EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

TESTOVÁNÍ BEZPEČNOSTI

Základy forenzního auditu

Metodický list

Autor: doc. Ing. Jaroslav Dočkal, CSc., Metodik: Bc. Jaroslav Tihlařík

Recenzent: Ing. Vladimír Šulc Ph.D.

Rok vydání: 2023

Obsah

Cíle

Naučit se základům počítačového forenzního auditu. V rámci toho žáky seznámit s externími zdroji informací obsažených v dostupných prestižních kurzech na internetu. Zde byla jako podklad scénáře použita úvodní část kurzu EdX o osmi částech s názvem RITx CYBER502x Computer Forensic. Samotný projekt Open edX provozuje The Center for Reimagining Learning (tCRIL), nezisková organizace řízená dvěma nejvýznamnějšími americkými univerzitami (Harvard a MIT).

Konkrétními cíli jsou

- Seznámit se s pojmem image a naučit se ho vytvořit
- Naučit se kontrolovat integritu souboru za pomoci jeho hashe

Dovednosti

V rámci scénáře budou získávány tyto dovednosti:

- Ovládání a využití softwaru FTK Imager
- Ovládnutí práce v prostředí md5sum resp. hashcalc

Pracovní prostředí

Úlohu lze realizovat v prostředí:

- Cylab JCEKB
- FTK Imager
  Na https://www.pluralsight.com/courses/accessdata-forensic-toolkit-ftk-imager?utm_source=google&utm_medium=paid-search&utm_campaign=upskilling-and-reskilling&utm_term=ssi-emea-xyz-dynamic&utm_content=free-trial&gclid=Cj0KCQjwwtWgBhDhARIsAEMcxeDIvAN134xSjF-DQlGc9Dsn8sBz5owYT0BXyLEFbupuXV1FVi7NaEu4aAlA4EALw_wcB
  Je bezplatný kurz práce s tímto nástrojem
- SIFT Workstation (https://www.sans.org/tools/sift-workstation/)
- Windows: hashcalc (www.slavasoft.com/hashcalc/)
- Linux/Unix: md5sum a shasum

Průběh výuky

1 Forenzní analýza a forenzní artefakty systému Windows

1.1 Koncept a typy forenzního šetření

Cílem forenzního vyšetřování je identifikovat, analyzovat, rekonstruovat minulé události nebo činnosti a předložit přípustné důkazy soudu.

Oblast počítačové forenzní je relativně mladá. V roce 1999 představili Dan Farmer a Wietse Venema – oba výzkumníci a programátoři počítačové bezpečnosti – forenzní proces a první počítačovou forenzní sadu nazvanou TCT[1] (The Coroners Toolkit), která znamenala začátek oboru počítačové forenzní analýzy. Ve své prezentaci (Farmer, Venema) Farmer a Venema definovali počítačovou forenzní analýzu jako shromažďování a analýzu dat způsobem, který ač je co nejvíce zkreslený nebo zkreslený, slouží k rekonstrukci dat nebo zjištění toho, co se v minulosti v systému stalo.

Počítačoví forenzní vyšetřovatelé používají forenzní nástroje a dodržují příslušné postupy ke shromažďování, uchovávání, analýze a hlášení přípustných důkazů soudu, který poskytuje své kritické úsudky o tom, co se přesně stalo. Termín „uchování“ zde znamená zajistit, aby uchované důkazy předložené soudu nebylo nikdy možné upravit. To je zásadní úkol forenzního auditu.

Je důležité dodržovat forenzní postup a používat vhodné nástroje. Digitální důkazy mohly být zaznamenávány v závislosti na tom, jak byly shromážděny a analyzovány a kde byly uloženy. Pokud zkopírujete soubor např. pomocí příkazu Linuxu, upravili jste tím pádem i soubory i přístupový čas, a tím poškodíte důkazy.

Při rekonstrukci důkazů je první otázkou: Odkud získáváme nebo shromažďujeme důkazy? Důkazy mohou spočívat v počítačových systémech, počítačových sítích, počítačových médiích, počítačových periferiích – v zásadě všude. Data mohou být v jednom ze tří stavů:

- v klidu (at rest), což znamená uložená v jednotce počítače, v cloudu nebo jednotce USB atd., v mobilním telefonu,
- používaná (in use) v paměti počítače,
- přenášená (in transit).

Forenzní nástroje, které shromažďují a analyzují údaje v klidu, se liší od nástrojů určených k přenosu dat svým použitím. Na základě toho lze kategorizovat počítačovou forenzní analýzu podle technologií pracujících s různými typy důkazů.

[1] TCT je sbírka programů Dana Farmera a Wietse Venemy pro posmrtnou analýzu systému UNIX. TCT byl nahrazen The Sleuth Kit, což je kolekce nástrojů příkazového řádku a C knihovna, která umožňuje analyzovat obrazy disků a obnovovat z nich soubory. Používá se na pozadí Autopsy a mnoha dalších open source a komerčních forenzních nástrojů.

Systémová forenzní analýza soustřeďuje pozornost na důkazy z dat závislých na napájení (volatilních) dat, jako jsou data v paměti, a dále na důkazy z energeticky nezávislých dat, která jsou uložena na pevných discích (patří sem počítačové disky, diskety, magnetické pásky, zip a disky JAZ[2], záznam souborů atd.) Forenzní analýza často určuje, co se stalo v systému na základě studie síťového provozu, jako je analýza časové osy, IP adresy nebo obsah paketů. Tento úkol je technicky náročný, protože tyto důkazy jsou často přechodné a nevydrží tak dlouho, jako uložené médium.

„Cloud forensics" je rozvíjející se oblast zaměřená na cloudové důkazy, jako jsou Google Drive, webový e-mail uložený na serverech vlastněných třetí stranou. I když se forenzní nástroje a technologie liší od různých typů operačních systémů, obecný forenzní postup zůstává stejný.

Existuje také protějšek zvaný v originále „anti-digital forensics" neboli ve zkratce ADF, což jsou technologie, jejichž cílem je zmařit objev těchto informací. Přístupy ADF mají za cíl manipulovat, mazat nebo zpřeházet digitální data, aby bylo forenzní vyšetření obtížné, časově náročné nebo prakticky nemožné. Jako příklad technologie ADF lze uvést přejmenovávání souborů změnou jejich přípon; skrývání dat přidružením dobrých bloků ke špatným inodům[3]; přepisování dat a metadat, lze rovněž skrývat nebo zamlžovat data pomocí kryptografie, steganografie[4], a dalších metod.

