Platforma pro forenzní analýzu USB disků

Bc. Jan Matoušek

Diplomová práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jan Matoušek**
Osobní číslo:	**A15233**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Platforma pro forenzní analýzu USB disků**
Téma anglicky:	**A Platform for the Forensic Analysis of USB Drives**

Zásady pro vypracování:

1. **Objasněte problematiku digitálních důkazů.**
2. **Popište možnosti forenzního zkoumání digitálních stop za využití operačního systému Linux.**
3. **Popište možnosti zkoumání bezpečnostního incidentu za pomocí open source nástrojů v Linuxu.**
4. **Navrhněte a realizujte HW a SW ARM platformu pro vytváření bitových kopií disků s USB rozhraním.**
5. **Prakticky toto zařízení otestujte a vyhodnoťte.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **J. Glenn Brookshear. INFORMATIKA. Computer Press, 2013. ISBN:978-80-251-3805-2.**
2. **Pavel Kameník. Příkazový řádek v Linuxu, Computer Press, 2013. ISBN:978-80-251-2819-0**
3. **Donald Norris. Raspberry Pi. Computer Press, 2015. ISBN:978-80-251-4346-9**
4. **Bruce Nikkel. Practical Forensic Imaging. No Starch Press,US,2016. ISBN:978-15-932-7793-2**
5. **Cory Altheide , Harlan Carvey. Digital Forensics with Open Source Tools. Syngress Media,U.S., 2011. ISBN: 978-15-974-9586-8**

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **8. prosince 2017**

Termín odevzdání diplomové práce: **28. května 2018**

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor,
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně dne 24.05.2018 …….

podpis diplomanta

ABSTRAKT

V teoretické části diplomové práce je pojednáno o digitálních důkazech. V první kapitole jsou probrány legislativní předpoklady zajišťování digitálních důkazů a jejich pramenech. Závěrečná část teoretické části diplomové práce pojednává o možnostech využití operačního systému Linux při forenzní analýze a v teoretické rovině se zabývá šetřením bezpečnostního incidentu. V praktické části je proveden výběr mikropočítače na HW architektuře ARM a následným vývojem SW řešení v programovacím jazyce PYTHON 3 pro platformu, která slouží k forenzní analýze USB disků. Platforma je v rámci praktické části otestována.

Klíčová slova: forenzní analýza, počítačové incidenty, digitální důkazy, disk blokátory, mikropočítače,

ABSTRACT

The theoretical part of this thesis describes digital evidences. The first chapter discusses the legislative prerequisites for providing digital evidences and their sources. The final part describes the possibilities of using the Linux operating system in forensic analysis and on the theoretical level which deals with investigation of a security incident. In the practical part it has been done the selection of microcomputers with HW architecture in processor ARM and subsequent development of SW solution in the programming language PYTHON 3 as a platform, which will serve for forensic analysis of USB drives. This platform is also tested in the practical part.

Keywords: forensic analysis, computer incidents, digital evidence, disk blockers, microcomputers

Poděkování

Děkuji své milované ženě Veronice za trpělivost, kterou projevila v období, kdy jsem musel psát tuto práci. “Vím, nebylo to jednoduché“ S láskou autor.

Obsah

ÚVOD **10**
I TEORETICKÁ ČÁST **11**
1 PROBLEMATIKA DIGITÁLNÍCH DŮKAZŮ **12**
1.1 DIGITÁLNÍ DŮKAZ Z POHLEDU TRESTNÍHO PRÁVA **13**
1.1.1 Vydání věci 13
1.1.2 Odnětí věci 13
1.1.3 Příkaz k domovní prohlídce 13
1.1.4 Prohlídka jiných prostor 14
1.1.5 Příkaz k osobní prohlídce 14
1.1.6 Odposlechy a záznam telekomunikačního provozu 14
1.1.7 Data Retention 15
1.1.8 Sledování osob a věcí 15
1.2 DIGITÁLNÍ DŮKAZ Z POHLEDU SOUKROMÝCH FIREM **15**
1.2.1 Příklad přiměřeného monitorování zaměstnanců firmy 16
1.2.2 Příklad monitorování zaměstnanců, který již je za hranou 16
1.3 UŽITÍ DIGITÁLNÍCH DŮKAZŮ PŘED SOUDEM **16**
1.4 DÍLČÍ ZÁVĚR **17**
2 PRAMENY ELEKTRONICKÝCH DŮKAZŮ **18**
2.1 OSOBNÍ POČÍTAČ **18**
2.2 DATOVÁ ÚLOŽIŠTĚ NAS **19**
2.3 MOBILNÍ TELEFONY A TABLETY **20**
2.4 PRŮMYSLOVÁ DATOVÁ CENTRA A CLOUDY **21**
2.5 POČÍTAČOVÁ SÍŤ **22**
2.6 PAMĚŤOVÁ MÉDIA **23**
2.6.1 Pevné disky 23
2.6.2 Operační paměti 24
2.6.3 DVD a Blue Ray 24
2.6.4 Další prameny důkazů 25
2.7 DÍLČÍ ZÁVĚR **25**
3 ORGANIZACE DAT NA PAMĚŤOVÝCH MÉDIÍCH **26**
3.1 ULOŽENÍ DAT NA PEVNÉM DISKU KLASICKÉHO TYPU **26**
3.2 ULOŽENÍ DAT NA DISKU SSD **28**
3.3 UKLÁDÁNÍ DAT NA OPTICKÁ MÉDIA **28**
3.4 DÍLČÍ ZÁVĚR **28**
4 OPERAČNÍ SYSTÉM LINUX **29**
4.1 DISTRIBUCE OPERAČNÍHO SYSTÉMU LINUX **29**
4.1.1 Distribuce podporující balíčkovací systém RPM 29
4.1.2 Distribuce podporující balíčkovací systém APT 30
4.1.3 Distribuce, které se zásadně kompilují ze zdrojového kódu 30
4.2 POSIX **30**

4.3 STRUKTURA OPERAČNÍHO SYSTÉMU LINUX 31
4.4 OVLÁDÁNÍ LINUXU 33
4.4.1 Základní příkazy v terminálu. 34
4.5 VYUŽITÍ OPERAČNÍHO SYSTÉMU LINUX PRO FORENZNÍ ZKOUMÁNÍ. 35
4.5.1 Vytváření bitových kopií. 35
4.5.2 Formáty bitových kopií 36
4.5.3 Linuxové nástroje pro vytváření bitových kopií 36
4.5.4 Dump operační paměti RAM 38
4.5.5 Zabezpečení integrity stopy 39
4.5.6 Ruční zkoumání filesystému pomocí hexaeditoru 40
4.5.7 Získání výpisu filesystému 44
4.5.8 Setřídění podle časových značek mactime 44
4.5.9 Získávání logů systému za pomocí log2time 45
4.5.10 Vytváření supertimeline 45
4.5.11 Obnova smazaných souborů za pomocí utility Scalpel 46
4.5.12 Analýza dumpu operační paměti 47
4.5.13 Autopsy 47
4.6 DÍLČÍ ZÁVĚR 48
5 VYŠETŘOVÁNÍ BEZPEČNOSTNÍHO INCIDENTU 50
5.1.1 Zjištění co se stalo 51
5.1.2 Vyhodnocení prvotních informací 51
5.1.3 Odpojení konektivity sítě 51
5.1.4 Následovat by mělo zajištění digitálních důkazů pro další analýzu 51
5.1.5 Fáze vytvoření časové osy 51
5.1.6 Fáze vyhodnocení časové osy 52
5.1.7 Fáze vyhodnocení a zvolení opatření, aby se incident nemohl opakovat. 53
5.1.8 Obnovení dat 53
5.1.9 Nahlášení incidentu na policii 53
5.2 DÍLČÍ ZÁVĚR 53
II PRAKTICKÁ ČÁST 55
6 CÍLE PRAKTICKÉ ČÁSTI 56
6.1 VSTUPNÍ POŽADAVKY NA ZAŘÍZENÍ 56
6.2 VÝBĚR VHODNÉHO ZAŘÍZENÍ 57
7 KOMPONENTY PŘÍSTROJE 60
8 INSTALACE SYSTÉMU, DOPLŇKŮ A NASTAVENÍ PARAMETRŮ 61
8.1 INSTALACE SYSTÉMU 61
8.2 ZÁKLADNÍ NASTAVENÍ SYSTÉMU 62

8.2.1 NASTAVENÍ PŘÍSTUPOVÉHO HESLA 62
8.2.2 NASTAVENÍ ROZLIŠENÍ OBRAZOVKY 62
8.2.3 NASTAVENÍ SPUŠTĚNÝCH SLUŽEB 62
8.2.4 NASTAVENÍ WIFI 63
8.3 INSTALACE DOPLŇKŮ PRO VÝVOJ 63
8.3.1 INSTALACE DC3DD 63
8.3.2 INSTALACE GUIZERO PRO PYTHON 3 63
8.3.3 INSTALACE PODPORY FILESYSTÉMU NTFS 64
8.3.4 INSTALACE OVLADAČE DOTYKOVÉHO DISPLEJE 64
8.3.5 NASTAVENÍ SPUŠTĚNÍ APLIKACE 65
8.3.6 ZAKÁZÁNÍ AUTOMATICKÉHO PŘIPOJENÍ USB DISKŮ K SOUBOROVÉMU SYSTÉMU 65
9 VÝVOJ APLIKACE 66
9.1 UŽIVATELSKÉ PROSTŘEDÍ 66
9.1.1 ZÁKLADNÍ MENU 66
9.1.2 DUPLIKAČNÍ MÓD 67
9.1.3 IMIGOVACÍ MÓD 68
9.1.4 WIPOVACÍ MÓD 69
9.1.5 ZDROJOVÝ KÓD PROGRAMU 70
9.2 DÍLČÍ ZÁVĚR 71
10 TESTOVÁNÍ ZAŘÍZENÍ 72
10.1 PŘEDPOKLADY 72
10.2 DUPLIKAČNÍ MÓD 72
10.3 IMAGE MÓD 73
10.3.1 TESTOVÁNÍ PŘI HASHOVACÍ FUNKCI SHA1 73
10.3.2 TESTOVÁNÍ PŘI HASHOVACÍ FUNKCI SHA256 73
10.3.3 TESTOVÁNÍ PŘI HASHOVACÍ FUNKCI SHA 512 74
10.4 WIPOVACÍ MÓD 74
10.5 TESTOVÁNÍ NA USB 3.0 75
11 ZÁVĚREČNÉ VYHODNOCENÍ 77
SEZNAM POUŽITÉ LITERATURY 78
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 81
SEZNAM OBRÁZKŮ 84
SEZNAM TABULEK 87
SEZNAM GRAFŮ 88

ÚVOD

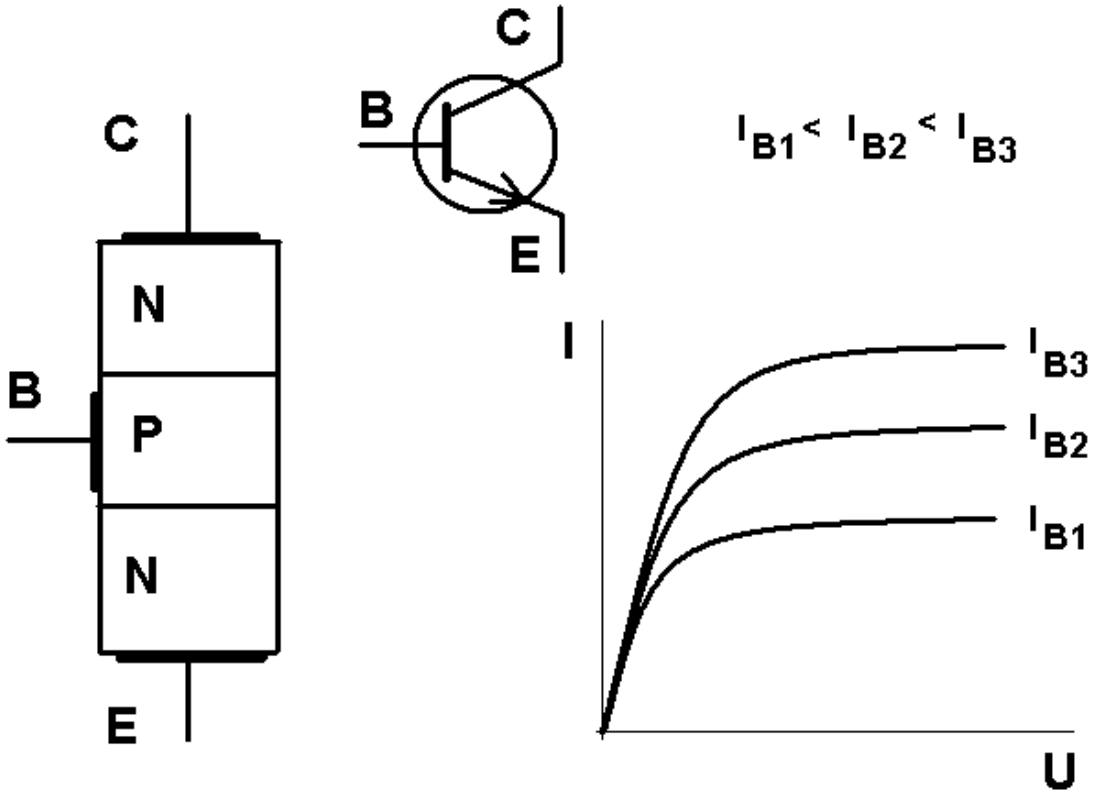
Diplomová práce má název Platforma pro analýzu USB disků. Je rozdělena do dvou částí. První část je čistě teoretická, kdy se zabývá problematikou digitálních důkazů. Problematika je rozebrána z legislativního pohledu na digitální důkazy. Nejdříve z roviny trestně právní, kdy jsou probrány legislativní pravomoci orgánů činných v trestním řízení, poté v rovině občanského práva. Druhá a třetí kapitole se věnuje prameny digitálních důkazů a organizaci dat na paměťových médiích. Aby práce směřovala k tématu, tak další kapitoly se věnují operačnímu systému Linux a jeho open soudcovým nástrojům, kterými je možno provádět forenzní analýzu digitálních důkazů. Je provedeno obecné vyhodnocení aspektů, které se týkají operačního systému Linux a celá teoretická část je završena modelovým příkladem možného šetření bezpečnostního incidentu.

V praktické části, této práce, je zmapován praktický vývoj zařízení na mikropočítači s HW architekturou procesoru ARM. Celá praktická část je členěna logicky za sebou, jako při projektovém vývoji. Zabývá se výběrem vhodného mikropočítače, což znamená vyhodnocení současné nabídky na trhu se zaměřením na cenu a výkonové požadavky na zařízení. Po výběru zařízení je sepsán průběh instalace dalších potřebných součástí do operačního systému a jeho vhodného nastavení, aby fungoval podle požadavků. Následuje popis vyvinuté aplikace s fotodokumentací a rozbor zdrojového kódu, který je přílohou této práce. Závěrečná kapitola je věnována kompletnímu otestování zařízení na vybraných úlohách, které jsou zahrnuty do tabulek. Vzhledem k překvapivým výsledkům je proveden komparační test na notebooku s rozhraním USB 3.0. V závěru je práce zhodnocena.

I. TEORETICKÁ ČÁST

1 PROBLEMATIKA DIGITÁLNÍCH DŮKAZŮ

Dne 16. prosince 1947 byl v Bellových laboratořích týmem vědců ve složení Williama Shockleyho, Johna Bardeena a Waltera Brattaina vynalezen tranzistor, kterým byl nutným předpokladem pro současný rychlý rozvoj techniky, tak jak ji známe dnes. V souvislosti s tím je třeba zmínit i tzv. Moorův zákon. *Moorův zákon: složitost integrovaných obvodů se zdvojnásobuje každých 24 měsíců*. [1]



Obrázek 1. Schéma tranzistoru NPN

Vysoká rychlost rozvoje nových technologií lidstvu usnadňuje práci ve všech oborech napříč lidskou činností. Bohužel, souběžně s tímto pozitivním vývojem se objevují i nové příležitosti zisku pro osoby z kriminálního prostředí, které páchají trestné činy za pomocí nových technologií. Vzhledem k tomu, že lidstvo je již takovým způsobem závislé na fungování techniky, je třeba se zamýšlet nad způsoby obrany, detekce a vyšetřování, a to jak z hlediska technické, tak procesně právní roviny.

1.1 Digitální důkaz z pohledu trestního práva.

V českém trestním řádu neexistuje pojem digitální elektronický důkaz a ani neobsahuje žádné specifické procesní postupy nebo instituty, které by byly zaměřeny na zvláštnosti digitálních důkazů. Orgány činné v trestním řízení tedy musí využívat obecná oprávnění mající v trestním řádu k dispozici. Hlavním účelem zajišťování těchto důkazů z pohledu trestního práva je zjištění pachatele trestného činu a jeho následné potrestání soudem.
Mezi základní instituty, které využívají policejní orgány k zajišťování digitálních důkazů jsou tyto:

1.1.1 Vydání věci

Vychází z ust. § 78 zák. č. 141/1961 Sb. trestního řádu. Znamená že každý, kdo má u sebe věc, která je důležitá pro trestní řízení, je povinen ji na vyzvání předložit soudu, státnímu zástupci, nebo policii. Na základě tohoto ustanovení může policejní orgán vyzvat k vydání věci nejen podezřelého z trestného činu, ale prakticky jakoukoliv osobu, o které se policejní orgán domnívá, že má u sebe věc důležitou pro trestní řízení. Jedná se o nejčastěji využívané oprávnění orgánů činných v trestním řízení.

1.1.2 Odnětí věci

Vychází z ust. § 79 zák. č. 141/1961 Sb. trestního řádu. Svým způsobem jde o pokračování výše uvedeného ustanovení o vydání věci a znamená, že nebude-li na výzvu vydána může být odňata. V případě, že tohoto ustanovení využívá policejní orgán, musí mít předchozí souhlas státního zástupce. Policejní orgán může tohoto ustanovení využít i bez předchozího souhlasu státního zástupce. To pouze v případě, nelze-li předchozího souhlasu dosáhnout a věc nesnese odkladu.

1.1.3 Příkaz k domovní prohlídce

Vychází z ust. § 83 zák. č. 141/1961 Sb. trestního řádu. Z hlediska trestního řádu může nařídit domovní prohlídku pouze předseda senátu, na návrh státního zástupce. Domovní prohlídku lze vykonat za předpokladu, kdy se na základě prověřování orgány činné v trestním řízení domnívají, že v prostorách užívaných k bydlení (dům, byt, případně jiný prostor, který prokazatelně slouží ke stálému bydlení osob) se nachází věc důležitá pro trestní řízení. Policejní orgán, který domovní prohlídku provádí by měl vědět co hledá.

1.1.4 Prohlídka jiných prostor

Vychází z ust. § 83a zák. č. 141/1961 Sb. trestního řádu. Z hlediska trestního řádu může nařídit domovní prohlídku pouze předseda senátu, na návrh státního zástupce. Domovní prohlídku lze vykonat za předpokladu, kdy se na základě prověřování orgány činné v trestním řízení domnívají, že v prostorách, které nejsou určeny k bydlení osob (garáže, sklady, vozidla atp.) se nachází věc důležitá pro trestní řízení.

1.1.5 Příkaz k osobní prohlídce

Vychází z ust. § 83a zák. č. 141/1961 Sb. trestního řádu. Z hlediska trestního řádu může nařídit osobní prohlídku pouze předseda senátu a v přípravném řízení státní zástupce. Policejní orgán bez příkazu soudce nebo souhlasu státního zástupce může prohlídku vykonat pouze v případě, kdy příkazu či souhlasu nelze předem dosáhnout, věc nesnese odklad, nebo jde o osobu přistiženou při činu či na kterou byl vydán příkaz k zatčení. Osobní prohlídku smí vykonávat pouze osoba stejného pohlaví. Pokud se při osobní prohlídce naleznou důkazy, které policejní orgán vyhodnotí jako důležité pro trestní řízení aplikuje se zde vydání či odnětí věci.

1.1.6 Odposlechy a záznam telekomunikačního provozu

Vychází z ust. § 88 zák. č. 141/1961 Sb. trestního řádu. Toto oprávnění lze využít v trestním řízení pro zločin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let a dalších taxativně vyjmenovaných. Nařídit odposlech či záznam telekomunikačního provozu smí předseda senátu, v přípravném řízení na návrh státního zástupce pak soudce. Jedná se o významný zásah do práv osob. Odposlech a záznam telekomunikačního provozu provádí pro potřeby orgánů činných v trestním řízení Policie České republiky. *Útvar zvláštních činností služby kriminální policie a vyšetřování (dále jen „ÚZČ SKPV“) je útvarem Policie České republiky, který v souladu s příslušnými ustanoveními trestního řádu, zákona o Policii České republiky a dalších právních předpisů provádí ve prospěch oprávněných bezpečnostních subjektů odposlech a záznam telekomunikačního provozu, sledování osob a věcí a další specializované úkony.* [2]

1.1.7 Data Retention

Vychází z úst. § 88a zák. č. 141/1961 Sb. trestního řádu. Prakticky za stejných podmínek, jako v případě odposlechu telekomunikačního provozu, které jsou popsány výše, může policejní orgán zjistit údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství. Jedná se například o kompletní záznamy provozu počítačové sítě, přidělení IP adres jednotlivým uživatelům v určitém čase, případně kam se který uživatel připojoval atp.

