Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

Vytvoření forenzní live distribuce Linuxu za použití volně šiřitelných aplikací

Bakalářská práce

Marek Šobra

Školitel: Mgr. Jakub Kothánek

Garant: Ing. Jaroslav Kothánek, Ph.D.

České Budějovice 2017

Bibliografické údaje

Marek Šobra, 2017: Vytvoření forenzní live distribuce Linuxu za použití volně šiřitelných aplikací

[Create a forensics live distribution of Linux using an open source applications. Bc. Thesis, in Czech.] – 40 p. (počet stran), Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic

Anotace

Bakalářská práce je zaměřena na vytvoření forenzní live distribuce Linuxu za použití open source software, tedy takové distribuce, která je způsobilá pro forenzní analýzu a práci s daty. První část je věnována seznámení čtenáře s legislativními problémy a problematikou forenzního zkoumání. V druhé části práce je vysvětlený pojem open source, představen operační systém Linux a základní software použitý v distribuci. Informace o použitém software jsou doplněny obrázky s příkladem použití software.

Klíčová slova:

Legislativa, problematika forenzního zkoumání, Linux, open source software, forenzní live distribuce

Annotation

The thesis is focused on creating a forensics live distribution of Linux using an open source software. Forensics live distribution means a operating systém useable for digital forensics and work with datas. First part is dedicated to legislative issues and issues connected to the digital forensics itself. There is explained a term open source, briefly introduced operating systém Linux and basic software used in the distribution in the second part. Informations about the software are completed with using pictures to demonstrate how did they work.

Keywords:

Legislation, forensics investigation issues, Linux, open source software, forensics live distribution

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě – v úpravě vzniklé vypuštěním vyznačených částí archivovaných Přírodovědeckou fakultou - elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích, dne 18.4. 2017

……

Marek Šobra

Poděkování

Rád bych využil této možnosti k poděkování všem mým blízkým za podporu během studia i mimo ni a panu Mgr. Jakubu Kothánkovi za ochotu, se kterou ke mně přistupoval během realizace této práce.

Obsah

1. Úvod

Již od doby, kdy se počítače zmenšily do podoby tzv. osobních počítačů, je možné setkat se s kriminalitou v oblasti výpočetních technologií. Zpočátku se jednalo zejména o trestné činy, které byly spojené pouze s informačními technologiemi a zřídkakdy se mísily s případy tzv. obecné kriminality. Ovšem technologický pokrok v této oblasti zapříčinil rozšíření počítačů do každé domácnosti, rozšíření sítě internet a propojení počítačů po celém světě. Tím se zjednodušila dálková komunikace mezi dvěma subjekty. Rozšířily se tak legislativní prohřešky o porušování autorských práv, pomluvy prostřednictvím sociálních sítí, ale i šíření dětské pornografie nebo terorismus. S rozšířením datových kapacit paměťových médií se zároveň pozměnil způsob archivace dat a většina informací se postupně uchovává v elektronické formě.

S další revolucí v oblasti mobilních telefonů se objem komunikace přenášené v digitální podobě opět znásobil a promítnul do našich každodenních životů. Navíc z podstaty mobilního telefonu a jeho užívání v dnešní době se digitální stopy promítnuly do téměř každého trestného činu.

Z toho vyplývá, že informační kriminalita se nevyskytuje pouze v případech jasně spojených s informačními technologiemi, ale objevuje se v každodenním životě. Nepromítá se pouze do vyšetřování trestné činnosti bezpečnostními složkami, ale stala se součástí pracovně-právních a občansko-právních sporů, během kterých je možné naleznout zkoumáním digitálních technologií veliké množství relevantních informací.

Požadavky na boj s tímto odvětvím kriminální činnosti budou daleko přísnější, bude na něj kladen daleko větší důraz a bude požadována daleko větší přesnost zkoumání dat.

2. Obecný úvod do problematiky

Stopa v kriminalistice značí jakoukoliv změnu na místě, kde se odehrál trestný čin. Kriminalistické stopy nám poskytují informace o samotném spáchaném trestném činu nebo jiné události, tzv. kriminalisticky relevantní události, ze kterých získáváme informace k vyšetření trestného činu. Zajištění stop, jakožto důkazů patří ke stěžejním úkonům každého oboru kriminalistiky. Bez nich nelze trestné činy vyšetřovat. Vyhledání, zajištění, zdokumentování a vyhodnocení těchto stop by nám mělo poskytnout odpovědi na základní kriminalistické otázky. Kdo? Co? Kdy? Kde? Jak? Čím? Proč [1]?

2.1 Digitální stopy

Každé zařízení, které získává, uchovává, předává, nebo zpracovává data, zanechává o své činnosti záznamy. Takové záznamy jsou z kriminalistického hlediska stopa. Digitální stopa je jakákoliv informace s vypovídající hodnotou, uložená nebo přenášená v digitální podobě.

Abychom mohli stopy řádně zkoumat, musejí se i důkladně zajistit a zdokumentovat. Mezi digitálními stopami platí toto pravidlo dvojnásob. Zatímco v jiných oborech jsou dané postupy a pravidla zajištění, zde tomu tak není. Způsob zajištění závisí pouze na expertovi pověřeným touto činností. Samozřejmě i u digitálních stop jsou nějaké doporučené postupy, ale ty nelze aplikovat vždy a na každý případ. Připomeňme si základní poučky o zajištěné stopě – s tou by nemělo být manipulováno, neměla by být modifikována, měla by být zajištěna celá. Díky moderním výdobytkům technologie, jako je vzdálená správa, různé metody šifrování dat, ale už i ze samotné podstaty fungování počítačů, je zajištění všech těchto kroků celkem obtížné až nemožné.

Celý proces zajištění digitálních stop probíhá za předpokladu, že tyto stopy budou před soudními orgány akceptovány jako důkaz, proto musí být celý proces přiměřený a legální pro práci s důkazním materiálem. Nejčastěji jsou stopy zajišťovány orgány činnými v trestném řízení podle trestního řádu nebo dalšími legálními způsoby. Jedná se hlavně o tyto úkony: domovní prohlídka, osobní prohlídka, prohlídka jiných prostor a pozemků, vydání nebo odnětí věci, ohledání místa činu, zajištění dat z internetu.

2.2 Legislativní stránka věci

Orgány činné v trestním řízení mají dané zákony a postupy, kterými se musí řídit při vymáhání práva a zajišťování digitálních stop. Pro tyto účely slouží trestní řád, tj. zákon

141/1961 Sb. V tomto zákoně se uvádí, že zajištění digitálních stop lze provádět během uskutečnění domovní prohlídky, prohlídky jiných prostor a pozemků dle § 82, dále během osobní prohlídky či dobrovolným vydáním nebo odnětím věci podle § 78 a § 79 trestního řádu [2].

S postupným vývojem a rozšířením nejen telekomunikační techniky jakou jsou mobilní telefony a tablety, ale i přenosných paměťových zařízení, se stalo neméně důležité zajištění digitálních stop na místě spáchání trestného činu jako je vražda a jiné. I data z těchto zařízení mohou vést k odhalení pachatele.

2.2.1 Domovní prohlídka, prohlídka jiných prostor a pozemků

Tyto zákroky se řídí ustanovením § 82 trestního řádu. Jak je uváděno v prvním odstavci „Domovní prohlídku lze vykonat, je-li důvodné podezření, že v bytě nebo v jiné prostoře sloužící k bydlení nebo v prostorách k nim náležejících (obydlí) je věc nebo osoba důležitá pro trestní řízení“ [2].

Příkaz k domovní prohlídce uvádí § 83 a § 83a. „Nařídit domovní prohlídku je oprávněn předseda senátu a v přípravném řízení na návrh státního zástupce soudce. V neodkladných případech tak může namísto příslušného předsedy senátu nebo soudce (§ 18) učinit předseda senátu nebo soudce, v jehož obvodu má být prohlídka vykonána. Příkaz k domovní prohlídce musí být vydán písemně a musí být odůvodněn. Doručí se osobě, u níž se prohlídka koná, při prohlídce, a není-li to možné, nejpozději do 24 hodin po odpadnutí překážky, která brání doručení“ [2].

Domovní prohlídku lze provést také bez příkazu, ovšem pouze tehdy, pokud „vydání příkazu nelze předem dosáhnout a věc nesnese odkladu. Policejní orgán je však povinen si bezodkladně dodatečně vyžádat souhlas orgánu oprávněného k vydání příkazu; v přípravném řízení tak činí prostřednictvím státního zástupce“ [2]. Pokud dodatečný souhlas nebude schválen, „nelze výsledky prohlídky použít v dalším řízení jako důkaz“ [2]. Další možnost prohlídky bez příkazu nastává tehdy, pokud uživatel dotčených prostor písemně prohlásí, že s prohlídkou souhlasí a své prohlášení předá policejnímu orgánu. Ten však musí „bezodkladně vyrozumět předsedu senátu oprávněného k vydání příkazu a v přípravném řízení státního zástupce“ [2].

V odvětví kriminalistiky zaměřené na zajištění digitálních stop a důkazů hraje enormní roli důkladná příprava těchto zákroků. Vzhledem ke všem možným způsobům

úpravy a mazání dat po síti, možnosti uložení dat na různá zařízení, šifrování pevných disků, je důležité znát ke komu, kde, kdy a z jakého důvodu se bude konat domovní prohlídka. Dále je dobré znát, jaká data se budou zajišťovat.

Ke komu znamená, že nás zajímají jaké znalosti a zkušenosti s počítači ona osoba má, na jaké druhy zabezpečení dat se můžeme připravit. Je totiž velmi rozdílné, zdali se bude prohledávat byt účetní, která je podezřelá z ekonomických trestných činů a její očekávané schopnosti při práci s počítačovým systémem jsou práce s účetními programy, e-mailovým klientem a „brouzdání po internetu“. U takového případu se nepředpokládá šifrování disku, či vzdálená správa počítače a smazání důležitých dat pro trestné řízení během provádění domovní prohlídky.

Na druhou stranu, pokud bude osoba znalá a bude mít zařízená výše zmíněná bezpečností opatření, může nás jakákoliv překážka a zpoždění při zajištění dat stát tyto data, a tím pádem i důležité důkazy pro onen případ. S tímto bodem úzce souvisí i z jakého důvodu se prohlídka bude konat.

Kam, znamená udělat si přehled o prostorech, ve kterých se bude prohlídka odehrávat a získat informace, jaká se tam nachází topologie sítě, kolik zařízení pro zajištění dat můžeme očekávat. Rozmístění techniky, odbornost personálu, bezpečnostní technologie. Tyto informace jsou pro kriminalisty důležité kvůli způsobu provádění prohlídky a kolik specialistů je potřeba pro zajištění dat. Zároveň si kriminalista udělá odhad datové kapacity, protože pokud v objektu se 30 počítači bude data zajišťovat pouze jedna osoba, patrně bude zajištění trvat velmi dlouho a pokud se nezamezí přístupu počítačům k síti, je vysoká pravděpodobnost, že někdo může smazat důležitá data v některém z počítačů.

Povědomí o tom jaká data budou zajišťována, může výrazně snížit dobu konání prohlídky. Zároveň je možné zajištění experta v daném oboru [3].

2.2.2 Osobní prohlídka

Osobní prohlídka je další úkon, během kterého lze zajistit zařízení s digitálními stopami. Typickým příkladem je mobilní telefon. O právní úpravu se stará § 82-85a trestního řádu. „Osobní prohlídku lze vykonat, je-li důvodné podezření, že někdo má u sebe věc důležitou pro trestní řízení“ [2]. „U osoby zadržené a u osoby, která byla zatčena“ [2] lze vykonat osobní prohlídku i pokud existuje podezření, „že má u sebe zbraň nebo jinou věc, která by mohla ohrozit život či zdraví, ať vlastní nebo cizí“ [2].