V soudních jednáních hrají nepominutelnou roli soudní znalci. Znalec u soudu vystupuje před soudci, právníky, obhájci a dalšími účastníky, a v rámci soudního řízení uvádí svá zjištění, názory a závěry. Znalci sledují postup soudu, předkládají zjištění, provádí analýzy a formulují závěry, čímž prokazují své odborné znalosti. Je zásadní, aby odborník v jednání nevykazoval zaujatost a mluvil jen pravdu.

1.2 Procedury forenzního vyšetřování

V předchozím textu bylo zdůrazněno, že forenzní postup a technologie jsou dva nejdůležitější aspekty počítačové forenzní techniky. Věnujme se nyní soudnímu řízení. Po potvrzení počítačové události začíná forenzní vyšetřování. Pokud je podezřelý počítač stále zapnutý a připojený k síti, jak začneme?

Měli bychom vypnout systém? Odpovědí je, že bychom se měli řídit zásadami a postupy reakce na incidenty společnosti, abychom rozhodli, zda podezřelý stroj okamžitě vypnout či ne.

Měli bychom si však být vědomi toho, že pokud systém vypneme, ztratíme obsah paměti počítače a nestálá data, například přihlášené uživatele, připojení PCP[5] a běžící procesy atd. Pokud je to možné, měli bychom shromáždit volatilní (nestálá) data před vypnutí stroje.

Pokud lze podezřelý stroj vypnout, druhá otázka zní, jak to správně provést? Máme počítač vypnout elegantně nebo násilně? Pokud systém elegantně vypnete, zajistíte, že systém zůstane v konzistentním stavu, protože elegantní vypnutí

[2] výměnný disk

[3] i-uzel je datová struktura uchovávající metadata o souborech a adresářích používaná v unixových souborových systémech.

[4] vědní disciplína (speciální podobor kryptografie) zabývající se utajením komunikace prostřednictvím ukrytí zprávy (např. do obrazu či zvuku).

5 Port Control Protocol (PCP) je počítačový síťový protokol, který umožňuje hostitelům v sítích IPv4 nebo IPv6 řídit, jak jsou příchozí pakety IPv4 nebo IPv6 překládány a předávány směrovačem.

zahrnuje čerstvé vyrovnávací paměti pro ukládání informací na disky, upozorňování uživatelů a služeb atd. Pachatelé však pravděpodobně nainstalovali rootkity[6], aby zničili důkazy po přijetí příkaz k vypnutí. Mohou například smazat určité nebo všechny soubory v systému. Ztratíte nestálá data, včetně stavu sítě, jako jsou síťová připojení a ARP tabulky, spolu s běžícími procesy, přihlášenými uživateli, obsahem jádra a swap[7] (odkládacího) prostoru.

Pokud systém vypnete násilím vytržením napájecího kabelu, vyhnete se potenciální ztrátě důkazů způsobené rootkity. Může vás to však stát data v cache[8] paměti, která nejsou zapsána na disk, data zůstanou v nekonzistentním stavu a ztratíte nestálá data.

Porovnáním uvedených dvou scénářů vypnutí z hlediska forenzní perspektivy byste měli dojít k názoru, že pokud je pachatel profesionální zločinec orientující se v práci s počítačem, je lépe vytrhnout napájecí kabel a každou akci pečlivě zdokumentovat.

Forenzní řízení začíná stanovením podrobného řetězce důkazů. Koncept řetězce důkazů není nový. Má vést záznamy o tom, jak bylo s důkazy nakládáno, a to od okamžiku, kdy byly shromážděny, do okamžiku, kdy byly předloženy soudu. Řetězové vazby zahrnují datum a čas, kdy byly důkazy shromážděny, celé jméno a podpis každé osoby, která má důkazy, a na jak dlouho, umístění a zda byly uloženy způsobem zabezpečeným proti neoprávněné manipulaci.

Je třeba zdokumentovat všechny činnosti a předávání důkazů od jedné osoby k druhé osobě. Pokud je počítač zabaven a vypnut, měly by být pevné disky vyjmuty a označeny odděleně od systému. Je třeba zaznamenat výrobce, model a sériové číslo pevných disků spolu s dalšími popisy důkazů, číslem případu a číslem položky na štítku (ticketu) důkazu.

1.3 Akvizice dat

Se zahájením řetězce úschovy zahajujeme proces získávání důkazů, jejich uchovávání, analýzy a podávání zpráv. V této podkapitole budou popsány dva nástroje pro každý krok, které pomohou porozumět procesu.

V počítačové forenzní oblasti, jak již bylo uvedeno, se zaměřujeme na digitální data. To zahrnuje veškeré zpracovávané, uložené nebo přenášené informace ve formě souborů, metadat, jako jsou oprávnění, a odstraněných dat. Z těchto dat vyšetřovatelé získají informace o jednotlivcích, určí, co se stalo, vytvoří časovou osu a objeví škodlivé nástroje či exploity používané útočníkem.

Různé počítačové zločiny mohou vést k různým digitálním důkazům. Cyberstalkers například mohou obtěžovat e-maily. Počítačoví hackeři obvykle nechávají zadní vrátka a další malware v souborech systémových protokolů. Dětští pornografové mají na svých zařízeních uloženy digitální obrázky, které jsou případně skryté.

Akvizice zahrnuje získání volatilních i energeticky nezávislých dat. Volatilní data vyžadují energii k udržení dat v paměti. Data uložená na pevných discích jsou běžným příkladem energeticky nezávislých dat.

---

6 Rootkit je typ softwaru, jehož úkolem je maskovat činnost útočníka a přítomnost škodlivých softwarů.

7 Swap je ve své podstatě druhá RAM paměť počítače, do které se mohou ukládat data z většinou neaktivního procesu z důvodu uvolnění místa pro jiné běžící či nové aplikace.

8 Cache je označení pro mezipaměť, do které se ukládají nejčastěji používaná data.

Neboli nejprve vždy získáme volatilní data, protože jsou krátkodobá. Abychom získali nestálá data, například síťové rozhraní, spustíme např. příkaz jako je ifconfig (UNIX) resp. ipconfig (Windows).

Při práci na shromažďování důkazů z podezřelého počítače mějte na paměti, že se musíte ujistit, že veškerý výstup bude přesměrován mimo podezřelý stroj, protože jinak manipulujete s daty. Kromě toho se musíte ujistit, že na jednotce přijímajícího stroje nejsou zachována nežádoucí data.

Přijímací stroj obvykle nazýváme forenzním strojem, abychom zabránili nebezpečí, že zbytková data na vaší cílové jednotce poškodí vaše důkazy. V běžné praxi provedete před získáním dat dezinfekci důkazní jednotky forenzního stroje. Bitstreamová kopie zaznamená každý jednotlivý bit každého bajtu na zařízení. Vystupuje na úrovni disku, ne na úrovni souboru, a ignoruje konec značky souboru; proto se tento proces často nazývá zobrazování na pevném disku, zobrazování bitového proudu resp. forenzní zobrazování (forensic imaging).

