Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Forenzní analýza v OS Windows – video tutoriály

Bakalářská práce

Autor: Dominik Kunert

Studijní obor: Informační management

Vedoucí práce: Svoboda Tomáš, Ing. Ph.D.

Hradec Králové 26. března 2023

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím veškeré uvedené literatury.

vlastnoruční podpis

V Hradci Králové dne 16.4.2023 Dominik Kunert

Poděkování:

Děkuji vedoucímu bakalářské práce **Svoboda Tomáš, Ing. Ph.D.** za metodické vedení práce a že si mě vzal pod svoje křídla. Pan doktor si na mě vždy našel čas a dokázal mi poradit, když jsem si nevěděl rady. Velmi oceňuji jeho pozitivní přístup při online i fyzických konzultacích. Jsem velmi rád, že jsem si vybral právě pana doktora, jelikož jsem si nikoho lepšího přát ani nemohl a nezbývá mi nic jiného, než ho s obrovským spokojením doporučit každému za úžasné vedení bakalářské práce. Děkuji

Anotace

Cílem bakalářské práce je vytvořit podpůrné materiály v oblasti forenzní analýzy. V teoretické části autor práce představí a podrobně popíše vývoj operačních systémů s dalším zaměřením na operační systém Windows. Následně teoretická část představí úvod do operačních systému, zejména jejich bezpečnosti. V rámci bezpečnosti budou popsány různé formy útoků a představení základních zásad pro lepší ochranu systému proti takovým útokům. Autor dále představí principy a techniky forenzní analýzy, které budou rovněž součástí práce.

V praktické části práce autor představí a podrobně popíše postupy a řešení možných úloh forenzní analýzy operačních systémů se zaměřením na OS Windows. Praktické řešení je realizováno také v jiné formě pro lepší pochopení – video tutoriály.

Annotation

Title: Forensic analysis in OS Windows - video tutorials

The aim of the bachelor thesis is to create supporting materials in the field of forensic analysis. In the theoretical part, the author of the thesis presents and describes in detail the development of operating systems with a further focus on the Windows operating system. Subsequently, the theoretical part will present an introduction to operating systems, especially to their security. As part of security, various forms of attacks will be described and the basic principles for better protection of the system against such attacks will be presented. The author will also present the principles and techniques of forensic analysis, which will also be part of the thesis.

In the practical part of the work, the author presents and describes in detail the procedures and solutions for possible tasks of forensic analysis of operating systems with a focus on the Windows OS. The practical solution is also implemented in another form for better understanding – video tutorials.

Klíčová slova

Windows OS; forenzní analýza; video tutoriály; disková úložiště; bezpečnost OS;

Keywords

Windows OS; forensic analysis; video tutorials; disk storage; OS safety;

Obsah

Seznam obrázků

Seznam grafů

1 Úvod

Forenzní analýza je pojem, který je spjatý určitou formou se zkoumáním digitálních dat. Jednou z oblastí forenzní analýzy je analýza datových úložišť (disky v osobních počítačích, telefonech, USB flashdisky, …). Jedná se o úložiště, která uchovávají cenná data rozvíjející se den co den. Taková data je potřeba chránit před různými útoky zvenčí, či vnitřním selháním. Díky rozšíření komunikačních a informačních technologií vznikla vysoká návaznost na počítačovou kriminalitu pro páchání trestných činů. Právě z tohoto důvodu byla vytvořena metoda, která takové prostředí dat bude umět zkoumat – forenzní analýza.

Práce se ale nejdříve zabývá teoretickými základy operačních systému jako je například popis vývoje operačních systémů od samého začátku, až po aktuální období s využívanými architektury (monolitická, mikro a hybridní jádra) s dalším zaměřením na konkrétní operační systém Windows. V oblasti operačního systému Windows se již klade důraz na jeho funkcionalitu a možné hrozby jako je například Malware nebo síťové útoky. V návaznosti na bezpečností hrozby se také práce zabývá úvodem do bezpečnosti dat a základními pokyny bezpečnostních zásad jako je ACL, CIA triáda a slabiny systému. V rámci kapitoly bezpečnosti operačního systému Windows

Tato práce dále poskytuje základní průchod forenzní analýzou pro Windows, se zvláštním zaměřením na dva nástroje, FTK Imager a Autopsy. FTK Imager je nástrojem pro pořizování digitálních důkazů. Umožňuje vyšetřovatelům vytvářet forenzní obrazy digitálních důkazů při zachování integrity dat. Autopsy je digitální forenzní nástroj s otevřeným zdrojovým kódem, který je široce používán díky svému uživatelsky přívětivému rozhraní a široké škále funkcí. Jedná se tedy o program, který slouží ke zkoumání například právě obrazu disku pořízený skrz program FTK Imager. Závěrem práce je také popsaná praktická část včetně video tutoriálů o forenzní analýze ve Windows, která zobrazuje proces možného forenzního případu včetně podrobných pokynů, jak používat Autopsy a FTK Imager. Video tutoriály nabízí další možnou formu pohledu na forenzní analýzu pro lepší pochopení možného forenzního případu.

1.1 Důvod výběru tématu bakalářské práce

Hlavním důvodem výběru této bakalářské práce je zaujatí z oblasti operačních systémů a diskových úložišť. Dalším důvodem je zvolení tématu díky osobním zkušenostem se psaním seminárních prací z těchto oblastí na střední škole (FREENAS, LAMP). Osobní, možná poněkud zvláštní zaujetí bylo vzbuzeno také díky přítelkyni, která studuje kriminalistiku a proto slovo „vyšetřování“ je v obou našich oborech významným prvkem.

1.2 Cíle bakalářské práce

Prvním cílem práce je seznámit čtenáře s úvodem do operačních systémů se zaměřením na operační systém Windows. Dalším cílem je představit bezpečnost OS, jako je seznámení s CIA triádou, hrozbami a zranitelností OS. Poslední cíl zahrnuje praktické představení problematiky právě do forenzní analýzy, výběru nejpoužívanějších softwarů a věnovat se jejich podrobnému praktickému představení. Přínosem práce je pomoci s výběrem těchto nástrojů budoucím možným zájemcům o takové systémy zkoumání disků a přiblížit jim fungování nástrojů díky video tutoriálům.

1.3 Účel práce

Účelem práce je vytvořit odborný pohled do forenzní analýzy OS Windows s možností využitím video tutoriálů pro lepší pochopení fungování nástrojů forenzní analýzy.

1.4 Výzkumné otázky

1) Jaké jsou hlavní typy (jádra) operačních systémů?
2) Kolik, či jaké hrozby a zranitelnosti existují u OS Windows?
3) Co všechno lze zkoumat pomocí forenzní analýzy?
4) Jaké jsou nejpoužívanější nástroje forenzní analýzy a jejich odlišnosti?

1.5 Pracovní hypotéza(y)

Předpokládanými typy operačních systému je svatá trojice Unix, Windows a MacOS s nespočtem možných hrozeb (viry, červy, trojské koně)

U forenzní analýzy je předpokládaným očekáváním teorie, že se dají zkoumat libovolná datová úložiště a u nástrojů se nachází nepatrná odlišnost mezi těmi tools, co jsou zdarma (například rozdílnost v GUI či zaměřením), ale s velmi podobnou funkcionalitou. Dalším předpokladem je také fakt, že placené tools forenzní analýzy by měli být lepší a mít určité funkce, vizuál, ovladatelnost či zabezpečení na vyšší úrovni.

2 Metodika zpracování

Sběr informací byl realizován buď přes poskytnuté zdroje vedoucím práce nebo vlastnoručně sehnané zdroje. Tyto zdroje jsou tvořené elektronickými dokumenty jako jsou vědecké databáze, odborné články a diplomové práce v daném tématu za využití dedukce. Dané hypotézy budou ověřovány především z teoretických poznatků a dostatku nalezených informací. Postupné šetření v bakalářské práci navazující na forenzní analýzu již bude zahrnovat konkrétní praktický výzkum zahrnující například instalaci, vlastnoruční vyzkoušení jednotlivých tools a vytvoření praktického příkladu forenzní analýzy.

3 Úvod do operačních systémů

První kapitola je věnována úvodu do operačních systémů, jelikož v dnešní době je operační systém nezbytnou součástí každého počítače, telefonu, chytrých hodinek a dokonce i třeba ledniček. V dnešní době je zkrátka velmi absurdní představit si počítač, bez žádného systému. Ze začátku vzniku počítačů tomu ale tak zkrátka bylo.