„Nařídit osobní prohlídku je oprávněn předseda senátu a v přípravném řízení státní zástupce. S jeho souhlasem i policejní orgán“ [2].

Bez příkazu nebo souhlasu státního zástupce může policejní orgán vykonat osobní prohlídku pouze, pokud příkazu či souhlasu nelze předem dosáhnout a věc nesnese odkladu. Výjimka nastává v případě, že se jedná o osobu přistiženou při činu, o osobu na kterou byl vydán příkaz k zatčení nebo v případě uvedeném v prvním odstavci.

V trestním řádu je dále uvedeno, že osobní prohlídka musí být vykonána osobou stejného pohlaví [2].

2.2.3 Vydání a odnětí věci

Tento úkon se řídí dle § 78 trestního řádu. „Vyzvat k vydání věci je oprávněn předseda senátu, v přípravném řízení státní zástupce nebo policejní orgán“ [2].

„Kdo má u sebe věc důležitou pro trestní řízení, je povinen ji na vyzvání předložit soudu, státnímu zástupci nebo policejnímu orgánu“ [2]. V případě, že je nutné onu věc pro účely trestního řízení zajistit, je povinen věc na vyzvání těmto orgánům vydat. Při vyzvání je nutné upozornit ho, že pokud nevyhoví výzvě, může mu být věc odňata. Z nevyhovění výzvě plynou i jisté následky, kterými se zaobírá § 66 [2].

Pokud osoba negativně zareaguje na výzvu k vydání věci, může mu být odňata dle § 79, tj. na příkaz předsedy senátu, v přípravném řízení státního zástupce nebo policejního orgánu. Policejní orgán potřebuje předchozí souhlas státního zástupce. Může dojít k odnětí věci i bez předchozího souhlasu státního zástupce, ovšem pouze v případě, kdy ho nelze dosáhnout a věc nesnese odkladu.

Pokud je možnost, k odnětí věci se přibere osoba, která není na věci zúčastněna. O vydání a odnětí věci se vypracuje protokol, který musí obsahovat dostatečně přesný popis věci tak, aby umožnil určit její totožnost. Osobě, která věc vydala nebo jí byla odňata, se ihned předá písemné potvrzení o převzetí nebo opis protokolu [2].

2.2.4 Ohledání místa činu

Ohledání místa činu je obecně velmi významný druh ohledání. Tento úkon je svázán s § 158 a § 113 trestního řádu. Místo činu je prostor, ve kterém se odehrál akt protiprávního jednání a je tak místem trestné činnosti pachatele. Nemusí to však být výhradně místo

spáchání trestného činu, ale také místo, které pachatel nebo další osoby zúčastněné pozměnil nebo pozměnily svým jednáním.

Ohledání má svá pravidla a platná tvrzení jako jsou neopakovatelnost, nezastupitelnost, neodkladnost a je tak nutné zamezit možnému úmyslnému nebo nedbalostnímu zničení stop. Jelikož každé místo činu je svým způsobem jedinečné, váže se k tomu i více metod ohledání. Tato metoda může být koncentrická, při které se místo činu ohledá ve spirále od kraje ke středu nebo excentrická, při které se ohledává od středu ke kraji [1].

3. Příprava před zajištěním digitálních stop

3.1 Získání údajů o IT technologiích

Získání informací o systémech, které se na místě zajištění mohou vyskytovat, je velmi důležitým bodem pro kriminalisty nebo znalce, kteří na místě činu techniku zajišťují. Ti by si měli udělat představu o rozmístění techniky v objektu, zvlášť pokud se prohlídka koná např. ve větším, průmyslovém objektu. S tím souvisí rychlost zajištění a počet policistů potřebných k provedení prohlídky.

Velmi důležitý je přehled o počtu zařízení, odhadované datové kapacity a provozovaném software. Technici tak mají možnost připravit si veškerá zařízení a prostředky pro zajištění různých technologií, tím se vyvarují dalšímu nežádoucímu zdržení při zajišťování. Znalost struktury počítačové sítě umožní její případné odpojení a lze tak zabránit nežádoucí modifikaci dat. Často bývají přístupové body k internetu ukryté v jiném objektu, např. v bytě sousedů. Příkaz k prohlídce se tím pádem na tato zařízení nevztahuje. Pokud vyšetřovatelé s tímto počítají, mají možnost se náležitě připravit a vyvarovat se tak nepříjemnostem vzniklým na místě a jejich následnému řešení.

V neposlední řadě je důležité zjistit maximum o odbornosti případného personálu v objektu nebo pachatele o používaných bezpečnostních technologiích, které znemožní rychlé a důkladné zajištění, případně o používaných kryptografických prostředcích [3].

3.2 Vyhodnocení včasnosti úkonů

Vzhledem k podstatě digitálních stop, jejich vytváření, modifikace či mazání, může dojít velmi snadno a velmi rychle k jejich ztrátě. Nemluvíme pouze o úmyslném jednání, ale tyto nežádoucí stavy nastávají i běžným užíváním výpočetních technologií či nedbalostním zacházením.

Tento krok závisí na zkušenostech soudního znalce nebo technika policejního orgánu, protože nejsou přesně dané metodiky jak v takových okamžicích postupovat. Pomoci v rozhodování by měla právě příprava kroků zmíněných v předchozí kapitole [3].

3.3 Poučení soudního znalce, technika OKTE s důležitými informacemi o vyšetřování

Seznámení specialistů na zajišťování dat s těmito informacemi vede k lepšímu posouzení, jaká data se budou zajišťovat a jakým způsobem.

Pokud jsou odborníci poučeni, mohou se předem připravit na případ a touto cestou se dají výrazně snížit jak náklady vynaložené na potřebné technické vybavení, tak čas potřebný k zajištění a vyhodnocení dat. Všechny tyto aspekty přispějí k brzkému podání znaleckého posudku a posunu vyšetřování [3].

3.4 Zohlednění dopadů postupů na firmy a organizace

Firmy jsou mnohokrát závislé na funkčnosti výpočetní techniky, zejména pokud se jedná o e-shopy a jejich servery. Finanční ztráty se mohou v některých případech vyšplhat za krátkou dobu do velmi vysokých částek. Vyhodnocení těchto dopadů je pro ně hodně důležité.

Tyto aspekty vyvolávají tlak na odborníka zajišťujícího techniku, zdali se technika zajistí a následné zajištění bitové kopie proběhne až na pracovišti soudního znalce nebo policejního orgánu. Další možností je provedení zkoumání na místě, které umožní firmě dřívější zprovoznění systémů. Pokud je zvoleno znalecké zkoumání na místě, je nutné zajistit přítomnost soudního znalce [3].

3.5 Příprava potřebného technického vybavení

Celá třetí kapitola pojednává o důkladné přípravě na zajištění dat. Všechny tyto kroky se provádí kvůli základnímu požadavku na zkoumaná data, kterým je zajištění jejich integrity. Integrita je stav, kdy data zajištěná jsou shodná s daty přečtenými (tj. s totožnými daty, která jsou na zkoumaném zařízení).

V první řadě hraje roli odhad množství dat, jaké se může na místě vyskytovat. Adekvátně k tomuto odhadu si musí technici připravit potřebné počty datových uložišť tak, aby v případě zajištění dat na místě bylo možné provést bitovou kopii všech potřebných objektů.

Kvůli zajištění digitálních stop na místě je nutné mít s sebou technologické prostředky, které jsou speciálně navržené pro práci s daty tak, aby bylo možné tato data využít v trestním řízení. Jedná se o tzv. hardwarové blokátory nebo duplikátory, které umožní vytvořit bitovou kopii dat bez zásahu do dat původních. Další možností je použití forenzní live distribuce Linuxu. Ta se načte pouze do operační paměti počítače a nehrozí tak modifikace dat na datovém úložišti.

Všechny zajišťované objekty musí být zabezpečené proti neautorizované manipulaci. Toho se dosáhne pomocí uložení, zabalení a zapečetění zařízení do vhodných obalů.

Samozřejmostí je uložit tato zařízení tak, aby nedošlo k jejich poškození. K tomu se používají bezpečnostní sáčky ORGATECH, silné plastové neprůhledné pytle, lepenkové krabice (lze použít i původní obaly od výrobce) a bezpečnostní plomby [3].

4. Základní pojmy

4.1 Linux

Linux je podobně jako Windows 7, Windows 8, Windows 10 či Mac OS X označován za operační systém, ovšem správně by měl být označován GNU/Linux. Původně jako Linux bylo označováno jádro tohoto operačního systému.

Operační systém je software, který řídí přidělování hardwarových zdrojů softwaru v našem počítači. V podstatě zprostředkovává komunikaci mezi software a hardware. Tento operační systém se skládá z mnoha komponent.

Těmi jsou např. zavaděč - software, který řídí spouštěcí proces počítače, dále jádro – hlavní program počítače, který je spuštěný od zapnutí až po vypnutí počítače. Hlavními funkcemi jádra je přidělování procesoru jednotlivým procesům, přidělovaní paměti programům a řízení vstupně/výstupních zařízení připojených k počítači. Mezi tyto komponenty se ještě řadí tzv. daemons, neboli služby, které nejsou v přítomném kontaktu s uživatelem. Většinou se jedná o služby běžící na pozadí jako zvuk a tiskové fronty. Jinou komponentou je Shell (Bash), tedy příkazová řádka systému, která umožňuje ovládat počítač skrze příkazy zadávané do textového rozhraní. Dalším dílem celku je pracovní prostředí, což je prostředí, se kterým uživatel komunikuje. Právě u Linuxu jich je na výběr mnoho (Unity, GNOME, Cinnamon, Enlightenment, KDE, XFCE, LXDE, atd.) Poslední komponentou jsou aplikace, kterými si uživatel dotváří prostředí k obrazu svému.

Vývojářské týmy kombinací těchto komponent vytvářejí tzv. distribuce, tedy konkrétní verze operačního systému. Těchto distribucí je mnoho variant (Ubuntu, CentOS, Mandriva Linux, Debian, Slax, Linux Mint, Knoppix, Fedora, Lubuntu a další) a závisí pouze na každém, jakou si vybere. Všechny tyto systémy mají ale společné jádro, tedy samotný Linux [4, 5].

Největšími klady tohoto systému jsou flexibilita, modernost, evolučnost a svobodnost. Linux je flexibilní, protože může být nasazen na superpočítačích, ale i např. na síťovém prvku či strojku na jízdenky. Moderní, protože nejnovější technologie, protokoly, algoritmy atd. se v linuxovém jádře objevují velmi brzy. Evoluční, protože změny jsou prováděny na základě požadavků uživatelů či diskuzích na veřejném fóru. Svobodný, protože na základě licenčního ujednání může kdokoliv jádro studovat, upravovat, případně nové funkce přidávat a následně pak takové upravené jádro šířit dál [5].

4.2 Open source software

4.2.1 Co je open source software?

Pojmem open source označujeme takový software, jehož zdrojový kód je veřejně dostupný, upravitelný a ve většině případů volně šiřitelný. Zdrojový kód je část programu, kterou většina uživatelů nikdy neuvidí. Právě on zajišťuje, jak daná aplikace pracuje. Programátoři, kteří získají přístup ke zdrojovému kódu, mohou ovlivnit chování aplikace. Mohou ji také rozšířit o nějaké funkce, případně opravit části, které ne vždy pracují správně [6, 7].

