FTK Imager - Quick Reference Guide

Zajišťování digitálních stop

Anotace:

Zajištění digitálních stop je první a jednou z nejdůležitějších etap práce digitální forenzní analýzy. Pouze taková data, která jsou zajištěna forenzně správným způsobem, mohou poskytnout kvalitní základ pro získání relevantních důkazů. Proto se procesu forenzního zajištění digitálních stop musí věnovat patřičná pozornost a pro tento proces by měly existovat specifické procesy, postupy a také specifické nástroje.

Jedním z nejčastěji používaných programů pro forenzní zajištění digitálních stop je FTK Imager. Stručný postup zajištění obsahu operační paměti (RAM) a pevných disků počítače je popsán v následujícím článku.

Úvod

Forenzní analytický SW Forensic Toolkit (FTK) je počítačový forenzní softwarový produkt společnosti AccessData. Je to komerční produkt založený na systému Windows. Pro forenzní analýzy vytvořil stejný vývojový tým bezplatnou verzi komerčního produktu s limitovanými funkcemi - FTK Imager. Tento nástroj je jedním z nejlepších pro pořizování forenzních kopií (obrazů) pevných a i volatil (RAM) pamětí a lze s jeho pomocí provádět i základní jednoduché analýzy (prohlížet a extrahovat data z již pořízených forenzních kopií disků).

Získávání forenzních kopií pamětí lze rozdělit do dvou hlavních částí:

1. Získání forenzních kopií volatilní paměti

2. Získání forenzních kopií trvalé paměti (pevný disk)

Existují dva možné způsoby, jak tento nástroj lze použít při pořizování forenzních kopií:

1. Použití přenosné verze FTK Imageru (např. na USB nebo HDD) a spuštění přímo ze zajišťovaného počítače. Tato možnost se nejčastěji používá při získávání živých dat v případech, kde je počítač v momentě zajištění zapnut.

2. Instalace FTK Imageru na analytickém počítači.V takovém případě by měl být zdrojový disk připojen k počítači pomocí writeblockeru. Blokování zápisu zabraňuje změnám dat na zdrojovém disku a poskytuje přístup pouze pro čtení. Tím zajistíme integritu dat zdrojového disku.

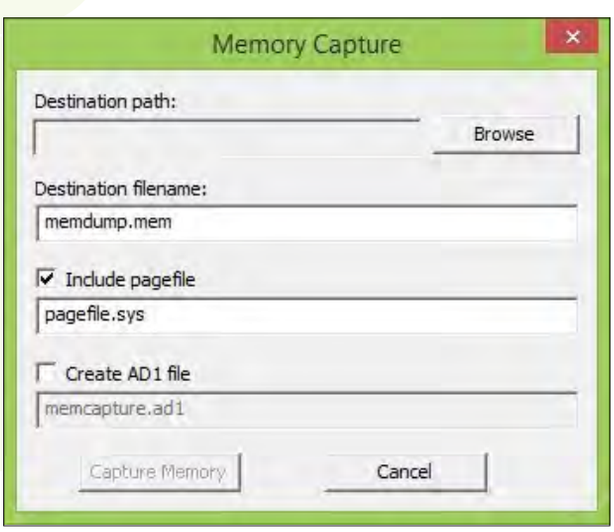
Získání volatilní paměti pomocí FTK Imageru

FTK Imager umožňuje forenzním expertům získat úplnou forenzní kopii volatilní paměti (RAM) počítače.

Následující stručné kroky popisují zajištění RAM paměti počítače.