Operační systém je základním programovým vybavením počítače (software), které se zavadí do operační paměti při startu počítače, zůstává v činnosti až do jeho vypnutí a v dnešní době je nezbytný pro jeho činnost. Hlavní úkolem operačního systému je propojení komunikace s uživatelem, aby mohl počítač lépe ovládat. Krom jiného se operační systém stará o inicializaci hardware, správu prostředků a rozdělování funkcí v počítači. Lépe řečeno nejdříve vytvoří novou vrstvu pro ovládání hardware s funkcemi, takzvané API, přes kterou přiděluje procesům systémové prostředky (CPU, paměti, I/O zařízení), které mají určitý čas. Pokud tento čas proces překročí, může novodobý operační systém přidělené prostředky odebrat násilím pomocí přerušení. [1]

Operační systémy dělíme dle počtu uživatelů buď na jedno nebo více uživatelské a podle počtu úloh, které jsou schopny zpracovávat v jednom momentu na jedno/více úlohové. Více úlohové představují multitasking, což označuje běh více procesů současně. Multitasking může být buď kooperativní (předávání řídí procesy, zastaralé) nebo preemptivní (předávání řídí jádro). Proces je spuštěný program, který se právě vykonává procesorem. Takový program může mít i několik oddělených procesů, kterým přiděluje prostředky právě operační systém. Další formou dělení procesu je vlákno. Vláknům je přidělován právě čas prostředku a po vypršení tohoto času je přidělen čas jinému vláknu zejména dle priority. Oproti procesům dokážou spolu sdílet prostředky, jako je například paměť. Pokud ale přeci jenom máme procesor s více jádry a vlákny, pak skutečně dochází k souběžnému běhu vláken, nikoliv pouze k iluzi pomocí velmi rychlého přepínání mezi vlákny. [1]

Operační systém tedy není opravdu nic jednoduchého a proto se nejdříve práce pokusí poukázat na historický vývoj operačních systémů minulostí a až následně naváže na problematiku kernelu.

3.1 Základní historie

První podkapitola je věnována historii operačních systémů V první části bude vysvětleno, jak probíhal vývoj operačních systémů a v té druhé se již práce bude plně věnovat historii systému Windows. Třetí a poslední podkapitola zahrnuje úvod do kernelu a jeho vývoj. Pokud není uvedeno jinak, vychází texty v následujících podkapitolách ze zdrojů [3, 4 a 7].

3.1.1 Prehistorie (50. léta)

Jak již bylo zmíněno, první počítače zkrátka neměly žádný operační systém, tudíž každý jednotlivý počítač byl unikátním a bylo nutné napsat program přímo pro něj. Tato realita byla velmi neefektivní a náročná, jelikož kód samotný musel být často psán přímo v binárním kódu. Nutno podotknout, že tyto počítače byly sálové (obrovské rozměry) a hlavním výrobcem byla americká firma IBM.

3.1.2 První operační systémy (60. léta)

Postupem času došlu ke vzniku prvních náznaků operačních systémů často označovaných jako Monitor. Monitor zaváděl velmi základní systém ochrany paměti, kde program nemohl zapisovat do oblasti paměti monitoru. Dále byl schopen již využít IO operace, kde tyto operace umožňovaly přepínaní mezi módy čtení a zápisu přes takzvané děrné štítky. Poslední funkcí bylo provedení programu a s ním související kontrola nekonečné smyčky „Time out“ – po určitém časovém intervalu přeruší program.

3.1.3 Zrod Unixu (70. léta)

V době, kde každý výrobce má vlastní, naprosto odlišný operační systém, přichází zrod jednoho z nejvýznamnějších OS vůbec – UNIX. Tento systém je výjimečný především svou jednoduchostí a nezávislostí na hardware. Dokázal také běh více programů zároveň a přepínaní mezi nimi díky SPOOLu. Tento systém se navzdory konkurence systému Multics a VSM stal standardem.

3.1.4 Nástup DOS a MacOS (80. léta)

Tato doba zaznamenala vysoké rozšíření 8 a 16bitových počítačů, jejichž rozšíření vedlo přes firmy až k domácnostem. Velmi revolučním se stal ale zmiňovaný proprietární MacOS, který jako první OS využil integraci grafického rozhraní. Obrovský marketingový tah ale vyhrála firma Microsoft, která licencovala OS DOS. Tento systém však měl mnoho omezení jako velikost paměti a disků, podpora pouze jednoho uživatele či nepodpora multitaskingu (provádění několika procesů současně). Tyto faktory však zapříčinily nízkou cenu, díky které měl tento systém vysoké rozšíření v domácnostech.

3.1.5 Příchod Linuxu (90.léta)

V tomto období se již Microsoft vyznačuje jako monopolní firma pro osobní počítače a postupně se snažil proniknout na trh serverů s NT. Nicméně dochází k příchodu Linuxu pod licencí GNU, která zaručuje právo všem lidem na získání programu včetně zdrojových kódů zdarma. Z toho důvodů vzniká mnoho rozdílných distribucí, do kterých distributoři přidávají řadu dalších programů. [2]

3.2 Windows historie

Jak již bylo zmíněno, první OS od firmy Microsoft s názvem MS-DOS, měl určitou řadu omezení. Tyto problémy byly ale vyřešeny jeho první verzí s názvem Windows 1.0 který přináší uživatelskou přívětivost a také podporu multitaskingu, kde vznikla možnost přepínaní mezi programy avšak bez překrývání oken. Tento nedostatek poté odstranila verze 2.0. Verze 3.0 přinesla GUI, virtuální paměť (využití pro swapování na disk) či stromový správce souborů.

Někomu již více známý Windows 95 přinášel mnoho dalších vylepšení. Mezi hlavní patří například částečně 32bitový systém, velmi chválené zcela nové GUI, a integrace TCP/IP pro lepší podporu sítí. Následovník Windows 98 přinášel podporu USB, plných 32bitů a podporu směrnic AGP. Jednalo se tak o jeden z posledních systémů založených na starém jádře. Windows 2000 ještě přichází s funkcí Plug and Play pro automatické instalace ovladačů či se sadou knihoven API pod názvem DirectX.

Nyní se pojďme podívat více do přítomnosti a 21. století s příchodem Windows XP. Zkratka XP vyznačuje „zkušenost“ od strany Microsoftu. Tento systém vychází z jádra Windows NT a byl vydáván ve dvou hlavních verzích – Home pro domácnosti a Professional pro vývojáře. Tento velmi kvalitní a úspěšný systém se vyznačoval nárůstem rychlosti. Hlavní výhodou je nové uživatelské rozhraní pro lepší zkoumání systému a jeho možností. Následuje Windows Vista s Aero rozhraním. Tento ne příliš oblíbený systém vyčnívá novou vizuální stránkou za využití průhlednosti, animací či podporou vyššího rozlišení. Přichází s novým formátem dokumentů XPS podobný PDF, podporou IPv6, integrovaným Defenderem a mnoha více verzemi.

Windows 7 je hrdým následovníkem fiaska Windows Vista, vydaný v roce 2009. Tento systém se vyznačuje plnou kompatibilitou s ovladači zařízení, aplikací a hardwarem. Krom opětovného nárustu výkonu a grafických vylepšení (nová nabídka start, hlavní panel, vylepšené vyhledávání, gadgets) přichází také s podporou virtuálních disků, rozpoznáním řeči či rukopisu a především optimalizací. Ohledně Windows 8 bych se nejradši nezmiňoval, jednalo se o systém, který byl navržen spíše pro tablety a mobilní zařízení. Kromě nového grafického prostředí Metro, podpory USB 3.0, více monitorů a NTFS v5 nepřináší systém nic zásadního. Následovný update na verzi 8.1 již opravuje své chyby a vytváří tak více přístupný systém.