4.2.2 Proč je dobré využívat open source?

Kontrola. Uživatelé mají větší přehled o aplikacích, které používají. Mohou prozkoumat zdrojový kód a ujistit se, že program nevykonává žádnou nechtěnou akci, případně si ho mohou upravit tak, aby ji nadále nevykonával.

Bezpečnost. Spousta lidí upřednostňuje open source software, protože ho považují za bezpečnější a stabilnější než software proprietární, tedy takový, ke kterému má přístup pouze vývojář/firma. Takovýto přístup je možný, jelikož si může zdrojový kód prohlédnout kdokoliv, a opravit chybu, kterou mohl původní autor přehlédnout. Zároveň je tento přístup také mnohem rychlejší, neboť ostatní vývojáři nepotřebují povolení od originálních autorů. Samozřejmostí je i možné zneužití otevřeného kódu a využití chyb ve prospěch osoby, která chce ostatním uživatelům uškodit, ale předpokládá se, že „uživatelská strana“ má větší prostředky (především lidské zdroje) pro zachování bezpečnosti aplikace.

Stabilita. Otevřenost zdrojového kódu přináší v této oblasti dlouhodobou podporu, vývoj a aktualizace. Pokud se původní vývojáři přestanou zabývat určitým projektem, bývá pravidlem, že se v rámci komunity najdou zástupci, kteří pokračují v dalším vývoji aplikace [6, 7].

4.3 Live distribuce

Toto označení se používá pro takový operační systém, který je uložený na externím médiu a dle potřeby může být použit na různých systémech. Takové externí médium se nazývá bootovací. Dříve se v této oblasti uplatňovaly hlavně paměti CD-ROM, později s nárůstem velikosti operačních systémů a programům k nim připojeným se začaly využívat DVD. Dnes je běžnou praxí používání zařízení typu USB Mass Storage, jakými jsou třeba externí disky nebo flash disky.

Bootovatelné médium umožňuje zavedení distribuce a následného spuštění aplikací bez jakékoliv potřeby instalace systému do pevné paměti, ale např. do paměti RAM. V podstatě jde takto uložit jakýkoliv operační systém, ovšem nejčastěji se setkáme s operačními systémy postavenými na linuxovém jádře.

Tento způsob spouštění je vhodný pro uživatele, kteří si chtějí vyzkoušet jakýkoliv operační systém bez potřeby jeho instalace. Vyhovuje i potřebám forenzních znalců, kteří při své práci kladou důraz na to, aby s důkazními daty bylo co nejméně manipulováno [8].

5. Forenzní live distribuce Linuxu

5.1 Lubuntu

Jako operační systém jsem zvolil distribuci Linuxu zvanou Lubuntu. Lubuntu vychází z distribuce Ubuntu vystavěné v prostředí LXDE se snahou vytvořit úspornější a rychlejší verzi operačního systému.

Hlavním důvodem zvolení této distribuce byla nenáročnost tohoto systému. Webová stránka ubuntu.com uvádí, že je možné spustit systém s dnes již pouhými 128 MB operační paměti, procesorem o frekvenci 233 MHz a 1,5 GB volné paměti na pevném disku. Tyto nároky by měli zajišťovat možnost spuštění distribuce dnes již na jakémkoliv počítači [9].

Distribuce je postavená na verzi Lubuntu 16.04 LTS.

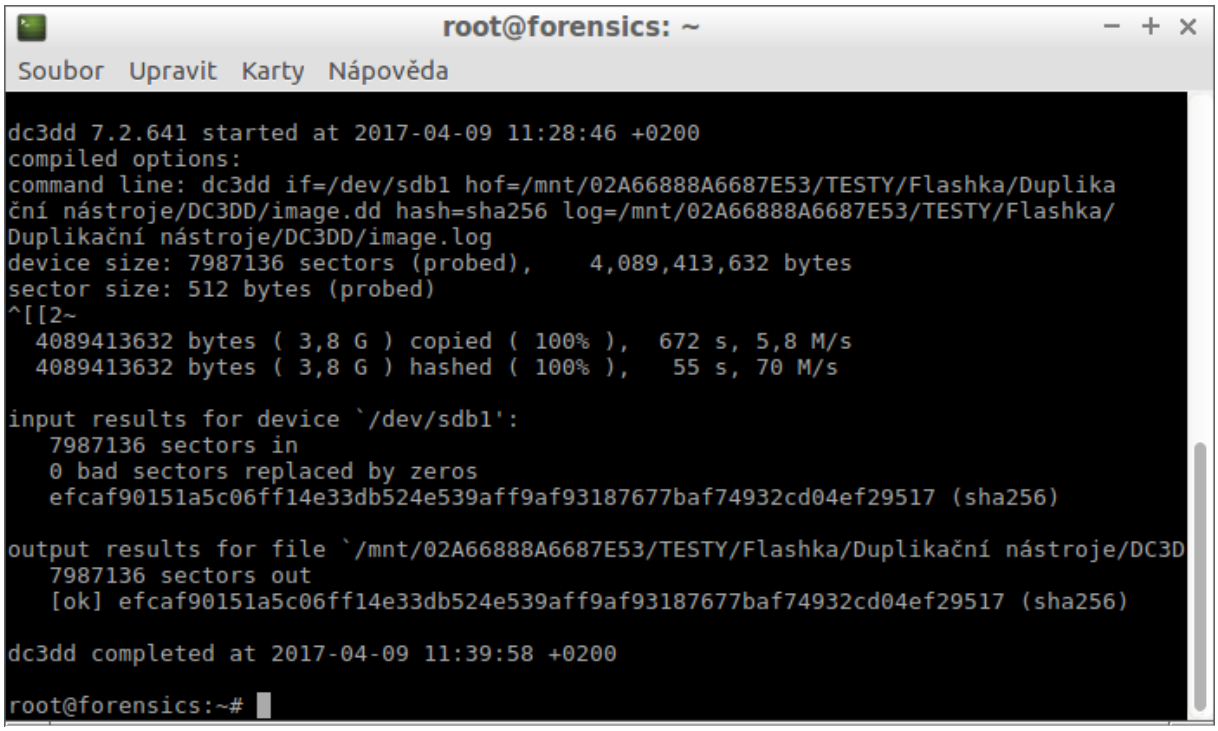
5.2 Duplikační nástroje

5.2.1 Dc3dd

Jedná se o vylepšení staršího programu dd, který je nejstarší používaný nástroj pro duplikaci disků. Ačkoliv jeho funkcionalita vyžaduje minimální prostředky, postrádá některé funkce, které jsou dostupné v modernějších duplikačních nástrojích. Mezi ně patří např. získávání metadat nebo tzv. „user-friendly“ rozhraní. Navzdory výše zmíněným nedostatkům je dc3dd (Obr. 1) stále oblíbený a použitelný pro potřeby forenzní analýzy, ale i pro vytvoření zálohy uživatelských dat.

Na druhou stranu za běhu zobrazuje postup programu, umožňuje rozdělit výslednou kopii do pevně určených částí a ovládá tzv. „piecewise hashing“. Piecewise hashing vychází z předpokladu, že pokud jsou byty části souboru přepsány, je ohrožena integrita pouze té části. Ostatní, nezměněné části, by měly být použitelné k prokázání jejich integrity. Tento program je volně dostupný a bývá součástí téměř všech distribucí OS Linux.

Další výhoda je v možnosti využít spouštěcích parametrů a při běhu programu vypočítat kontrolní součet zajišťovaného média i vytvářeného obrazu a tyto haše porovnat. Použitelné algoritmy jsou MD5, SHA-1, SHA-256 a SHA-512. Tímto krokem tak vytvoříme bitovou kopii a zároveň zajistíme její integritu [10].



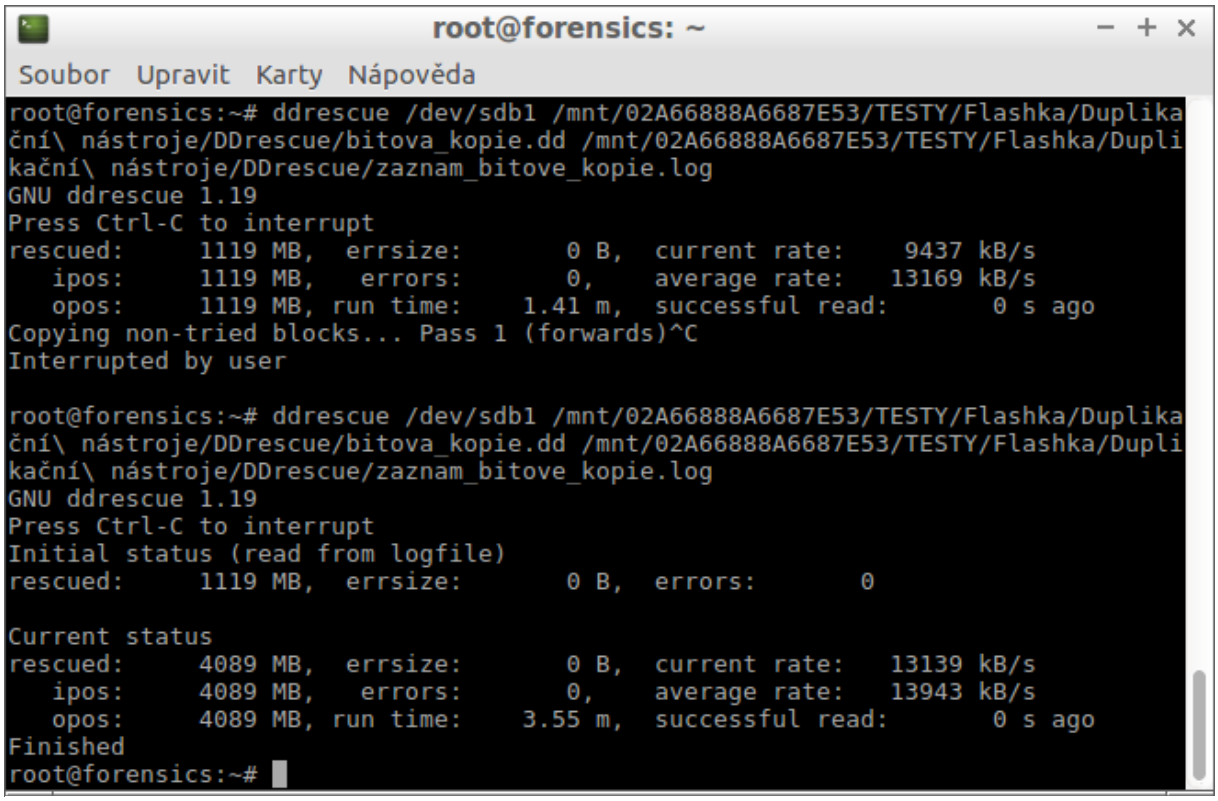
Obrázek 1 - Ukázka příkazu dc3dd. Vytvoření bitové kopie a porovnání kontrolní sumy originálních dat a jejich obrazu.

5.2.2 Ddrescue

Jedná se o další open source software, který je použitelný pro potřeby forenzní duplikace disku. Kopíruje data z oddílu disku na jiné paměťové médium. Ddrescue je optimalizováno tak, aby bylo schopné přečíst data i z poškozených médií, kde jiné duplikační nástroje selhávají a ukončují kopírování.

Základní princip jeho funkce je takový, že při prvním běhu programu zkopíruje data, která jsou lehce dostupná. V případě výskytu chyby ji zaznamená do logového souboru tzv. mapfile a daný úsek vynechá. K vynechané části se po dokončení prvního běhu vrací a postupně ji dělí na menší úseky. Tímto způsobem je schopný vykopírovat velké množství dat.