1.1.8 Sledování osob a věcí

Vychází z úst. § 158d zák. č. 141/1961 Sb. trestního řádu. Toto ustanovení znamená, že policejní orgán, s povolením soudce, získává poznatky o osobách a věcech, kdy musí vše provádět utajovaným způsobem. I za pomocí technických či jiných prostředků například sledování emailové komunikace.

1.2 Digitální důkaz z pohledu soukromých firem

Soukromé osoby také potřebují získávat digitální důkazy. Pomineme-li jednotlivé uživatele, jedná se tedy především o soukromé firmy, kdy je v jejich zájmu chránit svojí ICT infrastrukturu. Především z důvodu svého know-how, sítě zákazníků, finančních toků apod. Z pohledu získávání těchto důkazů to mají oproti orgánům činným v trestním řízení jednodušší, neboť infrastruktura ICT je v jejich vlastnictví. Nicméně to neznamená, že by mohli nakládat s daty nekontrolovatelně, i zde platí zákony upravující možnosti a limity zásahu (**zákoník práce č.262/2006 Sb.**). Zejména v u*st. § 316 odst. 1 Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.* [3] Ze zákona rovněž vyplývá, že zaměstnanci by měli být seznámeni s politikou kontroly firmy. A to nejlépe písemným poučením, které stvrdí svým podpisem, aby bylo prokazatelně dokázané, že zaměstnanci firmy byly poučeni o svých právech a povinnostech, které v souvislosti s užíváním ICT mají. Musí být dále poučeni o tom, že soukromá firma o nich sbírá osobní údaje, které uchovává a na jakou dobu. V souvislosti s tímto v brzké době tedy 24.05.2018 nabyde platnosti evropské nařízení 679/2016 o ochraně osobních údajů tzv. GDPR. Tato směrnice je v současné době ožehavé téma, a to jak u soukromých firem, tak státní správy. Vzhledem

k tomu, že při psaní diplomové práce ještě není účinné platnosti nebude se tímto nařízením diplomová práce dále zabývat.

1.2.1 Příklad přiměřeného monitorování zaměstnanců firmy

- *sledování doby strávené na internetu, včetně přehledu o navštívených*
- *sledování doby strávené chatováním, včetně přehledu o tom, s kým se chatovalo,*
- *přehled telefonické komunikace (příchozí i odchozí hovory) zaměstnance*
- *obsah pevného disku firemního počítače - zejména z hlediska legálnosti nebo nelegálnosti nainstalovaného a používaného software*
- *obsah přenosných médií (typicky USB flashdisků apod.) – zejména ve kvůli ochraně firemních tajemství a možnému úniku dat* [4]

1.2.2 Příklad monitorování zaměstnanců, který již je za hranou

- *skenování monitoru zaměstnance (myšleno obrazovka plochy PC)*
- *použití keyloggerů*
- *sledování obsahu soukromé konverzace, ať už chatování či e-mailů (vyjma zákonem stanovených případů)* [4]

1.3 Užití digitálních důkazů před soudem

Aby bylo možno využít digitální důkazy v rámci soudního řízení, byly proto nastavené postupy, které se liší na základě toho, zda jsou v rovině trestně právní nebo občanskoprávní a je-li je možné využít. V trestním řádu je stanoveno, že jako důkaz může sloužit vše, co může přispět k objasnění věci. Z hlediska trestního řádu se jedná například o výpovědi obviněných, svědků nebo znalců. Z hlediska posuzování digitálních důkazů se bude však v tomto případě využívat nejčastěji znalecký posudek z oboru informačních technologií, který odpoví na otázky, jejíchž odpovědi by mohli směřovat k řádnému objasnění věci. Znalecké posudky z této problematiky zpracovávají zejména osoby, které jsou zapsány u příslušného krajského soudu jako znalci z uvedené problematiky. Podmínky pro zapsání osoby do seznamu znalců upravuje v současné době zákon č. 36/1967 Sb. o znalcích a tlumočnících. Mimo soukromé znalce mohou znalecké posudky vypracovávat i znalecké ústavy. Z hlediska zpracování znaleckých posudků pro ICT, v rovině trestně právní, je možné vyjmenovat

významné instituce např. OKTE (odbory kriminalistické techniky a expertíz), oddělení analýzy dat a nosičů, které jsou součástí krajských ředitelství policie České republiky. Dále je možné jmenovat Kriminalistický ústav Praha, kde se problematikou posudku zabývá oddělení kyberkriminality a elekrotechniky.

1.4 Dílčí závěr

Tato kapitola se stručně zabývala legislativními možnostmi sběru digitálních důkazů z pohledu orgánů činných v trestním řízení, kdy jsou v mnoha případech závislé na činnosti státního zástupce, popřípadě soudce. Byly vyjmenovány oprávnění, které v trestním řízení využívají pro získávání digitálních důkazů. Toto vše může nahrávat především trestné činnosti v oblasti kyberkriminality, která nezná hranice, Kdy pro řádné prošetření je především rychlá reakce a nutnost rychlého šetření. Na základě posledního vývoje a zkušeností s kyberkriminalitou bychom mohli vyvodit, že do budoucna bude potřeba změna legislativy i struktury orgánů činné v trestním řízení, které se kyberkriminalitou zabývají, neboť stávající legislativa vychází pouze ze zkušeností z reálného světa. Virtuální svět je jiný, má jiné zákonitosti. Tyto změny budou potřeba vyřešit jak na národní, tak na nadnárodní úrovni. Je třeba se domnívat, že touto problematikou se do budoucna budou zabývat nejen specializované oddělení policie, ale i cíleně zaměření státní zástupci a soudci, kteří budou v oblasti kyberkriminality řádně proškolení.

Toto už se tak zcela netýká soukromých firem, které při dobrém nastavení bezpečnostní politiky, v podnikové ICT infrastruktuře, mohou vážně incidenty šetřit v reálném čase.

2 PRAMENY ELEKTRONICKÝCH DŮKAZŮ

Touto kapitolou se budu zabývat prameny digitálních důkazů, které lze definovat takto: r*ůzná zařízení jsou způsobilá generovat či uchovávat data, která mohou být využitelná jako zdroj elektronických důkazů v trestním řízení. V závislosti na zdroji mohou mít taková data různý charakter a musí k nim být při dokazování různě přistupováno jak z technického, tak procesního hlediska.* [5] V následujících odstavcích popíšu hlavní základy:

2.1 Osobní počítač

Slovo počítač není jednoznačně definováno, ale obecněji lze říci, že počítač je elektronické zařízení, které je schopné přijímat informace a na základě aritmetických instrukcí zpracovávat, uchovávat a generovat nové. V souvislosti se zajišťováním digitálních důkazů budeme v této práci hovořit o tzv. PC (personal computer), kdy se bude jednat o tzv. personální počítač nebo notebook, který má příslušná zařízení pro interakci s osobou (uživatelem) tedy klávesnici, monitor.

Z pohledu zajišťování digitálních důkazů je osobní počítač pramenem takovýchto informací, které se z větší části nacházejí na paměťových médiích. Tímto jsou myšleny systémová a uživatelská data uložená na pevných discích osobního počítače v operační paměti (RAM) v případě, že se zajišťují digitální důkazy ze zapnutého počítače.

Obrázek č.2 Osobní počítač

2.2 Datová úložiště NAS

Datové úložiště, která se zkratkou z anglické terminologie říká NAS (**Network Attached Storage).** V informatice se takto označuje úložiště, které je připojené k místní síti LAN. Data z takovéhoto úložiště jsou přístupná uživatelům místní počítačové sítě, a to dle příslušných oprávnění. Takovéto zařízení nemusí sloužit pouze jako souborový server, ale například jako klient sítě P2P, případně jako webový server a další. NAS z hlediska hardwarové konstrukce obsahuje obvykle jeden nebo více pevných disků, které se mohou sloučit do větší datové struktury a vytvořit tzv. RAID pole. Na takovémto zařízení obvykle běží nějaký operační systém (LINUX, BSD atp.), který zabezpečuje administraci a zprávu síťového úložiště. V poslední době takováto zařízení nabývají popularitě nejen v rámci firemního prostředí, ale i u soukromých osob, neboť celá rodina může v rámci vlastní sítě sdílet společná data. Z hlediska zajišťování digitálních důkazů jsou především zájmová data uložená na discích, které datové úložiště obsahuje, ale také systémové informace z operačního systému, který slouží k administraci zařízení.

Obrázek č. 3 síťové úložiště NAS

2.3 Mobilní telefony a tablety

Mobilní telefony jsou zařízení, bez kterých by si v současné době skoro žádný člověk nedokázal život představit, společnost je na nich závislá. Slouží k vzájemné komunikaci. S rychlým rozvojem techniky, díky plnohodnotnému operačnímu systému (např. IOS, ANDROID), již neslouží pouze ke zprostředkování telefonních hovorů, ale lze je fakticky používat jako osobní počítač, někdy by se dalo dokonce říci, že jsou používané i k více činnostem než klasické PC. Můžeme je používat jako platební kartu (přes technologii NFC), navigaci díky integrované technologii (např. GPS, Galileo, Glonass). Z pohledu digitálních důkazů je zájmová oblast vnitřní paměti mobilních telefonů, případně rozšiřitelných paměťových MicroSD karet. Zajišťování vnitřní paměti je poměrně problematické a technici, kteří je zajišťují pro tuto potřebu potřebují jednoúčelové sofistikované nástroje. Pro příklad je možno uvést zařízení UFED od izraelské společnosti Celebrite, švédské zařízení X-RY nebo software české společnosti MobilEdit.

Obrázek č.4 Mobilní telefon

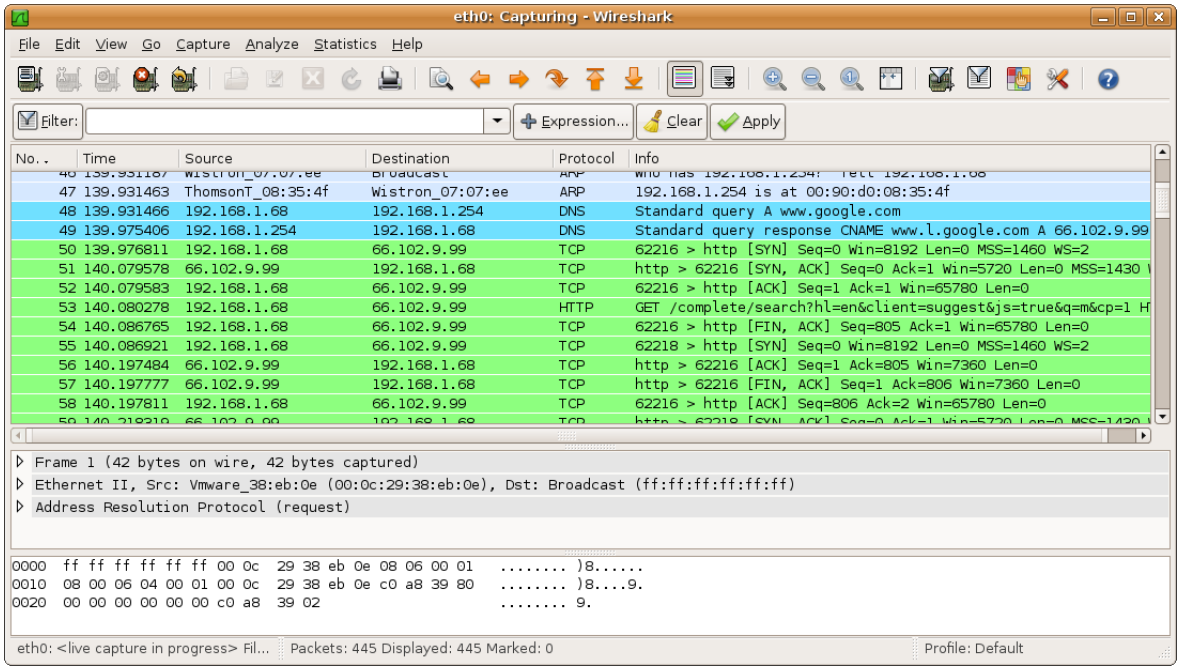
2.4 Průmyslová datová centra a cloudy

Datovými centry se označují specializované prostory pro techniku serverového typu, která jsou určena k nepřetržitému provozu a mají zajistit bezproblémový provoz. Budova bývá obvykle zabezpečena a je vybavena klimatizací kvůli regulaci teploty, aby nedošlo k přehřátí techniky. Taková to centra se využívají k provozování tzv. cloud computingu, což v principu znamená, že majitelé datových center propůjčují zákazníkům za poplatek určitý výpočetní výkon serverů. V současné době je trendem nepropůjčovat „železo“, ale datová centra jsou virtualizovaná a prakticky propůjčují virtualizované stanice. Zajišťování digitálních důkazů pro orgány činné v trestním řízení je komplikované a nikdy se neobejde bez spolupráce administrátorů datacenter. Protože bez znalosti celkového uspořádání, struktury a systému nelze, aby případně přibraný soudní znalec v rámci nějakého časově rozumného úseku zajistil zájmové digitální důkazy.

Obrázek č.5 Datacentrum

2.5 Počítačová síť

Počítačová síť je rovněž pramenem digitálních důkazů. Podstatné je, že při komunikaci mezi jednotlivými síťovými zařízeními nedochází pouze k přenosu obsahových dat, ale také k vytváření dat provozních, které se váží k jednotlivým vrstvám sítě. Tato provozní a lokalizační data poskytují informace o tom odkud a kam byla data přenášena, prostřednictvím jakého protokolu, zda byla zašifrována, případně mezi jakými aplikacemi ke komunikaci docházelo. Síťovou komunikaci lze odposlouchávat, a to za pomoci sniffovacího zařízení nebo softwaru. Odposlech lze provádět na různých vrstvách komunikace a lze tak získávat i přenášená data. Pokud jsou však obsahová data na aplikační vrstvě šifrována nemůžeme tímto způsobem dojít k obsahu dat. Mezi nejvíce známé zařízení, které soukromé firmy využívají tzv.data retention je specializovaný software od české společnosti Flow Mon. Z hlediska open source softwaru je možné využít k monitorování sítě, a to i v případě vytváření jednoúčelových sond například program TCPDUMP, případně uživatelsky přívětivý Wireshark.



Obrázek č.6 ukázka monitoringu sítě za pomocí programu Wireshark

2.6 Paměťová média

Hlavním pramenem digitálních důkazů, z hlediska zajišťování, jsou paměťová média. Jsou důležitým prvkem, na který se ukládají a uchovávají data výše uvedených pramenů digitálních důkazů. Stejně jako počítačová technika procházejí bouřlivým vývojem. Mezi základní paměťová média můžeme jmenovat tyto:

2.6.1 Pevné disky

Pevný disk (zkratka HDD z anglického termínu Hard Disk Drive). Jedná se o komponent, který se používá v osobních počítačích, noteboocích, datových úložištích, elektronicky spotřebních, případně jednoúčelových zařízeních k dočasnému nebo trvalému ukládání dat. Podle použití pevného disku je můžeme rozdělit na externí (přenosný disk, který můžeme k počítači či serveru připojit pomocí sběrnice USB 3.0, jejíž teoretická datová propustnost je 671 MB/s) a na interní (nepřenosný komponent počítače připojený přes příslušnou sběrnici, v současné době je nejpoužívanější SATA revize 3 jejíchž teoretická datová propustnost je 600 MB/S). Dále můžeme pevné disky rozdělit podle principu ukládání dat pomocí magnetické indukce, nebo polovodičů (tzv SSD disky), případně za pomocí obou dvou těchto metod, kdy se jedná o tzv. kombinované neboli hybridní disky. Kapacita na uložení dat se v současné době pohybuje u disků založených na magnetické indukci o maximální výši 12 TB, u SSD disků je to v současné době 4,8 TB. Co se týče hybridních disků dle šetření provedeného na současném trhu byly nalezeny nejvyšší hodnoty kolem 2TB. Mezi další parametry pevných disků patří například vyrovnávací paměť nebo propustnost datového toku (rychlost čtení, rychlost zápisu). Jsou samozřejmě disky, které využívají i jiné komunikační sběrnice. Byly uvedeny v textu výše, pro příklad uvádím mSata, M.2 sata dříve PATA atp. Digitální důkazy z tohoto paměťového média se získávají pomocí vytváření bitových kopií.

Obrázek č.7 Pevný disk

2.6.2 Operační paměti

Operační paměť RAM (dle anglického výrazu Random Acces Memory) je vnitřní paměť, která je připojena k základní desce počítače či jiného zařízení přes příslušnou sběrnici. Umožňuje čtení a zápis zpracovávaných dat, která jsou v ní dočasně uložena. Přístup k operační paměti je mnohem rychlejší, než k paměťovému médiu jako je například pevný disk. Při vypnutí počítače se veškerá data z této paměti ztrácí. Z hlediska klasifikace lze dodat, že operační paměti se v současné době vyrábějí o kapacitě maximálně 8 GB na sběrnici DDR2, DDR3 a DDR4. Za účelem získání digitálních důkazů z operační paměti se za pomoci specifických programů vytváří bitová kopie operační paměti.

Obrázek č. 8 Operační paměť RAM

2.6.3 DVD a Blue Ray

DVD neboli Digital Versatile Disc. Jedná se o formát digitálního optického datového nosiče, který se používá zejména pro přenos nového softwaru, filmů o vysoké obrazové kvalitě, případně jiná data jako pevný disk. Předchůdcem tohoto optického paměťového média bylo CD a nástupcem je právě Blue Ray. Co se týče maximální kapacity dat, tak CD mělo maximální teoretickou kapacitu 700 MB, u DVD je to 17,1 GB a u Blue Ray je maximální teoretická kapacita 128 GB. Z hlediska zajišťování digitálních důkazů se všechny tato optická média zajišťují in natura.

2.6.4 Další prameny důkazů

Samozřejmě existují i další prameny digitálních důkazů. V rámci této diplomové práce jsou jmenovány jen nejčastější z nich, které jsou prakticky zajišťovány. Ale pro potřeby diplomové práce je vhodné uvést i další prameny např. tzv. chytré hodinky určené k propojení s mobilním telefonem, herní konzole, jednoúčelové programovatelné automaty s vnitřní pamětí tzv. PLC atp. Vzhledem k tématu diplomové práce jsou opomenuty zdroje OSINT, která se dají brát také jako digitální důkazy ať se jedná třeba o informace z různých webových stránek, sociálních sítí, případně tzv. Dark Netu.

2.7 Dílčí závěr

Tato kapitola se zabývala jednotlivými prameny digitálních důkazů, které při realizaci případů zajišťují orgány činné v trestním řízení, popřípadě administrativní pracovníci firem při řešení bezpečnostních incidentů. I při stručném shrnutí můžeme si všimnout, že se jedná o nepřeberné množství věcí. Vzhledem k rychlému vývoji techniky lze vyvodit, jak velké nároky to klade na znalosti soudních znalců z oblasti ICT, administrátorů a dalších osob, které tyto data vyhodnocují a nemenší finanční nároky na nákup nových forenzních nástrojů, ať již se jedná o software nebo jednoúčelové zařízení, za pomoci, kterých provádí kompetentní osoby vyhodnocení zajištěných pramenů digitálních důkazů. Vzhledem k vývoji kyberkriminality je třeba zvyšovat investice do odborníků, kteří se zabývají touto činností.

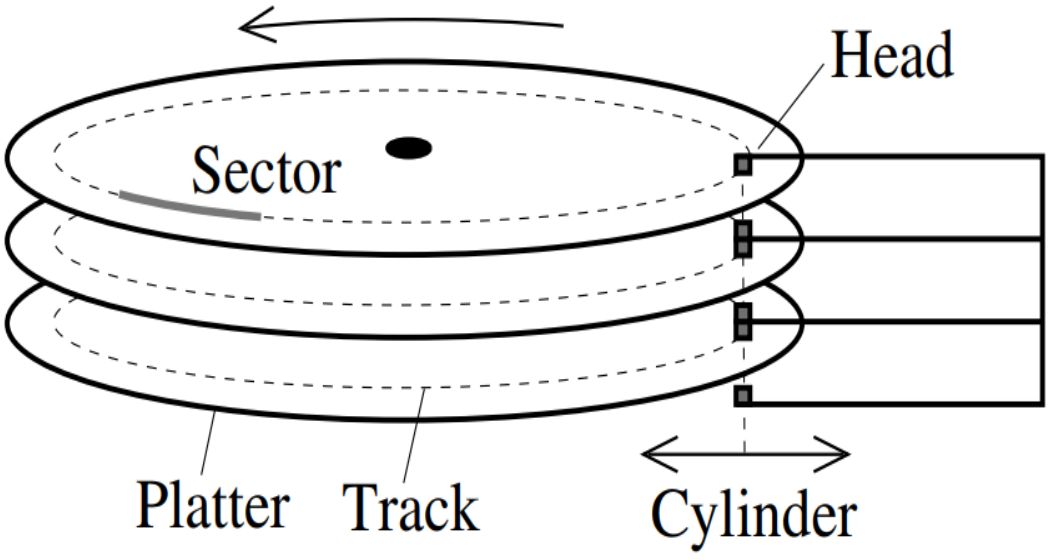
3 ORGANIZACE DAT NA PAMĚŤOVÝCH MÉDIÍCH

První dvě kapitoly diplomové práce se zabývaly legislativním rámcem zajištění digitálních důkazů a jejich prameny. Tato kapitola se bude zabývat samostatným uložením digitálních důkazů na paměťovém médiu.