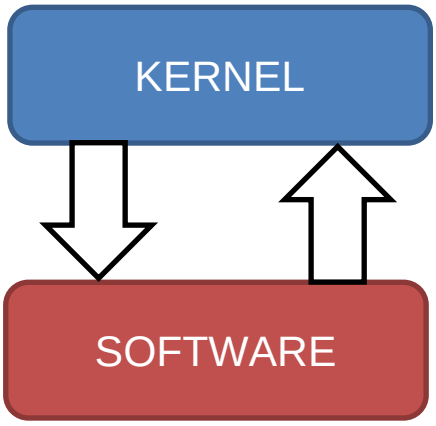
Windows 10 je momentálním vládcem trhu s novými funkcemi zabezpečení jako je například biometrické rozpoznávání Windows Hello (obličej, otisk, PIN). Tato verze přináší především aktualizované a oblíbené rozhraní z Windows 7 či nové společníka s názvem Cortana, pro hlasové příkazy. Přichází také nový a přehlednější průzkumník souborů či podpora virtuálních ploch, pro využití běhu různých aplikacích na oddělených plochách. Windows 11 je posledním momentálním nástupcem. Jeho předností jsou především grafické vylepšení a lepší přístup k určitým aplikacím (Android a iOS store, Teams).

3.3 Kernel

Pod názvem kernel se skrývá jádro operačního systému kde kvalita takového kernelu rozhoduje prakticky o kvalitě celého systému. Jak již bylo zmíněno, operační systém obstarává přidělování prostředků programům. O tuto funkci se stará právě jádro, kde přiděluje nejčastěji paměť, procesor a vstupně výstupní zařízení. Jádro rozhoduje právě o tom, který program dostane tyto prostředky přiděleny a na jak dlouho. Krom přidělování ale dokáže také prostředky odebírat a to buď preemptivně (násilím) či nepreemptivní (proces se musí sám vzdát prostředku). Dále zajišťuje multitasking, víceuživatelské prostředí, ovládá zařízení počítače pomocí ovladačů a funkcí, či provádí systémová volání. Systémové volání je ve zkratce proces, který žádá jádro o provedení nějaké operace. Jedná se tak o přepnutí kontextu z uživatelského do jaderného prostoru. Jádro tudíž funguje ve dvou hlavních módech pro zajištění bezpečnosti systému. Tyto dva módy se nazývají omezený a privilegovaný. Již dle názvu lze poznat, že privilegovaný mód je ten vyšší, který zajišťuje bezpečnost programu, aby nemohl zasahovat mimo svůj vymezený prostor. V tomto privilegovaném režimu běží právě jádro operačního systému a ostatní procesy běží v omezeném režimu. Díky tomu neztratí jádro nikdy kontrolu nad počítačem a nedochází ani k ohrožení špatně napsaným programem, který by mohl negativně ovlivnit činnost operačního systému. Při nastání problému bude způsobena havárie programu a nikoliv OS, který bude nadále stabilní. Privilegovaný stav dokáže provádět privilegované instrukce, které dokáže provádět pouze zmíněné jádro. Mezi tyto instrukce patří například řízení procesoru, práce se speciálními registry či zákaz přerušení. [5, 6]

Nyní autor vysvětlí, jaké typy jader operačního systému existují. Typů existuje více, my se ale zaměříme na tři základní typy a to jsou jádra monolitická, mikro a hybridní, které používají právě systémy z rodiny Windows NT (NT 3.1 – Win 10).

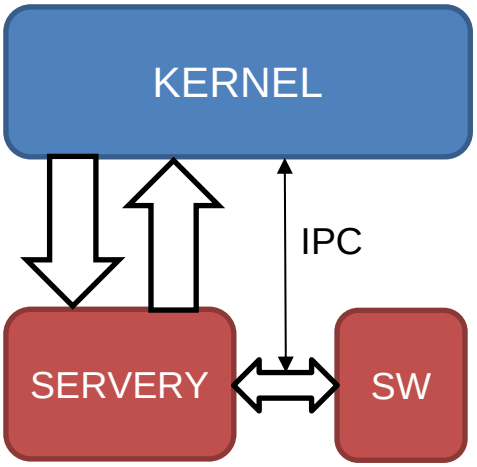
Monolitická jádra jsou jedny z prvních typů jader operačního systému dříve označována jako nemodulární. Tyto jádra jsou stavěna jako jeden souvislý celek, využívající stejnou oblast paměti pro všechny služby, díky tomu funguje vše na stejné úrovni oprávnění. Mezi hlavní výhody toho typu jádra patří především rychlost a výkonnost. Oproti tomu nevýhody mohou spočívat například v případné chybě ovladače, která by mohla ohrozit celé jádro. Tento problém ale vyřešil příchod modulárního monolitického jádra, které odděluje ovladače do jiného bloku kódu (nezávislé bloky jádra) Další nevýhodou je náročnost na vývoji a obtížné udržování kvůli velkému jádru. S neustále rozšiřujícím se kódem postupem času je tak nutno znát jednotlivé funkce jádra. Tohoto typu jádra se ujal převážně UNIX se svými systémy.



Obrázek 1 Monolitické jádro

Zdroj: upraveno dle [34]

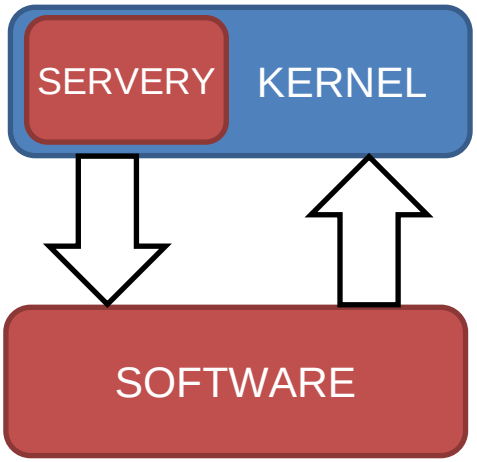
Další formou jádra jsou takzvané **mikrojádra**. Dle názvu si lze usmyslet, že se jedná o jakousi minimalizovat verzi monolitického jádra. Je tomu tak a toto jádro zahrnuje pouze nejnutnější části nutné pro provoz se smyslem zjednodušení. Jádro zde není stavěno jako jeden souvislý celek, ale je rozděleno do logických částí. Jaderný prostor je využíván právě pro ty nejdůležitější části a zbytek služeb operačního systému funguje v uživatelském prostoru, o který se starají „servery“. Mezi hlavní výhodu patří snadnější programování a údržba jádra, bohužel na častou úkoru rychlosti. Další nevýhodou je, že samotné procesy nemohou manipulovat se společnými daty. Jedni z hlavních představitelů jsou Symbian či GNU Hurd.



Obrázek 3 Mikrojádro

Zdroj: upraveno dle [34]

Poslední formou kernelu jsou **hybridní jádra**, která jsou ale spíše podobná mikrojádru s vlastnostmi monolitického jádra. Tato jádra měla za cíl spojit výhody obou předchozích typů, jak rychlost, tak jednoduchost. Některé funkce jsou tak opět integrovány do prostoru jádra aby kód běžel rychleji, jiné zůstávají nadále oddělené. Hlavním rozdílem oproti monolitickému jádru je, že samo nedokáže zavádět modulu za běhu a proto opět musí využívat zmíněné servery. [5, 6] *Málo kdo ale ví, že modulární monolitické jádro a hybridní jádro, prezentuje naprosto stejnou věc.*



Obrázek 2 Hybridní jádro

Zdroj: upraveno dle [34]

Mezi další jádra které existují, ale již v této práci nebudou rozebírána jsou například jádra v reálném čase, které Windows vyloučil pro přechod, nanojádra, či exojádra.

4 Bezpečnost OS Windows

Předchozí kapitola již pojednávala o jakési formě bezpečnosti systému při zmínce kernelu a jeho práci mezi režim jádra a uživatelským režimem. Jelikož Windows patří mezi nejrozšířenější systém především mezi domácnostmi, nachází se zde mnoho útočníků, kteří chtějí náš systém neprávem zkoumat či poškodit. Některá data v dnešní době mohou mít i nevyčíslitelnou hodnotu, proto je potřeba mít kvalitní ochranu systému, bohužel existuje jedno známe přísloví „bezpečnost systému je tak silná, jak je silný její nejslabší článek“. Pokud není uvedeno jinak, vychází následující text v kapitole 4 ze zdroje [9].

Takovéto zranitelné místo, na které se váže mnoho hrozeb, bývá často cílem útoku. Hrozba je tedy ve zkratce využití zranitelného místa systému k útoku na zařízení. Existují celkem dvě hlavní formy útoku:

1) **Fyzické útoky** – Jedná se o útok za využití odcizení, poškození hardwaru, ale také získání přístupu k počítači pro provedení škod, smazání důležitých dat či fyzické nainstalování sledovacího softwaru.
2) **Nefyzické útoky** – Veškeré útoky které jsou realizovány přes síť, k takovým útokům stačí mít počítač připojení k internetu skrze ethernetový kabel nebo Wi-Fi.