Zatímco unixové příkazy jako cp, tar, cpio[9], dump a restore pouze kopírují obsah souborů a zastaví se na koncové značce souboru, kopie bitového toku zkopíruje každý bit na jednotce, včetně odstraněných dat. Pracujeme zde s image disku, jeho diskovým obrazem, což je archivní soubor obsahující digitální kopii dat disku. Kromě datových souborů obsahuje image také všechna metadata souborového systému, a to včetně Boot sektoru, struktur a atributů.

V tomto scénáři budeme pracovat s nástroji dd a FTK imager, Oba jsou všeobecně známé forenzní zobrazovací nástroje. V praktické části scénáře si ukážeme, jak použít FTK Imager k vytvoření obrazu, a následně se budeme věnovat příkazu dd.

1.4 Prevence

Jelikož soudy vyžadují, aby důkazy byly autentické a nezměněné, musí být získané digitální důkazy uchovány v původním stavu. Forenzní audit používá k uchování důkazů kryptografické hash algoritmy.

Kryptografický hash algoritmus je jednosměrná funkce, která mapuje data libovolné velikosti, jako je zpráva, na bitstream s pevnou velikostí, což se nazývá hash hodnota. Stejná zpráva má vždy za následek stejnou hodnotu hash. Zde „jednosměrnost“ znamená, že nelze vygenerovat zprávu z její hodnoty hashe.

Kryptografický hash by měl být algoritmus bez kolizí. To znamená, že je funkčně nemožné najít dvě různé zprávy se stejnou hodnotou hashe. Pokud tedy chceme dokázat nebo autorizovat, že dva image pevného disku jsou identické, musíme vypočítat jejich hash hodnoty. Pokud jsou hodnoty hash stejné, musí být dva image stejné podle vlastnosti bez kolize.

Jeden běžně používaný kryptografický hash algoritmus se používá MD5, který produkuje 128bitovou hodnotu hashe. Další algoritmus nazvaný SHA algoritmus produkuje hash o velikostech 160, 256 a 512 bitů (SHA1, SHA256 a SHA512).

[9] tar i cpio mají jediný účel: zřetězit mnoho samostatných souborů do jednoho streamu. Nekomprimují data. (V současnosti je tar populárnější díky své relativní jednoduchosti – může vstupní soubory brát jako argumenty, místo aby byl spojen s findem, jak je tomu u cpio.)

Algoritmy, které generují kratší hash, jako je MD5, generují hodnoty hash rychleji, ale s větší pravděpodobností způsobí kolizi. Vědci zjistili kolize při použití jak algoritmu MD5, tak algoritmu SHA-1, takže z dnešního hlediska ani jeden z těchto dvou bezpečnostně neobstojí.

Forenzní vyšetřovatelé používají kryptografický hash k uchování důkazů. My si procvičme kryptografické hashovací funkce na stroji s Linuxem a prozkoumejme, jaké změny zprávy ovlivní změny hodnot hash souborů. Jako nástroj použijeme SANS Investigative Forensic Toolkit – ve zkratce pro SIFT – Workstation, který je ke stažení zdarma – a používá se obvykle na Ubuntu (např. na Virtual Boxu je třeba zaškrtnout patřičný typ souboru). Login = sansforensics, Password = forensics.

SIFT Workstation je sbírka bezplatných a open source nástrojů pro odezvu na incidenty a forenzních nástrojů navržených k provádění podrobných digitálních forenzních zkoumání v různých prostředích. Může odpovídat jakékoli aktuální reakci na incident a sadě forenzních nástrojů. SIFT ukazuje, že pokročilé schopnosti reakce na incidenty a hluboké digitální forenzní techniky lze dosáhnout pomocí špičkových open source nástrojů, které jsou volně dostupné a často aktualizované. Pracovní stanici SIFT vytvořil a aktualizuje mezinárodní tým vedený forenzním vyšetřovatelem SANS[10] Robertem Lee[11]. Je k dispozici celé komunitě jako veřejná služba. SIFT zahrnuje mnoho reakcí na incidenty a sadu nástrojů pro digitální forenzní analýzu.

1.5 Analýza dat a hlášení

Poté, co jsme vytvořili kopii bitového proudu a uchovali důkazy, můžeme pokračovat v analýze důkazů pracujících na kopii. Kdykoli je to možné, měli bychom chránit původní fyzické důkazy a pracovat pouze s digitální kopií.

Analýzu začneme tím, že se podíváme na tabulku oddílů na podezřelé jednotce, abychom zjistili počet oddílů a zkontrolovali mezery mezi oddíly pro skrytá data.

Mezi další kroky analýzy patří načítání smazaných souborů, generování časové osy na základě časových razítek a souborů protokolu, hledání skrytých dat, vyhledávání klíčových slov pro výrazy související s vaším případem. Dále analýza podpisu k identifikaci falešných rozšíření a hash analýza k odfiltrování nevinných i škodlivých souborů a analýza médií specifická pro operační systém.

Po dokončení forenzního vyšetření s příslušnými důkazy a nálezy je posledním krokem **hlášení nálezů**.

Napsání zprávy a prezentace zjištění a technických vysvětlení převážně netechnickému publiku, včetně právníků, soudců a poroty, je velmi důležitým, ale náročným úkolem. Během všech aspektů forenzního vyšetřování je třeba dokumentovat podrobné poznámky.

Zde je několik obecných pokynů pro psaní zprávy:

[10] SANS Institute je soukromá americká zisková společnost založená v roce 1989, která se specializuje na informační bezpečnost, školení v oblasti kybernetické bezpečnosti a prodej certifikátů.

[11] (https://www.sans.org/profiles/robert-m-lee/).

Typická zpráva začíná konkrétním úkolem přiděleným soudnímu znalci a zjištěným faktickým prohlášením. Tato část obsahuje přinejmenším popis případu, způsob zapojení zkoušejících a počáteční důkazy, jako je podezřelý stroj nebo daný získaný obraz a hodnota hashe. Dále je třeba uvést použitá forenzní zařízení, metodiku použitou k duplikaci dat a metodika použitou k forenznímu vymazání úložiště.

V další části naší výuky se budeme zabývat procesem analýzy a nástroji používanými k analýze forenzního obrazu. Toto je nejpodrobnější část popisující vyšetřování. Měla by být zaznamenána všechna zjištění, včetně obnovených souborů, hodnot registru, přístupů k vyhledávání klíčových slov, e-mailů, obrázků a webového obsahu atd. Jelikož zprávu píše odborník, lze do zprávy zahrnout osobní názory.

