klikněte "Finish"

3) Vyberte následující položky do "Custom Image"
(klikněte pravým tlačítkem na danou položku,
vyberte "Add to Custom Image (AD1)")

- [root]\pagefile.sys
- [root]\hiberfil.sys
- [root]\$MFT
- [root]\$LogFile
- [root]\$Extend\$UsnJrnl
- [root]\$Recycle.Bin
- [root]\Windows\System32\config\SAM
- [root]\Windows\System32\config\SYSTEM
- [root]\Windows\System32\config\SOFTWARE
- [root]\Windows\System32\config\DEFAULT
- [root]\Windows\Prefetch
- [root]\Windows\inf\setupapi.dev.log
- [root]\Windows\LogFiles
- [root]\Windows\Appcompat\Programs
- [root]\Windows\Tasks
- [root]\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

4) Pro následující položky klikněte na "New",
vyberte nově přidanou položku,
doplňte text a klikněte "Edit",
zaškrtněte "Match all occurences",
zaškrtněte "Include Subdirectories"

- NTUSER.DAT
- UsrClass.dat
- AppData
- *.lnk
- *.evtx

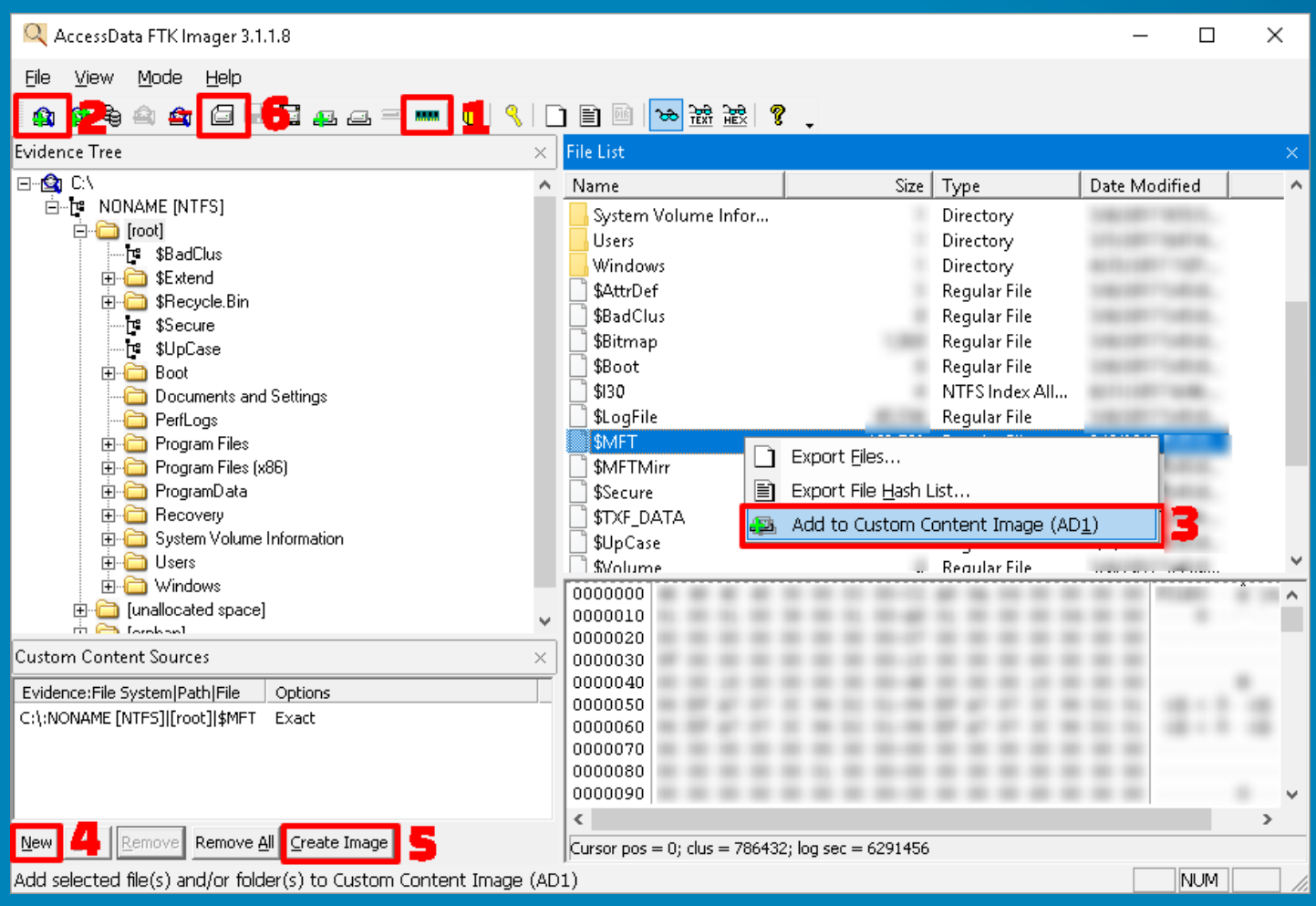
5) Klikněte na "Create Image",
"Add" pro výběr cílového umístění,
zaškrtněte "Verify image after they are created",
klikněte na "Start"

Oba vytvořené soubory (obraz paměti RAM a přehledový soubor) předejte k analýze.
Zasažený systém můžete nyní odpojit od sítě.
Pokračujte vytvořením kopie celého interního úložiště.

6) Klikněte na ikonu "Create Disk Image",
vyberte “Physical Drive”, "Next",
vyberte jednotku interního úložiště, "Finish"

- Klikněte na "Add", vyberte formát "Raw (dd)", "Next",
"Next", vyberte cílové umístění,
"Finish", zaškrtněte "Verify images after they are created",
klikněte na "Start"
- Opakujte pro všechny jednotky interního úložiště

Při použití šifrování předejte také klíče pro obnovení.
Vytvořený obraz interního úložiště předejte k analýze.
S přemazáním systému vyčkejte na potvrzení analytického týmu.



ALTERNATIVA
Pokud není možné použit nástroj FTK Imager, vytvořte obraz paměti RAM pomocí nástroje DumpIt.

DUMPIT (https://my.comae.io/tools)
DumpIt je součástí sady nástrojů "comae-toolkit-light", je dostupný v 32 i 64bitové verzi. Musí být spuštěný s právy administrátora. Po spuštění vytvoří obraz paměti a JSON soubor s informacemi o systému a obrazu. Tyto soubory vytvoří ve složce, kde se program DumpIt nachází (externí úložiště).

KOPIE INTERNÍHO ÚLOŽIŠTĚ
Systém vypněte a postupujte podle pokynů v sekci "Vypnutý počítač".

VYPNUTÝ POČÍTAČ

Vypnutý počítač nezapínejte. Pokud je to možné, vyjměte a předejte celé interní úložiště. V opačném případě připojte disk pouze pro čtení a vytvořte obraz disku pomocí nástrojů FTK Imager nebo dd. Při použití šifrování předejte také klíče pro obnovení.