3.1 Uložení dat na pevném disku klasického typu

Konstrukce pevného disku (s magnetickým principem ukládání dat) se obecně skládá z klasického stejnosměrného krokového motoru, který je obvykle napájen napětím 12V a otáčí jednotlivými plotny disku, na kterých jsou fakticky ukládány data. Ty se na pevný disk ukládají za pomocí zařízení, které se nazývá hlava disku (anglicky Head). Pevné disky samozřejmě obsahují i řídící elektroniku koordinující otáčení disku a ukládání dat. Mezi další funkce řídící elektroniky patří i diagnostika stavu.

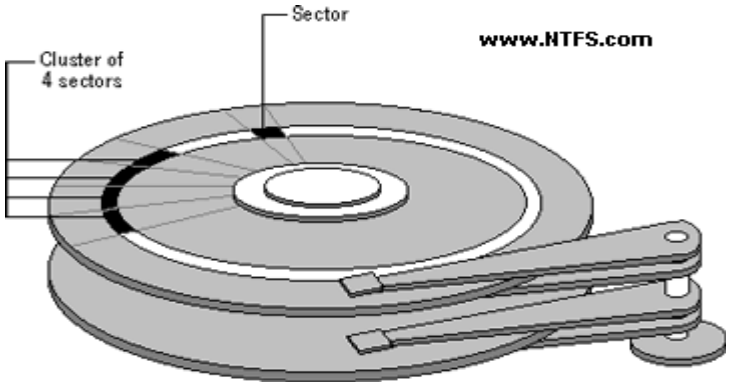
Data u klasického pevného disku s magnetickým záznamem organizována do soustředných kružnic. Každá tato soustředná kružnice se nazývá stopou (anglicky Track), stopa je obvykle rozdělena na proměnný nebo pěvně stanovený počet sektorů na stopu. Hlava disku může na takovouto stopu jednu chvíli číst nebo zapisovat. Na disku o velikosti 3,5 palce se může nacházet i více jak 1000 stop. Na dalším obrázku můžeme vidět principiální konstrukci disku s jednotlivými plotnami, sektory a stopami. Pokud disk obsahuje více ploten, tak všechny stopy, které se nacházejí přesně nad sebou jsou shluknuty do tzv. cylindru. Tohoto principu se využívalo při starší adresaci.



Obrázek č. 9 Konstrukce disku

Sektor je nejmenší adresovatelná jednotka na disku. Vyznačuje se tím, že má pevnou délku obvykle se jedná o 512 bytů, ale u novějších disků se již používá velikost sektoru 4 KB. Identifikační údaje o sektorech jsou zapsány bezprostředně před obsahem sektoru a identifikují jednoznačnou adresu každého sektoru. Optimální způsob ukládání dat na disk je ukládání v řádku na jedné stopě za sebou. Pokud bychom chtěli uložit soubor o velikosti 600 bytů muselo by k takovému to uložení být využity dva sektory.

Sektory je možné shlukovat do větších oblastí, které nazýváme clustery, kdy se jedná o jeden nebo po sobě více jdoucích sektorů. Počet sektorů je vždycky exponentem dvou. To znamená, že můžeme mít cluster o velikosti jednoho sektoru, dvou sektorů, čtyř sektorů, osmi, šestnácti atp. Proces ukládání dat do clusterů chrání data, před možným přepsáním.



Obrázek č. 10 Sectory a Clustery

Adresování sektorů dříve probíhalo metodou tzv. CHS (cylindr-hlava-cector), v současné době se ovšem využívá metoda tzv. LBA (linear block adress) to znamená, že každý sector má přidělené číslo (0.N), které ho jednoznačně identifikuje. Systém LBA dříve využíval 28 bitovou adresu a pokud by měl sektor velikost 512 bytů, byla by teoreticky nejvyšší možná kapacita disku 128 GB. V současné době již systém LBA využívá 48 bitovou adresu tzn., že v současné době je možné teoreticky zkonstruovat nejvyšší disk o kapacitě 128 PB. Starý způsob adresace dle konstrukce umožňoval teoreticky nejvyšší možnou kapacitu disku o velikosti asi 7,8 GB. Což by pro potřeby dnešní doby byla zcela nedostatečná kapacita. [6]

3.2 Uložení dat na disku SSD

SSD disk neboli solit state drive je označení paměťového média, který na rozdíl od klasických disků neobsahuje žádné pohyblivé části (plotny), ale data se ukládají na principu NAND flash pamětí. Nejmenší adresovatelnou jednotkou jsou v tomto případě stránky o velikosti 4KB, které se řadí do bloků o velikosti 512 KB. To znamená, že jeden blok obsahuje 128 stránek. Prázdné stránky lze zapisovat jednotlivě. V případě přepisu je potřeba načíst celý blok dat, přepsat hodnoty a tento blok zpátky uložit v přepsané podobě. Výhoda tohoto systému je jeho rychlost. Nevýhodou tohoto systému je, že na rozdíl od pevných disků klasického typu neumožňuje takový systém přepisů, proto je vhodné tyto disky využívat především jako systémové, protože nedochází k vysoké míře přepisů na rozdíl od disků, které jsou využívány na ukládání uživatelských dat. Tato technologie se dále využívá pro výrobu USB disků, operačních pamětí a SD karet. [5]

3.3 Ukládání dat na optická média

Ukládání dat na optická paměťová média pracují na principu světla neboli elektromagnetických vln, které jsou blízké světelnému spektru, ty slouží jak pro čtení, tak i k zápisu dat. Některé optické mechaniky umožňují pouze čtení dat, jiné umožňují jak čtení, tak i zápis dat. Technologie optického zápisu se využívá zejména u paměťových médií CD, DVD a Blue Ray.

3.4 Dílčí závěr

V uvedené kapitole byly probrány základní principy, jakým způsobem dochází k ukládáni dat na paměťová média. Základní znalosti této problematiky jsou důležité pro všechny pracovníky v informatice, zejména však pro osoby, které se zabývají forenzní analýzou digitálních důkazů. Z hlediska zajišťování digitálních důkazů pro potřeby orgánů činných v trestním řízení jsou pevné disky zatím pořád nejpočetnějším digitálním důkazem, který je dále zkoumán.

4 OPERAČNÍ SYSTÉM LINUX

Počátek vývoje operačního systému Linux můžeme datovat kolem roku 1991. Student Helsinské univerzity jménem Linus Tonvald byl fascinován jádrem operačního systému Minix (odvozeno od sousloví Mini Unix). Vzhledem k tomu, že jádro nebylo složeno z proprietárního kódu a že k tomuto jádru nebyly dostupné zdrojové kódy, začal vyvíjet svůj vlastní. První verze vznikla někdy v první polovině září a nesla označení 0.01. Jádro systému bylo v té době absolutně nepoužitelné pro jakoukoliv implementaci, ale vzhledem k tomu, že byl veřejně znám jeho zdrojový kód, tak vzbudil na straně internetové komunity obrovský zájem. Ukázalo se, že otevřený zdrojový kód byla jeho hlavní výhoda oproti jádru operačního systému MINIX. Byl to krok správným směrem a jádro operačního systému Linux se začalo vydávat pod tzv. GNU GPL licencí. Zkratka GNU znamená GN is not unix a GPL je zkratkou výrazu General Public Licence. Tato licence zaručuje původnímu autorovi, že další změny v programech nezpůsobí následnou komercializaci. K tomu lze uvést to, že operační systém Linux je dosud bezplatný. Je tedy pravda, že v současné době existují již komerční verze Linuxu, ale stále mají otevřený kód. Platí se v podstatě za uživatelskou podporu. Například distribuce RED HAT (distribuce budou probrány v další kapitole). Vývoj dále již pokračoval za přispění komunity. V roce 1994 byla konečně vydaná verze jádra 1.0, která již podporovala TCT/IP sítě, ovladače síťových karet a mělo přepracovaný souborový systém. [7] V současné době to je k 08.05.2018 nejnovější verze jádra 4.9.98. [8]

4.1 Distribuce operačního systému Linux

Operační systém Linux umožňuje zkompilování programů balíčků přímo ze zdrojového kódu. Vzhledem k tomu, že tato operace může být příliš zdlouhavá to vedlo ke vzniku již zkompilovaných balíčků. Za pomoci těchto balíčků se do operačního systému instaluje nový software. V současné době se používá několik hlavních balíčkovacích systémů a podle toho jaký balíčkovací systém různé distribuce podporují, tak je rozdělujeme.

4.1.1 Distribuce podporující balíčkovací systém RPM

- Red Hat
- Open SUSE
- Cent OS

4.1.2 Distribuce podporující balíčkovací systém APT

- Debian
- Ubuntu
- Mind

4.1.3 Distribuce, které se zásadně kompilují ze zdrojového kódu

- Gentoo
- Pentoo

Tyto distribuce jsou určeny pouze pro pokročilé uživatele, kteří si svůj systém sestavují po svém. Instalace takového systému je poměrně náročná. V komerčním použití se tento systém nedoporučuje, neboť co systém to originál. S tímto tvrzením asi nebudou souhlasit uživatelé Gentoo, kteří zastávají princip, že v systému mají mít nejnovější software od jádra počínaje, uživatelským prostředím konče. Autorovi práce instalace tohoto systému zabrala týden dovolené.

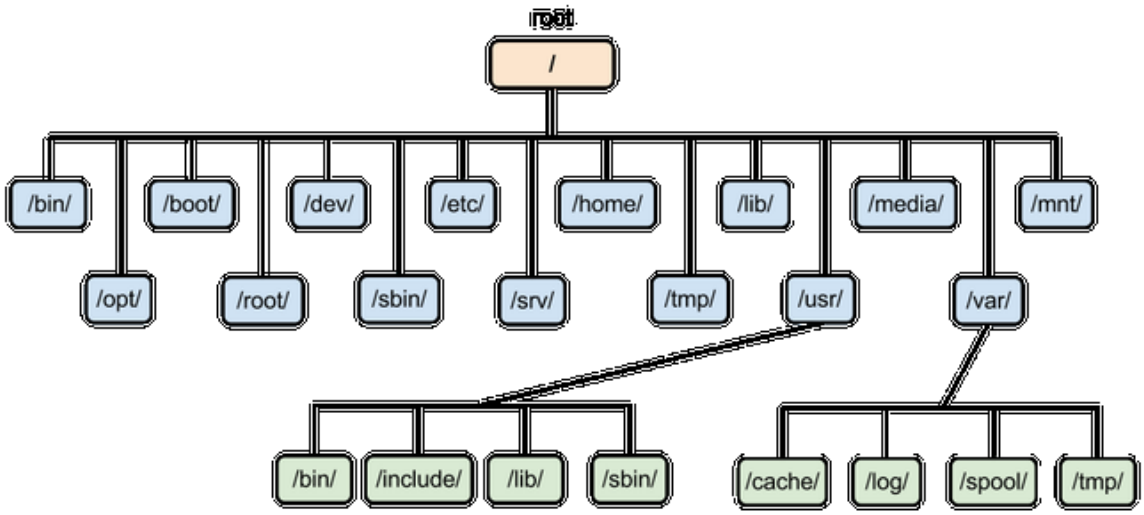
Co se týče rozdělení jedná se pouze o základní, existuje více balíčkovacích systémů a počet distribucí. V roce 2014 bylo odhadnuto, že existovalo 285 distribucí a trendem bylo, že počet distribucí klesá. [9]. Vidíme, že počet distribucí je obrovský a z toho můžeme vyvozovat, že jsou distribuce, které se přímo specializují na forenzní analýzu digitálních důkazů. Mimo jiné jsou to například distribuce s názvem Kali Linux, Parrot (použitelné především pro provádění penetračních testů), dále pak systémy Cayne Linux a Deft Linux, které jsou určené přímo pro forenzní analýzu digitálních důkazů. Musíme zmínit ještě jeden systém a to PALADIN, jedná se o distribuci, která je určená pro forenzní zkoumání systémů Mac OS.

4.2 Posix

Portable Operating System Interface, přenositelné rozhraní pro operační systémy, standardizované jako IEEE 1003 a ISO/IEC 9945. Vychází ze systémů UNIX, a určuje, jak mají POSIX-konformní systémy vypadat, co mají umět, co se jak dělá apod. POSIX zahrnuje různé aspekty operačních systémů, např. správu procesů, práci se soubory, meziprocesovou komunikaci, základní programy (ed, awk, Korn Shell apod.), síťové záležitosti atd. - celkem se jedná o 15 dokumentů. GNU/Linux je od základu navržen podle POSIX, a zajišťuje tedy dobrou přenositelnost z a na jiné systémy splňující tento standard. [11]

4.3 Struktura operačního systému Linux

K adresářové struktuře operačního systému Linux lze říci, že se jedná o velkou stromovou strukturu, jehož začátek je u tzv. kořene, který je označený lomítkem „/“. Za tímto kořenem pokračuje kompletní adresářová struktura, ke které se mohou připojovat další diskové oddíly. Linux se vyznačuje tím, že cokoliv, co se nachází v systému je soubor, v případě že to není soubor, tak se jedná o proces. Adresářem v Linuxu je pouze soubor, který obsahuje názvy dalších souborů. V kořenu Linuxu se nacházejí systémové adresáře operačního systému. Které mají přesně definovanou funkci v systému a obsahují další soubory, které jsou potřeba pro chod systému. Pro lepší znázornění se můžeme podívat na následující obrázek.



Obrázek č. 11 Adresářová struktura Linuxu

Adresář /bin

Obsahuje veškeré uživatelské programy, které používá systém, přístup k nim má i uživatel s administrátorským oprávněním (tzv. ROOT) a běžní uživatelé.

Adresář /boot

Obsahuje spouštěcí soubory systému, jádro systému (tzv. Kernell) a jeho předchozí verze. Dále obsahuje také data spouštěče tzv. GRUB. Tato zkratka znamená Grand Unifield Boot – Loader.

Adresář /dev

Obsahuje veškerá periferní zařízení počítače a jsou zde reprezentovány soubory se speciálními vlastnostmi. Tento adresář například obsahuje připojená paměťová média k počítači. Pevný disk je zde reprezentován jako soubor pod adresou např. /dev/sda. Toto je soubor, který reprezentuje celý pevný disk. Oddíly jsou pak následně prezentovány jako soubory /dev/sda1..n.

Adresář /etc

V tomto adresáři jsou umístěny nejdůležitější konfigurační soubory systému. Jako příklad můžeme uvést soubor /etc/fstab. Tento konfigurační soubor popisuje jednotlivá paměťová média připojená do systému a ukládá jim různé parametry. Určuje paměťové médium a místo v souborovém systému, kam ho budeme připojovat. Typ souborového systému na oddílu. Určuje, jestli daný oddíl bude zálohován a jako kolikátý v pořadí bude kontrolován při startu.

Adresář /home

V tomto adresáři se nacházejí adresáře jednotlivých obyčejných uživatelů v systému. V jednotlivých uživatelských adresářích se pak následně nachází adresář plochy, dokumentů, obrázků videí a dalších libovolných adresářů a souborů, které jednotlivý uživatelé vytvoří.

Adresář /lib

Obsahuje knihovny, které využívají jak systémové, tak uživatelské programy.

Adresář /media

Jedná se o adresář, který obsahuje podadresáře, které se používají jako body pro připojení externích zařízení, jako jsou například CD, DVD mechaniky, Blue-Ray atp.

Adresář /mnt

Toto je standartní přípojné místo externích souborových systémů.

Adresář /opt

Obvykle tento adresář obsahuje nainstalované programy třetích stran.

Adresář /root

Jedná se o domovský adresář administrátora systému tzv. superuživatele hovorově ROOTA.

Adresář /sbin

Obsahuje programy, které jsou využívány systémem, administrátorem a uživateli, kteří mají administrátorská oprávnění a mohou použít příkaz SUDO (uživatelé musí být umístěni do skupiny uživatelů SUDOERS)

Adresář /tmp

Jedná se o odkládací Adresář dočasných souborů. Při každém startu systému se tento adresář automaticky smaže, proto by uživatelé neměly svá data do tohoto prostoru nikdy ukládat.

Adresář /usr

Obsahuje programy, knihovny, dokumentaci ke všem uživatelským programům.

Adresář /var

Obsahuje soubory, které se za běhu systému většinou mění. Jsou zde umístěny logovací soubory systému např. messages, syslog, maillog, cron atp.

Adresář /proc

Jsou zde soubory, které indikují aktuální nastavení systému, v podstatě by se dalo říct, že se jedná o mapu aktuálního stavu paměti.

Adresář /sys

Jedná se o virtuální adresář jádra systému. A to od verze 2.6.

Adresář /lost+found

Jsou zde umístěny soubory, které byly poškozeny při nestandartním vypnutím systému. [12]

4.4 Ovládání Linuxu

Stejně tak jako jiné operační systémy například Microsoft Windows, OS X od společnosti Apple, tak i různé distribuce Linuxu mají i svá uživatelsky přívětivá rozhraní. Nejčastěji se jedná o systémy KDE a GNOME. Pro počítače, které mají nízký výpočetní výkon můžeme používat uživatelské prostředí zvané XFCE. Nejčastěji se však pro administraci a práci s Linuxem používá příkazová řádka (tzv. terminal), za pomoci, které lze systém jednoduchým způsobem ovládat, a i automatizovaně zadávat systému různé úkoly. Nejčastěji používaná verze příkazové řádky je tzv. BASH (Born Again Shell).

4.4.1 Základní příkazy v terminálu.

pwd

Pomocí tohoto příkazu zjistíme v jakém jsme adresáři.

cd

Tento příkaz zajišťuje přechod mezi adresáři.

ls

Slouží k výpisu jmen, práv a velikostí souborů v určeném adresáři.

touch

Vytvoří nový soubor.

rm

Smaže složku nebo adresář.

move

Tímto příkazem můžeme přesunout soubor nebo jej přejmenovat.

cat

Příkazem můžeme zajistit výpis obsahu souboru na obrazovku.

cp

Zkopírujeme určený soubor na požadovanou adresu.

sudo

V případě, že před nějakým příkazem napíšeme sudo, tak to znamená, že jsme ho spustili s administrátorským oprávněním superuživatele.

ps

Slouží k vypsání běžících procesů.

kill

Slouží k ukončení požadovaného procesu.

chmod

Pomocí tohoto příkazu měníme oprávnění vybraného souboru.

PIPE (neboli hovorově pajpa označená „|“)

Jedná se o důležitou implementaci, kdy standartní výstup nějakého příkazu můžeme přesměrovat na standartní vstup dalšího příkazu.

Jedná se pouze o základní vybrané soubory z terminálu, každý z těchto příkazů může mít různé parametry. V rámci těchto příkazů lze vytvářet jednoduché skriptovací programy pro ovládání systému Linux, běžně hovorově jim říkáme skripty. Soubory mají obvykle koncovku sh např. skript.sh. [13]

4.5 Využití operačního systému Linux pro forenzní zkoumání.

Jak bylo popsané v předchozích kapitolách, operační systém Linux je systém, který vytvořili především programátoři pro programátory. Vzhledem k zavedeným standardům viz POSIX a otevřený zdrojový kód je jednoznačně čitelné a odhadnutelné, jakým způsobem se bude chovat. Totéž nemůžeme říci o systémech od společnosti Microsoft nebo Apple. Pro účely forenzní analýzy digitálních důkazů je především nutné tuto stopu uchovat ve výchozím neměnném stavu a systém Linux je proto nejvhodnější formou, protože při zapnutém stavu po zasunutí média automaticky tyto média nepřipojí k systému a nezapisuje na ně. To jinými slovy znamená, že neznehodnocuje zajištěný digitální důkaz (U čistě neforenzních distribucí Linuxu je potřeba zkontrolovat konfiguraci, protože po zasunutí paměťového media by mohlo dojít k „automountnutí“ k souborovému systému. Toto chování bylo zjištěno u uživatelského prostředí GNOME, kde je potřeba tuto konfiguraci změnit).

4.5.1 Vytváření bitových kopií.

Bitová kopie je přesný „otisk“ paměťového média. V rámci zkoumání digitálních důkazů je to prvotní a velmi důležitý úkol. Vytváříme je proto, abychom digitální důkaz uchovali, nepozměnili a mohli ho dále zkoumat za pomocí forenzních nástrojů. Tento úkon se dá provozovat, jak na paměťovém médiu, tak ze živého systému. Existují různé nástroje pro vytváření bitových kopií, tak i různé formáty ve kterých můžeme uchovávat digitální důkazy.