U každého stanoviska lze poskytnout podpůrná data z analýzy. Nakonec je třeba zprávu uzavřít prohlášeními. Zkoušející často v rámci prohlášení používají fráze, jako např. „na základě mých znalostí“, „to je můj profesionální názor“, „jak naznačuje nález“.

2 Praktická část

2.1 Práce s FTK Imagerem

DOBA: Tato aktivita by vám měla trvat přibližně 30 minut, pokud používáte malý USB disk.

SOFTWARE

K provredení této činnosti si budete muset stáhnout software FTK Imager

USB DISK

Pro toto cvičení budete potřebovat USB disk s minimálně třemi soubory libovolného formátu. Můžete použít libovolnou velikost disku, ale pokud použijete jeden GB nebo méně, proces vytváření image nebude příliš dlouhý. Aby byla tato činnost realistická, nepoužívejte zcela nový disk. Místo toho použijte ten, ze kterého jste časem načetli a odstranili soubory.

CÍL

POZNÁMKA: FTK Imager nezaručuje, že data nebudou zapsána na disk během zobrazování. Z tohoto důvodu budou vyšetřovatelé používat blokátor zápisu při použití FTK Imager ve skutečném případě. Chcete-li dokončit tuto činnost, můžete předpokládat, že máte blokování zápisu na USB.

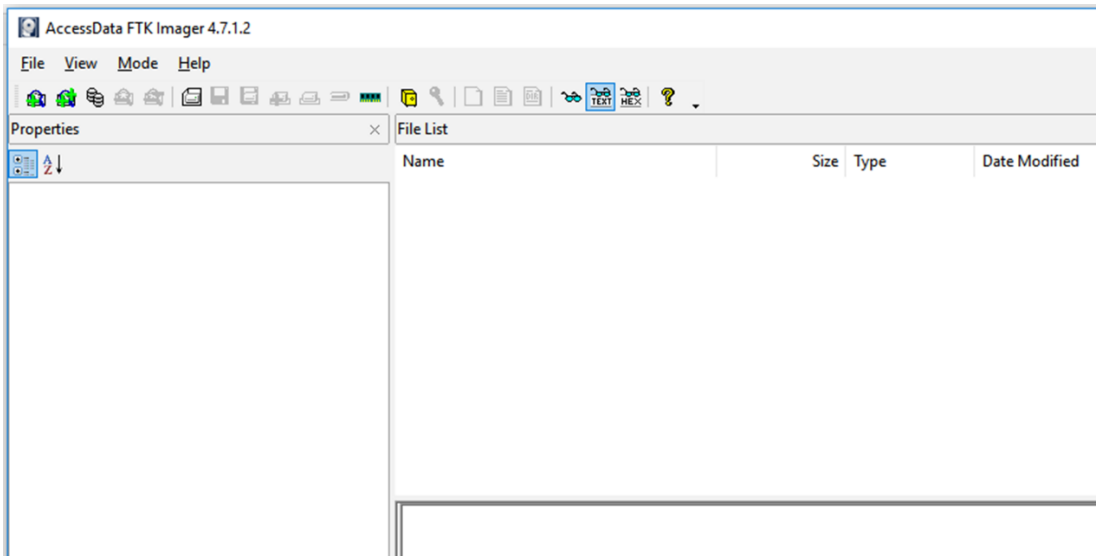
POKYNY

Spusťte FTK imager a vložte USB.

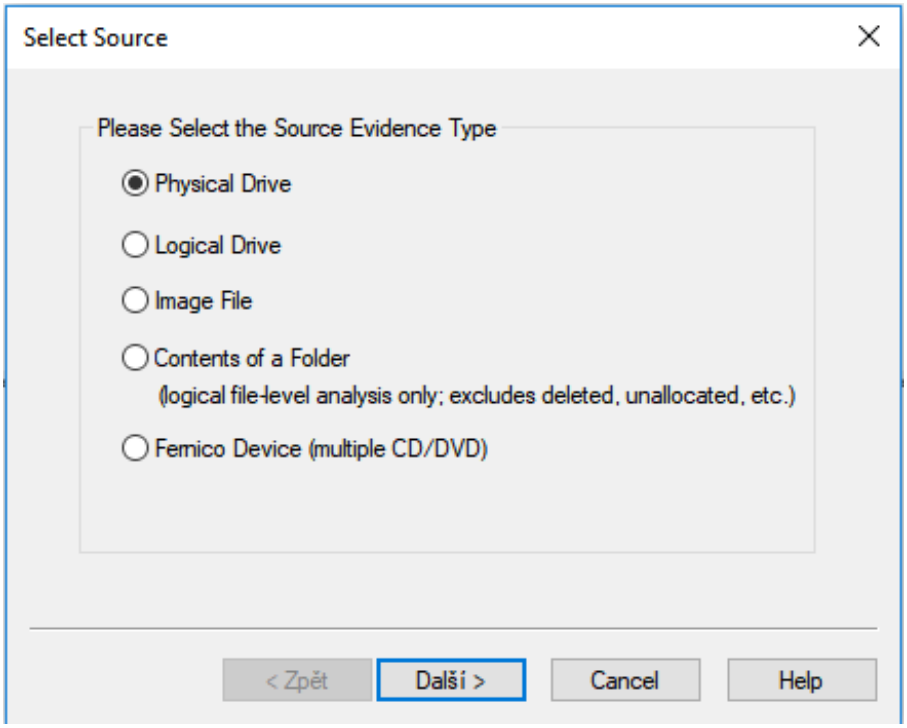
Vytvořte obraz vašeho USB disku ve formátu Raw (dd) a uložte kopii na plochu.

SOUHRN KROKŮ

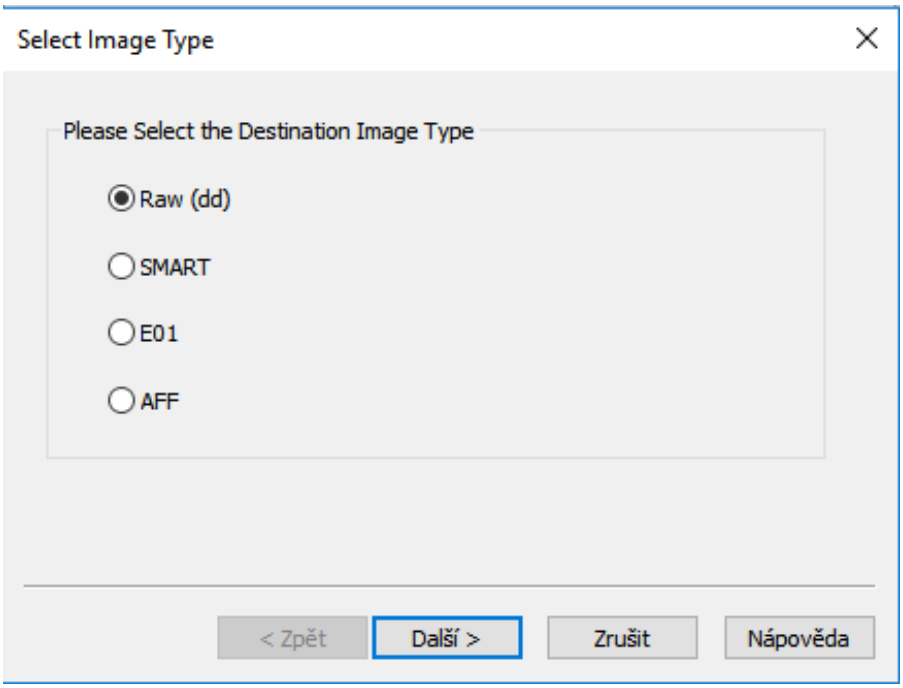
Vyberte File -> Create Disk Image...