U běžícího počítače přiojte USB s instalací (kopií) FTK Imageru a spusťte jej z tohoto USB. Přejděte na ikonu pro zajištění volatilní paměti („Capture memory“):

Následující dialogové okno vám umožní zadat cílový adresář („Destination path:“ pod tlačítkem „Browse“), kde chcete uložit zaznamenanou volatilní paměť a zadat název souboru (do pole „Destination filename“):

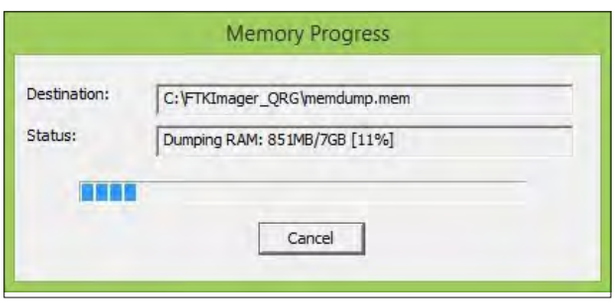


Pomocí FTK Imageru máte také možnost zahrnout do kopírovaných dat také stránkovací soubor „pagefile.sys“ a také oba stažené soubory uložit společně do formátu AD1 (tzv. „evidence file“ ve formátu AD1), který je proprietálním formátem společnosti Accessdata ale z důvodu zajištění maximální kompatibility to není příliš vhodné.

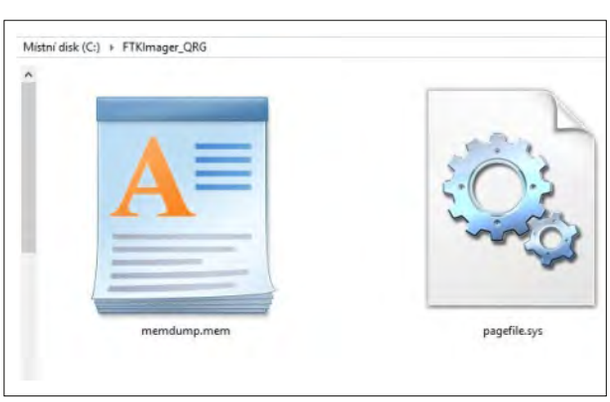
Stránkovací soubor (pagefile.sys) se v operačních systémech Windows používá jako volatilní paměť kvůli omezení fyzické paměti RAM. Je umístěn v oddílu "C:" a je připraven k použití jako volatilní paměť při požadavku na překročení kapacity fyzické paměti

RAM. Takže tento soubor může mít poměrně hodně hodnotných dat. Proto se doporučuje vždy zajistit s operační pamětí (RAM) také tento soubor.

Klepnutím na tlačítko "Capture memory" začne FTK Imager kopírovat volatilní paměť:



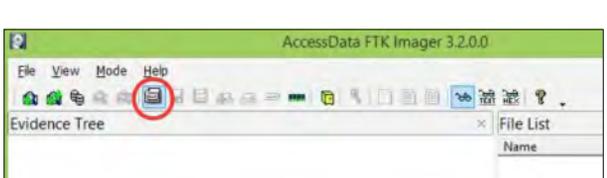
Po dokončení kopírování bude cílový adresář („Destination“) obsahovat zadané soubory - kopie paměti (v našem případě soubory „memdump.mem“ a „pagefile.sys“):



Získání forenzního obrazu disku (Disk Image) pomocí FTK Imageru

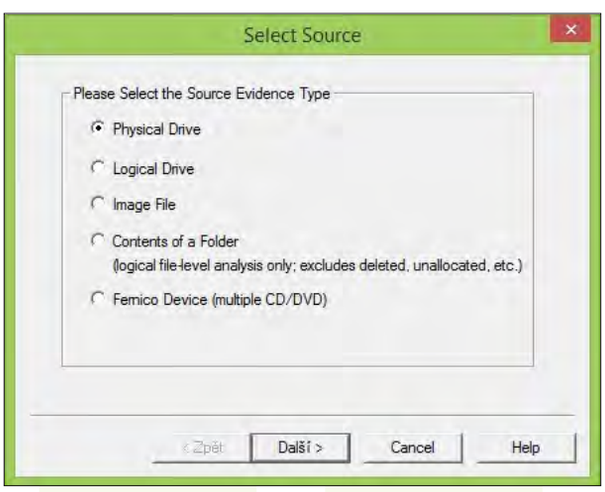
Jak již bylo řečeno, lze tento nástroj použít i k pořízení forenzních kopií (obrazu) disku.