4.5.2 Formáty bitových kopií

RAW image formát

Tento formát je kopie originálu bit-by-bit RAW. Jedná se o nejčastější formát, který podporují linuxové nástroje.

Encase image file format tzv. E01

Jedná se o druhý nejpoužívanější formát pro forenzní zkoumání. Užívají ho obvykle bezpečnostní složky. Mezi jeho výhodu patří ta, že je komprimovaný a velikost výsledné bitové kopie je menší než původního disku. Tento formát podporují v současné době veškeré forenzní nástroje.

SMART

Jedná se o dřívější forenzní formát pro bitové kopie od společnosti Encase. Mohl být jak komprimovaný, tak nekomprimovaný. Býval opatřen kontrolním součtem CRC. V současné době se již nepoužívá. [14]

4.5.3 Linuxové nástroje pro vytváření bitových kopií

NAME	SIZE	TYP
SDB	223 GB	disk
SDB1	4 GB	part
SDB2	512 MB	part
SDB3	218,5 GB	part

Tabulka č. 1 Seznam disků

Z výpisu vidíme, že se jedná o harddisk označený jako sdb, který má velikost 223 GB, je rozdělený na tři logické oddíly o velikostech 4GB, 512MB a 218,5 GB. Jednotlivé oddíly jsou označeny jako sdb1, sdb2 a sdb3. Celá adresa disku je /dev/sdb.

cat

Jak bylo řečeno, všechno v systému Linux je bráno jako soubor. Lze tedy i tímto jednoduchým příkazem vytvořit bitovou kopii paměťového média. Prakticky bychom to vyřešili následujícím způsobem.

 # cat /dev/sdb >> /zkoumani/image.dd

Výpis souboru by byl přesměrován do souboru bitové kopie na našem disku. Jednalo by se o přesnou kopii disku a nedošlo by při tomto úkonu k manipulaci se stopou. Toto je naprosto nouzový přístup v případě, že by nebyl k dispozici žádný jiný nástroj. Neboť nelze nastavit žádný parametr pro ovlivnění čtení disku. V případě vadného disku by mohlo dojít k pádu aplikace. Nicméně postup je použitelný, a to nejen v teoretické rovině. Autorem práce bylo vyzkoušeno prakticky a bitová kopie byla totožná s paměťovým médiem.

dd

Jedná se o úplně první nástroj v Linuxu k vytváření bitových kopií**.** K provedení bitové kopie zapíšeme následující příkaz:

 # dd if=/dev/sdb of=/zkoumani/image.dd bs=512 conv= noerror, notrunc, nosync

Parametr if příkazu znamená input file a tedy zájmový disk sdb. Parametr of znamená output file a přesná bitová kopie bude uložena do souboru image.dd. Parametry za conv znamenají, že se disk nebude zkracovat v případě, že by na konci byly nuly a že se budou přeskakovat chyby na disku, takže nedojde k pádu v případě, že jsou vadné sektory a systém by je nemohl přečíst. Parametr bs v tomto případě znamená, že se data budou načítat po 512 bytech. Můžeme v tomto parametru samozřejmě nastavit i jinou hodnotu typicky například 4K (4 kilobajty). [15]

dc3dd

 # dc3dd if=/dev/sdb of=/zkoumani/image.dd log=/zkoumani/image.log hash=sha1

Z tohoto příkazu můžeme vidět, že program po vytvoření bitové kopie vytvoří ještě HASH v tomto případě za pomocí hashovací funkce SHA1, aby byla zabezpečena neměnnost digitálního důkazu. [16]

ddrescue

 # ddrescue -r2 /dev/sdb /zkoumani/image.dd /zkoumani/image.log

Příkaz ddrescue vytvoří bitovou kopii a průběh zkoumání zapisuje do logovacího souboru v tomto případě image.log. Program čte disk po větších blocích. V případě, že narazí na chybu, tak jí přeskočí a chybné sektory se pokouší číst znovu. V tomto případě dle nastavení dvakrát. Dělá to tím způsobem, že se snaží vadnou oblast číst po menších objemech dat, až narazí na hardwarový strop což bývá 512 bytů. [17]

dcfldd

 # dcfldd if=/dev/sdb of=/zkoumani/image.dd bs=512 hash=SHA512 errorlog=/zloumani/image.log hashlog=/zkoumani/hash.txt

Význam následujícího příkazu je obdobný, jako u předchozích s tím rozdílem, že byla vytvořena hash funkcí SHA512. [18]

Je možné využít i dalších nástrojů pro vytvoření bitové kopie, jako je například software třetí strany FTK Imager. Tento nástroj podporuje vytvoření bitové kopie i ve formátu E01. Mezi nástroje, které lze využít v prostředí GUI jsou například GUYMAGER, který podporuje rovněž komprimovaný formát bitových kopií E01. Dále pak můžeme jmenovat ještě PALADIN TOOLBOX, který je implementován v linuxové forenzní distribuci PALADIN.

4.5.4 Dump operační paměti RAM

Pro vyšetřování bezpečnostních incidentů je většinou důležité získat data z operační paměti počítače. Taková to data se mohou stát velmi důležitým důkazem, a to jak pro bezpečnostní analytiky, tak pro orgány činné v trestním řízení. Tato se získává ze zapnutého napadeného stroje. Postup zálohy operační paměti je závislý na operačním systému, který běží na zdrojovém zařízení. U operačního systému Windows zálohu operační paměti můžeme provést programem FTK Imager, který má tuto funkci v sobě implementovanou. V případě, že se jedná o zařízení, na kterém běží operační systém Linux, tak je třeba mít administrátorské oprávnění a dump lze provést za pomocí open source utility LIME následovně. Stáhneme zdrojové kódy tohoto programu a ve zdrojové složce této utility spustíme v terminálu příkaz:

 # make

Tímto příkazem zkompilujeme modul, který je v souboru lime.ko a následně za běhu systému nainstalujeme do systému. A to tímto způsobem:

 # insmod /source/lime.ko "path=/zkoumani/ram.lime format=lime"

Pomocí příkazu insmod je možné instalovat další moduly do linuxového jádra. První část příkazu odkazuje na zkompilovaný modul, která do jádra instalujeme. Adresa v uvozovkách určuje prostor, kam se nám má tento dump uložit. Posledním parametrem, který je označený format= určujeme, v jakém formátu se paměť uloží. Nejvhodnější je dle dokumentace nastavení na formát lime, a to i vzhledem k dalšímu forenznímu zkoumání tohoto dumpu. [19]

4.5.5 Zabezpečení integrity stopy

K tomu, abychom prokazatelně zabezpečili neměnnost digitálního důkazu využíváme tzv. hashovacích funkcí. Co to je hashovací funkce? Jedná se o matematickou funkci pro převod vstupních dat do relativně malého čísla. Tomuto číslu se hovorově říká hash. Základní vlastnosti jsou:

- z jakéhokoliv množství vstupních dat vytvoříme stejně dlouhý hash,
- malou změnou vstupních dat dosáhneme velké změny na výstupu,
- z výstupu funkce je nemožné rekonstruovat původní zprávu,
- v praxi musí být vysoce nepravděpodobné, že dvěma rozdílným vstupním datům odpovídá jiný hash.

Pro vytvoření kontrolní hashe za využití funkce SHA256 z bitové kopie image.dd můžeme využít následující příkaz:

#sha256sum /zkoumani/image.dd >>hash.txt

V současné době se používají tyto Hashovací funkce MD5, SHA1, SHA256, SHA384 a SHA512. Hashovací funkce MD5 a SHA1 již se nepovažují za bezpečné v případě MD5, a proto je vhodnější používat poslední tři jmenované, případně kombinaci hashí k zajištění integrity stopy např. MD5 a zároveň SHA1. [20]

V následující tabulce vidíme ukázky výstupů hashovacích funkcí pro řetězec **„ahoj“:**

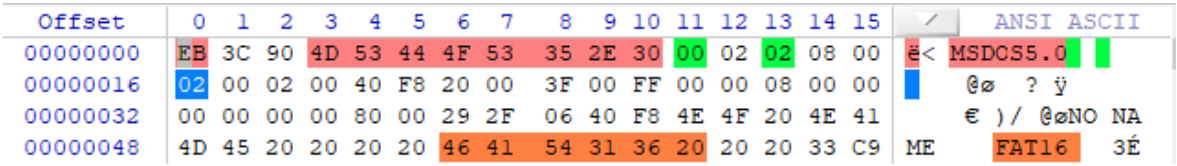
FCE	Výstup
MD5	79C2B46CE2594ECBCB5B73E928345492
SHA1	edb433bdd7c13851c7c68cb31a5acf33a80cd2cc
SHA256	3f3b08eca62c21d76256e6e1d0b8bf99f4efbe376f64335b72f4163a8fc50dba

Tabulka č. 2 Výstup hashovacích funkcí ze vstupního řetězce ahoj

4.5.6 Ruční zkoumání filesystému pomocí hexaeditoru

Dalším krokem, který můžeme provádět v rámci analýzy za pomocí linuxových nástrojů, je analýza jednotlivých oddílů paměťových médií na úrovni souborového systému. Jednotlivé oddíly můžeme analyzovat za pomocí hexa editorů, které lze spustit v terminálu, případně v rámci uživatelského rozhraní. Příklady hexa-exitorů pro terminál hd, hexdump, hexeeditor. Pro uživatelské rozhraní GUI můžeme uvést například BLESS. Příklady takového zkoumání jsou následující:

a) Analýza zaváděcího sektoru (souborového systému FAT 16)



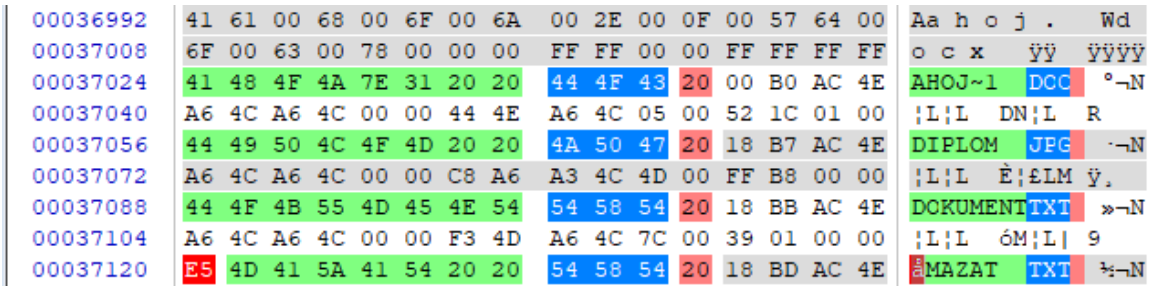
Obrázek č. 12 zaváděcí sektor FAT

Na výše uvedeném obrázku vidíme uživatelské prostředí HEXA editoru. Na levé části je zobrazený offset neboli adresace jednotlivých dat. V prostřední části jsou hodnoty jednotlivých bytů zapsaných v hexadecimální podobě po 16ti hodnotách. To znamená, že každý řádek obsahuje data o 16 bytech. V úplně pravém sloupci jsou programem tyto hodnoty interpretovány do ASCI tabulky, pokud daná hodnota z HEXA interpretuje nějaký znak z této tabulky.

K popisu zaváděcího bloku. V prvních třech bytech (0,1,2) je uložena skoková instrukce tzv. jump na boot strap, což je zaváděcí program operačního systému. V dalších 8 bytech je umístěn název Vendora, který vytvořil souborový systém. Jedná se o hodnoty 4D, 53, 44, 4F, 53, 35, 2E, 30. Jak je vidět z pravého sloupce tato hodnota interpretuje vlastníka MS DOS 5.0, ale může tam být např. IBM atp. Další jeden byte č. 11 je nastaven v hodnotě 00. Tato defaultní hodnota znamená, že velikost jednoho sektoru je defaultně nastavená na hodnotu 512 bytů. Na obrázku je zvýrazněn zelenou barvou. Byte č. 13 je nastaven na hodnotu 02. Tato hodnota znamená, že jeden klastr obsahuje dva sektory. Defaultně je při formátování oddílu v operačním systému Microsoft Windows nastavena tato hodnota na 01 a to znamená, že velikost clusteru je právě o velikosti jednoto sektoru. Byte č. 16 je zvýrazněn modrou barvou a má v této podobě nastavenou hodnotu na 02. Tato hodnota znamená, že na oddíle je umís-

těna jedna FAT tabulka a za ní je umístěna její kopie. Na posledním řádku souboru je oranžově zvýrazněna hodnota, která nám určí, jaký souborový systém je na oddíle nahrán. zvýrazněna hodnota, která nám určí, jaký souborový systém je na oddíle nahrán. V tomto případě se tedy jedná o souborový systém FAT 16, jak je možné intuitivně rozpoznat z pravého sloupce, kde jsou jednotlivé hodnoty interpretovány znaky z ASCI tabulky. Zaváděcí blok samozřejmě v sobě nese daleko více informací, jako je například offset clusteru, kde se nachází alokační tabulka, dále offset tzv. root direktory, ale pro základní pochopení funkce souborového systému byly popsány jen ty základní.

b) Analýza tzv. ROOT DIRECTORY (FAT 16)



Obrázek č. 13 ROOT DIRECTORY

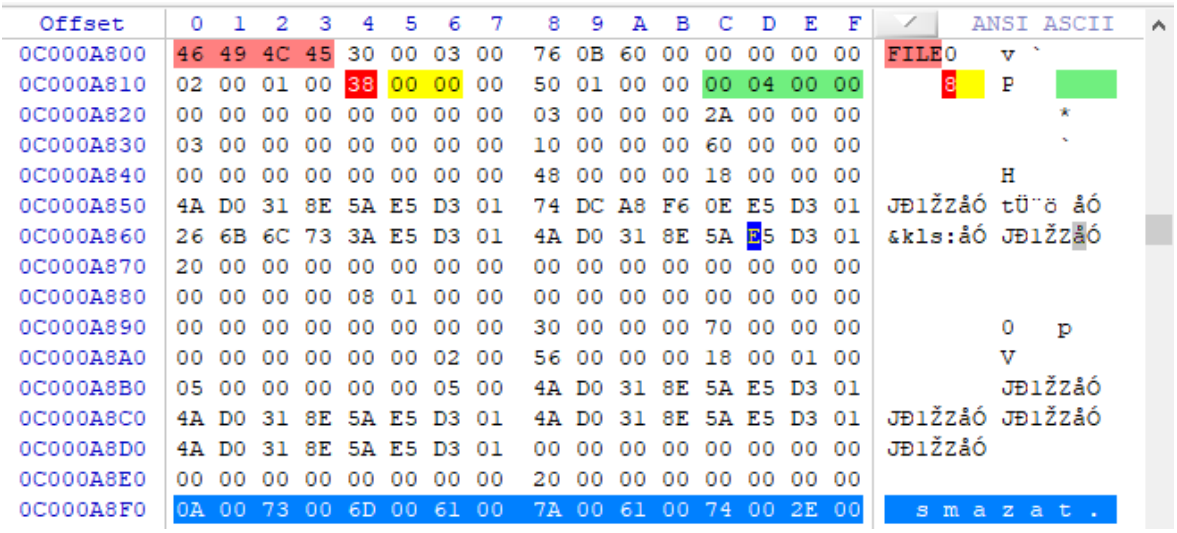
První záznam začíná na offsetu 37024. Prvních 8 bytů vyznačeno zeleně je vyhrazeno pro název souboru. Jak můžeme vidět v pravém sloupci, kde jsou interpretovány znaky ASCII, tak zde vidíme název prvního souboru AHOJ. Další 3 byty jsou určeny pro koncovku souboru. Koncovka souboru je vyznačena modrou barvou. V tomto případě systém ukazuje, že se jedná o koncovku doc, ačkoliv ve skutečnosti se jedná o soubor docx. Defaultně souborový systém FAT 16 je schopen zobrazovat koncovky o velikosti maximálně 3 znaků. Z tohoto důvodu je nad tímto souborem ještě jeden záznam, který je vyznačen šedivou barvou. Poslední položka, která je vyznačena oranžovou barvou určuje atribut souboru. Co jednotlivé atributy souboru znamenají můžeme vidět v následující tabulce.

Hodnota attributu v HEXA	Význam atributu
01	Soubor jen ke čtení
02	Skrytý soubor
04	Systémový soubor
08	Jedná se o popis svazku
10	Popisuje podadresář
20	Je vždy vyznačen při změně souboru

Tabulka č. 3 Atributy záznamů v ROOT DIRECTORY

Z tabulky můžeme vidět, že atributy našich záznamů v root direktory všechny nabývají hodnoty 20. Tato hodnota bytu je taková z toho důvodu, že soubory byly na pokusný svazek zkopírovány. Je ještě potřeba se zaměřit na poslední záznam v této složce a to soubor smazat. Jak je vidět první byte, který je určen k zaznamenávání názvu souboru nabývá hodnoty E5. Tato hodnota v souborových systémech rodiny FAT znamená, že soubor je smazaný. Pro uživatele, který připojí pokusný USB disk do systému není normálně viditelný. To ale neznamená, že data tohoto souboru nejsou na disku uložená. Takovýto soubor by šel jednoduše obnovit, a to tím způsobem, že hodnotu E5 v tomto záznamu změníme na jakoukoliv jinou hodnotu z ASCII tabulky a soubor se nám poté zobrazí jako obnovený a můžeme s nim normálně pracovat. Této vlastnosti využívají forenzní programy pro obnovu smazaných souborů. Vychází to ovšem z předpokladu, že datová část souboru nebyla přepsána jiným souborem, neboť v případě, že je záznam označení touto hodnotou E5, tak operační systém může na datovou část zapisovat. V případě, že by došlo k poškození FAT tabulky nebo k částečnému přepsání dat, lze se již pokusit smazaná data jen tzv. carvingem. Tyto záznamy obsahují ještě další položky, které nebyly podrobně popsány, jako např. časové značky vytvoření, přístupu a modifikace souboru. Dále obsahují adresu klastru datové části, kde začíná datová část souboru a hodnotu o velikosti souboru. Pro jednoduché pochopení funkce souborového systému byly v této části popsány jen tyto základní. [21]

c) Analýza MFT tabulky (NTFS)



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0C000A800	46	49	4C	45	30	00	03	00	76	0B	60	00	00	00	00	00	FILE0 v `
0C000A810	02	00	01	00	38	00	00	00	50	01	00	00	00	04	00	00	8 P
0C000A820	00	00	00	00	00	00	00	00	03	00	00	00	2A	00	00	00	*
0C000A830	03	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	`
0C000A840	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	H
0C000A850	4A	D0	31	8E	5A	E5	D3	01	74	DC	A8	F6	0E	E5	D3	01	JÐ1ŽZåÓ tÜ¨ö åÓ
0C000A860	26	6B	6C	73	3A	E5	D3	01	4A	D0	31	8E	5A	E5	D3	01	&kls:åÓ JÐ1ŽZåÓ
0C000A870	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0C000A880	00	00	00	00	08	01	00	00	00	00	00	00	00	00	00	00	
0C000A890	00	00	00	00	00	00	00	00	30	00	00	00	70	00	00	00	0 p
0C000A8A0	00	00	00	00	00	00	02	00	56	00	00	00	18	00	01	00	V
0C000A8B0	05	00	00	00	00	00	05	00	4A	D0	31	8E	5A	E5	D3	01	JÐ1ŽZåÓ
0C000A8C0	4A	D0	31	8E	5A	E5	D3	01	4A	D0	31	8E	5A	E5	D3	01	JÐ1ŽZåÓ JÐ1ŽZåÓ
0C000A8D0	4A	D0	31	8E	5A	E5	D3	01	00	00	00	00	00	00	00	00	JÐ1ŽZåÓ
0C000A8E0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	
0C000A8F0	0A	00	73	00	6D	00	61	00	7A	00	61	00	74	00	2E	00	s m a z a t .