Útoky bývají nejčastěji cíleny na zařízení, program či data a jejich forma je neoprávněná (neoprávněné používání PC / síťové komunikace / využití prostředků / přístup k datům). Osoba která za takovými útoky se nazývá hacker. Jedná se o specialistu, který ví, jak funguje systém a dokáže ho upravit dle vlastních potřeb. Na internetu se můžeme také setkat s crackerem, jehož cílem je pouze odstranění ochranných prvků (například placené hry). Tento soubor se nazývá warez a je nejčastěji šířen formou P2P sítě. Hackery dělíme na tři základní skupiny:

1) **Black hat** – za tímto názvem se skrývá hacker se špatným úmyslem škodit uživateli či zařízení, vytváří malware, prolomuje bezpečnostní protokoly, špehuje či krade data. Jejich podklad bývá velmi často finančně ohodnocen.
2) **Gray hat** – je pomezí mezi dobrým a zlým hackerem, nechtějí škodit. Často se nabourají do systému a následně informují o této zranitelnosti veřejnost či majitele systému, stále se ale jedná o ilegální typ hackování.
3) **White hat** – dobrý hacker se skrytým názvem etického hackování. Bývají mnohdy najímáni firmami, aby našli zranitelnosti systému a následně je opravili.

4.1 Malware

Jedná se o souhrnné označení pro programy, jejichž účelem je škodit buď se zaměřením na poškození zařízení nebo uživatele. Tato podkapitola poukáže, který škodlivý software je nejčastější pro setkání s uživatelem. Následující podkapitoly vychází ze zdrojů [7, 8, 10].

4.1.1 Vir

Počítačový vir je program, který se dokáže šířit sám bez vědomí uživatele pomocí replikace (tvorba vlastní kopie), dokáže se tedy šířit z počítače na počítač s cílem ničit či poškodit data. V nejčastější formě se s viry setkáme ve spustitelných souborech (.exe), dokumentech (.pdf) nebo prostřednictvím pošty. Většina kvalitních virů v první fázi napadne systémovou oblast pevného disku, díky čemu si zajistí spuštění se startem počítače. Následkem toho dokáže vir útočit na registry, nahrazovat soubory nebo přebrat kontrolu nad programy. Jako zásadní ochranu proti virům platí mít kvalitní, aktualizovaný antivir a neklikat na podezřelé odkazy.

4.1.2 Červ

Červ by se dal prakticky považovat za jistý druh počítačového viru, jelikož se také dokážou samy množit a šířit se. Jeho cílem je nakazit co největší množství počítačů a převzít kontrolu nad systémovými prostředky, které mohou způsobit například zpomalení systému. Hlavním rozdílem oproti viru je fakt, že červ se snaží skrýt svoji přítomnost a dokáže se šířit automaticky, kdežto vir potřebuje akci uživatele. Například se využívá pro sběr informací a tvorbu „zadních vrátek“ jako cestu k infikování další nákazou.

4.1.3 Trojský kůň

Jedná se o program, který se liší od viru tím způsobem, že není schopen vlastní replikace a další infekce jiných souborů. Trojský kůň tak označuje spíše typ škodlivého kódu, který je skrytý uvnitř programu a proto vychází přirovnání ze známého příběhu o dobytí Troji. Na venek se tak program tváří jako naprosto legitimní a uživatel si ho následně spustí sám v dobré víře. Co trojský kůň dokáže, záleží na jeho naprogramování. Nejčastější využití je pro převzetí kontroly nad zařízením, získání dat a odeslání je útočníkovi či kompletní kolaps systému.

4.1.4 Ostatní

Typů malwaru je opravdu mnoho a psát o každém z nich by mohlo být téma minimálně na seminární práci. Kvůli jinému tematickému zadání se pojďme pouze okrajově podívat, které další typy malware existují.

- **Spyware** – obtížně odhalitelný malware, který se rád skrývá a sbírá potají data o chování uživatele na internetu, historii prohlížených stránek či osobní údaje a následně je posílá třetí straně
- **Keylogger** – spadá pod spyware a dokáže skrytě zaznamenat každé stisknutí klávesy na počítači
- **Ransomware** – profesionální program k zašifrování důležitých dat, po zašifrování například celého disku požadují hackeři výkupné za odblokování.
- **Adware** – pravděpodobně nejméně nebezpečný typ malware, který uživatele spíše otravuje svými vyskakovacími okny, nebezpečný se stane v případě kliknutí na takové vyskakovací okno
- **Rootkit** – jedná se program navržený pro získání vyšších oprávnění (například administrátorských), díky čemuž dosáhne lepší kontroly a dálkovému přístupu na zařízení
- **Phishing** – v tomto případě se nejedná o žádný program, ale spíše o techniku podvodníků k získání citlivých a osobních informací, jejichž kombinace může být například využita pro uhodnutí hesla

4.2 Síťové útoky

Jedná se útok realizovaný vzdáleně a často bývá konkrétně cílený. Takovýto přímý útok využívá mezer, které jsou součástí síťových protokolů pro překonání ochrany. Mezi nejznámější síťové útoky spadá DOS (odmítnutí služby) a DDOS (distribuovaný DOS). Rozdíl mezi těmito útoky je v počtu zařízení, které útočí na zařízení. V případě DOS útoku se jedná o útok pouze z jednoho konkrétního zařízení, který je soustředěn na jedno koncové zařízení nebo server. DDOS útoky jsou prováděny přes více zařízení, které jsou ovládány jedním útočníkem tzv. síť infikovaných počítačů klidně i z celého světa. Oproti DOS nelze útoku zamezit zablokováním jednoho konkrétního zařízení a jejich cílem je například shození celých firemních sítí.

Takovéto útoky fungují na poměrně jednoduché bázi, jejich cílem je útok na internetové služby, kde dochází k přehlcení požadavky a následnému pádu, nefunkčnosti, zpomalení, čí nedostupnosti služeb (webová stránka, aplikace, e-shop). Útočník nemá za cíl ovládnout službu, ale pouze ji znepřístupnit ostatním uživatelům a využít tak některé chyby. Nejčastěji se útoky vyznačují zaplavením náhodnými daty, zatížením procesoru cílového serveru, narušením konfiguračního nastavení a dokonce může dojít i k pádu operačního systému. Vhodnou ochranou proti takovým útokům je firewall, který dokáže řídit a zabezpečit síťový provoz blokováním IP adres nebo celých protokolů přes filtr kontrolního bodu. [11, 12]

Některé další síťové útoky a formy DOS:

- **Pasivní útoky** – tyto útoky nemají za cíl škodit, ale například odposlouchávat síťovou komunikaci nebo analyzovat její provoz pro budoucí útok
- **Ping smrti** – typ DOS, kde dochází z přehlcení nadměrným pingováním, takovéto ICMP pakety mají velikost větší, než maximální velikost 64KB
- **DNS nákaza** – podsunutí klamných informací o DNS serveru
- **Muž uprostřed** – útočník zachytí komunikaci mezi dvěma stranami a následně odposlouchá čí mění zprávy mezi nimi
- **Zahlcení SYN** – odeslání obrovského počtu žádostí o komunikaci

4.3 Bezpečnost dat

Data jsou prakticky to nejdůležitější, co na našich zařízeních můžeme najít, jelikož bez zálohy jsou zkrátka nenahraditelná a v některých případech enormního množství dat i nevyčíslitelná. Příčin ztráty dat může být více, mezi nejhlavnější patří poškození čí ztráta hardware, v případě softwaru nechtěné smazání, nevhodné uložení či napadnutí počítače zmíněným malwarem. Princip takového zálohování je velmi jednoduchý, jelikož dochází ke kopírovaní dat na dvě nebo více **fyzicky oddělených místech** (RAID pod tuto kategorii nespadá!). Může se jednat například o cloud, externí disk, DVD. V dnešní době však převládají cloudová úložiště (OneDrive, Google Drive), která s podporou moderních softwarů dokážou například plánovat pravidelné zálohy, šifrovat data či zasílat upozornění. Záloha je tedy první z možností k využití při ochraně dat. V informatice existují dva hlavní, ale celkem odlišné pojmy, které se dle anglického jazyka oba překládají jako bezpečnost, jedná se o Security a Safety. [13]