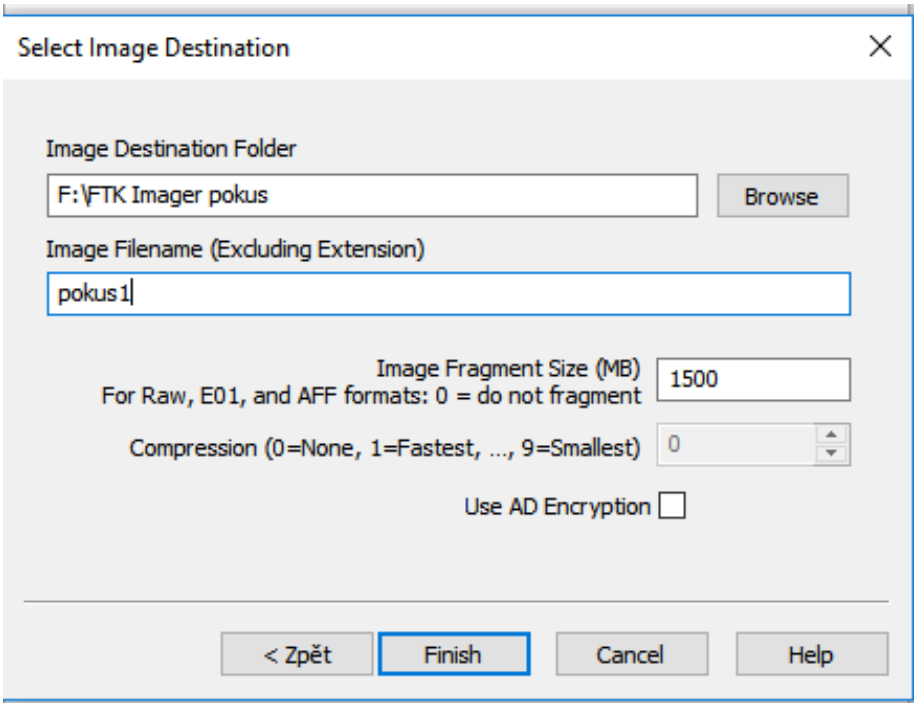
Vyberte Physical Drive



Zvolte umístění image. Jako formát vyberte Raw (dd).