Obrázek č. 14 MFT Table

Z obrázku můžeme vidět, že každý záznam, který je uveden v tabulce MFT začíná hlavičkou, která je do ASCII řetězců interpretovaná jako FILE. Na bytu č. 21 je obvykle uložená informace o hodnotě HEXA 38. Toto znamená, že za tímto offsetem začínají informace o metadatech souboru. Byte č. 22 a 23 je důležitý atribut, který nám vyznačuje, zda se jedná o soubor, adresář, smazaný soubor nebo smazaný adresář. V tomto případě je zde uvedena hodnota v HEXA 00 00, což znamená, že se jedná o smazaný soubor. Je to zkušební soubor, který byl nahrán na testovací USB disk a byl posléze smazán. Byte č.28-32 nám jako atribut vyznačuje velikost prostoru v rámci MFT tabulky na jeden záznam. Hodnota, která je vyznačena zeleně nám signalizuje, že záznam je nastaven na defaultní velikost 1024 Byte a zabírá tedy dva sektory disku. Modrou barvou je vyznačen offset, kde se ukládá název souboru. V rámci zkoumání tohoto souborového systému byly probrány pouze základní atributy. MFT záznam jich samozřejmě obsahuje mnohem více, ale podrobný průzkum, byť jen jednoho souborového systému, by vydal na téma jedné diplomové práce. [22]

d) Analýza zdrojových dat

Na datové části souboru jsou již uložena zdrojová data, která neobsahují metadata. Jedná se již o obsah vnitřku souboru. Pro lepší pochopení je možné se podívat na následující obrázek. Jedná se o obsahovou část textového dokumentu dokument.txt, který byl vytvořen na zkušebním disku.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0002B800	54	6F	74	6F	20	6A	65	20	7A	6B	75	73	65	62	6E	69	Toto je zkusebni
0002B810	20	74	65	78	74	6F	76	79	20	64	6F	6B	75	6D	65	6E	textovy dokumen
0002B820	74	0D	0A	54	6F	74	6F	20	6A	65	20	7A	6B	75	73	65	t Toto je zkuse
0002B830	62	6E	69	20	74	65	78	74	6F	76	79	20	64	6F	6B	75	bni textovy doku
0002B840	6D	65	6E	74	0D	0A	54	6F	74	6F	20	6A	65	20	7A	6B	ment Toto je zk
0002B850	75	73	65	62	6E	69	20	74	65	78	74	6F	76	79	20	64	usebni textovy d
0002B860	6F	6B	75	6D	65	6E	74	0D	0A	54	6F	74	6F	20	6A	65	okument Toto je
0002B870	20	7A	6B	75	73	65	62	6E	69	20	74	65	78	74	6F	76	zkusebni textov
0002B880	79	20	64	6F	6B	75	6D	65	6E	74	0D	0A	54	6F	74	6F	y dokument Toto
0002B890	20	6A	65	20	7A	6B	75	73	65	62	6E	69	20	74	65	78	je zkusebni tex
0002B8A0	74	6F	76	79	20	64	6F	6B	75	6D	65	6E	74	0D	0A	54	tovy dokument T
0002B8B0	6F	74	6F	20	6A	65	20	7A	6B	75	73	65	62	6E	69	20	oto je zkusebni
0002B8C0	74	65	78	74	6F	76	79	20	64	6F	6B	75	6D	65	6E	74	textovy dokument

Obrázek č. 15 obsah souboru

Jak je vidět, tak offset této datové části je na bytu 0002B800 a obsah tohoto souboru je vyznačen žlutým písmem. Z pravého sloupečku můžeme vidět, že v souboru se nachází text: *Toto je zkušební textový dokument*. Souhrn těchto řetězců byl v dokumentu zkopírován několikrát za sebou. Tato datová část je z hlediska forenzního šetření digitálních důkazů rovněž důležitá, neboť i na této datové části jsou začátky určitých typů datových souborů označeny tzv. hlavičkou a konce, i když už méně obvykle zápatím. Pro příklad můžeme vidět z pokusného souboru diplom.jpg.

4.5.7 Získání výpisu filesystému

Pro analýzu bezpečnostních incidentů je získat kompletní výpis souborového systému s časovými značkami. Pro tento úkon můžeme využít terminálový příkaz fls.

 # fls -r -l / zkoumani/image.dd > filelist.txt

Tento příkaz nám provede kompletní výpis souborového systému do souboru filelist.txt. Parametr r znamená, že celou adresářovou strukturu ze zkoumané bitové kopie nazvané image.dd prozkoumá rekurzivně, parametr -l znamená, že jednotlivé položky souborů budou obsahovat časové značky a oprávnění ke zpuštění souboru jednotlivých uživatelů. [23]

4.5.8 Setřídění podle časových značek mactime

Za pomocí předchozího příkladu jsme získali výpis souborového systému s časovými značkami. Příkazem mactime je setřídíme podle času a vznikne nám časová osa. Použít můžeme následující příkaz. [24]

#mactime -b filelist.txt -d -i hour data/tl-hour-sum.txt > timelinefile.txt

4.5.9 Získávání logů systému za pomocí log2time

V rámci forenzní analýzy je důležité získávat i logy systému. Logy je možné extrahovat ze souborů, kde jsou uloženy příkazem log2time a uložit si je do souboru. Tato utilita je naprogramována ve dvou programovacích jazycích, a to buďto v jazyce Python nebo Pearl. Pro jednoduchý příklad uvedeme utilitu v jazyce Python. Program spustíme následovně:

 # log2timeline.py timelinelog.txt /zkoumani/image.dd

Logika spuštění je opačná, než je standartní u utilit tohoto typu. Prvním parametrem je cílový soubor pro výpis logů a druhý parametr je bitová kopie ze které tyto logy chceme získat. Výstup může vypadat následovně.

2015-07-16 16:53:58,808 [INFO] (MainProcess) PID:98252 <interface> [PreProcess] Set attribute: sysregistry to /WINDOWS/system32/config

2015-07-16 16:53:58,820 [INFO] (MainProcess) PID:98252 <interface> [PreProcess] Set attribute: systemroot to /WINDOWS

2015-07-16 16:53:58,834 [INFO] (MainProcess) PID:98252 <interface> [PreProcess] Set attribute: windir to /WINDOWS

4.5.10 Vytváření supertimeline

Z výše uvedených souborů je možné pro lepší vyhodnocení incidentu složit výpisy z logů a souborového systému do jedné časové řady. Tuto metodu vyvinula společnost SANS, která se zabývá bezpečnostní analýzou incidentů, výukou a vytváření metodiky pro takovéto případy. Supertimeline můžeme vytvořit principiálně následujícím způsobem.

Nejdříve musíme sloučit výpis souborů s logy. To provedeme pomocí příkazu cat:

#cat /zkoumani/timelinefile.txt /zkoumani/timelinelog.txt >> supertimeline.txt

Následně tento soubor setřídíme podle času:

#mactime -b supertimeline.txt -d -i hour data > > dataforanalyst.txt

Nyní máme vytvořenou časovou osu, ze které můžeme zkoumat, k čemu ve zkoumaném systému došlo. [25]

4.5.11 Obnova smazaných souborů za pomocí utility Scalpel

Mezi další program, který slouží ke zkoumání digitálních důkazů musíme zařadit linuxový program, který se spouští v terminálu a to Scalpel. Jedná se o mocný nástroj, který slouží k vyřezání smazaných souborů z datové části souborového systému. Využívá k tomu známé hlavičky a zápatí souborů. V případě, že soubory, které chceme obnovit mají známé pouze hlavičku, nastavíme podle situace a osobních zkušeností maximální délku vyřezaného souboru. Před použitím tohoto příkazu musíme nejdříve správně nastavit konfigurační soubor, ve kterém nachází veškeré záznamy a zápatí souborů. Program funguje tím způsobem, že obnovuje veškeré soubory, které v tomto konfiguračním souboru nejsou „zakomentované" mřížkou **#.** Soubor nastavujeme podle potřeby a můžeme do něj libovolně přidávat další hlavičky a zápatí nových druhů souborů. Příklady záznamů v konfiguračním souboru jsou uvedeny v následující tabulce.

Typ souboru	Délka (v bytech)	hlavička	zápatí
gif	5000000	\x47\x49\x46\x38\x37\x61	\x00\x3b
gif	5000000	\x47\x49\x46\x38\x39\x61	\x00\x00\x3b
jpg	5000000	\xff\xd8\xff\xe0\x00\x10	\xff\xd9
jpg	5000000	\xff\xd8\xff\xe1	\xff\xd9

Tabulka č. 4 hlavička a zápatí v hexa

Po nastavení konfiguračního souboru již jen spustíme samostatný program na vytvořenou bitovou kopii následujícím způsobem.

#scalpel -c scalpel.conf -o /zkoumani/obnova /zkoumani/image.dd

Příkaz znamená že program načte konfigurační soubor, který je adresovaný za parametrem c. Dále načte bitovou kopii. V tomto případě se jedná o soubor image.dd a vyřezané soubory uloží do složky obnova. Bude se jednat pravděpodobně o větší soubor dat, které je následně třeba ještě profiltrovat. Samozřejmě existuje více nástrojů pro obnovu dat v operačním systému Linux. Můžeme uvést ještě např. **rstudio**, **extundelete** atp. [26]

4.5.12 Analýza dumpu operační paměti

K analýze operační paměti je nejvhodnější využít sofistikovaný nástroj, který nese název Volatility. Jedná se o otevřený framework pro analýzu operačních pamětí, který byl napsán v jazyce Python podnikatelem a vědcem Aaronem Waltersem. Tento framework podporuje analýzu operačních pamětí, které běží na operačních systémech z rodiny Windows, Mac OS a Linux.

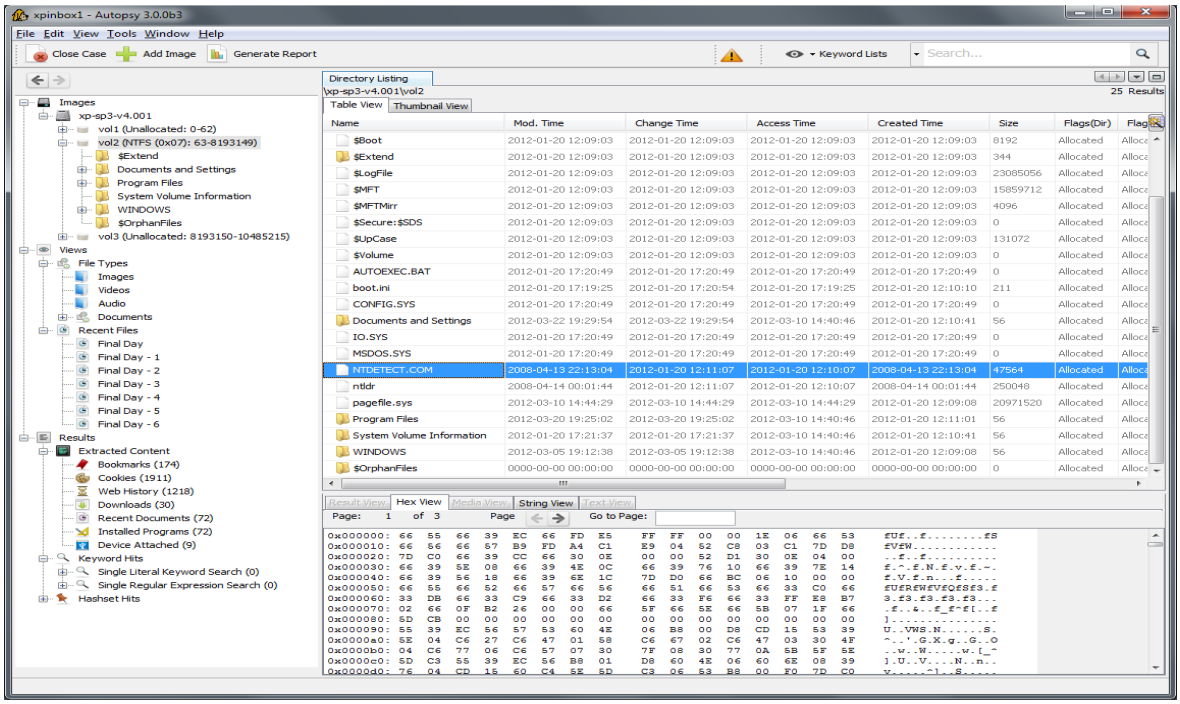
Pomocí frameworku Volatility můžeme zjistit:

- procesy běžící na počítači,
- verze jádra systému,
- uživatele, kteří byli přihlášení do systému,
- zdali na počítači byly spuštěny zašifrované kontejnery TRUE CRYPT,
- užití klávesnice na běžícím stroji,
- vyhledávat hesla.

Jedná se o mocný nástroj pro forenzní zkoumání operačních pamětí a možnosti analýzy jsou velmi rozsáhlé. Metodika na použití tohoto frameworku by vydala obsahem na samostatnou diplomovou práci.

4.5.13 Autopsy

Jedná se o forenzní nástroj pro analýzu bitových kopií v operačním systému Linux. Bohužel ve většině distribucí je možné nainstalovat pouze do verze 2.6, které má uživatelské rozhraní implementované prostřednictvím webového rozhraní. Ve forenzní verzi s názvem PALADIN je již implementovaná verze 4.6, která je nejvhodněji použitelná do současných podmínek.



Obrázek č. 16 ukázka GUI prostředí Autopsy

Tento nástroj umožňuje:

- načtení bitových kopií,
- zobrazení adresářové struktury,
- třídění souborů podle typu,
- obnovu smazaných souborů,
- analýzu bitové kopie v hexa editoru,
- filtrování podle různých parametrů,
- vytváření časových os tzv. timeline.

Dle provedeného průzkumu na internetu se dle parametrů jedná o nejlepší komplexní nástroj využitelný pro forenzní analýzu bitových kopií pro Linux.

4.6 Dílčí závěr

V této kapitole byl probrán vznik operačního systému Linux. Jedná se o průhledný, komplexní a bezpečný operační systém, který je využitelný pro mnoho úloh současné techniky. Implementuje se jak do velkých výpočetních center, tak do malých jednoúčelových systémů.

Typickým příkladem mohou být například routery. Pro využití zajišťování digitálních důkazů je jednoznačně nejlepší volbou. Mezi jeho jednoznačnou výhodu patří zejména to, že tzv. live verzi lze nainstalovat na malé přenosné USB disky, ze kterých lze spustit operační systém např. na zkoumaném PC a vytvořit bitové kopie paměťových médií na externí technologický disk, aniž by tomuto úkonu muselo předcházet složité rozebírání zájmového počítače. Bohužel, co se týče analýzy vytvořených bitových kopií nejvhodnějším nástrojem je v současné době jenom open source nástroj Autopsy, který se nemůže měřit s komerčními nástroji jako je například EnCase, x-way, Black Light nebo FTK Forenzisc. Pokud bychom se podívali na poměr cena výkon, jedná se o jednoznačně software nejlepší volby. V následující tabulce vidíme ceny komerčních nástrojů. [27]

Software	**Cena(v dolarech)**
Acces Data FTK	3995
Black Light	3400
Encase Forensic	3594

Tabulka č. 5 Ceny komerčních forenzních programů

5 VYŠETŘOVÁNÍ BEZPEČNOSTNÍHO INCIDENTU

Nejdříve bychom měli definovat pojem bezpečnostní incident. V zákoně o kybernetické bezpečnosti je definovaný takto:*“ Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací[1]) v důsledku kybernetické bezpečnostní události.“* [28]

Můžeme si všimnout, že definici bezpečnostního incidentu je celkem široká a není z ní zřejmé, zdali se za bezpečnostní incident považuje i např. zásah vyšší moci např. záplavy, black out atp. Nicméně v rámci této diplomové práce se budeme zabývat vyšetřováním bezpečnostním incidentem, který zapříčiní vůle a konání člověka o to takovýto incident vyvolat, a to z jakékoliv pohnutky. Pro lepší znázornění vyšetřování bezpečnostního incidentu to probereme na následujícím příkladu. Na úvod je třeba říci, že příklad je pro ilustraci značně zjednodušený.

Příklad:

Jedná se o soukromou společnost, která se zabývá prodejem koberců. Společnost sídlí v jedné budově, ve které je umístěna veškerá ICT infrastruktura. Mimo jiné je součástí této infrastruktury serverové uložiště smluv, které má nastavenou veřejnou IP adresu verze. 4. Na toto úložiště obchodní zástupci ukládají své smlouvy, které sjednají v terénu se svými zákazníky a ukládají je přes ftp připojení. Na serveru je otevřený port pro ftp č. 21. Na server je možný dále přístup přes ssh protokol po otevřeném portu č. 22. Jednotlivý obchodní zástupci mají oprávnění na tento úložný prostor v případě, že se přihlašují z vnějšku sítě pouze ukládat, nikoliv mazat. Server běží na operačním systému Linux na 1TB disku. Dne 11.05.2018 kolem 09:00 hodin volá administrátorovi obchodní zástupce, který se přihlásil na úložiště a zjistil, že v jeho zdrojové složce nejsou žádná data. Naposledy, kdy se přes ftp přístup k úložišti připojil bylo v 08:00 hodin uvedeného dne a veškerá data tam byla. Ze strany administrátora by měl následovat tento postup:

5.1.1 Zjištění, co se stalo

Administrátor by měl pracovníka důkladně vytěžit k provedenému incidentu a toto v reálném čase vyhodnocovat. V našem případě administrátor zjistí, že jsou smazány veškeré složky ostatních uživatelů datového úložiště. Vzhledem k tomu, že v době mezi 08-09 hodinou probíhá porada ostatních pracovníků administrátor vyloučil, že by se tohoto mohl dopustit někdo ze zaměstnanců a jeho podezření začne směřovat na někoho tzv. „z venku“.

5.1.2 Vyhodnocení prvotních informací

Na základě těchto zjištění administrátor může předpokládat, že došlo k napadení firemní sítě z vnější sítě nikoliv sítě firmy a to i jak na základě toho, že byla porada ostatních zaměstnanců společnosti, ale i toho, že došlo ke smazání dat i ostatních uživatelů, a pravděpodobný útočník musel mít nejspíš oprávnění administrátora, aby takovouto činnost mohl vykonat.

5.1.3 Odpojení konektivity sítě

Vzhledem k tomu, že situace byla vyhodnocena jako útok z vnější sítě, administrátor by měl neprodleně odpojit připojení do vnější sítě, a to buďto softwarově nebo nejlépe fyzickým odpojením od sítě.

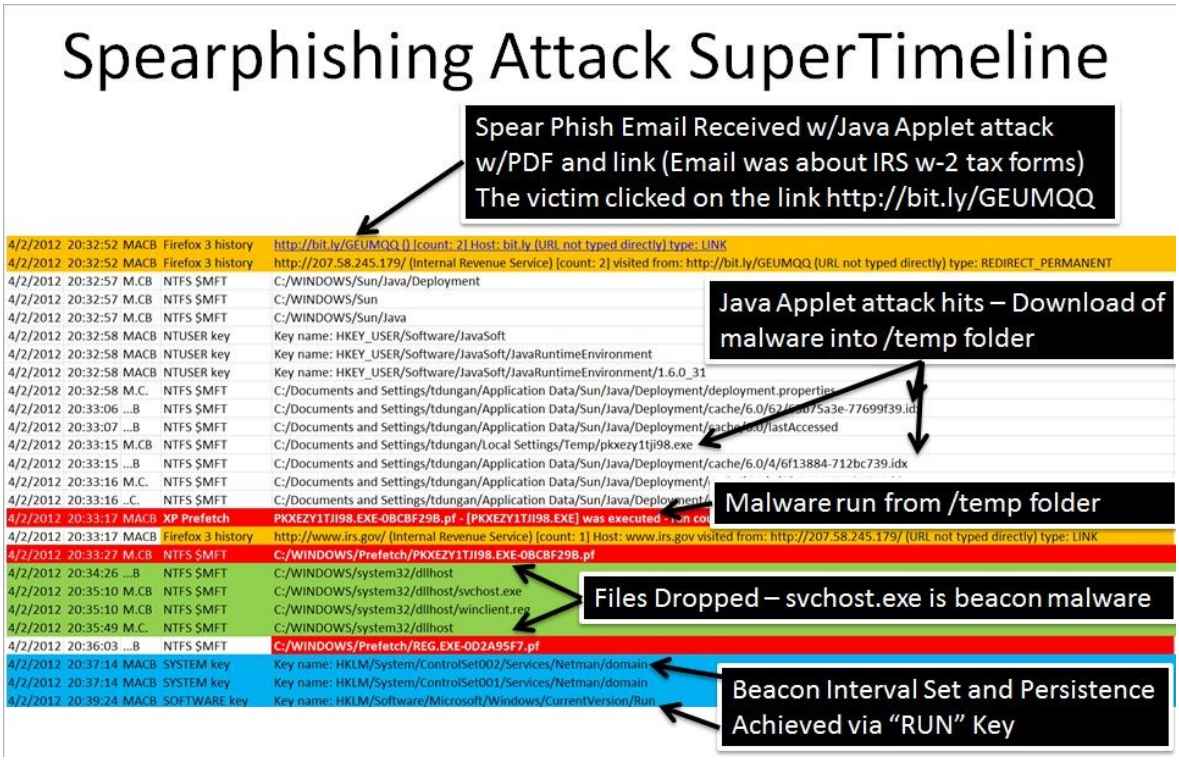
5.1.4 Následovat by mělo zajištění digitálních důkazů pro další analýzu

Vzhledem k tomu, že již veškerá data byla smazána, bylo by vhodné za pomocí již popsané utility lime vytvořit dump operační paměti napadeného serveru a toto uložit pro potřeby dalšího zkoumání. Dále by měl administrátor vypnout server a vytvořit bitovou kopii pro další zkoumání napadeného zařízení například za pomocí programu ddrescue. Bitová kopie by měla být opatřena kontrolním hashem, za pomocí některé z hashovacích funkcí.