- **Security** – ochrana systému před okolím
- **Safety** – ochrana okolí před systémem

Tyto dva pilíře tvoří základy bezpečnosti. Nejdříve se pojďme podívat na takzvanou **CIA triádu**, která spadá pod pojem Security. CIA triáda tvoří základ pojmu bezpečnosti služby: „*Bezpečnostní služba je služba, která zajišťuje odpovídající úroveň zabezpečení systémů nebo datových přenosů. Bezpečnostní služby vycházejí z bezpečnostních mechanismů, které jsou vytvořeny na základě předem deklarovaných bezpečnostních pravidel.*“ [14]

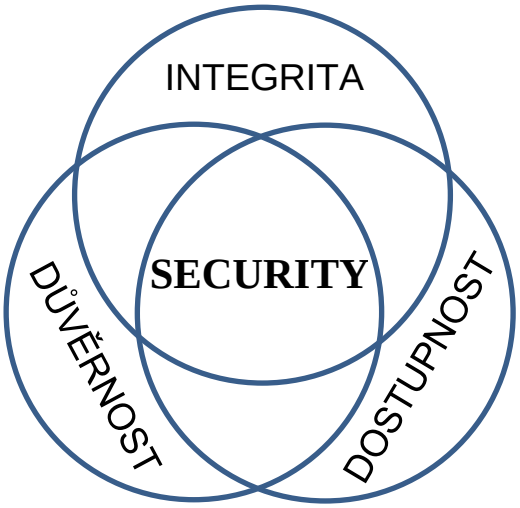
4.3.1 CIA triáda

Zjednodušeně se dá CIA triáda, tvořená důvěrností (Confidentality), integritou (Integrity) a dostupností (Availability) považovat za bezpečnostní model pro organizace, aby jejich data chránila před neoprávněným přístupem a jakým způsobem by je měla nejlépe chránit. Dalo by se to tak považovat za jakýsi benchmark, který měří bezpečnost informací. Tyto tři atributy chrání systém před odhalením, modifikací a zničením informací neboli takzvanou DAD triádou. Informace v této kapitole vychází ze zdrojů [15, 16, 17].

Důvěrnost značí přístup informací pouze oprávněným uživatelům. Většina organizací pracuje s několika klasifikačními stupni, kterým musí všichni zaměstnanci rozumět, aby věděli s jakými informacemi mohou zacházet a k jakým nemají přístup. Ty nejcitlivější informace mají nejvyšší klasifikační stupeň, často definován jako top-secret. Takové informace by měli být i nejlépe zabezpečeny, aby se nedostaly do nesprávných rukou. Šifrování je základem pro zajištění důvěrnosti dat (například hesel). Mezi další bezpečnostní systémy patří například biometrické ověření typu otisk prstu a dlaně nebo sken očí či obličeje. Organizace by v poslední řadě měla udržovat seznamy pro řízení přístupu a oprávnění k souborům.

Integrita definuje kvalitu dat (správnost a úplnost informací), jako problémové se tedy považují data zastaralá, neúplná či naprosto chybějící. Za narušení integrity je tedy považována nežádoucí či neočekávaná změna dat, která může být vyvolána omylem, úmyslně či selháním. Čím déle se na takovou problematiku přijde, tím horší bude mít dopad na systém. Díky integritě se také zajišťuje, že data nemohou být měněna někým, kdo nemá dostatečné oprávnění pro jejich změnu. Nejčastější implementace integrity je zajištěna zálohovacím či obnovovacím softwarem a minimalizací lidských chyb s využíváním řízení přístupu, verzí a datových logů.

Dostupnost znamená, že data by měla být neustále k dispozici a přístupna pro čtení všem autorizovaným uživatelům (zákazníci, organizace, zaměstnanci). Jinak řečeno systémy, sítě a aplikaci musí nepřetržitě fungovat tak jak mají a vhodnou rychlostí, aby přístup k informacím netrval příliš dlouho. Takový systém by měl tedy být schopný odolat výpadkům, haváriím, DOS útokům či dokonce i živelným pohromám. Vhodné je využívat redundantní opatření, RAID či monitorovací systémy při narušení primárního systému. Dále by systém a aplikace v něm měli zůstat aktualizované v nejnovější verzi (vhodné zálohy při problematice s nejnovější verzí).



Obrázek 4 CIA triáda

Zdroj: vlastní

Někteří odborníci se ale obávají, že CIA triáda je nedostatečná a požadují její rozšíření alespoň o jeden ze tří atributů. Prvním je **vlastnictví**, tento atribut se projevuje získáním kontroly neoprávněnou osobou a tím ztrátou vlastnictví. Druhým je **užitečnost**, kdy pokud dojde ke ztrátě šifrovacího klíče, tak se data stávají nepoužitelnými a jsou tak neužitečná. Třetím a poslední je **autenticita** kdy například v podvrhu elektronického podpisu dojde k jejímu narušení, nikoliv důvěrnosti, integrity nebo dostupnosti.

4.3.2 ACL

Takzvaný Access Control List neboli seznam řízení přístupu. Jedná se o jednu z možností, díky které můžeme zmírnit následky nějakého škodlivého programu (vir). Díky uživatelským oprávněním tak dokážeme eliminovat z části škody, pokud se program spustí s omezenými právy uživatele. Problém nastává v případě, kdy takový škodlivý program bude spuštěn s právy vyšší úrovně jako mohou být například administrátorská oprávnění, ve kterých administrátor může cokoliv mazat z disku, odesílat data, konfigurovat systém, přistupovat k registrům a systémovým prostředkům. Takové rozšířené oprávnění může napáchat velké škody a stává se hrozbou pro systém při získání vyšších práv. Z toho důvodu je dobré uživatelům přiřazovat často nejnižší uživatelská práva. Pro usnadnění práce je vhodné využívat skupiny a těm přímo definovat oprávnění. Ve Windows máme celkem dva typy účtů [13, 20]:

- **Systémové** – tyto účty jsou předem definované v operačním systému výrobcem a implicitně navazují na zabezpečení operačního a souborového systému
    - **Spravovatelné** – u takových účtů můžeme měnit hodnoty jako heslo či členství a dají se nalézt ve správci uživatelů (Administrator, User)
    - **Nespravovatelné** – využívají se pro vnitřní účely OS a jejich členství určuje sám operační sytém, nemůžeme měnit hodnoty (Everyone, System)
- **Uživatelské** – účty které vytvoří sám uživatel, používají se k detailnější konfiguraci a využívají se pro přístup k prostředkům operačního a souborového systému

Tři základní pravidla vytváření účtů:

1. Každý uživatel musí být alespoň v jedné skupině
2. Nedelegujeme uživatele zároveň do skupiny Administrators a Users
3. Pojmenováváme uživatele i skupiny intuitivně

O přidělování práv a řízení přístupu ve Windows, se stará Access Control List (ACL). Jedná se o seznam oprávnění, které jsou připojeny a tudíž se vážou na nějaký objekt. Takový seznam obsahuje několik položek (ACE). V doslovném překladu se jedná o seznam pro řízení přístupu, který určuje kdo nebo co má povolení a co všechno může provádět. Existují určité předem definované oprávnění souborového systému.

Tyto tři oprávnění jsou **Úplné řízení**, kde administrátor může provádět vše, včetně změny vlastnictví a oprávnění. Druhým je **Měnit**, což je již nižší úroveň oprávnění, kde uživatel může mazat a provádět změny. Posledním je **Číst a spouštět**, jehož funkcionalita je poměrně daná názvem. ACL dokáže využít možnost dědičnosti, kde práva nadřazeného objektu automaticky propadají na podřazené objekty, samozřejmě se tato možnost dá zakázat pokud ji nechceme využívat.

Problém může nastat u skupin Everyone a Creator Owner, při Everyone dostává automaticky každý uživatel (i ten nevítaný) nějaká základní oprávnění, proto to je vhodné tuto skupinu odstranit. Creator Owner může nastavit problém v podobě vlastnictví, pokud například uživatel vytvoří soubor, dostane automaticky aplikovaná práva vyšší úrovně (často úplné řízení) na tento soubor.