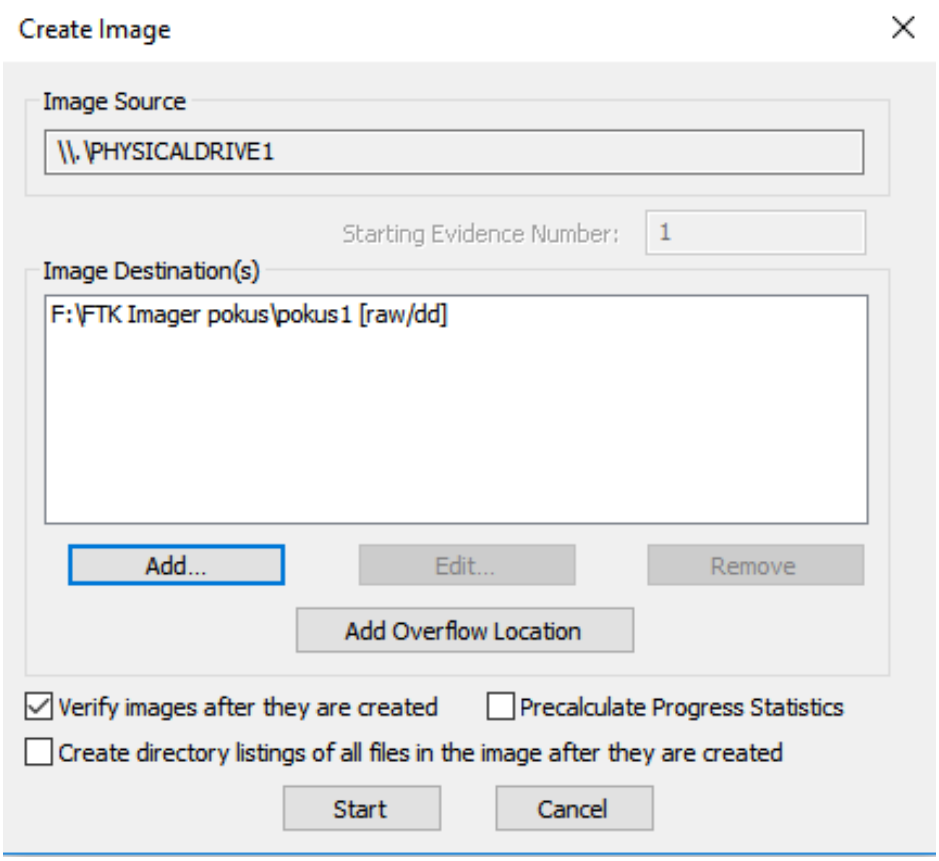


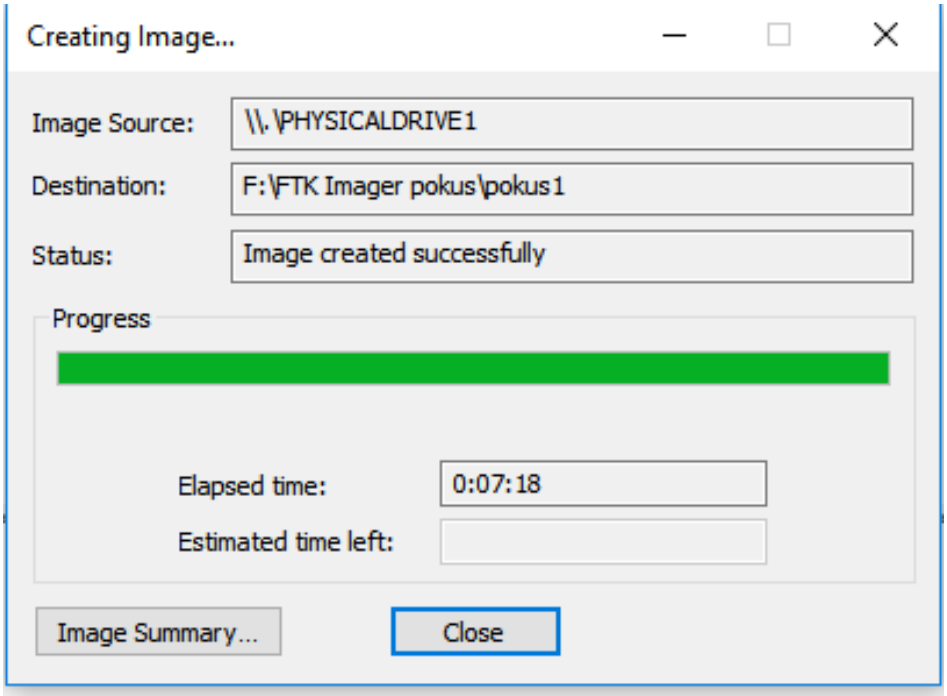
Zvolte cílové umístění a název souboru.



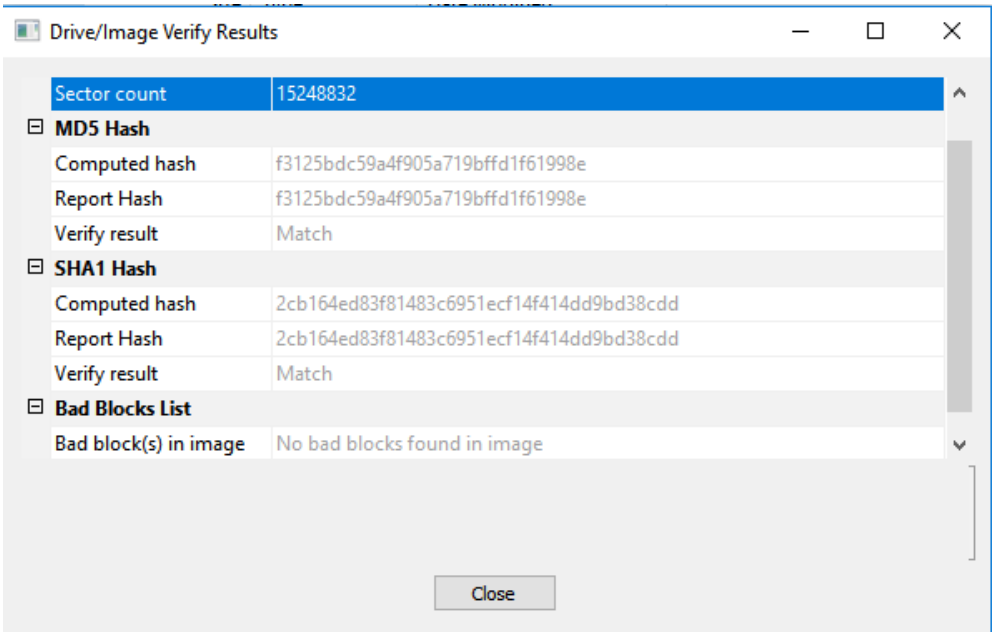
- Příkaz dd: Původně byl zamýšlen pro převod mezi ASCII a EBCDIC. Objevil se poprvé v Unix verze 5. Je specifikován v IEEE Std 1003.1-2008, který je součástí Single UNIX Specification. Může být použit pro mnoho různých účelů. Ve výchozím nastavení čte ze standardního vstupu a zapisuje do standardního výstupu. Toto chování lze měnit pomocí parametrů if (vstupní soubor) a of (výstupní soubor).
- Přípona souboru E01: Znamená formát souboru obrázku EnCase používaný softwarem EnCase. Soubor se používá k ukládání digitálních důkazů včetně obrázků svazků, obrazu disku, paměti a logických souborů. Encase vytváří více souborů E01 jednotné velikosti 640 MB pro ukládání získaných digitálních dat. Jednou z nejvýraznějších vlastností tohoto formátu souboru je to, že pro každý nový soubor E01 se přípona souboru změní pro každý nový soubor, který je vytvořen. Protože EnCase byl původně představen s názvem Expert Witness, soubor E01 může být často označován jako soubory Expert Witness.
- Soubory AFF mají více použití a image Advanced Forensic Format je jedním z nich. Tento formát souboru je používaný pro přesná image disků s kompresí nebo bez ní. Ukládá také související metadata v rámci image disku nebo samostatně. Soubory AFF jsou rozděleny do dvou vrstev. Jedna je vrstva reprezentace disku a druhá vrstva ukládání dat. Vrstva reprezentace disku určuje názvy segmentů a představuje informace o image disku. Vrstva úložiště dat používá k ukládání segmentů XML nebo binární kód. Image disku obsahuje přesnou kopii zařízení podezřelého, kterou mohou soudní znalci analyzovat.

Vytvořte image

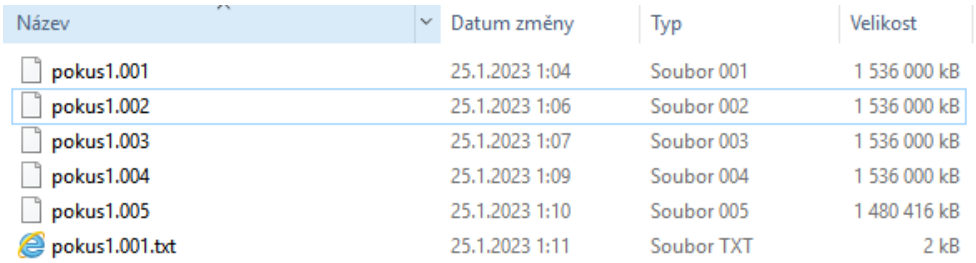




Zkontrolujte hashe



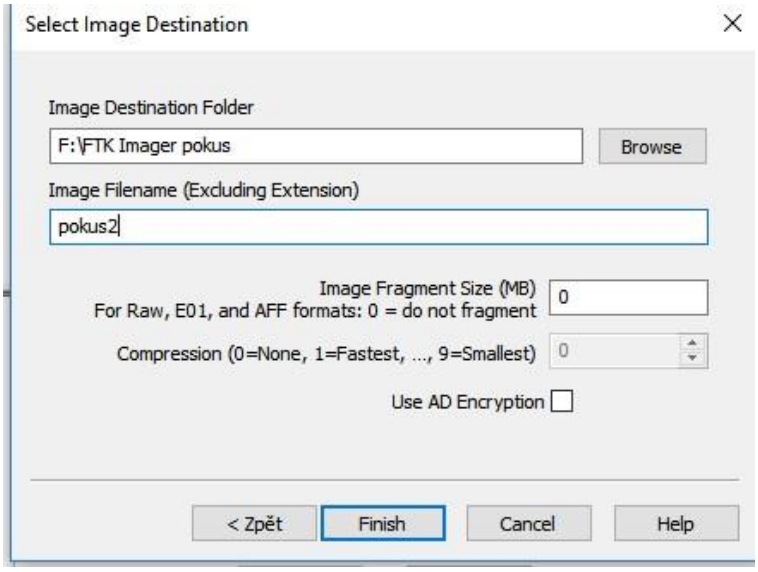
Pokud bude čas mohou žáci udělat více variant