5.1.5 Fáze vytvoření časové osy

Za pomocí probraných příkazů by měl administrátor vytvořit časovou osu, a to rekurzivně ze všech souborů, které se nacházejí na provedené bitové kopii. Zájmové pro vyhodnocení jsou zejména metadata těchto souborů, tedy časové značky Modificate, Acces, Create v češtině modifikace, přístup, vytvoření. Toto lze vytvořit za pomocí příkazu z linuxového terminálu FLS. Dále je třeba vyexportovat veškeré logy, které se nachází v systému, případně i zasílané ze syslogu (jedná se o soubor ve kterém se uchovávají veškeré záznamy o stavu a chodu systému) na jiný server, aby bylo možné vyhodnotit incident v případě, že by došlo

ze strany útočníka ke smazání tohoto souboru na napadeném počítači. Tyto dvě časové osy je třeba následně spojit do jednoho souboru a setřídit podle času.



Obrázek č.17 Supertimeline

5.1.6 Fáze vyhodnocení časové osy

Na základě zjištěných informací od obchodního zástupce bylo provedeno zkoumání časové osy v zájmovém čase a to tedy mezi 8-9 hodinou. Bylo zjištěno, že v době mezi 08:20 -08:30 hodin uživatel s administrátorským oprávněním zadal na úložišti příkaz **rm -rf**, tedy smazat veškeré uživatelské soubory a složky. Tímto způsobem se tedy podařilo vysvětlit, jakým způsobem došlo ke smazání uživatelských dat. Při postupu časem zpětně bylo zjištěno, že se neznámý útočník přihlásil v 08:19 hodin za pomocí protokolu SSH k požadovanému serveru přes administrátorský účet. Bohužel administrátor měl nastavený přístup na SSH pod uživatelským jménem admin a heslem admin 123. Bylo tedy zjištěno, že neznámý útočník se připojil v 08:19 hodin pod administrátorským účtem z IP ADRESY, která po šetření přes službu who is byla lokalizována v Rusku. Přihlášení, dle časové osy, předcházelo několik opětovných pokusů o přihlášení v krátké časové prodlevě. Z čehož můžeme vyvozovat automatizovaný slovníkový útok.

5.1.7 Fáze vyhodnocení a zvolení opatření, aby se incident nemohl opakovat.

Na základě zjištění, jakým způsobem došlo k útoku bylo vyhodnoceno, že příčinou průniku do systému byla nedbalost administrátora systému, který pro přístup přes ssh nastavil jednoduché uživatelské jméno a heslo. Jako nápravné opatření by bylo vhodné zvolit lepší politiku co se týče přihlašování, zejména blokaci IP adresy v případě, že dojde ke třem špatným pokusům o přihlášení. Dále by bylo vhodné pro přihlašování přes SSH používat vygenerovaný RSA klíč. Z časové osy nebylo zjištěno, že by útočník na server instaloval nějaké další nástroje.

5.1.8 Obnovení dat

Pokud data, která byla nahrána na server mezi 08-09 hodinou nebyla kvůli nastavení cyklu zálohy zálohována např. v nočních hodinách, mohl by se administrátor pokusit je obnovit za pomocí linuxového forenzního nástroje scalpel. Neboť nebylo zaznamenáno, že by útočník na server nahrával nějaká další data, a tak nemohlo dojít k jejich přepsání a obnova z nealokovaného prostoru pomocí tohoto nástroje by byla možná.

5.1.9 Nahlášení incidentu na policii

Vzhledem k tomu, že výše popsaný incident naplňuje skutkovou podstatu trestného činu neoprávněného přístupu k počítačovému systému, podle ust. § 230 Trestního zákoníku, bylo by vhodné nahlásit tento incident na policii k dalšímu prošetření.

5.2 Dílčí závěr

V této kapitole byla popsána možnost, jakým způsobem vyšetřovat bezpečnostní incident za pomocí linuxových nástrojů. Byly podrobně rozebrány jednotlivé fáze. Jednalo se o zjednodušený principiální případ pro vyšetřování takovéhoto incidentu. Situace v praxi není vždy tak jednoduchá a s tak jednoznačným závěrem. Zejména v případě nějakého sofistikovaného APT útoku. *APT je označení pro skupinu útočníků (pokud se jedná o jednotlivce, neoznačuje se jako APT), která cíleně napadá konkrétní společnosti. S cílem získat úplný přístup k celé síti a všem jejím datům. Jinými slovy, APT lze považovat za špionážní skupinu. APT skupiny postupují systematicky a využívají pestrou škálu útoků známých ze všedního života.* [29] V principu však šetření i takovéhoto sofistikovaného útoku může probíhat velmi obdobně.

Touto kapitolou byla ukončena teoretická část této diplomové práce, která slouží jako podklad pro zařízení, které je vyvíjeno v rámci praktické části. Aby bylo pochopeno, k čemu slouží, proč je důležité takovéto zařízení mít, jakým způsobem funguje a jakým způsobem se zpracovávají jeho výstupy.

II. PRAKTICKÁ ČÁST

.

6 CÍLE PRAKTICKÉ ČÁSTI

Praktická část diplomové práce se zabývá způsobem vytvoření platformy pro forenzní analýzu USB disků. Platforma by měla být vystavena na HW architektuře procesorů ARM. Jedná se o architekturu procesorů, která se díky své nízké spotřebě elektrické energie používá v mobilních zařízeních. Zařízení by mělo být schopné provádět bitové kopie, duplikovat a tzv. „wipovat“ paměťová média připojitelná přes rozhraní USB. Tato část se bude zabývat výběrem vhodného zařízení, instalací potřebných součástí, vývojem softwaru a nakonec testováním zařízení. Na závěr bude praktická část práce vyhodnocena.

Obrázek č. 18 procesor na architektuře ARM Broadcom BCM2837B0

6.1 Vstupní požadavky na zařízení

- kompatibilní s operačním systémem Linux,
- alespoň 2 USB vstupy,
- dotykový multifunkční barevný display,
- více jádrový procesor na HW Architektuře ARM,
- cenově dostupný,
- kvalitní dokumentace,
- dostupnost dalších komponentů,
- rozhraní Wi-Fi z důvodu jednoduššího vývoje přes VNC server.

6.2 Výběr vhodného zařízení

Na základě vstupních požadavků na zařízení byl proveden průzkum trhu a byla vytipována zařízení, která by mohla být vhodná pro vývoj takovéhoto zařízení. Jako krok správným směrem se ukázalo možné použití mikropočítačů. Byl proveden výběr z následujících mikropočítačů:

a) **BANANA PI R2**

Obrázek. č 19. BANANA PI R2

Miniaturní počítač/router board, který je schopen zastat funkci routeru, WiFi AP, síťového úložiště NAS i domácího serveru. 4jádrový procesor MediaTek MT7623N ARM Cortex-A7, 2GB RAM, grafická karta Mali 450 MP4, rozhraní SATA, slot pro microSD karty; slot mini PCIe, HDMI, USB 3.0/3.1 Gen 1, microUSB, 4x GLAN, 1x GWAN, WiFi, Bluetooth, OTG, GPIO, CSI, DSI, bez operačního systému. [30] Jedná se o absolutní špičku mezi mikropočítači, která je v současné době na trhu. Velkou výhodou jsou zejména rozhraní USB 3.0 a SATA 3. Veškerými parametry přesahuje všechny ostatní produkty, které jsou dostupné na trhu. Nevýhodou je vyšší cena oproti ostatním produktům, která se v době psaní diplomové práce pohybuje okolo 3139,- Kč. Tento mikropočítač je kompatibilní s OS Linux a Android. Co se týče operačního systému nejčastěji se na něm používá OS Bananian. Nevýhodou je rovněž to, že komunita uživatelů tohoto mikropočítače není tak velká a s tím souvisí i méně dostupné dokumentace a různých projektů. Mikropočítač byl vyhodnocen jako nevhodný pro potřeby vývoje této diplomové práce.

b) Odroid C2

Obrázek č. 20 Odroid C2

Mikropočítač ODROID C2 od jihokorejské společnosti HARDKERNEL je opatřen 4 jádrovým procesorem CORTEX A53 o frekvenci 1,5 GHZ, 2GB operační pamětí RAM na technologii DDR3 a 4 x USB 2.0. rozhraním. Jedná se o vyrovnané parametry, které příjemně korespondují s cenou, která se pohybuje kolem 40 USD. Nevýhodou je, že neobsahuje rozhraní Wi-Fi, dále že toto zařízení neprodává v České republice žádný výrobce Rovněž, co považuji za nevýhodu je méně rozšířená komunita a dokumentace k tomuto zařízení. Jako příklad mohu uvést, že když jsem studoval dokumentaci k ovladači displeje pro toto zařízení, bylo v souvislosti s tímto mnoho problémů, které na internetových fórech nebyly zodpovězeny a vyřešeny. Fóra v souvislosti s displejem byla pročtena poměrně důsledně. A to ty, která jsou součástí komunity pod oficiálním výrobcem, tak i různé IT komunity třetích stran. Vzhledem k těmto okolnostem bylo zařízení ze strany autora této práce vyhodnoceno jako nevhodné pro vývoj. Zejména tedy je třeba zdůraznit obavy z toho, že nepůjde zprovoznit displej pro toto zařízení, což by mohlo výrazně ohrozit dokončení této práce.

c) Raspberry Pi 3 Model B+

Obrázek č. 21 Raspberry Pi 3 Model B+

Jedná se o nejnovější model na trhu z rodiny Raspberry, který byl vydán v březnu 2018. Obsahuje výkonnější 64 bitový 4 jádrový procesor s označením Broadcom BCM2837B0. Dále obsahuje 4 x USB rozhraní 2.0. Mezi nespornou výhodu je možnost WiFi připojení, a to jak na 2,4 Ghz, tak i na 5 Ghz technologii. Oproti předchozímu modelu se Raspberry při vyšším výkonu nepřehřívá. V poměru cena/výkon se jedná o jednoznačně nejlepší volbu, neboť tržní cena se pohybuje kolem 35 USD za kus. Mezi jeho nespornou výhodu je operační systém Raspbian, který je založen na distribuci Debianu a je od začátku vyvíjený pro toto zařízení. Další výhodou je to, že jde o celosvětově nejrozšířenější komunitu, zabývající se vývojem různých projektů pro tuto platformu. Od jednoúčelové regulátory pro různé úlohy počínaje po inteligentními domácnostmi konče. Dostupnost komunity pro tento mikropočítač je naprosto zásadní, neboť lze poměrně snadno dohledat řešení pro různé problémy, které ve vývoji mohou nastat. Stejně tak se musí velmi pozitivně zhodnotit dostupnost dalších rozšiřujících zařízení, která lze i v České republice snadno dokoupit. Tento mikropočítač byl nakonec vybrán pro potřeby této diplomové práce. Ukázalo se to jako skvělá volba. Systém fungoval naprosto bezchybně a během běhu zařízení nedošlo k žádnému problému.

7 KOMPONENTY PŘÍSTROJE

Na základě předběžného výběru byl zakoupen mikropočítač uvedeného typu. Dále bylo potřeba zakoupit napájecí zdroj, MicroSD Kartu s SD adaptérem pro instalaci systému, dotykový 3,5 palcový display a HDMI kabel pro zapojení do monitoru.

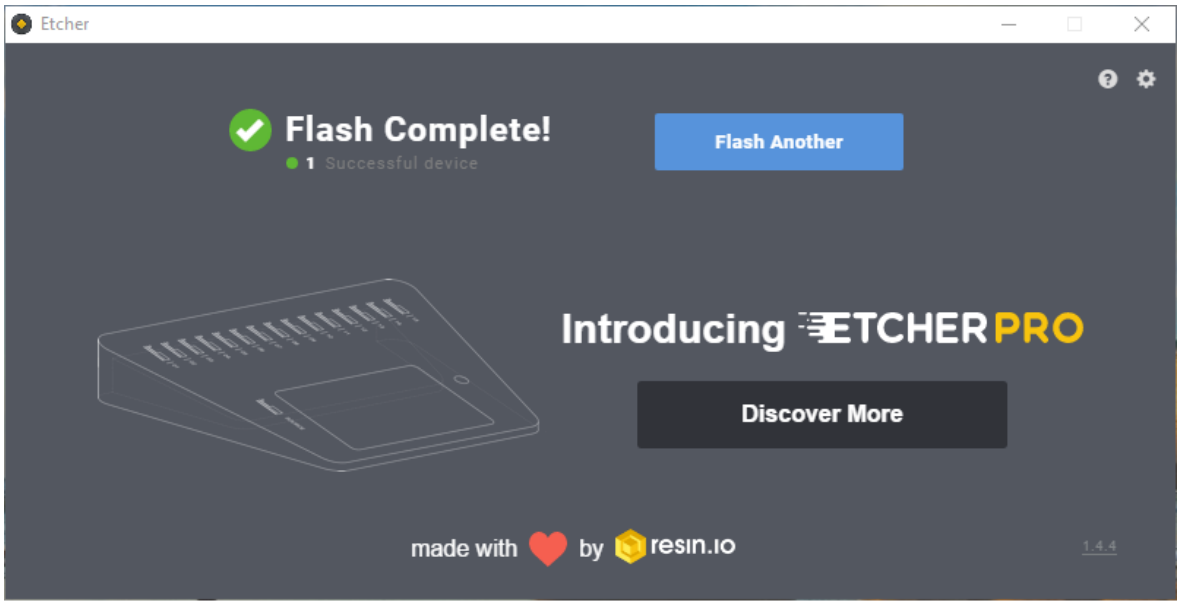
Obrázek č.22 Sestavení zařízení

Na obrázku můžeme vidět originální napájecí zdroj Rapsberry PI 3 a již samostatný přístroj se zapojeným displejem. V takovéto konfiguraci bude zařízení připraveno pro modelovou ukázku při obhajobě diplomové práce při státních závěrečných zkouškách.

8 INSTALACE SYSTÉMU, DOPLŇKŮ A NASTAVENÍ PARAMETRŮ

8.1 Instalace systému

Jako systém vhodný pro vybrané zařízení tedy Raspberry Pi 3 Model B+ byl vybrán OS Raspbian, který je založený na distribuci Debianu a je po celou dobu vyvíjen pro tento mikropočítač. Konkrétně byl vybrán RASPBIAN STRETCH WITH DESKTOP
Version: April 2018 Datum vydání: 2018-04-18 Kernel version: 4.14
SHA-256:0e2922e551a895b136f2ea83d1bc0ca71e016e6d50244ba3da52bd764df5d1b6.
A to přímo z webových stránek výrobce v komprimovaném formátu .ZIP. Po rozbalení archivu byla získána image 2018-04-18-raspbian-stretch.img. Systém byl překopírován na 8GB kartu doporučeným způsobem za pomocí programu Etcher.



Obrázek č. 23 Instalace operačního systému na SD Kartu.

8.2 Základní nastavení systému

Po zapojení veškerých periferií přístroje došlo k prvnímu startu operačního systému a bylo třeba nastavit základní nastavení systému.

8.2.1 Nastavení přístupového hesla

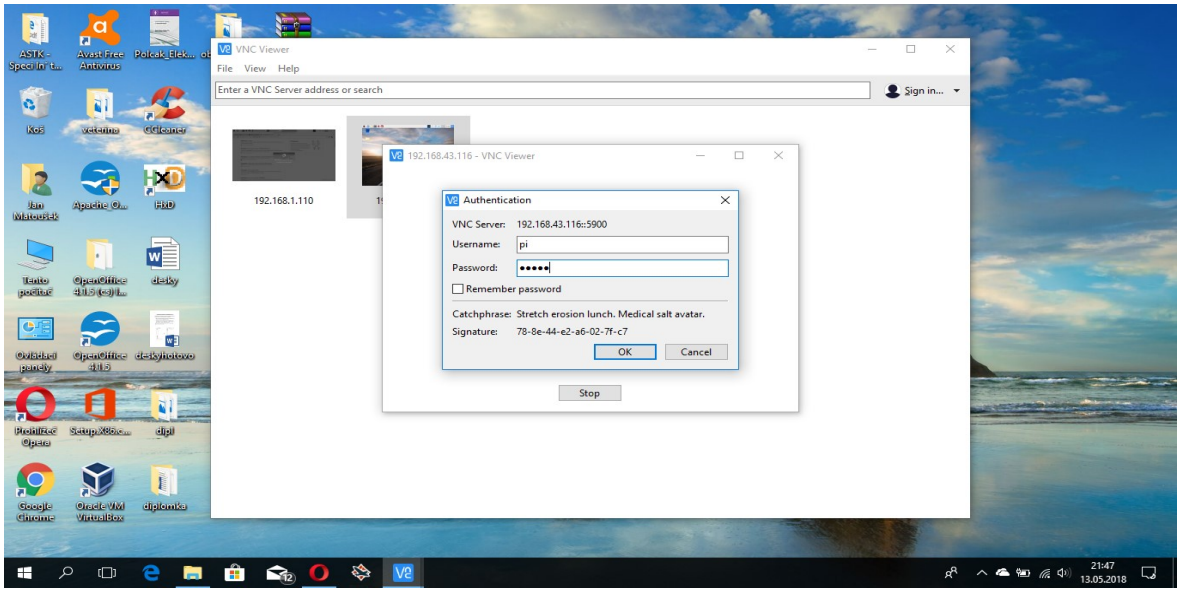
Jak již bylo zmíněno po zapojení přístroje a prvního startu jsem musel nastavit základní nastavení. Toto se v grafickém uživatelském prostředí provede tak, že se klikne na tlačítko v levém horním rohu a v následujícím menu se zobrazí volby systému. Nejdříve se muselo změnit heslo pro přístup k operačnímu systému. Symbolicky bylo zvoleno heslo podle českého programovacího jazyku „karel“.

8.2.2 Nastavení rozlišení obrazovky

V rámci výše uvedeného rozhraní dále bylo zvoleno rozlišení 1360x768. Toto rozlišení jsem zvolil důmyslně proto, aby se obrazovka systému dobře zobrazovala při vzdáleném připojení přes síť.

8.2.3 Nastavení spuštěných služeb

V rámci tohoto rozhraní byl spuštěn SSH server a VNC server. Obě služby byly spuštěny z důvodu, že vývoj softwaru byl vytvářen za pochodu při zaměstnání. Vyřešil se tím zejména problém s logistikou, protože přenášení více periférií by byl při takovém to mobilním vývoji problematický.



Obrázek č. 24 Ukázka připojení přes VNC do Raspberry PI 3 z notebooku.

8.2.4 Nastavení WIFI

V hlavním menu, v horní části obrazovky, bylo nastaveno automatické připojení přes bezdrátovou síť Wi-Fi na frekvenci 2,4 Ghz na AP, které mám na svém mobilním telefonu se zabezpečením WPA2-PSK.

8.3 Instalace doplňků pro vývoj

Pro potřeby vývoje SOFTWARU bylo nutné do zařízení doinstalovat další programy, neboť operační systém neobsahoval mnoho prvků, které byly potřeba.

8.3.1 Instalace DC3DD

Bylo potřeba doinstalovat program, který slouží k provádění bitových kopií paměťových zařízení. Z několika možností (dd, dc3dd, dcfld, ddrescue) byl vybrán právě program DC3DD. Zejména kvůli jednoduchosti nastavení a také proto, že program takový jaký je v rámci svého běhu z vytvářené bitové kopie rovnou provede HASH, což je velmi důležité. Tím, že na rozdíl od programu DD a DDRESCUE má v sobě tuto funkci implementovanou přímo to následně zjednodušuje vývoj softwaru. Program DCFLD rovněž disponuje výše popsanou vlastností, nicméně nemá tak hezký „progres“ při běhu programu. Instalace proběhla následovně. Byl otevřený terminál programu a zapsán následující řádek:

 # sudo apt-get install dc3dd

Po zadání tohoto příkazu se stáhnul z repozitáře příslušný balíček ve formátu .deb a nainstaloval se do systému.

8.3.2 Instalace GUIZERO pro Python 3

Pro vytvoření aplikace byl použitý programovací jazyk Python 3, který je v každé linuxové distribuci defaultně nainstalován, nezbylo tedy než vybrat GUI rozhraní, ve kterém bude probíhat vývoj softwaru. V rámci vývoje softwaru byly zvažovány možnosti vytvořit grafické uživatelské rozhraní aplikace buďto v QT, TK. Po delším průzkumu v rámci diskuzních fór na internetu byla nakonec zvolena možnost vývojového frameworku GUIZERO, který je nadstavbou GUI TK. Mezi výhody tohoto frameworku patří jednoduchost a rychlost aplikace bez zbytečných složitých nastavení. Instalace do systému byla provedena následujícím způsobem. V terminálu byl zapsán následující příkaz:

 # sudo pip3 install GUIZERO

Po zadání tohoto příkazu došlo k instalaci potřebných knihoven tohoto frameworku do systému, aby jej bylo možné při vývoji používat. Uvedený framework obsahuje možnosti využívat okna aplikací, layouty, tlačítka, chybové hlášky atp.[31]

8.3.3 Instalace podpory filesystému NTFS

Aby bylo možné k počítači Raspberry připojovat paměťová média na kterých jsou nainstalovány filesystémy, které běžně používají systémy z rodiny Microsoft Windows bylo třeba doinstalovat ovladač, a to následujícím příkazem:

 # apt-get install ntfs-3g

Po instalaci tohoto ovladače bylo již možné bezproblémově zapisovat na paměťová média. Na kterých je zaveden tento typ filesystému.