Po spuštění FTK Imageru použijte ikonu "Create Disk Image":

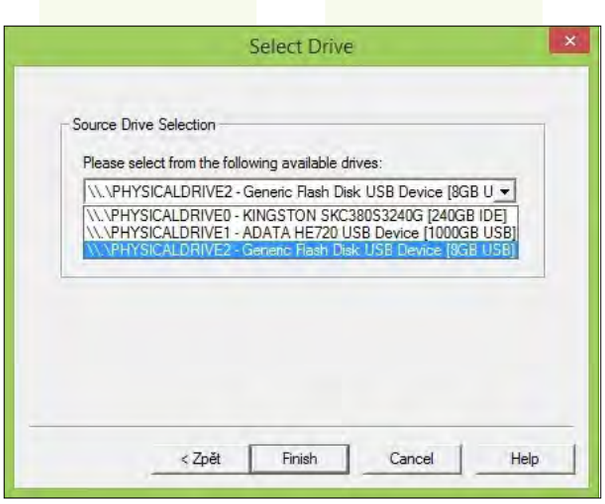


V následně zobrazeném dialogu vyberte typ zdrojových dat. FTK Imager je schopen získat data z fyzických disků, z logických disků (diskové oddíly), z jiného forenzního obrazu, z obsahu složky (adresáře) nebo z CD / DVD disků.

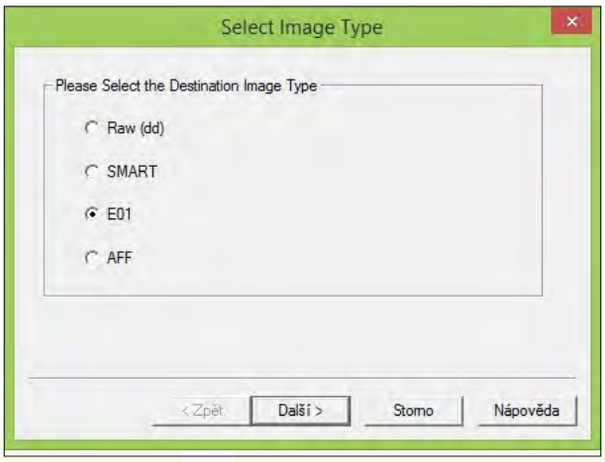
Zdrojový pevný disk se připojuje k laboratornímu počítači pomocí writeblockeru a lze udělat forenzí kopii z celého fyzického disku volbou „Physical Drive“ nebo jen z učitého diskového oddílu volbou "Logical Drive":

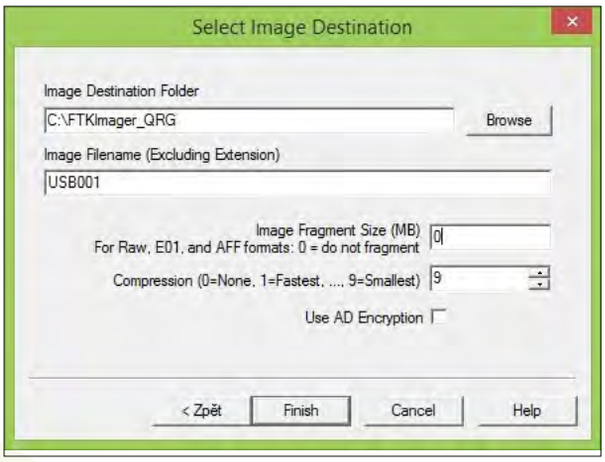


Pro forenzní kopii celého fyzického disku zvolte „Physical Drive“. V následujícím dialogu vyberte, který fizický disk potřebujete kopírovat a zvolte „Finish“:



V dalším dialogu zadáte cíl, kam se bude výsledná forenzní kopie ukládat (klepnutím na tlačítko „Add...“). Nejdříve je nutné zvolit formát výsledného forenzního obrazu:

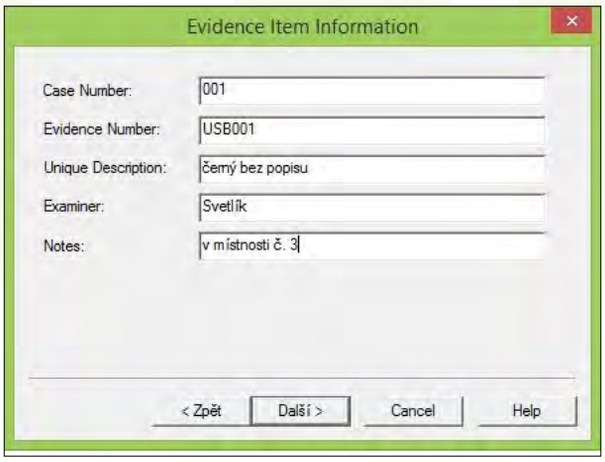




Z praxe lze doporučit použití formátu „E01“ jako nejrozšířenějšího formátu. Tento formát také podporuje kompresi dat a tím efektivní využití cílového diskového prostoru a tím i kratší čas zápisu dat. Formát E01 podporují téměř všechny v současnosti existující analytické nástroje a stal se prakticky standardem.

Jako další potenciálně použitelný formát je „Raw (dd)“, který je univerzálně použitelný, avšak bez komprese dat je nanejvýš neefektivní z hlediska objemu výsledných dat.

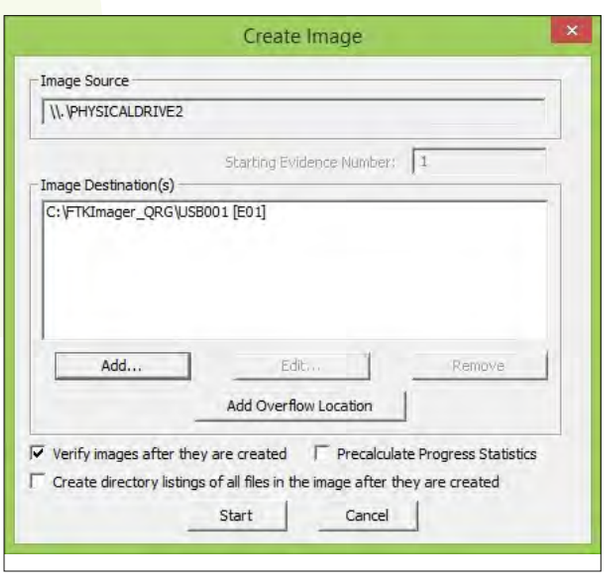
Po stisknutí tlačítka „Další>“ FTK Imager vyzve k zadání podrobností případu. Jsou to tzv. identifikační a evidenční údaje, kterými lze následně identifikovat výslednou forenzní kopii dat:



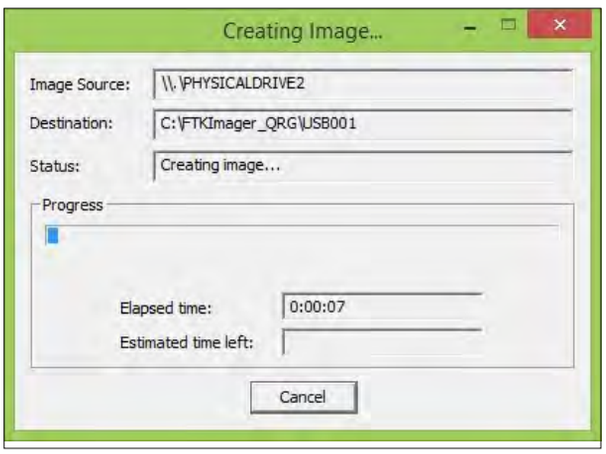
Po dalším stisnutí tlačítka „Další>“ budete vyzváni k zadání cíle (adresáře), kde bude uložena forenzní kopie dat (pod tlačítkem "Browse"), název výsledného souboru a velikost fragmentování:

Velikost fragmentování („Image Fragment Size (MB)“) umožňuje rozdělit výsledný soubor na více částí, které uloží je do stejného adresáře. Pokud potřebujete pouze jeden soubor namísto vytváření více fragmentovaných obrazů, musíte nastavit velikost fragmentu na hodnotu "0". U formátů, které to podporují, můžete nastavit sílu komprese (když máte výkonný počítač, můžete kompresi nastavit na „9“).