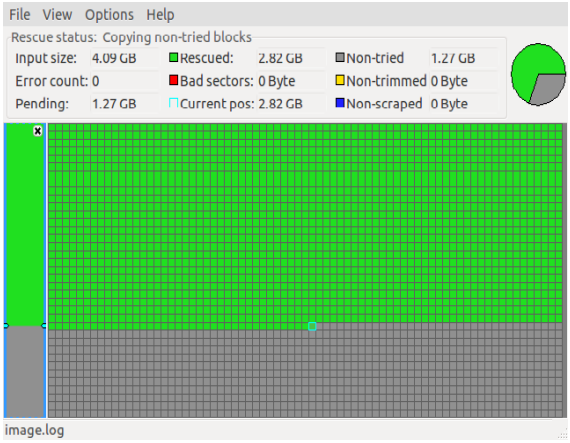
S pomocí mapfile lze také kopírování přerušit (Obr. 2) a později na něj navázat v momentě přerušení [11, 12].



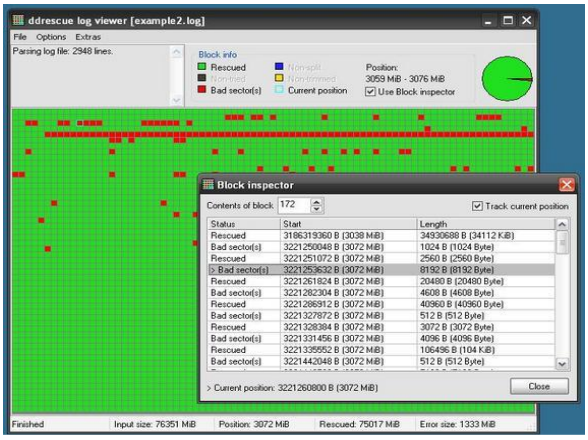
Obrázek 2 – Počátek spuštění bitové kopie, přerušení uživatelem a následné pokračování v kopírování za pomoci souboru zaznam_bitove_kopie.log

5.2.2.1 Ddrescueview

Ddrescueview je grafický interpret souboru mapfile. Pomocí souboru *.log vytvořeným při spuštění duplikace je možné sledovat postup klonování (Obr. 3) za běhu nebo po skončení duplikace a prohlédnout si tak její průběh. Zobrazuje například počet špatných sektorů (Obr. 4) a oblasti, ve kterých se nacházejí.



Obrázek 3 – Grafický náhled na průběh duplikace.



Obrázek 4 – Zobrazené poškozené sektory zajišťovaného média[13].

5.2.3 Guymager

Guymager je klonovací nástroj s grafickým rozhraním přívětivým pro uživatele. Prostředí je velmi intuitivní a tudíž jednoduché na ovládání. Výhodou je, že pro zajištění kopie nemusí být zařízení ani namountováno, takže nehrozí náhodné zapsání dat na zkoumané médium.

Program nabízí dva způsoby zajištění dat. Buďto zajištění ve formátech dd/EWF/aff, které jsou uzpůsobené pro další zkoumání nebo „klon“ vzorového zařízení, čímž nám vznikne naprosto totožné médium.

Před spuštěním klonování umožňuje Guymager zvolit možnost hašovací funkce MD5, SHA-1 nebo SHA-256 a zajistit tak porovnání haše originálních dat s daty vytvořenými klonováním. Tyto informace společně s dalšími umisťuje do logového souboru (Obr. 5) obsahující tzv. metadata [14, 15].

```
Acquisition
==========

Linux device          : /dev/sdb
Device size           : 4089446400 (4,1GB)
Format                : Linux dd raw image - file extension is .dd
Image path and file name: /mnt/02A66888A6687E53/TESTY/Flashka/GUYMAGER/obraz.dd
Info  path and file name: /mnt/02A66888A6687E53/TESTY/Flashka/GUYMAGER/obraz.info
Hash calculation      : SHA-256
Source verification   : off
Image verification    : on

No bad sectors encountered during acquisition.
State: Finished successfully

MD5 hash              : --
MD5 hash verified source  : --
MD5 hash verified image   : --
SHA1 hash             : --
SHA1 hash verified source : --
SHA1 hash verified image  : --
SHA256 hash           : 141ac5d560d9b72bba3e3bd7c72c22e6e85e124c2506783014e427b55d775015
SHA256 hash verified source: --
SHA256 hash verified image : 141ac5d560d9b72bba3e3bd7c72c22e6e85e124c2506783014e427b55d775015
Image verification OK. The image contains exactly the data that was written.

Acquisition started : 2017-04-08 16:05:31 (ISO format YYYY-MM-DD HH:MM:SS)
Verification started: 2017-04-08 16:10:10
Ended               : 2017-04-08 16:10:57 (0 hours, 5 minutes and 25 seconds)
Acquisition speed   : 14.03 MByte/s (0 hours, 4 minutes and 38 seconds)
Verification speed  : 82.98 MByte/s (0 hours, 0 minutes and 47 seconds)
```

Obrázek 5 – Část logového souboru vytvořeného programem Guymager. Obsahuje informace o klonovaném zařízení, výsledné kopii, dále o umístění tohoto souboru, zvoleném algoritmu pro vypočítání kontrolního součtu, kontrolní součet originálu, kopie a jejich porovnání a ještě o informace o právě proběhlém procesu.

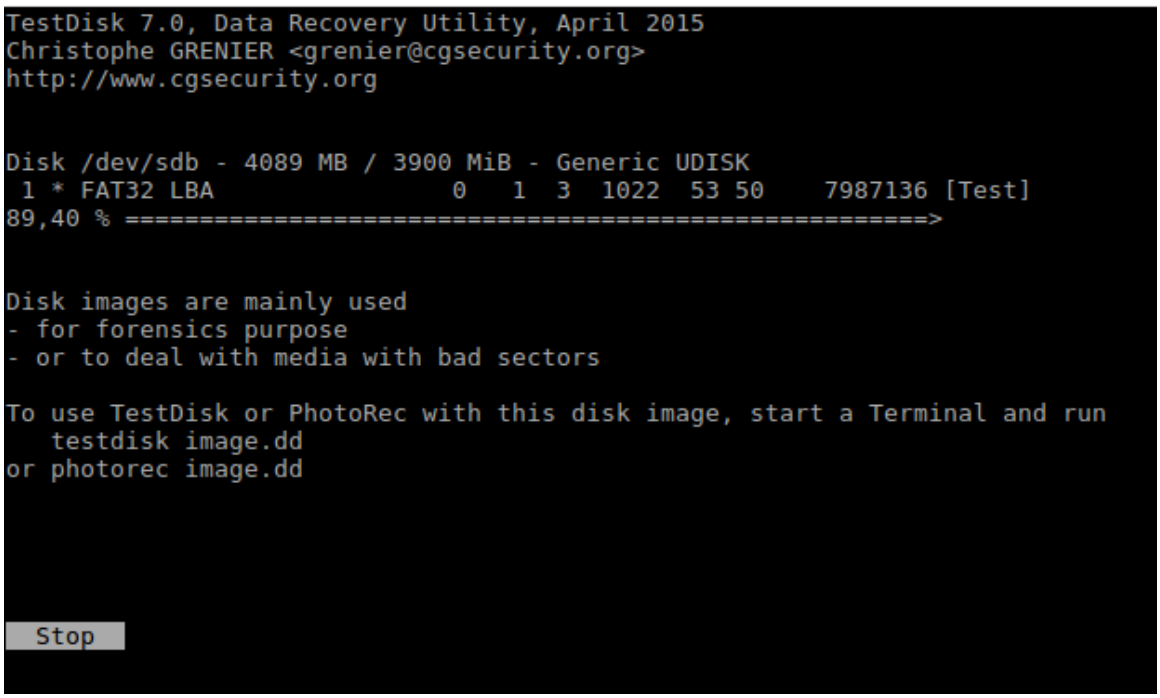
5.2.4 TestDisk

TestDisk je software navržený pro širokou práci s paměťovým médiem. Primárně je určený k obnově ztracených oddílů a opravě bootovacích disků za předpokladu, že chyba byla způsobena chybným softwarem, např. virus nebo lidská chyba.

TestDisk je možné využít pro opravu tzv. „partition table“, což je tabulka s informacemi o rozdělení jednoho média na více logických částí. Jeden pevný disk se nám poté jeví jako více disků a je například možné mít na každé části jiný souborový systém nebo operační systém. TestDisk je také možno použít pro obnovení smazaných oddílů, opravu bootovacího sektoru a kopírování dat ze souborových systémů FAT, exFAT, NTFS, ext2/ext3/ext4.

S tímto programem je spojen nástroj PhotoRec, který navazuje na TestDisk a ze zajištěného obrazu disku je schopný extrahovat více než 440 datových formátů [16].

Přestože je TestDisk programem fungujícím v prostředí terminálu, jeho ovládání je velmi intuitivní a přizpůsobené k provedení uživatele celým procesem zajištění bitové kopie (Obr. 6). Takového zajištění je s tímto programem schopný každý uživatel se základní znalostí anglického jazyka.

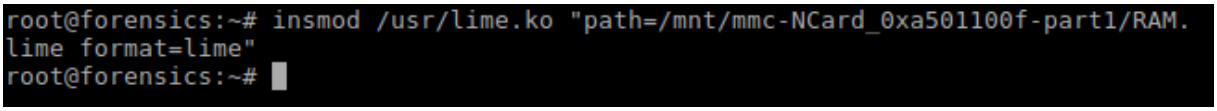


Obrázek 6 – TestDisk. Po spuštění funkce „Vytvořit obraz“, zobrazuje TestDisk stav procesu a napovídá jak nadále pracovat s vytvořenou bitovou kopií.

5.3 Analýza volatilní paměti

5.3.1 Linux Memory Extractor

Linux Memory Extractor, neboli LiME je externí modul linuxového jádra, který je zaveditelný (Obr. 7) za běhu operačního systému. Jako takový je používán pro zajištění volatilních pamětí na linuxových systémech. Řadí se mezi první nástroje určené pro zajištění operační paměti na zařízeních s operačním systémem Android. Nabízí zajištění paměti na datové uložiště nebo přenesení po síti například do vyšetřovatelské stanice [17].

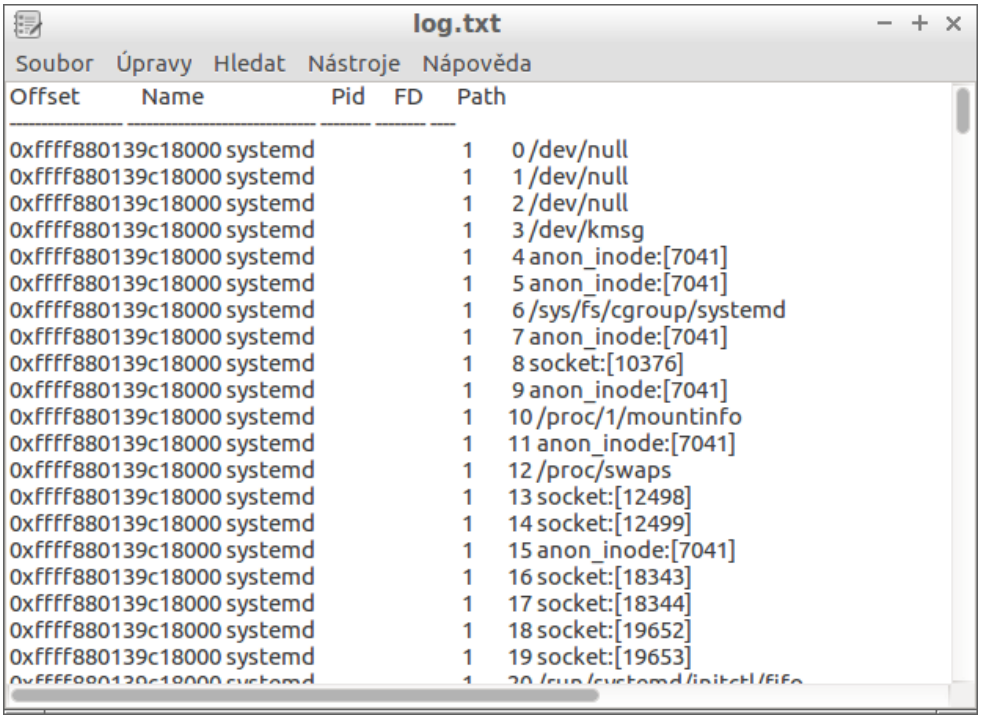


Obrázek 7 - Protože LiME není aplikace, ale pouze externí modul, zavádí se příkazem insmod a uvedením cesty k souboru lime.ko. Následující parametr path uvádí, do jakého souboru se vykopírují data z operační paměti. Takový soubor je pak způsobilý pro další analýzu nástrojem volatility.