Stejně jako u vytváření účtů, tak i u **ACL existují celkem čtyři hlavní pravidla**:

1. Oprávnění přidělovat skupinám, uživatelům pouze v nezbytných případech
2. Není-li oprávnění definováno, uživatel nemá automaticky přístup
3. Zákaz má automaticky větší prioritu než povolení
4. Explicitní oprávnění má automaticky větší prioritu než zděděné

4.4 Slabiny systému

Jak již bylo zmíněno, systém je stejně slabý jako jeho nejslabší článek. Z toho důvodu musí být systém dobře záplatovaný, aktualizovaný a nakonfigurovaný na každé jeho úrovni. Z toho důvodu vyžaduje práci administrátora, který se o systém bude starat. Nejčastěji špatně provedená konfigurace se nachází v oblasti uživatelské správy, proto by uživatelé měli být poučeni o používání systému, jelikož největší hrozbou mohou být oni samotní. Často se například stává, že uživatel svůj počítač neuzamkne, a tím ho vystavuje nebezpečí. Tím je myšleno buď, že uživatel nepoužívá žádné heslo pro přístup k jeho uživatelskému účtu, nebo ponechává odemčený počítač v jeho nepřítomnosti. Mezi další ze slabin patří slabé heslo. Pokud se potenciálnímu útočníkovi podaří získat heslo dostane automaticky vstup do systému a může na něm napáchat velkou škodu, jelikož bude pracovat s identitou uživatele včetně jeho oprávnění a bude mít automaticky přístup do systému. [7]

Dle moderních norem by každé správné a bezpečné heslo mělo [18]:

- **Být originální** – v žádném případě by neměli být všude stejná hesla
- **Těžce uhodnutelné** – neměli bychom volit hesla zahrnující datum narození či jméno buď naše nebo někoho ze členů rodiny
- **Dlouhé** – určitě ne menší než 12 znaků, ale nemělo by být ani příliš dlouhé (24 +)
- **Využívat celou znakovou sadu** – minimálně jedno mále písmeno, jedno velké písmeno, jeden speciální znak a jedno číslo
- **Nastavit bezpečností otázky** – pro případ zapomenutí hesla
- **Používat dvoufázové ověření** – dodatek v případě pokud se i někomu podaří získat heslo, bude nám na telefon nebo email zaslán kód pro další ověření
- **Být uloženo ve správci hesel** – pokud nedůvěřujeme správci hesel a chceme zapsat heslo na papír, tak určitě nikdy neponecháváme papír s heslem v pracovním prostředí, nejlépe uschováme někde v domácnosti

Nejen že by uživatel měl dodržovat zásady správného hesla, ale také hlavní zásady bezpečnosti, jedná se o sbírku deseti bezpečnostních pravidel, které představila samotná firma Microsoft při akci Štít bezpečí. Ačkoliv se jedná o poněkud starší iniciativu od Microsoftu, tak tato je problematika je stále aktuální. Má poukázat, jak by měl uživatel provádět samosprávu počítače. Mezi deset hlavních pravidel pro domácí uživatele platí [19]:

1. Pravidelné aktualizace operačního systému
2. Používat antivirus a pravidelně ho aktualizovat
3. Mít zapnutý firewall
4. Nesnižovat bezpečnostní nastavení ve Windows
5. Navštěvovat pouze důvěryhodné a zabezpečené stránky protokolem https
6. Neinstalovat neověřené a nedůvěryhodné aplikace
7. Než klikněte „Pokračovat“ nebo „Souhlasím“ vše si nejdříve přečtěte
8. Neodpovídat na nevyžádané emaily
9. Neotevírejte přílohy takových emailů
10. Když si nevíte rady, kontaktujte odborníka

5 Forenzní analýza

Dnešní doba je prakticky závislá na digitálních zařízeních, kterým se nelze vyhnout. Takové zařízení jsou cenově dostupné, mají různé formy (počítače, telefony, chytré hodinky, smarthome, …) a hlavně jsou důležitou součástí našich každodenních životů. Takováto zařízení se mohou stát terčem nefyzického útoku, kde útok je brán jako zločin a spadá pod odvětví kybernetické kriminality, zkráceně kyberkriminality.

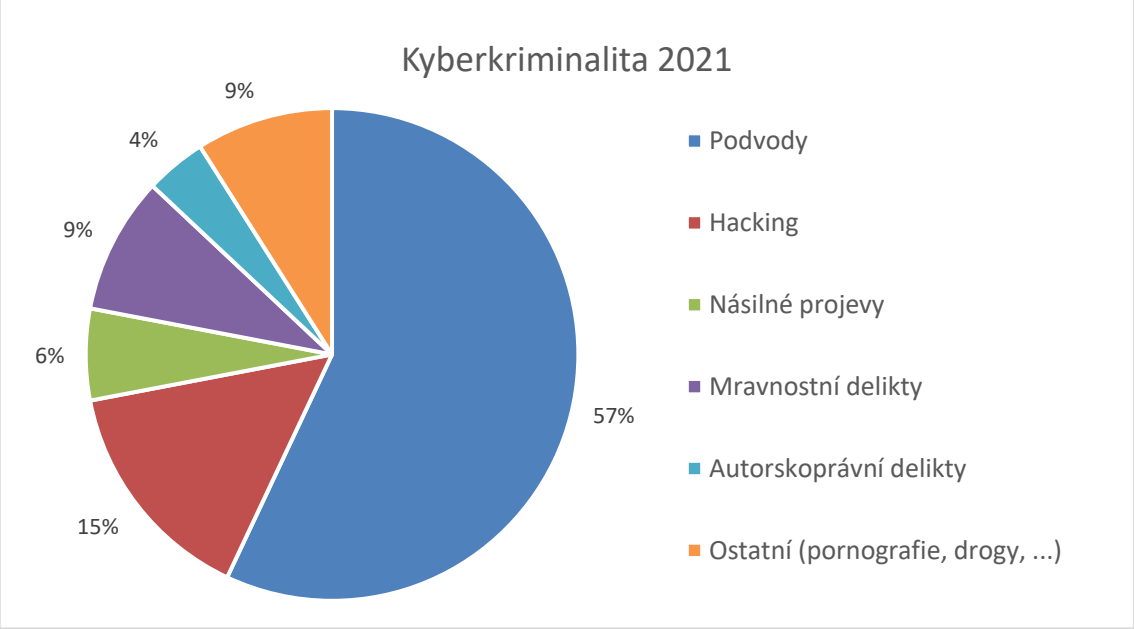
5.1 Kyberkriminalita

Kyberkriminalita je neoprávněné chování uživatele vedené jako trestný čin, který je vykonáván prostřednictvím internetu či informačních a komunikačních technologií. Takovýto trestný čin se odehrává v rámci kyberprostoru, což je označení pro libovolné virtuální prostředí počítačů, mezi které se může například zahrnovat i internet. Do součástí kyberkriminality také zapadá [21, 22, 25]:

- **Kyberšpionáž (Cyber epsionage)** – jedná se o formu kybernetického útoku, jejíž cílem je krádež tajných a citlivých dat za smyslem získání výhody nad velkým subjektem (vláda, konkurenční společnost) či zisku, využívá tedy špióny pro špehování, získání a shromažďování informací o plánech nebo aktivitách.
- **Kybernetická válka (Cyber warfare)** – jedná se o sérii útoku zaměřenou na určitou zemi s cílem vyvoláním zmatků ve vládě a civilní infrastruktuře, může tedy vést až ke poškozením systémů či ztrátám na životech. Mezi kybernetickou válku můžou zapadat DoS útoky (odmítnutí služby), útoky na síť elektřiny (narušení komunikace/infrastruktury), propaganda (odhalení pravd, šíření lží -> ovlivnění myšlenek lidí) či ekonomické narušení (burzy, platební brány, banky)

Dle Policie ČR je definována kybernetická kriminalita jako:
„*Trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je páchána trestná činnost za výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchání.*“
(Policie ČR)

Na základě zdrojů ze stránek Policie ČR. Kyberkriminalita nadále nabývá na své velikost a od roku 2011 ze zaznamenaných 1 500 trestných činů v kyberprostoru vzrostlo toto číslo na počet případů blíží se k 10 000 za rok 2021 a je tak velmi pravděpodobné, že toto číslo nadále poroste. Více jak polovina trestných činů páchaných v kyberprostoru jsou podvody (podvodné weby, inzeráty, emaily, identity …). Další součásti struktury kyberkriminality mohou být například hackování, autorskoprávní delikty či násilné projevy.