8.3.4 Instalace ovladače dotykového displeje

Ovladače pro tento displej jsou zdarma volně dostupné na GITHUBU, proto je možné instalaci provést následujícím způsobem. Je nutné spustit terminál a zadat příkaz:

 # git clone https://github.com/Elecrow-keen/Elecrow-LCD35.git

Tímto příkazem se do adresáře, ve kterém se nacházíme, stáhne složka s příslušným ovladačem. Stačí již jen jednoduchým příkazem přejít do uvedené složky:

#cd Elecrow-LCD35

A následně v této složce, s oprávněními superuživatele, spustit pouze instalační skript ovladače:

#sudo ./Elecrow-LCD35

Provedením skriptu se ovladač nainstaluje. Nyní, již po startu systému, najede uživatelské rozhraní na displeji. Problematické je, že nejde dynamicky přepínat mezi zobrazováním na displeji a přes HDMI rozhraní, takže celý program byl nejdříve naprogramován. Posledním krokem byla instalace tohoto ovladače.

8.3.5 Nastavení spuštění aplikace

Aby vytvořené jednoúčelové zařízení správně fungovalo, a to i z hlediska uživatelského ovládání bylo třeba nastavit, aby se po startu operačního systému automaticky spustil program pro ovládání zařízení. Toto jsem vytvořil následujícím způsobem:

- spustíme konfigurační soubor /etc/xdg/lxssion/LXDE/autostart,
- na konec tohoto souboru zapíšeme adresu naší aplikace.

Po této operaci se po každém spuštění systému na našem zařízení spustí program pro ovládání programu.

8.3.6 Zakázání automatického připojení USB disků k souborovému systému

Jedná se o naprosto zásadní funkci tohoto zařízení, neboť v případě že bychom zkoumaná, paměťová média zasunuly do USB rozhraní a operační systém by je připojil k souborovému systému, mohlo by dojít k zapisování na tyto média a defacto ke znehodnocení digitálního důkazu. Postup pro zákaz automatického připojení je následující. Otevřeme konfigurační soubor, který je umístěn na adrese:

/etc/xdg/lxssion/LXDE/ pcmanfm.conf

A do tohoto konfiguračního souboru zapíšeme následující text:

[volume]

mount_on_startup=0

mount_removable=0

Konfigurační soubor následně uložíme a provedeme restart zařízení. Po tomto opatření již nedochází k automatickému připojení USB disků k adresářové struktuře. Celý postup byl otestován příkazy lsblk, df, které nehlásily připojené disky jako připojené a dále i výpisem souboru cat /proc/partitions. Opatření se po tomto testu ukázalo, jako dostatečné. [32]

9 VÝVOJ APLIKACE

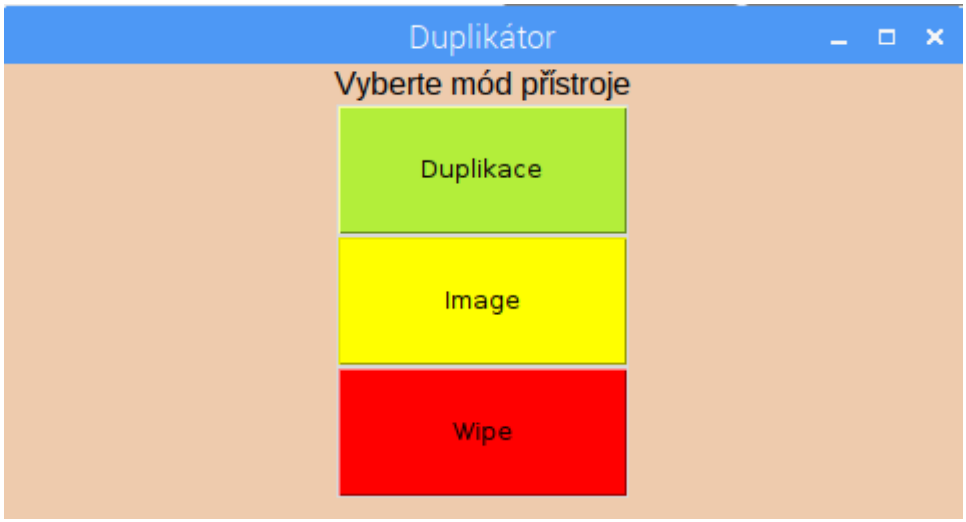
Pro vývoj aplikace byl vybrán programovací jazyk Python 3 a framework pro vytváření uživatelského rozhraní GUIZERO. Ke zdůvodnění tohoto výběru lze pouze napsat, že programovací jazyk Python 3 má poměrně jednoduchou syntaxi, je velmi kvalitně zadokumentován a na internetu je velmi rozsáhlá komunita uživatelů, kteří jsou případně schopni poradit s nějakým problémem. Dále, je třeba zohlednit, velké množství knihoven pro tento programovací jazyk s jejich důkladnou dokumentací. Při vytváření programu pro toto zařízení byly poměrně hodně využívány. Co se týče frameworku GUIZERO je nutné říct, že je teprve ve verzi 0,5, takže není zcela vyladěné. Proto mohlo být rizikem zvolit tento framework, ale nakonec se ukázalo, že i když verze není stabilní, aplikaci pro potřeby této diplomové práce je možné vytvořit.

9.1 Uživatelské prostředí

Z důvodu možné prezentace zařízení, při obhajobě diplomové práce, bylo zvoleno co nejjednodušší ovládání vytváření bitových kopií. Aplikace se skládá z hlavního menu pro ovládání aplikace a 4 oken dalších režimů.

9.1.1 Základní menu

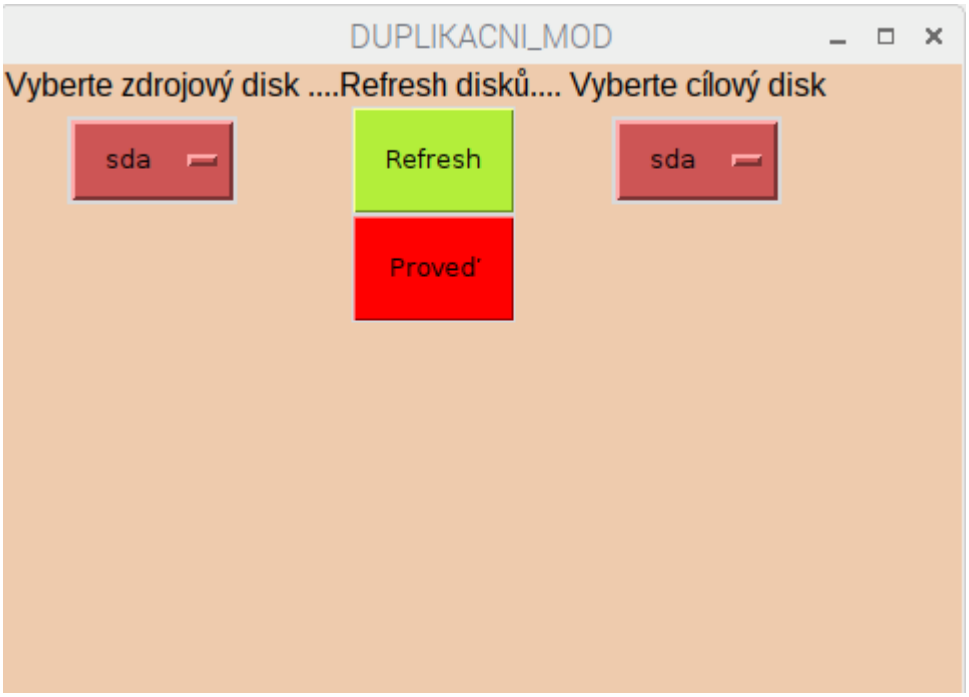
Základní menu obsahuje pouze 4 tlačítka, kterými se spouští podokna čtyřech možných režimů, které zařízení ovládá. Jsou to jediné ovládací prvky, které na tomto řídícím okně, celé aplikace, můžeme nalézt. Po kliknutí na tlačítko zvoleného režimu se otevře další okno, kde je možné nastavit další parametry. Pro lepší ilustraci je zobrazeno na následujícím obrázku.



Obrázek č. 25 Hlavní menu

9.1.2 Duplikační mód

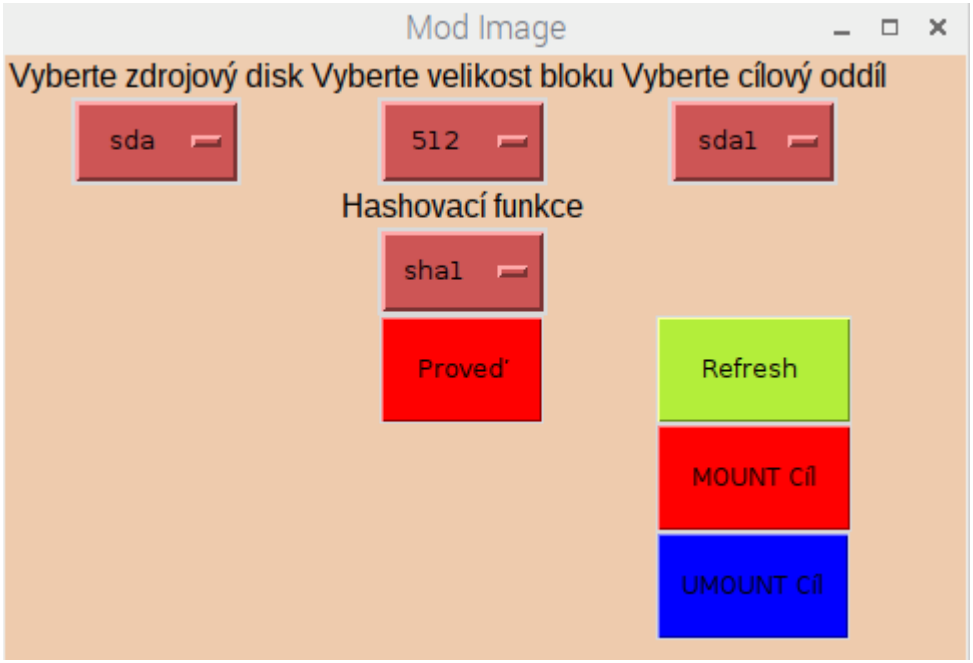
Duplikační mód slouží ke klonování připojených disků. Na levé straně je tzv. combo list, to znamená v terminologii rozbalovací seznam disků, které jsou připojeny k zařízení. Uživatel vybere disk, který chce klonovat. Režim duplikace bohužel umožňuje pouze načítání dat o nejmenší možné hodnotě načítání bloku 512 bytů. Na pravé straně se nachází rozbalovací seznam, ve kterém uživatel nastaví, na jaký disk má být provedena duplikace. Dále se na tomto okně ještě nachází tlačítko, pomocí kterého se obnoví aktuální seznam připojených disků k zařízení. Je třeba dát pozor, načtení aktuální konfigurace automaticky probíhá pouze v případě zvolení módu. Pokud dojde k odpojení nebo připojení paměťového média v případě, že již je zvolen mód, tak je třeba stisknout tlačítko pro obnovu disků. Následně již stačí jen stisknout poslední tlačítko pro duplikaci a program s příslušnými parametry zavolá program dc3dd a ten podle zvolených parametrů tuto duplikaci provede. Mód je pro lepší ilustraci zobrazen na následujícím obrázku.



Obrázek č. 26 Duplikační mód

9.1.3 Imigovací mód

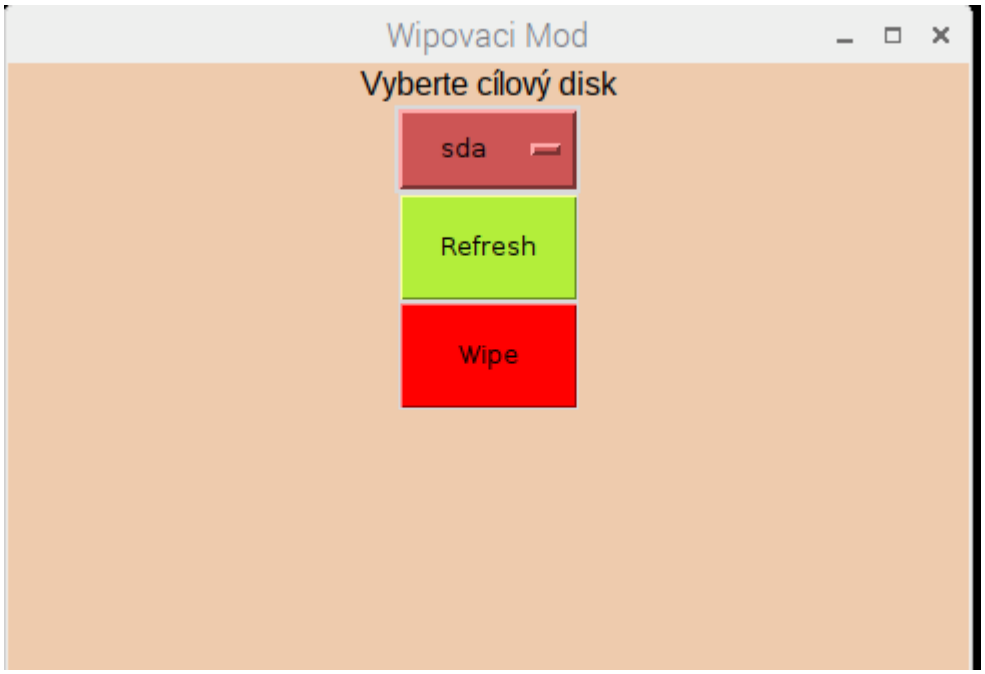
Imigovací mód, na rozdíl od duplikačního módu, vytvoří bitovou kopii zdrojového paměťového média, který vybereme ze zdrojového listu na příslušný logický oddíl, který si vybereme v cílovém seznamu. Pozor, v cílovém seznamu vybíráme logický oddíl, který musíme před spuštěním vytváření bitové kopie připojit k souborovému systému. Toto provedeme tlačítkem mount. Poté teprve můžeme stisknout tlačítko k vytvoření bitové kopie. Až se bitová kopie vytvoří je třeba následně stisknout tlačítko umount, které zaručí bezpečné odpojení paměťového média od souborového systému a následně teprve můžeme toto paměťové médium vysunout ze zařízení. V případě, že bychom nestiskli tlačítko umount mohlo by dojít k poškození dat na paměťovém médiu. Pro lepší ilustraci je tento mód zobrazen na následujícím obrázku.



Obrázek č. 27 Imigovací mód

9.1.4 Wipovací mód

Tento režim slouží ke smazání veškerých dat na vybraném paměťovém médiu. V horní části obsahuje pouze výběr paměťového média, na kterém chceme veškerá data smazat. Samozřejmě obsahuje tlačítko pro obnovení seznamu disků, které jsou připojené k zařízení, jako ve všech předchozích případech a tlačítko pro aktivaci tohoto módů. U tohoto režimu je třeba dát si pozor. Změny, které provede jsou nevratné a v případě neopatrnosti bychom vložení špatného paměťového média dojde k nezvratné ztrátě veškerých dat. Na závěr je třeba dodat, že program celé aplikace je ošetřen takovým způsobem, že není možné aby došlo k poškození operačního systému zařízení. Pro lepší ilustraci rovněž zobrazen na následujícím obrázku.



Obrázek č. 28 WIPE mód

9.1.5 Zdrojový kód programu

Zdrojový kód programu aplikace je veden jako příloha této diplomové práce. Ke struktuře programu je třeba říci, že se skládá ze tří částí. V první části jsou načítány knihovny programovacího jazyku python.

Guizero

Jedná se o knihovnu uživatelského prostředí. Pomocí níž jsou programově řešeny veškeré interakce s uživatelem aplikace (tlačítka, combo listy, popisky).

Re

Jedná se o standartní knihovnu Pythonu 3, která slouží k práci s textovými řetězci za pomocí regulérních výrazů. Využívá se v programu pro vyfiltrování jednotlivých disků a logických oddílů disků.

Subprocess

Tato knihovna slouží k volání dílčích procesů v systému, které mají být provedeny. V našem případě je volán program dc3dd, mount, umount.

Ve druhé části jsou samostatně vytvořené jednotlivé funkce systému, které jsou volány z grafického rozhraní při stisknutí ovládacích prvků v grafickém rozhraní. Jedná se o tyto:

mod_duplikace, mod_image. Mod_wipe

Jedná se o jednoduché funkce, které po stisknutí tlačítka zobrazí okna jednotlivých režimů, jako je duplikační mód, imigovací mód a nakonec mód smazání disku tzv. „WIPE“.

Duplikuj, porid_image, wipe

Funkce otevřou linuxové okno xterm a v něm spustí program dc3dd. Podle výchozího nastavení začne kopírovat data ze zdrojového disku na cílový. Okno je důležité zejména pro zobrazování progresu, tím je myšleno zobrazení aktuální rychlosti kopírování, počet zkopírovaných bloků v reálném čase. V případě funkce wipe funkce provede smazání určeného disku.

get_disks_list, get_partitions_list

Funkce získají informace o jednotlivých discích a logických oddílech připojených k Raspberry PI, které uloží do proměnných.

refresh_dsk_wi, refresh_dsk_wd

V případě zavolání těchto funkcí z grafického uživatelského rozhraní dojde k obnovení informací o aktuálně připojených discích k mikropočítači Rapsberry Pi a aktualizaci tohoto seznamu v grafickém uživatelském prostředí.

mount, umount

Funkce slouží k připojení nebo odpojení vybraného diskového oddílu na určené místo k souborovému systému mikropočítače Rapsberry PI. Funkce jsou logicky využity pouze v rámci módů pro provádění image USB disků. Přípojný bod je standardně nastaven na adrese /home/pi/mnt.

Třetí část programu je tvořena veškerým nastavením ovládacích prvků grafického uživatelského rozhraní, které běží cyklicky mezi řádky app = App() a app.display(). V rámci programu jsou zde nastaveny veškeré grafické prvky systému, a to od všech 4 grafických oken aplikace, až po jednotlivé akční prvky jako jsou tlačítka a combo listy. Podrobněji jsou zde definovány souřadnice tzv. GRID, barvy, rozlišení a funkce, které jsou volány v případě stisknutí tlačítek. Tato část programu je poměrně rozsáhlá, a to především kvůli tomu, že grafické uživatelské prostředí GUIZERO nefungovalo úplně standardně dle dokumentace, ale bylo potřeba dolaďovat některé parametry pro nastavení samostatně např. výška, šířka a barva tlačítek se musely nastavovat samostatně, a tak každý jednotlivý parametr zabral jeden řádek zdrojového kódů.

9.2 Dílčí závěr

Vývoj programu pro funkci přístroje pro forenzní zkoumání USB disků nebyl bezproblémový a zabral nejvíce času v rámci praktické části diplomové práce. Nejvíce problémů při vývoji způsobovalo grafické uživatelské rozhraní GUIZERO, které se mnohdy chovalo nestandardně, než bylo napsáno v manuálu tohoto frameworku. Byla aplikována metoda pokus omyl a v průběhu zkoušení bylo třeba intenzivně procházet i různá diskusní fóra, kde se zabývaly řešením různých problémů. Další nevýhoda byla v tom, že Raspberry si neudrží bez synchronizace s internetem datum a čas, a tak bylo nutné pojmenovávat image číselnou řadou nikoliv časovým znakem. Věřím, že v rámci rozsahu diplomové práce se však nakonec všechny problémy podařilo vyřešit ke zdárnému konci a aplikace v rámci školní roviny splňuje veškeré parametry pro obhajobu diplomové práce.

10 TESTOVÁNÍ ZAŘÍZENÍ

10.1 Předpoklady

Pro provedení testů byly pořízeny dva USB Flash Disky, disk A o velikosti 7,3 GB a disk B o velikosti 7,9 GB, které podporují USB 2.0. rozhraní. Následně byl vytvořen plán testování, kdy bylo rozhodnuto, že se otestují jednotlivé módy aplikace a výsledné hodnoty se zapíšou do tabulky.

10.2 Duplikační mód

Prvním módem aplikace je tzv. duplikační mód, který slouží ke kopírování veškerých dat z disku A na disk B. Vzhledem k tomu, že zdrojová aplikace, která je volána k provedení akce v případě duplikace podporuje pouze nastavení Block Size na 512 Bytů, tak aplikace neobsahuje možnosti nastavení tohoto bloku. V aplikaci klikneme na první tlačítko duplikačního módu a v novém okně, které se nám otevře vybereme zdrojový disk, cílový disk, na který chceme kopírovat a stiskneme tlačítko. Po provedené duplikaci nám vyšly hodnoty v následující tabulce.

Block Size	Time	Rychlost
512 Bytů	1615 s	4,6 MB/S

Tabulka č. 6 Výsledky duplikačního módu

Vyhodnocení:

V rámci měření, které bylo provedeno bylo zjištěno, že rychlost duplikace z jednoho disku na druhý, alespoň ze zobrazovaných hodnot je poměrně konstantní a nijak výrazně nekolísá. Vzhledem k tomu, že docházelo zároveň ke čtení a zapisování po jedné sdílené sběrnici, tak to vysvětluje nízkou rychlost zápisu 4,6 MB, což se tedy pohybuje výrazně silně pod teoretickou maximální rychlostí USB 2.0. Co se týče funkčnosti módu, tak program proběhl bezchybně.