5.3.2 Volatility

Jedná se o multiplatformní aplikaci určenou k analýze získané volatilní paměti s otevřeným zdrojovým kódem pro operační systémy Linux, Windows, Mac OS a Android. Struktura programu má seznámit uživatele s technikami a složitostmi spojenými s extrakcí informací z volatilní paměti. Techniky pro takové získání informací jsou naprosto nezávislé na zkoumaném systému.

Volatility (Obr. 8) je schopné analyzovat spousty různých formátů, např. klasické formáty bitových kopií jako je *.dd, *.img. Je také schopen analyzovat *.ewf, formát vytvářený programem Guymager nebo formát *.lime aplikace Linux Memory Extractor. Mimo jiné zpracovává tzv. „Hibernation file“, který je typický pro operační systémy Windows a slouží k uložení stavu počítače před navozením stavu hibernace. Disponuje schopností analyzovat kompletní „crash dump“ soubory, ve kterých se nachází veškerý obsah operační paměti v době neočekávaného ukončení systému. Rozezná i Mach-O formát systému iOS, Mac OS nebo formáty virtualizačních nástrojů QEMU, VirtualBox a WMware [18].



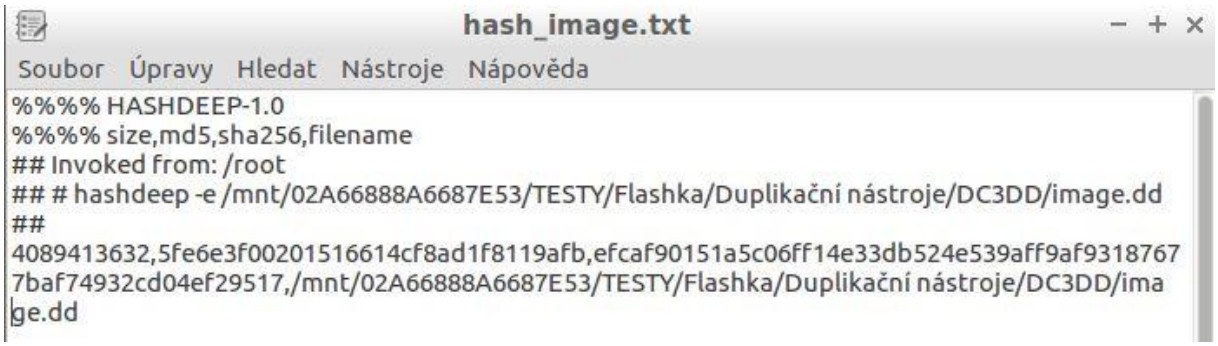
Obrázek 8 – Výstup aplikace Volatility, po zavolání funkce linux_lsof. Volatility dokáže převést zkoumaný formát *.lime do „surového“ formátu *.dd, který lze pak dále zkoumat třeba nástrojem PhotoRec a extrahovat tak např. obrázky, textové soubory a další z operační paměti.

5.4 Hašovací nástroje

5.4.1 Hashdeep

Tento program vychází z kryptografické hašovací funkce MD5 (Message-Digest algorithm), proto jej lze také najít pod názvem MD5deep. Vytváří kontrolní součet (tzv. otisk) a slouží k ověření integrity a autenticity souboru (Obr. 9). To nám zaručí, že pracujeme s požadovanými daty. Pokud toto ověření neproběhne, není jisté, že práce s daty nebude probíhat nad daty pozměněnými či úplně jinými.

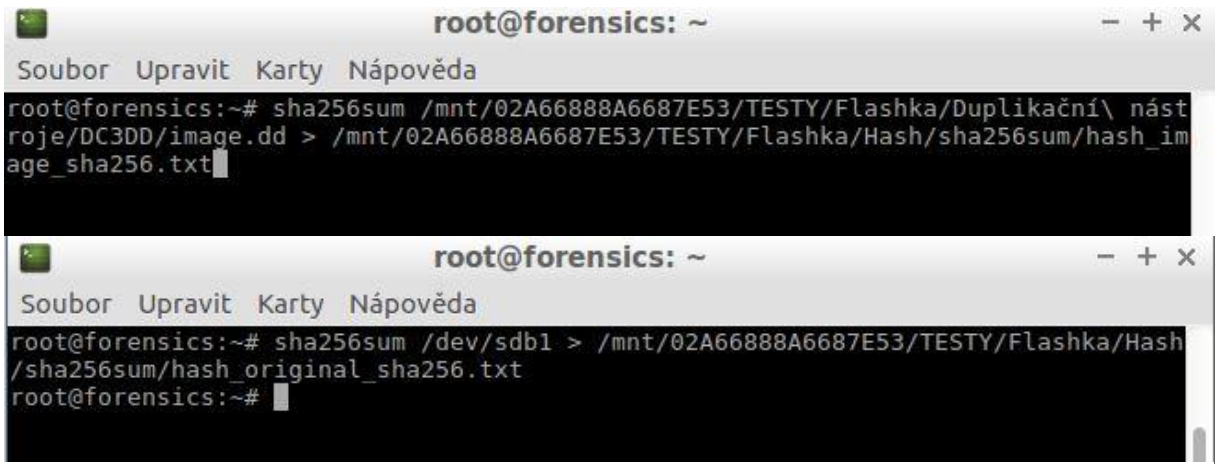
Výhodou tohoto programu je, že dokáže využít modernější, bezpečnější Secure Hash Algorithm a vytvořit tak bezpečnější šifru. Vzhledem k tomu, že starší funkce MD5 je v současnosti považována za prolomenou, doporučuje se používat např. právě tyto funkce z rodiny SHA (SHA-1, SHA-256, atd.). Pokud někomu tento software nevyhovuje, je možné použít např. MD5Sum nebo SHA1Sum, které bývají přítomné v mnoha verzích unixových systémů [19].



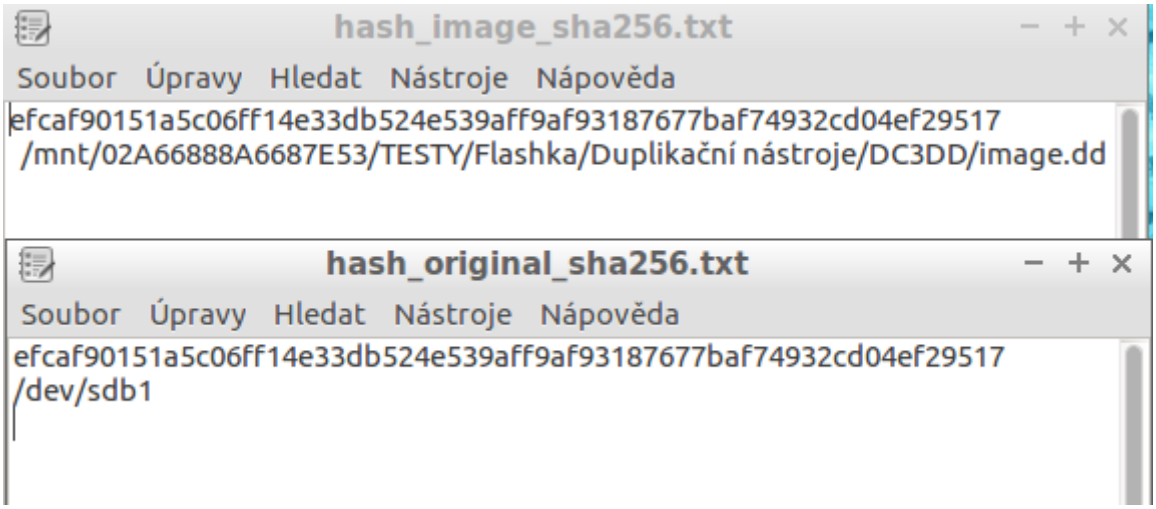
Obrázek 9 – Výstup aplikace Hashdeep uložený do souboru hash_image.txt.

5.4.2 MD5Sum, SHA1Sum, SHA256Sum, SHA512Sum

Jedná se o skupinu hašovacích algoritmů vyskytujících se téměř v každém operačním systému vystavěném na bázi Unixu. Datový výstup tohoto softwaru je jednoduchý a přehledný. Následující obrázky (Obr. 10) ukazují, jak lze porovnat výstup (Obr. 11) z těchto programů, konkrétně šifra SHA256.



Obrázek 10 – Aplikace programu sha256sum na originální médium a jeho obraz a následné uložení hodnot do souboru hash_original_sha256.txt a hash_image_sha256.txt



Obrázek 11 – Porovnání souborů hash_original_sha256.txt a hash_image_sha256.txt. První řádek zobrazuje vypočítanou sumu, druhý řádek médium, ze kterého byla vypočítána. Po porovnání sum lze konstatovat, že bitová kopie byla řádně vytvořena a integrita dat zůstala zachována.

5.5 Extrakce dat

5.5.1 Foremost

Foremost je jeden z prvních nástrojů vyvinutých pro potřebu extrakce dat, jinak tzv. data carving. Jedná se o aplikaci používanou příkazovým řádkem. Byl vyvinut v roce 2000 Úřadem vzdušných sil pro zvláštní vyšetřování. Jeho výsledky je možné použít v soudním řízení.

Pro svou práci využívá souborové hlavičky a patičky, na jejichž základě doplňuje zbylé části souborů. Prochází segment po segmentu a v paměti hledá takovou hlavičku, která se shoduje s konfiguračním souborem aplikace. Poté zapíše hlavičku a následující data do souboru a v případě, že nalezne i patičku nebo dosáhne jeho maximální velikosti (uvedenou v konfiguračním souboru) uzavírá ho a pokračuje dále. Maximální velikost souboru se zde používá proto, aby program nezapisoval následující data stále do jednoho souboru v případě, že se nepodaří souborová patička najít.