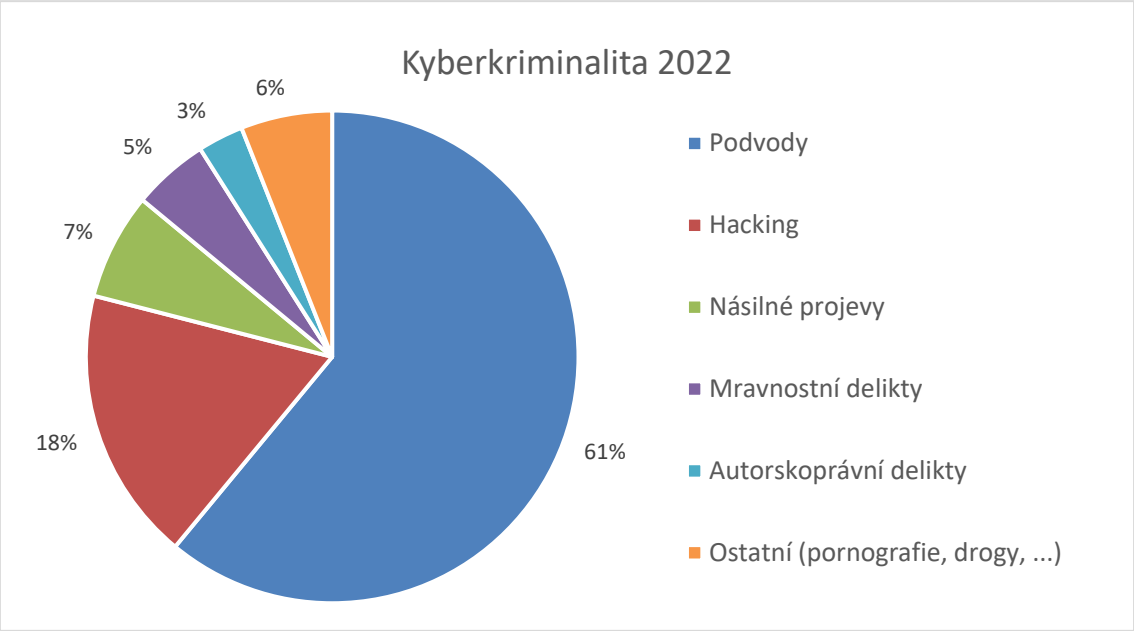


Graf 1 Kyberkriminalita 2021. Zdroj: vlastní

5.1.1 Kyberkriminalita 2022

Rok 2022 byl zatím s nejvyšším číslem v počtu trestných činů spáchaných v kyberprostoru. Toto číslo se až téměř neuvěřitelně zdvojnásobilo a pohybuje se kolem 18 500 případů (až 10 % z celkové kriminality, vzrůst o 95 %). Přesně z toho důvodu Policie ČR ve spolupráci s ČSOB propaguje reklamu, která upozorňuje na zvýšené množství případů pomocí dvojice Klikač a Volač. Velký vliv na množství kyberkriminality má také probíhající válka na Ukrajině. Kvůli této válce vznikl poměrně rozšířený malware s názvem Azov Ransomware, který cíleně maže data, aby upozornil na válku na Ukrajině. Odborníci následně zjistili, že přepisuje místní data v 666bajtových úsecích, což je nejen efektivní, ale i velmi rychlé a data již nelze následně obnovit. Rok 2022 také postihl velký únik dat s kterým se setkaly 2/3 firem. Zejména únik telefonních čísel z WhatsAppu na darknet. Na darknetu se tedy obchoduje s 360 miliony uniklých

telefonních čísel (1,3 milionu českých). Nejčastější byly opět podvody (60 % z celkové kyberkriminality), velký vzrůst zaznamenal také hacking (+50 %). [23, 24]



Graf 2 Kyberkriminalita 2022. Zdroj: vlastní

Většina trestných činů tedy útočí přímo na ohrožení CIA triády (důvěrnost, integrita a dostupnost) dat či systémů. Z toho důvodu je třeba se proti této kyberkriminalitě bránit, aby nedocházelo k jejímu ještě většímu rozšiřování a poškozování osob či zařízení. Právě z tohoto důvodu byla vytvořena metoda, která takové prostředí dat bude umět zkoumat – forenzní analýza.

5.2 Úvod do forenzní analýzy

Forenzní analýza se zabývá zjištěním důkazů v oblasti informačních technologií, jejích interpretací a prezentací. Pokud není uvedeno jinak, informace v této kapitole vychází z následujících zdrojů: [27, 28, 8]. Je to pojem spjatý určitou formou s primárním zkoumáním digitálních dat úložišť. Digitální data jsou vyjádřena v číslicové soustavě, často binární (nuly a jedničky). Jako zdroje takových dat můžeme považovat disky v osobních počítačích, telefonech, USB flashdisky, internet, auta, domy, internet věcí, dokonce klidně i chytrý toustovač. Jedná se o úložiště, která uchovávají i cenná data rozvíjející se den co den. Zejména taková důležitá data je potřeba chránit před různými útoky zvenčí, či vnitřním selháním. Při forenzní analýze pracujeme s těmito hlavními typy digitálních dat:

- **Volatilní** – existují pouze po dobu chodu paměti, při vypnutí data zmizí
- **Aktivní** – viditelné a uživatelsky dostupné, obsah souboru, při vypnutí nezmizí
- **Metadata** – informace o datech (formát souboru, čas vytvoření, autor, …)
- **Systémové logy** – informace o chodu zařízení, pro kontrolu činností
- **Dočasné soubory** – pomocný prostor pro mezivýsledky, nutno mazat
- **Reziduální** – fragmenty a původní data (smazané soubory, části souborů či paměti)

Forenzní analýza lze být rozdělena do několika hlavních oblastí zkoumání, jelikož dokáže zkoumat nejenom pouze digitální data úložišť. Forenzní analýza má tyto hlavní druhy:

- Forenzní analýza pro zachycení disku a dat
- Forenzní analýza pro souborové systémy
- Forenzní analýza pro analýzu registrů
- Forenzní analýza pro dočasné paměti (RAM)
- Forenzní analýza pro síťovou analýzu (včetně firewallu)
- Forenzní analýza pro mobilní zařízení (zařízení založené na GPS)

Programy, jež zkoumají události, viníky a důkazy se nazývají TOOLS forenzní analýzy (nástroje) a jsou schopny zkoumání digitálních zařízení či pouze dat. Pomocí těchto programů se snažíme najít v počítači určité důkazy, které zavinily problémy pomocí metod pro sběr, identifikaci, analýzu, zhodnocení a interpretaci s hlavním cílem usnadnit rekonstrukci dat nebo odhalení neautorizovaných akcí. Pomocí těchto TOOLS chceme tedy zjistit odpověď na otázky:

- **CO** se stalo – jakým způsobem problém ovlivnil fungování systému nebo zařízení
- **KDY** se to stalo – v jakém čase došlo k problému
- **JAK** se to stalo – jakým způsobem došlo k problému
- **KOHO** se to týká – jaké uživatele / lidi / odvětví zahrnuje tento problém
- **KDO** je viníkem – kdo či co zapříčinilo problém

Forenzní analýza má několik hlavních bodů, které je třeba si více přiblížit do hloubky. Před zahájením forenzní analýzy je třeba zachovat sterilitu dat – data, která nesmí být pozměněná ani z části ztracená. V praxi se to provádí takovým způsobem, že u dat dojde k duplikaci a vytvoření kopie, na které je tato forenzní analýza prováděna. Takové kopii se říká bitová kopie, kde probíhá kopírování bit po bitu do jiného souboru s kterým se poté pracuje. Nejedná se ale pouze o jedinou věc, kterou je třeba zajistit. Data jako taková se mohou měnit v průběhu času a proto je vhodné využít speciální funkce hash neboli otisk bitové kopie. Tato funkce je skvělá v tom, že dokáže ověřit totožnost zkoumaných dat a zda nedošlo k jejich pozměnění (máme data kterým uděláme otisk, následně dojde k odložení soudu, několik měsíců počkáme a uděláme opět otisk, pokud jsou otisky stejné, jsou data nepozměněná, pokud ne, tak došlo ke změně).