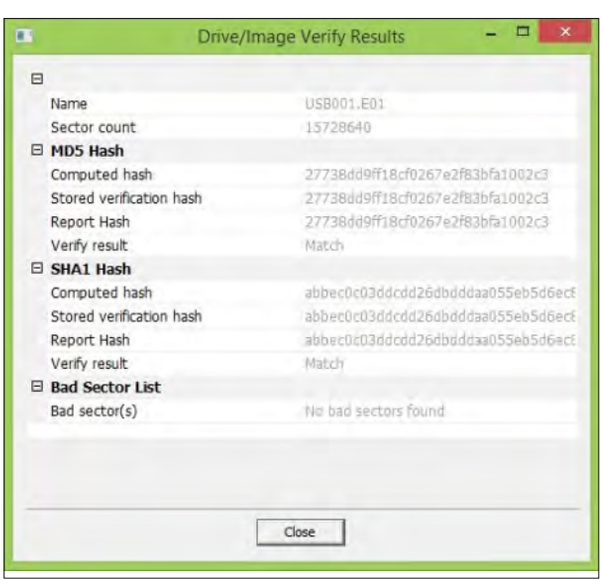
Po zmáčknutí tlačítka „Finish“ se vrátíte na předchozí dialog. Pak ještě zaškrtněte volbu „Verify images after they are created“ (pro ověření spolehlivosti kopírování) a zrušte zaškrtnutí „Precalculate Progress Statistics“ (zbytečně zdržuje kopírování a stejně nedává relevantní předpověď zbývajícího času do konce kopírování):



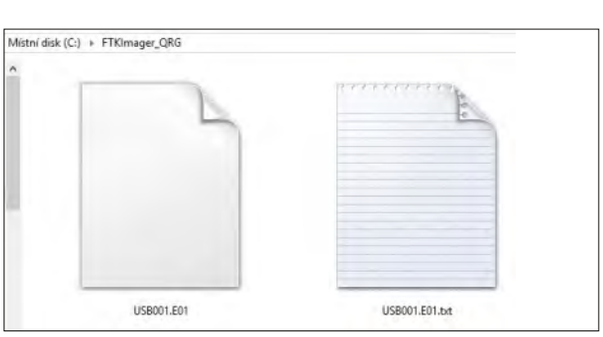
Samotné kopírování pak spustíte tlačítkem „Start“:



Po dokončení kopírování program FTK Imager zobrazí výsledek kopírování:



V cílovém adresáři vytvoří kromě samotného souboru forenzní kopie dat ("USB001.E01") navíc ještě textový soubor ("USB001.E01.txt") obsahující všechny informace, které jste zadali („Evidence Item Information“) a také další informace technického charakteru o zdrojovém disku a o forenzní kopii dat:



Jedná se o tzv. log soubor, který navíc obsahuje klíčovou informaci, a to spočtené hash součty MD5 a SHA1, které slouží pro ověření integrity získaných dat:

Závěr

Program FTK Imager patří mezi ty nejspolehlivější a nejčastěji používané programy pro forenzně korektní zajištění digitálních stop. Kromě zde popsané verze pro OS Windows existuje verze i pro OS LINUX, která je ovládána z příkazové řádky.

FTK Imager získal svoji popularitu ale nejenom pro snadné pořizování forenzních kopií digitálních stop, umí toho mnohem více. Ale o tom až někdy příště.