Ačkoliv je navržený tak, že může extrahovat data přímo z disku (souborové systémy ext3, NTFS či FAT), je vždy lepší napřed využít duplikačních nástrojů a následnou extrakci provádět až z obrazu média (Obr. 12). Zde je stručný přehled datových formátů, které je Foremost schopný extrahovat – jpg (Obr. 13), gif, exe, wav, mov, pdf, rar [20].

```
root@forensics:~# foremost -v -o /mnt/02A66888A6687E53/TESTY/Flashka/Extrakční/F
oremost/Image/ -i /mnt/02A66888A6687E53/TESTY/Flashka/Duplikační\ nástroje/DC3DD
/image.dd
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Sun Apr  9 12:12:40 2017
Invocation: foremost -v -o /mnt/02A66888A6687E53/TESTY/Flashka/Extrakční/Foremos
t/Image/ -i /mnt/02A66888A6687E53/TESTY/Flashka/Duplikační nástroje/DC3DD/image.
dd
Output directory: /mnt/02A66888A6687E53/TESTY/Flashka/Extrakční/Foremost/Image
Configuration file: /etc/foremost.conf
Processing: /mnt/02A66888A6687E53/TESTY/Flashka/Duplikační nástroje/DC3DD/image.
dd
|------------------------------------------------------------------
File: /mnt/02A66888A6687E53/TESTY/Flashka/Duplikační nástroje/DC3DD/image.dd
Start: Sun Apr  9 12:12:40 2017
Length: 3 GB (4089413632 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

0:      00025794.jpg           3 MB        13206528
1:      00033735.jpg         382 KB        17272320
2:      00034506.jpg           3 MB        17667072
3:      00042120.jpg         361 KB        21565440
4:      00042850.jpg           4 MB        21939200
5:      00051385.jpg         499 KB        26309120
6:      00052386.jpg          15 KB        26821632
foundat=_rels/.rels ▯▯▯▯
foundat=word/_rels/document.xml.rels ▯▯▯▯
```

Obrázek 12 – Inicializace extrakce dat pomocí nástroje Foremost.

```
364:    07367552.jpg           6 MB      3772186624
*365:   07381888.jpg           6 MB      3779526656
366:    07394952.jpg           6 MB      3786215424
367:    07408392.jpg           8 MB      3793096704
368:    07424864.jpg           6 MB      3801530368
369:    07438160.jpg           4 MB      3808337920
370:    07447920.jpg           4 MB      3813335040
371:    07457056.jpg           4 MB      3818012672
372:    07465440.jpg           4 MB      3822305280
373:    07475232.jpg           5 MB      3827318784
374:    07485496.jpg           4 MB      3832573952
375:    07494344.jpg           3 MB      3837104128
376:    07502072.jpg           4 MB      3841060864
***|
Finish: Sun Apr  9 12:15:08 2017

377 FILES EXTRACTED

jpg:= 331
zip:= 6
png:= 39
pdf:= 1
------------------------------------------------------------------

Foremost finished at Sun Apr  9 12:15:08 2017
```

Obrázek 13 – Výsledné hlášení o provedené extrakci.

5.5.2 Scalpel

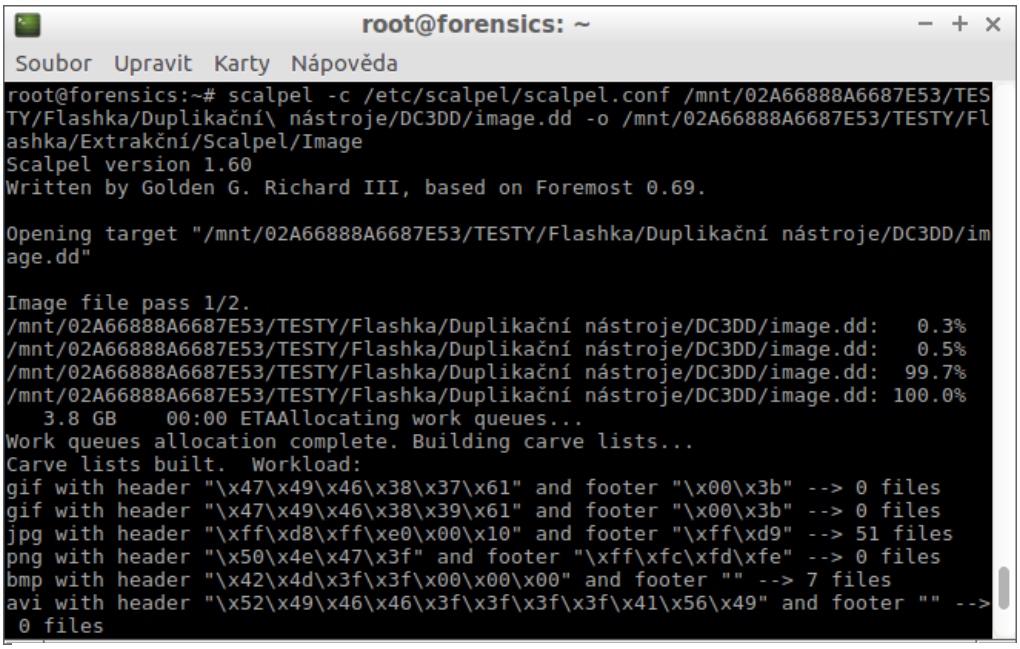
Scalpel je novější nástroj hojně využívaný při extrakci dat. Přestože má své základy postavené na aplikaci Foremost, je značně efektivnější.

Při svém běhu dvakrát prochází obraz disku. Při první fázi (Obr. 14) rozdělí objem dat obrazu do stejně velkých částí (standardně 10MB) a v každé části hledá hlavičky

souborů, které ukládá do databáze. Jakmile prohledá v dané části disku hlavičky, začne hledat a ukládat patičky souborů. Patičky jsou vyhledávány, pouze pokud může být v dané části odpovídající hlavička. Po skončení první fáze má Scalpel kompletní databázi hlaviček a patiček, kterou použije pro vytvoření tzv. „pracovního procesu“ a řízení druhé fáze. Jeden pracovní proces je spjatý s jednou částí obrazu a jedním souborem, který má být extrahován.

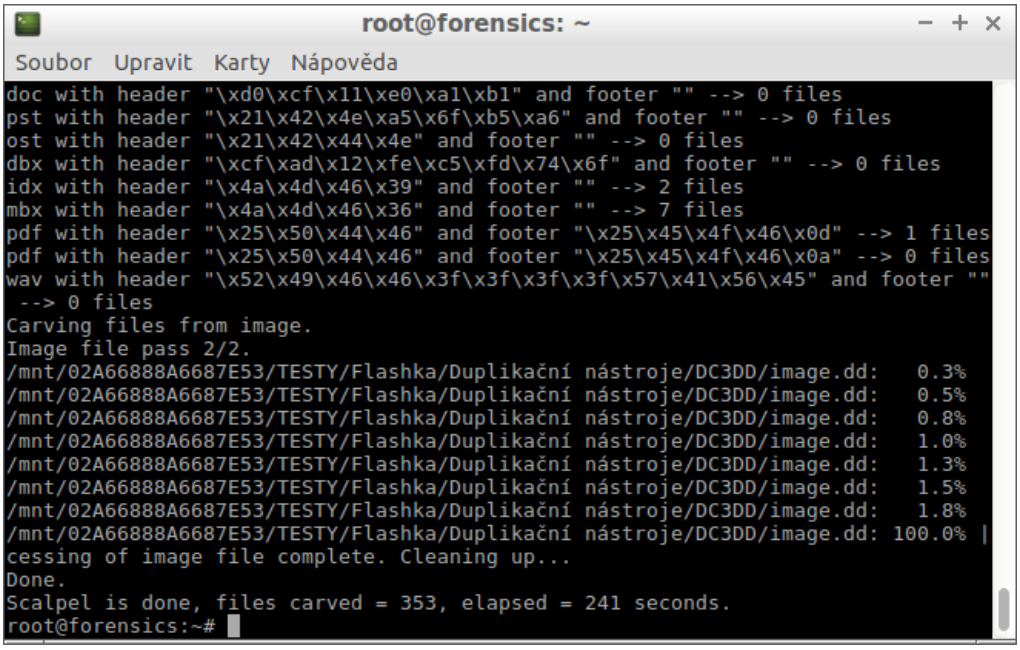
Obsahuje tak jeden z následujících příkazů:

- STARTCARVE – Extrakce souboru začne v této části. Soubor se otevře a jeho počáteční část je zapsána.
- STARTSTOPCARVE – Extrakce souboru začne a skončí v této části. Soubor se otevře, vymezená oblast dané části se zapíše a soubor se zavře.
- CONTINUECARVE – Extrakce souboru proběhne celou částí. Celý obsah části se zapíše a soubor zůstane otevřený.
- STOPCARVE – Extrakce souboru v této části skončí. Vymezená oblast se zapíše a soubor se zavře.



Obrázek 14 – První fáze, ve které má Scalpel již vytvořenou databázi hlaviček a patiček a začíná vytvářet pracovní procesy.

V druhé fázi (Obr. 15) prochází Scalpel opět části obrazu disku a aplikuje na každou část jí přiřazené pracovní procesy. Pro zrychlení procesu se ve druhé fázi přeskakují části, které nemají naplánovaný žádný pracovní proces [21].



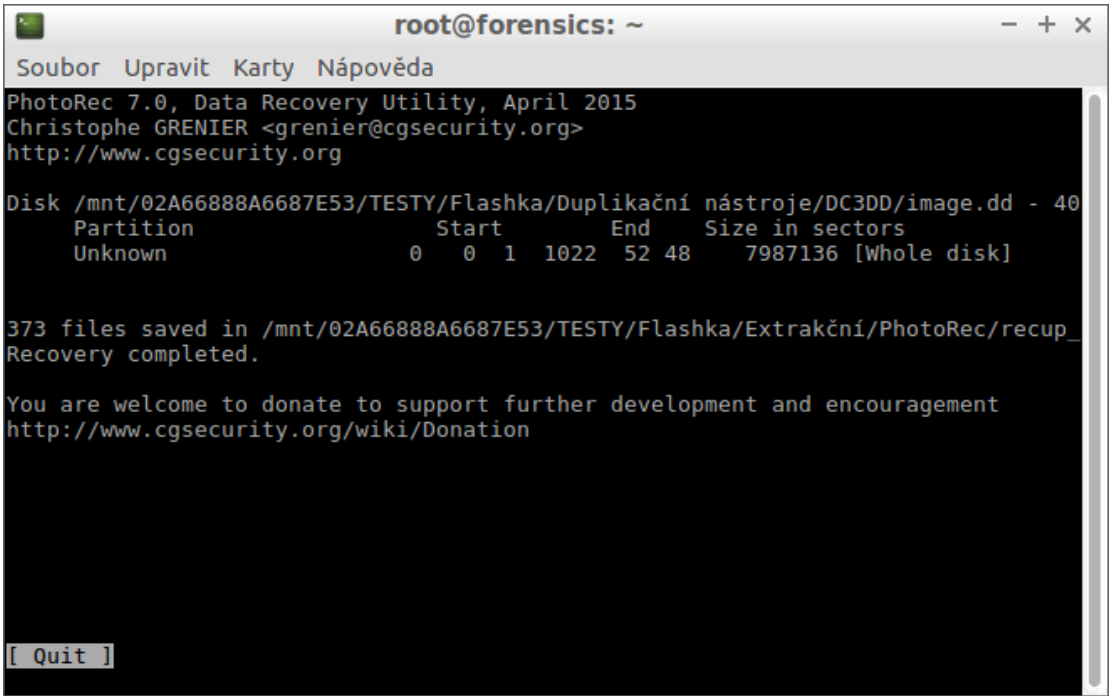
Obrázek 15 – Zobrazení druhé fáze, ve které Scalpel aplikuje pracovní procesy a extrahuje data.

5.5.3 PhotoRec

PhotoRec (Obr. 16) je multiplatformní aplikace určená k extrakci dat z pevných disků, CD-ROM, DVD a dalších datových uložišť. Je funkční na systémech Windows, Linux, FreeBSD, Sun Solaris, Mac OS X. PhotoRec je dostupný současně s programem TestDisk. Pro větší bezpečnost dat nelze uložit extrahovaná data na stejný diskový oddíl, jako ten, ze kterého jsou extrahována.