.

10.3 Image Mód

Image mód nám slouží k vytvoření přesné bitové kopie zdrojového disku. V rámci aplikace stiskneme druhé tlačítko Image módů. V tomto rozhraní si vybereme zdrojový disk, ze kterého chceme vytvořit bitovou kopii. Dále si vybereme zdrojovou partition cílového disku, na který chceme vytvořit image a tlačítkem mount tuto partition připojíme k souborovému systému Raspberry Pi. Připojovací bod je nastaven defaultně na adresu /home/pi/test. V rámci tohoto byly otestovány kombinace jednotlivých módů, které jsou uvedeny v tabulkách.

10.3.1 Testování při hashovací funkci SHA1

Block Size	Time	Rychlost
512	1624	46 MB /S
4096	1623	46 MB /S
32 KB	1624	46 MB /S

Tabulka č. 7 Testování image módu pro SHA1

10.3.2 Testování při hashovací funkci SHA256

Block Size	Time	Rychlost
512	1623	4,6 MB/s
4096	1622	4,6 MB/s
32 KB	1624	4,6 MB/s

Tabulka č. 8 Testování image módu pro SHA256

10.3.3 Testování při hashovací funkci SHA 512

Block Size	Time	Rychlost
512	1622	4,6 MB/s
4096	1622	4,6 MB/s
32 KB	1624	4,6 MB/s

Tabulka č. 9 Testování image módu pro SHA 512

Vyhodnocení:

Tento režim byl největším překvapením celého testování. Ukázalo se, alespoň na testovaných zařízení, že na rychlost provádění bitové kopie prakticky nemá žádný vliv nastavení velikosti bloku načtených dat, a i zvolení z následujících hashovacích funkcí. Průměrná rychlost vytváření bitové kopie byla konstantní 4,6 MB/s. Výsledné časy provedení bitové kopie byly ve všech případech pouze v řádech sekund. Očekávaly se alespoň nějaké rozdíly. Na základě vyhodnocení dat to přisuzuji tomu, že sdílená USB sběrnice Rapsberry Pi 3 je natolik pomalá a výkon procesoru naopak natolik velký, že výpočet hashovací funkce ve výsledku na celkový čas provedení nemá žádný vliv. Vzhledem ke stejným hodnotám nebyly vytvořeny žádné grafy, které byly původně plánovány, neboť by to vzhledem ke stejným hodnotám bylo neúčelné.

10.4 Wipovací mód

Po připojení paměťového média toto v režimu WIPE vybereme a spustíme program. Na testovaném USB disku byly naměřeny následující hodnoty:

Block Size	Time	Rychlost
512	767	9,3 MB/s

Tabula č. 10 WIPE mód

Vyhodnocení:

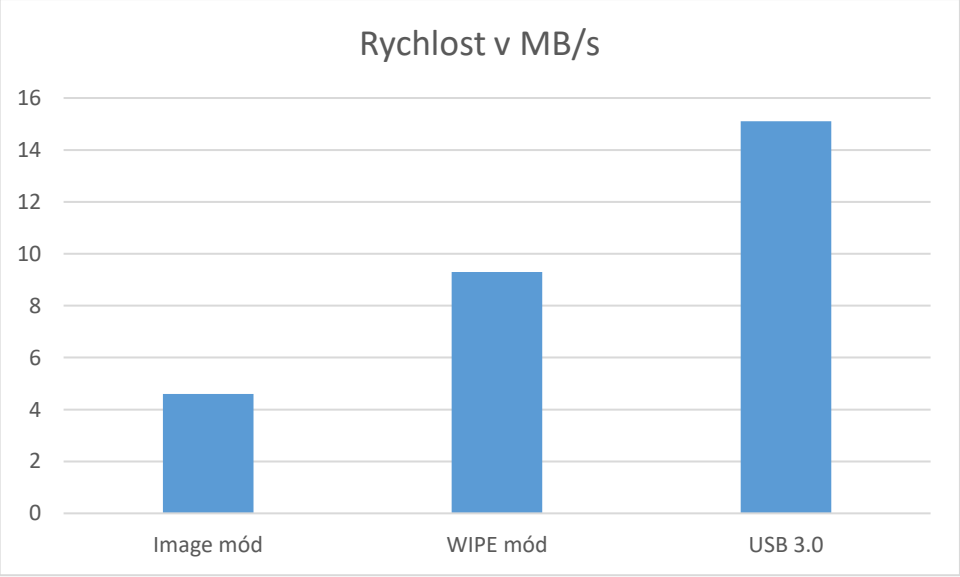
V rámci tohoto režimu bylo zjištěno, že rychlost mazání zařízení je dvakrát rychlejší oproti duplikaci nebo vytváření Image. Tuto dvakrát vyšší rychlost můžeme přisoudit tomu, že sdílená sběrnice USB na zařízení Raspberry Pi je zatížená pouze jedním zařízením. Jedná se o stejný testovací disk, který byl použit pro testy předchozích režimů.

10.5 Testování na USB 3.0

Pro posouzení vhodnosti zařízení k forenzní analýze byl proveden test zařízení ještě na počítači s USB rozhraním verze 3.0. Konkrétně byla z testovacího USB disku provedena bitová kopie v operačním systému Windows za pomocí forenzního nástroje FTK Imager. Byla naměřena průměrná rychlost vytváření bitové kopie ve výši 15,2 MB/s. Tato hodnota je více jak třikrát větší oproti provádění bitové kopie nebo duplikaci na zařízení Raspberry Pi 3 a skoro dvakrát vyšší než v módu Wipe u tohoto zařízení.

Block size	Time	Rychlost
4KB	480	15,2 MB/s

Tabulka č. 11 test USB disku na notebooku s USB 3.0



Graf č. 1 Zobrazení rychlosti kopírování dat

Vyhodnocení:

Z čistě technického pohledu nejsou naměřené hodnoty rychlostí, provádění bitových kopií, příliš optimistické, a to vzhledem k tomu, že maximální kapacita FLASH disků se v současné době pohybuje okolo 128 GB. O velikosti kapacity externích disků, které jsou připojitelné přes USB rozhraní raději nemluvě. Doba pro provedení tohoto zásadního úkonu, který je důležitý pro forenzní analýzu by byla neúměrně dlouhá. Nicméně cena takovéhoto zařízení se všemi komponenty byla celkem 2500,-Kč. Pokud bychom to porovnaly s cenou profesionálního forenzního duplikátoru, jakým je například zařízení Tableau TX1 Forensic Duplicator, které stojí v přepočtu 81.250,- Kč, tak se to v poměru cena/výkon nezdá tak špatné. Nicméně, pro potřeby vytvoření takovéhoto zařízení do funkční forenzní laboratoře, bych volil asi Banana Pi R2, které je sice dražší, ale samostatně již má implementováno rozhraní SATA verze 3 a USB verze 3. Rapsberry Pi 3 bych po provedených testech přeci jen do forenzní laboratoře nevolil. Pro fanoušky Rapsberry nezbývá než doufat, že 4. generace, která má vyjít příští rok bude již obsahovat alespoň rozhraní USB 3.0. V takovém případě by se dalo uvažovat o konstrukci i s takovýmto zařízením.

Obrázek č. 29 Profesionální duplikátor Tableau

11 ZÁVĚREČNÉ VYHODNOCENÍ

V praktické části diplomové práce bylo úkolem vytvořit platformu pro forenzní analýzu USB disků na HW architektuře ARM. Bylo to zajímavé technické dobrodružství. Na základě domluvy s vedoucím diplomové práce bylo rozhodnuto, že smyslem jednoúčelového zařízení bude provádění bitových kopií, duplikace a mazání USB disků. V rámci forenzního zkoumání digitálních důkazů se jedná o základní činnosti, které jsou prováděny znaleckými pracovišti a jsou pro další činnosti v tomto odvětví zcela zásadní. V rámci praktické části byl nejdříve proveden průzkum trhu a porovnání jednotlivých parametrů. Byl vybrán mikropočítač Raspberry PI 3 model B+, který nad ostatními jednoznačně vévodil, zejména v poměru cena/výkon a dostupnosti veškeré dokumentace k tomuto zařízení a komunitě uživatelů. Následně byl vyvíjen software. Tato položka zabrala nejvíce času, ale nakonec se podařilo vytvořit uživatelsky přívětivou aplikaci. Zařízení bylo kompletně otestováno a je plně funkční. Při testování nastal jediný problém, a to s teplotou mikropočítače, kdy na základě zvýšení teploty docházelo k rapidnímu snižování rychlosti zařízení. Toto bylo vyřešeno instalací aktivního větráku, který ochlazoval mikropočítač. Poté co se podařilo vyřešit chlazení mikropočítače již nedocházelo k žádnému kolísání rychlosti a chod zařízení byl velmi stabilní. Na základě poznání, které bylo získáno v rámci praktické části je možné konstatovat, že ARM platforma je v rámci forenzního zkoumání využitelná a je možné i za cenu o hodně nižších nákladů vytvořit zařízení, které zastane práci mnohem dražších profesionálních komerčních nástrojů na trhu.

SEZNAM POUŽITÉ LITERATURY

[1] Verifikace číslicových obvodů. Marcela Šimková, Michal Kajan. Fakulta informačních technologií, Vysoké učení technické v Brně. [online] © 2012

Dostupné z: http://www.fit.vutbr.cz/~isimkova/PCS_presentation/pcs2012.pdf

[2] Policie České republiky. Útvar zvláštních činností. [online] © 2018

Dostupná z: http://www.policie.cz/clanek/utvar-zvlastnich-cinnosti-sluzby-kriminalni-policie-a-vysetrovani-716842.aspx

[3] Zákon č. 262/2006 Sb. Zákoník práce

[4] Monitoring provozu z legislativního pohledu, Jan Kolouch, CESNET

Dostupná z: https://www.cesnet.cz/wp-content/uploads/2017/02/monitoring-provozu-legislativa.pdf

[5] Radim Polčák, František Púry, Jakub Harašta a kolektiv, ELEKTRONICKÉ DŮKAZY V TRESTNÍM ŘÍZENÍ, vyd. Brno: Masarykova univerzita, 2015. 254 s. ISBN 978-80-210-8073-7

[6] Operační systémy. Tomáš Vojnar. Vysoké učení technické v Brně Fakulta informačních technologií. Brno.

Dostupné z: http://www.fit.vutbr.cz/study/courses/IOS/public/prednasky/ios-prednaska-04.pdf

Dostupné z: https://flatcap.org/linux-ntfs/ntfs/attributes/attribute_list.html

[7] Historie Linuxu pěkně od začátku. Masarykova univerzita.

Dostupné z: https://www.fi.muni.cz/usr/jkucera/pv109/2003/xsumsky.htm

[8] The Linux Kernel Archives.

Dostupné z: https://www.kernel.org

[9] Linux dokumentační projekt. 3. aktualizované vydání.972 s ISBN 80-7226-761-2

[10] Why is the Number of Linux Distros Declining?

Dostupné z: https://www.linux.com/news/why-number-linux-distros-declining

[11] POSIX

Dostupné z: http://www.abclinuxu.cz/slovnik/posix

[12] Linux dokumentační projekt. 3. aktualizované vydání.972 s ISBN 80-7226-761

[13] Pavel Kameník. Příkazový řádek v Linuxu, Computer Press, 2013. ISBN:978-80-251-2819-0

[14] Bruce Nikkel. Practical Forensic Imaging. No Starch Press,US,2016. ISBN:978-15-932-7793-2

[15] dd(1) - Linux man page

Dostupné z:https://linux.die.net/man/1/dd

[16] dc3dd - convert and copy a file

Dostupné z:http://www.linuxcertif.com/man/1/dc3dd/

[17] DDRESCUE

Dostupné z:http://wiki.ubuntu.cz/ddrescue

[18] dcfldd (1) - Linux Man Pages

Dostupné z:https://www.systutorials.com/docs/linux/man/1-dcfldd/

[19] LiME ~ Linux Memory Extractor

Zdroj: https://github.com/504ensicsLabs/LiME/blob/master/README.md

[20] Hashovací funkce a její využití při autentizaci. Bc. Igor Piller. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. 2009 68 s.

Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=15712

[21] A tutorial on the FAT file systém. TACI PS/2 pages.

Dostupné z: http://www.tavi.co.uk/phobos/fat.html

[22] Attribute - $ATTRIBUTE_LIST. NTFS Documentation.

Dostupné z: https://flatcap.org/linux-ntfs/ntfs/attributes/attribute_list.html

[23] FLS

Dostupné z: https://wiki.sleuthkit.org/index.php?title=Fls

[24] MACTIME

Dostupné z: Zdroj: https://wiki.sleuthkit.org/index.php?title=Mactime

[25] Using Log2Timeline

Dostupné z: https://forensicaliente.blogspot.cz/2010/07/creating-timeline-wmmls-fls.html

[26] sleuthkit/scalpel

Dostupné z: https://github.com/sleuthkit/scalpel/

[27] Forensics computers

Dostupné z:https://www.forensiccomputers.com/software/guidance/encase-forensic/encase-v8-with-1-year-sms.html

[28] Zákon č. 181/2014 Sb. o kybernetické bezpečnosti

Dostupné z: Zdroj: https://www.zakonyprolidi.cz/cs/2014-181

[29] Seznamte se - APT

Dostupné z: http://www.security-portal.cz/clanky/seznamte-se-apt

[30] CZC Computers

Dostupné z:https://www.czc.cz/banana%20pi/hledat

[31] What is guizero?

Dostupné z:https://lawsie.github.io/guizero/

[32] Disable automount

Dostupné z: https://www.raspberrypi.org/forums/viewtopic.php?t=91677

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ČR	ČESKÁ REPUBLIKA
ICT	INFORMATION AND COMMUNICATION TECHNOLOGIES
GDPR	GENERAL DATA PROTECTION REGULATION
USB	UNIVERSAL SERIÁL BUS
HW	HARDWARE
ARM	ADVANCE RISC MACHINE
UZČ	ÚTVAR ZVLÁŠTNÍCH ČINNOSTÍ
SKPV	SLUŽBA KRIMINÁLNÍ POLICIE A VYŠETŘOVÁNÍ
IP	INTERNET PROCOL
OKTE	ODBOR KRIINALISTICKÉ TECHNIKY A EXPERTÍZ
PC	PERSONAL COMPUTER
NAS	NETWORK AREA STORAGE
LAN	LOCAL AREA NETWORK
P2P	PEER TO PEER
BSD	BERKLEY SOFTWARE DISTRIBUTIONS
NFC	NEAR FIELD COMMUNICATION
GPS	GLOBAL POSITIONING SYSTEM
SD	SECURE DIGITAL
HDD	HARD DISK DRIVE
SSD	SOLID STATE DRIVE
PATA	PARALELL ADVANCED TECHNOLOGY ATTACHMENT
RAM	READ ACCES MEMORY
DDR	DOUBLE DATA RATE
DVD	DIGITAL VIDEO DISC
CD	COMPACT DISC

PLC	PROGRAMMABLE LOGIC CONTROLED
OSINT	OPEN SOURCE INTELIGENS
CHS	CYLINDER HEAD SECTOR
LBA	LINEAR BLOCK ADDRES
NAND	NEGATIVE AND
TCP/IP	TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL
RPM	RED HAT PACPAGE MANAGER
APT	ADVANCED PACPAGE TOOLS
APT	ADVANCED PEARSISTANT THREAT
IEEE	INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
BASH	BOURN AGAIN SHELL
XTERM	X TERMINAL EMULATOR
GUI	GRAPHICAL USER INTERFACE
MD5	MESSAGE DIGGEST ALGORITHMS
SHA	SECURE HASH ALGORITHM
FAT	FILE ALLOCATION TABLE
NTFS	NEW TECHNOLOGY FILE SYSTEM
ASCII	AMERICAN STANDARD FOR INFORMATION INTERCHANGE
MFT	MASTER FILE TABLE
PID	PROCESS INDETIFICATION NUMBER
FTP	FILE TRANSFER PROTOCOL
SSH	SECURE SHELL
VNC	VIRTUAL NETWOR COMPUTING
WIFI	WIRELESS FIDELITY
OS	OPERATING SYSTEM
SATA	SERIAL ATA

HDMI	HIGH DEFINITION MULTIMEDIA INTERFACE
AP	ACCESS POINT
WPA	WIFI PROTECTED ACCESS
RAID	REDUNDANT ARRAY OF INDEPENDENT DISKS

SEZNAM OBRÁZKŮ

Obrázek č. 1 Schéma tranzistoru NPN…….……10

Zdroj: http://elek.wz.cz/d_tr_ty.html

Obrázek č. 2 Osobní počíč……16

Zdroj: https://goo.gl/images/CwCVZ2

Obrázek č. 3 Síťové datové úložiště NAS…….17

Zdroj: https://goo.gl/images/sxST62

Obrázek č. 4 Mobilní telefon ……....18

Zdroj: https://goo.gl/images/1ZXTKD

Obrázek č.5 Datacentrum…….19

Zdroj: https://goo.gl/images/8eRtQu

Obrázek č.6 Ukázka monitoringu sítě za pomocí programu Wireshark……....20

Zdroj: https://goo.gl/images/jqUJqG

Obrázek č. 7 Pevný disk……21

Zdroj: https://goo.gl/images/KxKbkq

Obrázek č. 8 Operační paměť……22

Zdroj: https://goo.gl/images/a4VomB

Obrázek č. 9 Konstrukce disku…….….24

Zdroj: http://www.fit.vutbr.cz/study/courses/IOS/public/prednasky/ios-prednaska-04.pdf

Obrázek č. 10 Sectory a clustery……...25

Zdroj: http://www.ntfs.com/hard-disk-basics.htm

Obrázek č. 11 Adresářová struktura Linuxu…….….30

Zdroj: Vlastní

Obrázek č. 12 zaváděcí sektor FAT……...39

Zdroj: vlastní

Obrázek č. 13 ROOT DIRECTORY…….40

Zdroj: vlastní

Obrázek č. 14 MFT Table…….43

Zdroj: vlastní

Obrázek č. 15 obsah souboru……44

Zdroj: vlastní

Obrázek č. 16 Ukázka GUI prostředí Autopsy……..……...47

Zdroj: vlastní

Obrázek č.17 Supertimeline…….51

Zdroj: https://digital-forensics.sans.org/blog/2013/02/16/idx-sample-file-malware

Obrázek č. 18 Procesor na architektuře ARM Broadcom BCM2837B0……..……55

Zdroj: https://www.raspberrypi.org/forums/viewtopic.php?t=210111

Obrázek. č 19. BANANA PI R2……56

Zdroj: www.czc.cz

Obrázek č. 20 Odroid C2……...57

Zdroj: http://www.hardkernel.com/main/products/prdt_info.php?g_code=G145457216438

Obrázek č. 21 Raspberry Pi 3 Model B+ …… 58

Zdroj: www.czc.cz

Obrázek č.22 Sestavení zařízení……...59

Zdroj: vlastní

Obrázek č. 23 Instalace operačního systému na SD Kartu……..…...60

Zdroj: vlastní

Obrázek č. 24 Ukázka připojení přes VNC do Raspberry PI 3 z notebooku……..61

Zdroj: vlastní

Obrázek č. 25 Hlavní menu ……..…65

Zdroj: vlastní

Obrázek č. 26 Duplikační mód……..…66

Zdroj: vlastní

Obrázek č. 27 Imigovací mód……...68

Zdroj: vlastní

Obrázek č. 28 WIPE mód……..68

Zdroj: vlastní

Obrázek č. 29 Profesionální duplikátor Tableau……...76

Zdroj: https://www.guidancesoftware.com/tableau/hardware/tx1

SEZNAM TABULEK

Tabulka č. 1 Seznam disků……35

Zdroj: vlastní

Tabulka č. 2 Výstup hashovacích funkcí ze vstupního řetězce ahoj……..39

Zdroj: vlastní

Tabulka č. 3 Atributy záznamů v ROOT DIRECTORY……...41

Zdroj:vlastní

Tabulka č. 4 hlavička a zápatí v hexa……45

Zdroj: https://github.com/sleuthkit/scalpel/blob/master/scalpel.conf

Tabulka č. 5 Ceny komerčních forenzních programů……48

Zdroj: https://www.forensiccomputers.com/software/guidance/encase-forensic/encase-v8-with-1-year-sms.html

Tabulka č. 6 Výsledky duplikačního módu……...71

Zdroj: vlastní

Tabulka č. 7 Testování image módu pro SHA1……..…72

Zdroj: vlastní

Tabulka č. 8 Testování image módu pro SHA256……72

Zdroj: vlastní

Tabulka č. 9 Testování image módu pro SHA 512……73

Zdroj: vlastní

Tabula č. 10 WIPE mód……73

Zdroj: vlastní

Tabulka č. 11 test USB disku na notebooku s USB 3.0……74

Zdroj: vlastní

SEZNAM GRAFŮ

Graf č. 1 Zobrazení rychlosti kopírování dat…….74

Zdroj: Vlastní