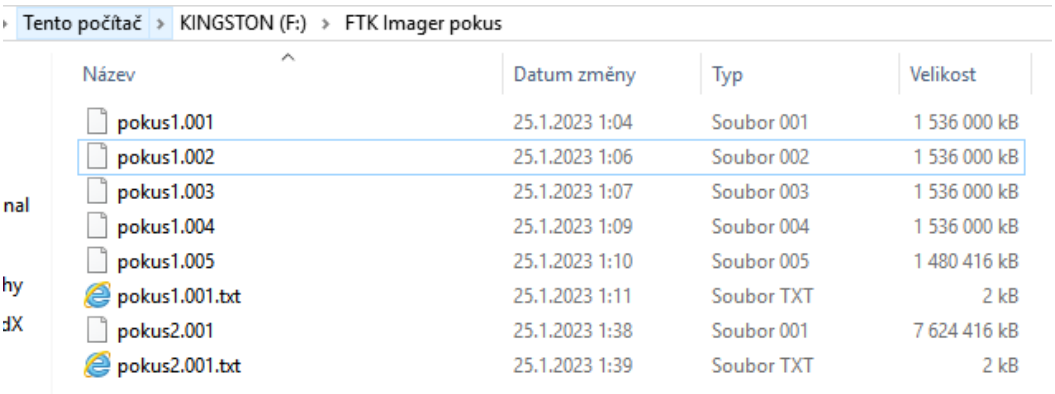
Prohlédněte si obsahy souborů

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 1
Evidence Number: 1
Unique description: 1
Examiner: 1
Notes: 1

---------------------------------------------------------------

Information for F:\FTK Imager pokus\pokus1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 949
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15 248 832
[Physical Drive Information]
 Drive Model: Kingston DataTraveler 2.0 USB Device
 Drive Serial Number: 1ECF66F06559
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7445 MB
 Sector count:    15248832
[Computed Hashes]
 MD5 checksum:    f3125bdc59a4f905a719bffd1f61998e
 SHA1 checksum:   2cb164ed83f81483c6951ecf14f414dd9bd38cdd

Image Information:
 Acquisition started:   Wed Jan 25 01:03:31 2023
 Acquisition finished:  Wed Jan 25 01:10:49 2023
 Segment list:
  F:\FTK Imager pokus\pokus1.001
  F:\FTK Imager pokus\pokus1.002
  F:\FTK Imager pokus\pokus1.003
  F:\FTK Imager pokus\pokus1.004
  F:\FTK Imager pokus\pokus1.005

Image Verification Results:
 Verification started:  Wed Jan 25 01:10:50 2023
 Verification finished: Wed Jan 25 01:11:41 2023
 MD5 checksum:    f3125bdc59a4f905a719bffd1f61998e : verified
 SHA1 checksum:   2cb164ed83f81483c6951ecf14f414dd9bd38cdd : verified
```

Mohou si vyzkoušet kromě defaultní velikosti fragmentace jiné velikosti případně zákaz fragmentace.



Lze diskutovat výhody a nevýhody různých řešení fragmentace: v následujícím případě byla u pokusu1 zvolena defaultní fragmentizace 1350 000 kb a u pokusu2 byla zakázána.



Tento počítač › KINGSTON (F:) › FTK Imager pokus

Název	Datum změny	Typ	Velikost
pokus1.001	25.1.2023 1:04	Soubor 001	1 536 000 kB
pokus1.002	25.1.2023 1:06	Soubor 002	1 536 000 kB
pokus1.003	25.1.2023 1:07	Soubor 003	1 536 000 kB
pokus1.004	25.1.2023 1:09	Soubor 004	1 536 000 kB
pokus1.005	25.1.2023 1:10	Soubor 005	1 480 416 kB
pokus1.001.txt	25.1.2023 1:11	Soubor TXT	2 kB
pokus2.001	25.1.2023 1:38	Soubor 001	7 624 416 kB
pokus2.001.txt	25.1.2023 1:39	Soubor TXT	2 kB

Lze i diskutovat rozdíly v metadatech.

F:\FTK Imager pokus\pokus2.001.txt - Notepad++

Soubor Úpravy Najít Zobrazit Formát Syntaxe Nastavení Nástroje Makro Spustit Pluginy Okna ?

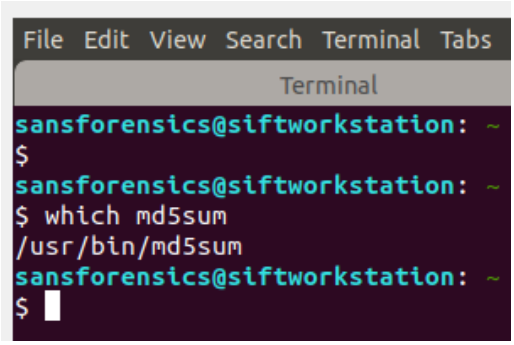
Wi-Fi 3-Aurora.xml | Wi-Fi 3-kongres.xml | test1.py | change.log | skenner.py | sken 1000 portů.txt

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: pokus2
Evidence Number: pokus2
Unique description: pokus2
Examiner: pokus2
Notes: pokus2

---------------------------------------------------------------

Information for F:\FTK Imager pokus\pokus2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 949
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15 248 832
[Physical Drive Information]
 Drive Model: Kingston DataTraveler 2.0 USB Device
 Drive Serial Number: 1ECF66F06559
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7445 MB
 Sector count:    15248832
[Computed Hashes]
 MD5 checksum:    f3125bdc59a4f905a719bffd1f61998e
 SHA1 checksum:   2cb164ed83f81483c6951ecf14f414dd9bd38cdd

Image Information:
 Acquisition started:   Wed Jan 25 01:31:15 2023
 Acquisition finished:  Wed Jan 25 01:38:28 2023
 Segment list:
  F:\FTK Imager pokus\pokus2.001

Image Verification Results:
 Verification started:  Wed Jan 25 01:38:28 2023
 Verification finished: Wed Jan 25 01:39:19 2023
 MD5 checksum:    f3125bdc59a4f905a719bffd1f61998e : verified
 SHA1 checksum:   2cb164ed83f81483c6951ecf14f414dd9bd38cdd : verified
```