PhotoRec funguje na principu tzv. clusterů. Pokud není poškozený souborový systém, hledá velikost clusteru v tzv. „superblock“ nebo „volume boot record“, což jsou sektory úložných zařízení, které obsahují metadata o používaném souborovém systému. V případě, že je souborový systém poškozený, prochází PhotoRec sektor po sektoru a hledá prvních 10 souborů, ze kterých vypočítá velikost clusteru. Jakmile zná jeho velikost, prochází cluster po clusteru, porovná jeho obsah se vzorovou databází a rozhodne, zdali umí obnovit data či nikoliv.

Například pokud cluster začíná „0xff, 0xd8, 0xff, 0xe0 nebo 0xff, 0xd8, 0xff, 0xe1 nebo 0xff, 0xd8, 0xff, 0xfe“ PhotoRec pozná, že se jedná o formát JPEG [16].



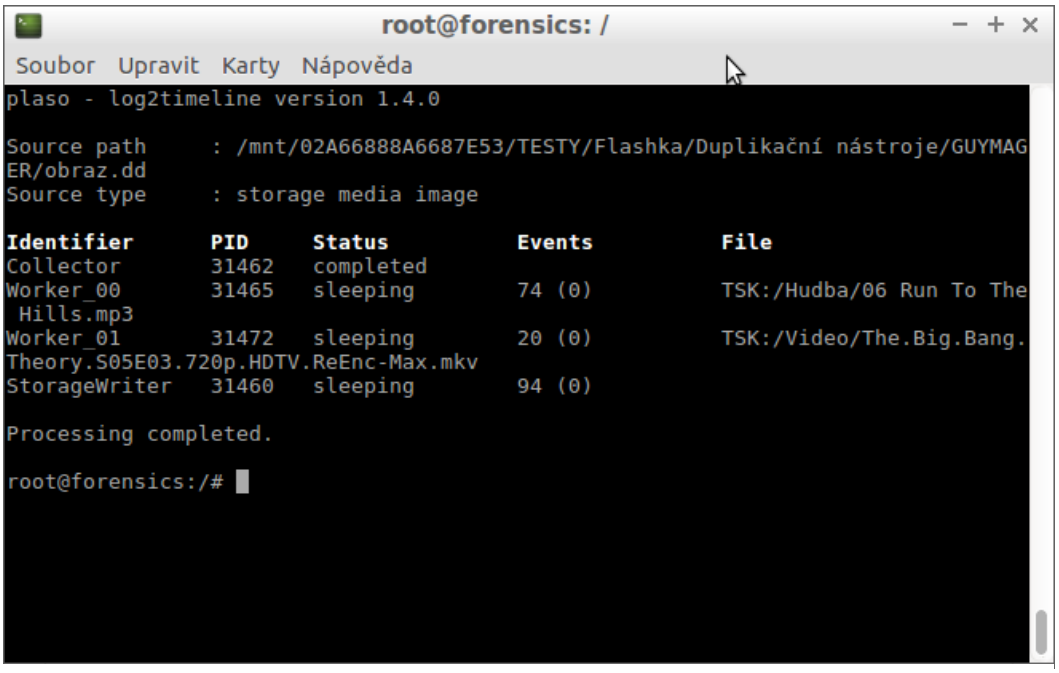
Obrázek 16 – Informace o proběhlé extrakci dat. Prostředí se chová stejně jako v nástroji TestDisk.

5.6 Analýza časové osy

5.6.1 Log2Timeline

Log2Timeline je program navržený pro vytvoření a analýzu časové osy. Hlavním účelem je poskytnout nástroj, který bude analyzovat různé logové soubory a fragmenty nalezené na podezřelých systémech a poskytnout soubor, na kterém bude možné vystavět časovou osu.

Log2Timeline použije soubor (nebo složku) a analyzuje ji, aby vytvořil soubor, který je pak možný importovat i do jiných nástrojů „časové“ analýzy. Základním účelem současné verze je vytvořit soubor, který bude čitelný softwarem The SleuthKit. Aplikace je vystavěná jako série skriptů (modulů) využívajících další skripty, které analyzují logové soubory (Obr. 17). Takto autoři zařídili jednoduché rozšíření pro všechny, kteří by chtěli připojit nový modul [22].

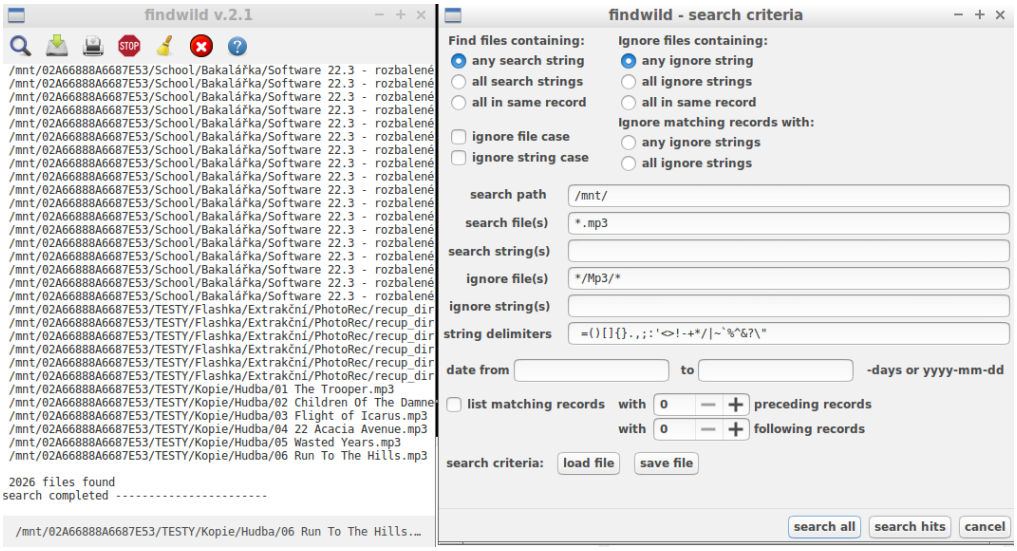


Obrázek 17 – Ukázka skriptu Log2Timeline.py

5.7 Analytické nástroje

5.7.1 Findwild

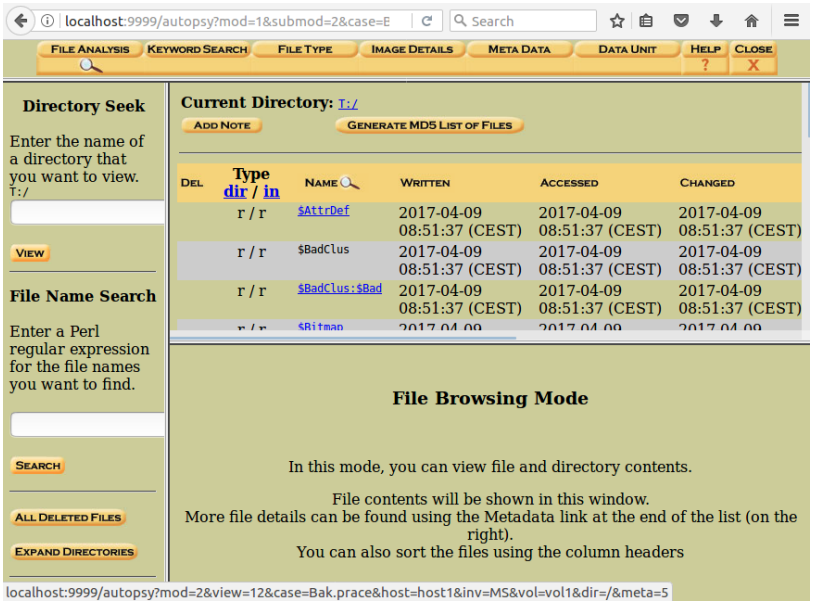
Findwild (Obr. 18) je grafická aplikace určená k prohledávání souborů. Nabízí široké spektrum možností jak vyhledávání přizpůsobit tak, aby bylo co nejefektivnější. Vyhledávací kritéria mohou být uložena a v budoucnu znovu zavolána, případně upravena a použita znovu [23].



Obrázek 18 – Vlevo se nachází výstup aplikace Findwild na základě kritérií definovaných v dialogovém okně vpravo.

5.7.2 The Sleuth Kit

The Sleuth Kit, dále jen TSK, je sbírka počítačových forenzních programů, které spojil dohromady Brian Carrier. Tyto programy dovolují uživateli prozkoumat systémové soubory neinvazivním způsobem. Protože se nástroje při zpracování souborů nespoléhají na operační systém, je nám zobrazený i smazaný a ukrytý obsah. Pomocí těchto nástrojů lze analyzovat data nalezená na discích jiných počítačů i jiných operačních systémů (např. Windows, Mac, Linux). V současnosti TSK podporuje následující souborové systémy – EXT 2-4, FAT, exFAT, NTFS, HFS, UFS 1-2. Tato sada obsahuje kolekci nástrojů příkazového řádku, ale i grafického prostředí, které je uživatelsky přátelštější. Tomuto rozhraní se říká Autopsy Forensic Browser (Obr. 19) [24].

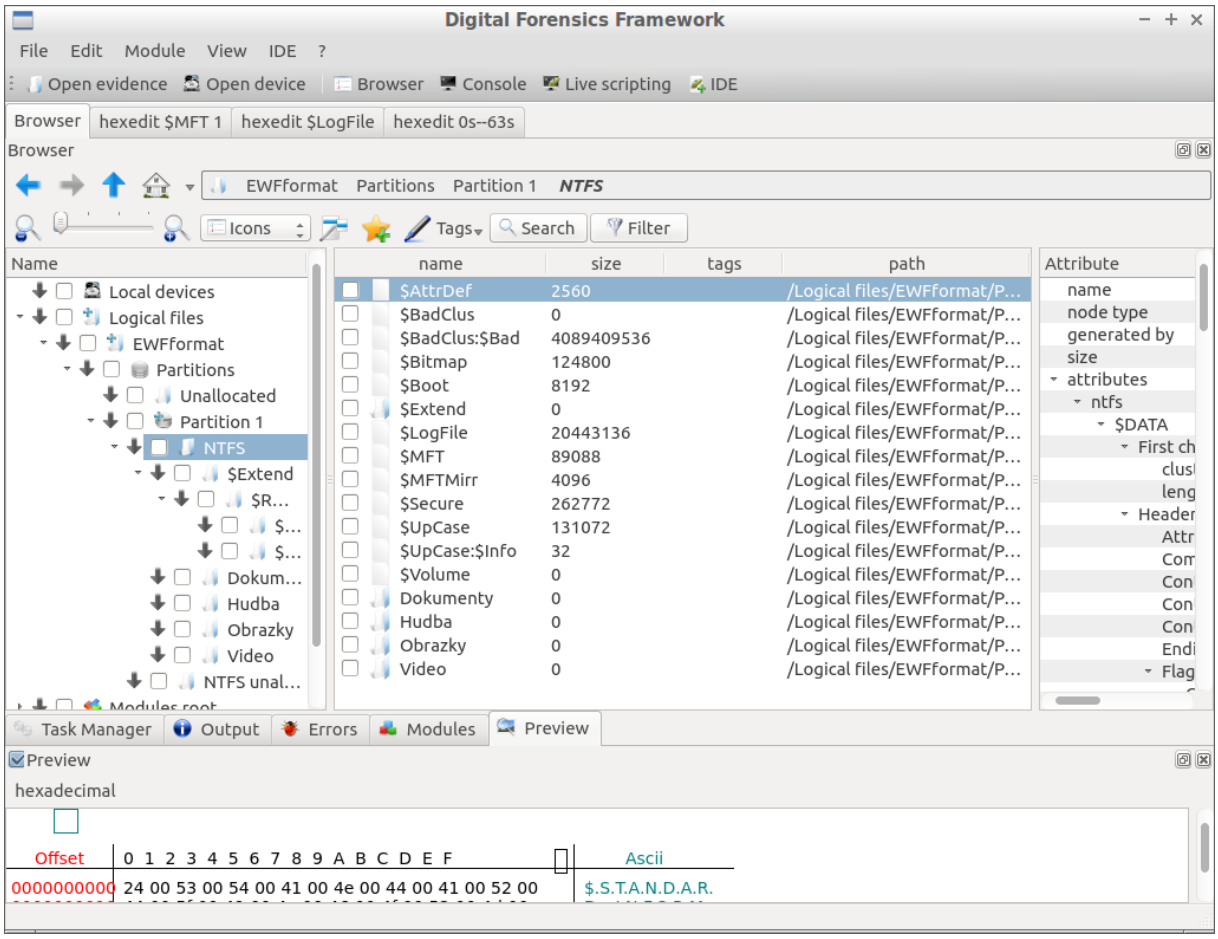


Obrázek 19 – Analýza bitové kopie nástrojem Autopsy, které používá pro vizualizaci kroků prostředí internetové prohlížeče.

5.7.3 Digital Forensics Framework

Digital Forensics Framework je analytický nástroj je vystavěn na širokém spektru zásuvných modulů, které usnadňují práci během forenzní analýzy. Disponuje jak příkazovým řádkem, tak grafickým prostředím. Grafické prostředí je navrženo tak, aby provedlo uživatele základními kroky forenzní analýzy (Obr. 20).

Hlavními cíli projektu bylo vytvořit forenzní nástroj, který bude modulární z důvodu jednodušší upravitelnosti, skriptovatelný kvůli větší flexibilitě a obecný. Pojem obecný skrývá cíl vytvořit projekt nezávislý na jednom operačním systému [25].

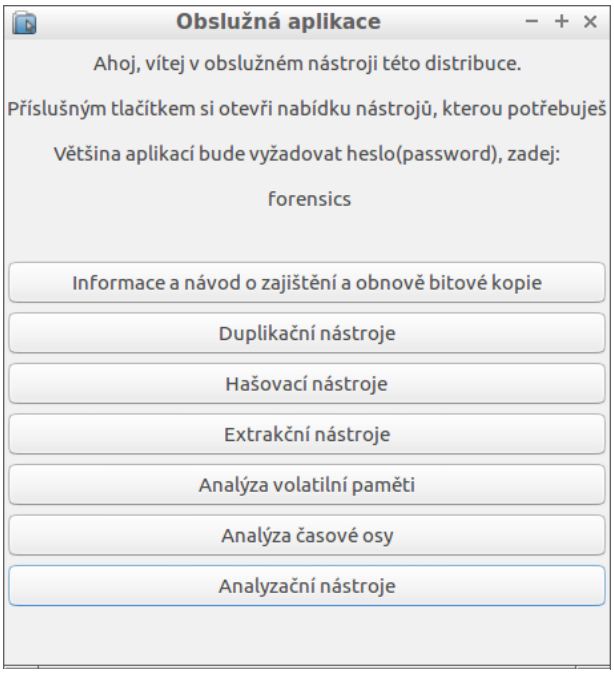


Obrázek 20 – Zobrazení a analýza bitové kopie nástrojem DFF.

5.8 Obslužná aplikace

Obslužná aplikace je nástroj, který jsem vytvořil pro usnadnění přístupu k jednotlivému software. Účelem tohoto prostředí je co nejvíce uživateli zjednodušit obsluhu této distribuce. Aplikace se spustí ihned po startu systému a seznámí uživatele se základními kroky. Základem této aplikace je jednoduchý skript, který využívá možnosti nástroje YAD.

Skript obsahuje sérii funkcí, které čtou spouštěče jednotlivých aplikací a umožňují uživateli spustit software ze zobrazené nabídky (Obr. 21). Tyto spouštěče jsou rozděleny do jednotlivých kategorií podle druhu práce s daty, ke kterému jsou určeny. Uživatel zvolí danou kategorii a jsou mu nabídnuty konkrétní nástroje, které může pro daný úkon zvolit. Pokud uživatel spustí některou z nabízených aplikací, otevře se mu český manuál a spustí daná aplikace. Ne vždy má aplikace ovládací rozhraní, ale je pouštěna pouze v terminálu. V takových případech se spustí terminál. U většiny aplikací s uživatelským rozhraním se otevře také prohlížeč obrázků s názorným příkladem jak aplikaci obsluhovat. Co všechno se spustí po zvolení některého z nástrojů, indikuje nápověda přiložená k aplikaci.



Obrázek 21 – Úvodní nabídka obslužné aplikace

6. Závěr

Tato bakalářská práce se snaží přiblížit čtenáři problematiku forenzní analýzy digitálních dat. První část pojednává o problematice spojené se zajištěním digitálních důkazů pro účely Policie České republiky a úkonech, které musí vyšetřovatel (popřípadě soudní znalec) zvážit před začátkem procesů spjatých s digitálními důkazy. Vzhledem k neustálému pokroku se metody postupů stále vyvíjí a ke každému případu se musí přistupovat individuálně. Ačkoliv existuje soubor pravidel, podle kterých postupovat, nelze vypracovat obecnou metodiku, jak postupovat v každém případě.

Stěžejním bodem této práce bylo vytvořit forenzní live distribuci Linuxu, kterou může obsluhovat uživatel se základní znalostí IT. Za tímto účelem jsem vytvořil skript, který nabízí uživateli možnosti spuštění aplikací zmíněných výše. Zároveň jsem přeložil manuálové stránky do českého jazyka a tento překlad přiložil jako nápovědu k obsluze nástrojů. Tím se stala obsluha většiny nástrojů opravdu jednoduchá a některé úkony jako zajištění bitové kopie zvládne téměř každý. Nicméně počítačová forenzika je stále se rozvíjejícím vědním oborem, a proto jsou pro odbornou analýzu důležité odborné znalosti.

7. Seznam literatury

1. PORADA, Viktor. *Kriminalistika: (úvod, technika, taktika)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2007. ISBN 978-80-7380-038-3.

2. ČESKÁ REPUBLIKA. *Zákon o trestním řízení soudním*. In: . Praha: Ministerstvo spravedlnosti, 1961, ročník 1961, částka 66, číslo 141. Dostupné také z: aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=1101

3. *Forenzní zkoumání digitálních důkazů*. Praha, 2005. Dostupné také z: http://www.rac.cz/rac/homepage.nsf/CZ/883AABB42333CB35C12570FC0034A328/$FILE/Guide%20051230.pdf

4. What is Linux? *Linux.com* [online]. San Francisco: The Linux Foundation, 2016 [cit. 2016-11-20]. Dostupné z: https://www.linux.com/what-is-linux

5. JELÍNEK, Lukáš. *Jádro systému Linux: kompletní průvodce programátora*. Brno: Computer Press, 2008. Programování (Computer Press). ISBN 9788025120842.

6. *Open Source Initiative* [online]. Palo Alto: Open Source Initiative, 1998 [cit. 2017-03-16]. Dostupné z: https://opensource.org/

7. *Opensource.com* [online]. Raleigh: Red Hat, 2010 [cit. 2017-03-16]. Dostupné z: https://opensource.com/

8. Live CD. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2017-03-17]. Dostupné z: https://en.wikipedia.org/wiki/Live_CD

9. *Lubuntu* [online]. London: Canonical, 2017 [cit. 2017-03-18]. Dostupné z: https://wiki.ubuntu.com/Lubuntu

10. Dc3dd. *SourceForge* [online]. La Jolla: Slashdot Media, 2016 [cit. 2016-11-20]. Dostupné z: https://sourceforge.net/projects/dc3dd/

11. Ddrescue. *The GNU Operating System and the Free Software Movement* [online]. Boston: Free Software Foundation, c2017 [cit. 2017-03-11]. Dostupné z: http://www.gnu.org/software/ddrescue/ddrescue.html

12. GNU ddrescue Manual. *The GNU Operating System and the Free Software Movement* [online]. Boston: Free Software Foundation, c2004-2017 [cit. 2017-03-11]. Dostupné z: https://www.gnu.org/software/ddrescue/manual/ddrescue_manual.html

13. Ddrescueview. In: *Freecode* [online]. La Jolla: Slashdot Media, c2015 [cit. 2017-03-11]. Dostupné z: http://freecode.com/screenshots/a7/ab/a7ab63ea4e027b63edf4fd9d2dbd1790_medium.jpeg?1377804350

14. Creating a Disk Image Using Guymager. *BitCurator* [online]. San Francisco: Wikimedia Foundation, 2017 [cit. 2017-03-15]. Dostupné z: https://wiki.bitcurator.net/index.php?title=Creating_a_Disk_Image_Using_Guymager

15. Guymager homepage. *Sourceforge* [online]. La Jolla: Slashdot Media, c2017 [cit. 2017-03-15]. Dostupné z: http://guymager.sourceforge.net/

16. *CGSecurity* [online]. Paris: Grenier, 2015 [cit. 2017-03-13]. Dostupné z: https://www.cgsecurity.org/

17. LiME/README.md. *GitHub* [online]. San Francisco: GitHub, c2017 [cit. 2017-03-08]. Dostupné z: https://github.com/504ensicsLabs/LiME/blob/master/doc/README.md#Disk

18. Volatility/README.txt. *GitHub* [online]. San Francisco: GitHub, c2017 [cit. 2017-03-11]. Dostupné z: https://github.com/volatilityfoundation/volatility/blob/master/README.txt

19. Md5deep and hashdeep - Latest version 4.4. *Sourceforge* [online]. La Jolla: Jesse Kornblum, 2014 [cit. 2017-02-27]. Dostupné z: http://md5deep.sourceforge.net/

20. The Foremost Open Source Forensic Tool. *Dr. Dobb's* [online]. San Francisco: Ray Strubinger, 2003 [cit. 2017-03-18]. Dostupné z: http://www.drdobbs.com/the-foremost-open-source-forensic-tool/199101633?pgno=1

21. RICHARD, Golden a Vassil ROUSSEV. Scalpel: A Frugal, High Performance File Carver. In: *DFRWS* [online]. New Orleans: Richard, 2005 [cit. 2017-03-16]. Dostupné z: http://dfrws.org/sites/default/files/session-files/paper-scalpel_-_a_frugal_high_performance_file_carver.pdf

22. Log2timeline. *GitHub* [online]. San Francisco: GitHub, c2017 [cit. 2017-03-24]. Dostupné z: https://github.com/log2timeline/plaso/wiki

23. Findwild. *Kornelix* [online]. Ann Arbor: A2 hosting, c2017 [cit. 2017-03-25]. Dostupné z: http://www.kornelix.net/findwild/findwild.html

24. The Sleuth Kit. *Open Source Digital Forensics* [online]. Brea: Carrier, c2003-2016 [cit. 2016-11-20]. Dostupné z: http://www.sleuthkit.org/sleuthkit/desc.php

25. DFF. *GitHub* [online]. San Francisco: GitHub, c2017 [cit. 2017-03-14]. Dostupné z: https://github.com/arxsys/dff

8. Přílohy

[1] Live DVD s vytvořenou forenzní distribucí Linuxu.