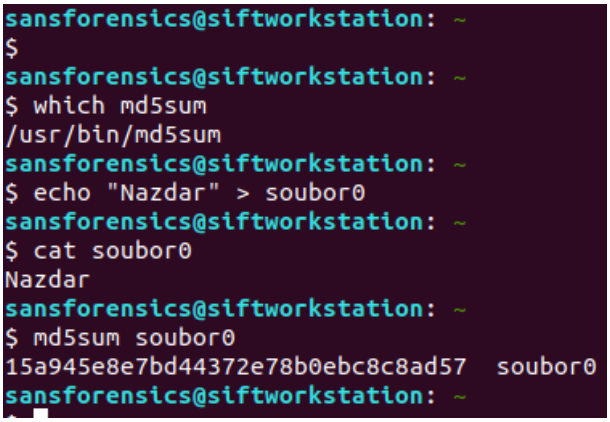
2.2 Práce s md5sum

Než začneme používat md5sum, chceme zjistit, kde je tento soubor umístěn? To je důležité, protože pokud máte dva soubory md5sum[12], jeden z nich je nebezpečný a musíte zjistit, který to je.

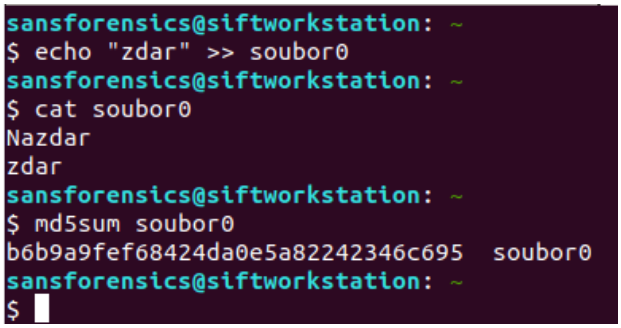
Vytvořme si v adresáři /usr/bin/ nový soubor pro vygenerování md5sum.



Pokud již máte soubor k výpočtu md5sum, pokračujte vytvořením nového souboru s názvem soubor0 a obsahem „Na-zdar“. Pro kontrolu se podívejte na obsah souboru a pak spusťte md5sum a zapamatujte si výsledek.



Poté upravte obsah soubor0, abychom zjistili, zda se MD5 změní nebo ne. Vytvoříme další terminál, abychom mohli porovnávat. Nyní upravíme file0, stačilo by přičíst 1, my doplníme „zdar. Soubor se stále se nazývá soubor0, ale obsah je jiný. Takže udělám md5sum znovu pro soubor0.

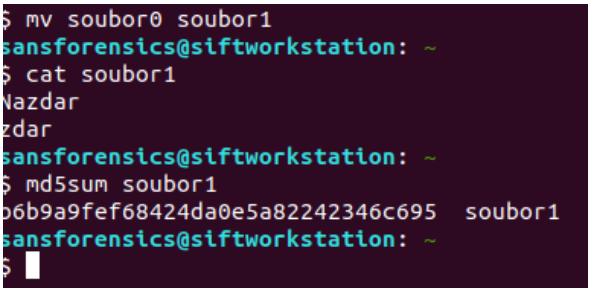


12 md5sum je počítačový program z balíku GNU Core Utilies, založený na kódování a ověřování 128bitové hash funkce MD5.

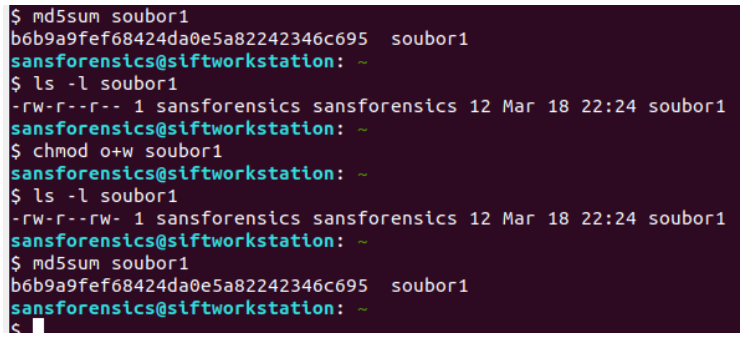
Pojďme porovnat hash. Takže nyní můžete vidět, že dva hashe jsou zcela odlišné, protože jejich obsah je odlišný. Neboli stačí změnit jeden bit obsahu a hash bude úplně jiný.

Takže teď jsme alespoň odpověděli na naši první otázku: Zda změna souboru ovlivní jeho hash. Odpovědí je, že ano.

Dále se podívejme na něco jiného. Například, co když jej přejmenuji, co když změním informace metadat? Přejmenujme tedy soubor0 na soubor1, obsahy souborů jsou shodné. Nyní spustíme md5sum pro soubor1. Hodnota hashe se nezmění, i když se názvy souborů liší – jeden se nazývá soubor0, druhý soubor1, neboli názvy souborů jsou odlišné, ale hash stejný. Důvodem je, že název není uvnitř obsahu a MD5 se dívá pouze na obsah. Jméno je uloženo někde jinde.



Obdobně změna oprávnění nemění obsah, protože informace o povolení se nenacházejí v tomto konkrétním datovém obsahu.



Co se tedy z tohoto jednoduchého příkladu naučíme?

Měli bychom pochopit, že hodnota hash souboru se změní, právě když se změní obsah souboru; proto pokud změníme metadata, například oprávnění, nebo pokud změníme název souboru, nezmění to obsah souboru.

Shrnutí a závěr

Prvních 10 let od svého vzniku bylo zlatým rokem pro počítačovou forenzní techniku. Jak technologie postupuje, počítačová forenzní služba čelí dalším výzvám. Například rostoucí hustota úložiště vyžaduje, abychom vyvinuli nástroje pro rychlé zobrazování. Forenzní analýzu komplikují cloudové výpočty, všudypřítomný disk a jeho šifrování. Použití disků SSD může případně zničit smazaná data, což je jeden z nejdůležitějších zdrojů důkazů ve forenzní analýze.

Seznam použitých zdrojů

(RegRipper 2023) Using OSForensics with RegRipper. PassMark Software. Dostupné z: https://www.osforensics.com/faqs-and-tutorials/using-with-regripper.html

Kurz RITx CYBER502x Computer Forensic. Unit 1: Computer Forensics Fundamentals. Dostupné z: https://learning.edx.org/course/course-v1:RITx+CYBER502x+1T2023/home