Aby nedocházelo k takovému pozměnění dat, je třeba vytvořit dvě bitové kopie. První je primární bitová kopie, kterou je vhodné bezpečně uložit a již s ní dále nepracovat, její využití přijde vhod až u soudu. Druhá je pracovní bitová kopie, s kterou již pracujeme a snažíme se nalézt informace a potvrdit hypotézy, k tomu ale musíme vědět, co vlastně hledáme a kde to máme hledat, případně vědět nějaké doplňující informace, které nám umožní zmenšit prostor k prozkoumání. V případě že není možné provést duplikaci, je vhodné nastavit zařízení pouze pro čtení.

Hlavní kroky forenzní analýzy:

1) **Sběr dat** – duplikace a extrahování dat na jiné médium
2) **Identifikace a analýza dat** – identifikace relevantních médií, kde by se mohli nacházet důležité informace a zjištění důkazů, které mohly zavinit problém
3) **Interpretace dat** – vhodným způsobem prezentovat vyšším složkám managementu, vyložit srozumitelným způsobem odpověď na všechny podstatné otázky a učinit závěr
4) **Dokumentace** – zaznamenat vše co se provádí při problému od začátku do konce

Zkoumaný počítač může působit v roli oběti, ale také i jako pachatel, který slouží jako nástroj pro provedení zločinu – viry, červy, odcizení dat, nechráněné zařízení… Z toho důvodu potřebujeme využitím forenzní analýzy zjistil pachatele trestného činu. Některé důkazy nelze ale najít pouze na zařízení, ale také v jejich blízkosti, jako jsou například napsaná hesla pod stolem, vstupy monitoru či klávesnice nebo také prvky sítě jako jsou porty routerů, servery a firewally. Některé případy tedy mohou končit i soudním procesem a výslechy lidí, kteří jsou s případem nějakým způsobem spjati.

U takového soudního sporu může být forenzní analýza využita tedy jako zásadní podklad pro závažná rozhodnutí. Při využití forenzní analýzy je třeba využít aspektu neutrality, tím je myšleno, že se předkládají pouze fakta a jakým způsobem bylo výsledů dosaženo (co bylo zjištěno) bez osobního hodnocení (například bez obviňování). Dále je třeba, aby závěry byly nezpochybnitelné a postup bylo možné zopakovat a ověřit tak jeho správnost, aby nedošlo k pozměnění dat, či jinému předmětu analýzy. Takové důkazy musí také vyhovovat právním předpisům, aby mohli být představeny před soud a dokázaly vyprávět celý příběh. Při vysvětlování by měli být důkazy spolehlivé, tedy nic, co by zpochybnilo jejich pravdivost uvěřitelnost.

Co je dobré interpretovat?

- Jak bylo zařízení infikováno? (aby se to nestalo znovu a zda za tím někdo nestojí)
- Jaké soubory se nacházely na zařízení? (výskyt konkrétní souboru zadaný PČR)
- Kdo používal dané zařízení? (jaké osoby v jaké době)
- Kdo se pohyboval kolem daného zařízení? (kdo mohl být také zúčastněný)
- Jaké aplikace byly instalovány a spouštěny?
- Byla připojena nějaká externí zařízení? (zejména pro šíření viru)

Při soudním řízení se soud může přiklánět i k sekundárním digitálním datům – obraz disku a paměti, informace zahrnující síťový provoz a komunikaci zařízení či informace ohledně logů služeb.

Jelikož je každý případ unikátní, tak přímo neexistuje nějaký univerzální postup, kterým by se měl forenzní analytik řídit. Vždy první částí je ale úvaha se zadavatelem, v které probíhá konzultace jaké informace se mají najít. Následně zadavatele zadá časový úsek pro nalezení takových informací. Analytik posléze musí zjistit, kde takové data jsou a kde by se ještě mohla nacházet. Obecný postup pro forenzního analytika je takový, že využije vhodné nástroje pro extrakci dat a jejich následné zkoumání, vyhodnocení a nalezení odpovědí. Z toho důvodu je také dobré znát formát dat, konkrétní nástroje forenzní analýzy a fungování zkoumaného systému nebo zařízení. Vhodnou pomůckou může být také data carving, který vyhledává v bitech například všechny spustitelné soubory, obrázky či textové řetězce. Poslední fází je prezentace výsledků, kde se musí dbát na komunikační bariéru s neodborníky IT. Z toho důvodu je vhodné vysvětlovat takovým způsobem, aby tomu každý rozuměl, nejčastěji zmiňujeme pouze princip, postup a dosažené výsledky.

5.3 Shrnutí zásad forenzní analýzy

- Zapojení vhodného personálu včetně právníků
- Vše zaznamenávat, zejména data a čas
- Pozor na různost systémových hodiny a reálného času
- Minimalizovat změny dat – omezit přístup i aktualizace
- Nejdříve sběr, poté analýza
- Nejdříve volatilní data (nejvýše), poté nevolatilní
    - Registry a Cache
    - Routovací a ARP tabulky, paměť, tabulka procesů a statistiky jádra
    - Dočasné souborové systémy
    - Disk
    - Fyzická konfigurace a topologie sítě
    - Archivní média
- Pokud je třeba vyšetřit více zařízení, vhodné využít paralelní práci v týmu

Čemu se vyhnout

- Nevypínat zařízení, dokud neprovedeme kompletní sběr evidence
- Nevěřit programům na zkoumaném zařízením

- Nespouštět programy, které mohou změnit přístup na soubory
- Pozor na odpojení od sítě, které může smazat určité důkazy

Při provedení forenzní analýzy je třeba brát také ohled směrem k osobním údajům, tím je myšleno respektování pravidel ochrany osobních údajů a řídit se pokyny naší firmy (případně zadavatele). Takové informace spolu s důkazy by tedy neměli být nikomu dostupné, aby nedošlo k jejich neplánovanému rozšíření. Stejně tak se prosazuje právo, že forenzní analytik by neměl zasahovat do soukromí lidí bez silného odůvodnění.

Stejně tak by forenzní analytik měl dokumentovat vlastní práci. Tím je myšleno kdy, kde a kým byly důkazy objeveny, zpracovány a kdo je měl v držení v jaké době, pokud se pracuje zejména v týmu. Jelikož se může stát, že i člen takového týmu může nakonec být hlavní škůdce.

Nástroje ke shromažďování důkazů a forenzní práci

- Programy pro zkoumání procesů
- Programy pro zkoumání stavu systému
- Programy pro vytváření bitových kopií
- Programy pro kontrolní součty a podpisy
- Programy pro generování obrazů
- Skripty pro automatické shromažďování důkazů

Takovéto části mohou být samozřejmě propojeny i do jednoho programu, který dokáže více zmíněných funkcí, stejně tak je nutné dosvědčit spolehlivost a pravost používaných nástrojů u soudního případu. [26]

5.4 Nejpoužívanější nástroje Forenzní analýzy

Jednoduché shrnutí pár nejpoužívanějších nástrojů pro forenzní analýzu. Téměř všechny zmíněné programy jsou volně dostupné ke stažení (výjimka placený ProDiscover Forensics) a jejich zaměření je směrováno na platformu Windows 10. Jednotlivé nástroje se tedy mohou například lišit dle zaměření na operační systém, různosti funkcí nebo peněžité částky. Na tyto nejpoužívanější nástroje odkazuje velká většina odborníků zabývající se forenzní analýzou na vysoké úrovni. S výběrem zmíněných nástrojů pomohli převážně vědecké články forenzních expertů. [29, 30, 31]

Na fiktivním forenzním případu bude demonstrováno praktické využití nástrojů FTK Imager, Autopsy a WriteProtect, které slouží pro zajištění digitálních stop pro použití v rámci forenzní analýzy.

Následující volně dostupné nástroje mají základ funkcionality velmi podobný, například pokud bychom porovnávali FTK a Autopsy, jedny z nejvíce používaných nástrojů pro forenzní analýzu systému Windows, výsledkem by byl pouze rozdíl, že FTK umožňuje vytvářet obrazy, ale Autopsy ne. Taková funkcionalita se dá ve většině případů rozšířit placenou verzí, která plně doplňuje funkcionalitu daného nástroje. Základní funkce nástrojů jsou vyhledávání klíčových slov, analýza souborového systému, hashování obrazu včetně ověřování či tvorba reportů. U těchto dvou nejznámějších nástrojů pro forenzní analýzu se využívá Autopsy zejména pro začátečníky a firmy s malým rozpočtem. FTK je více kompletní, cenově dražší a je soudně akceptovaný nástroj pro vyšetřování digitálních platforem.

5.4.1 Autopsy

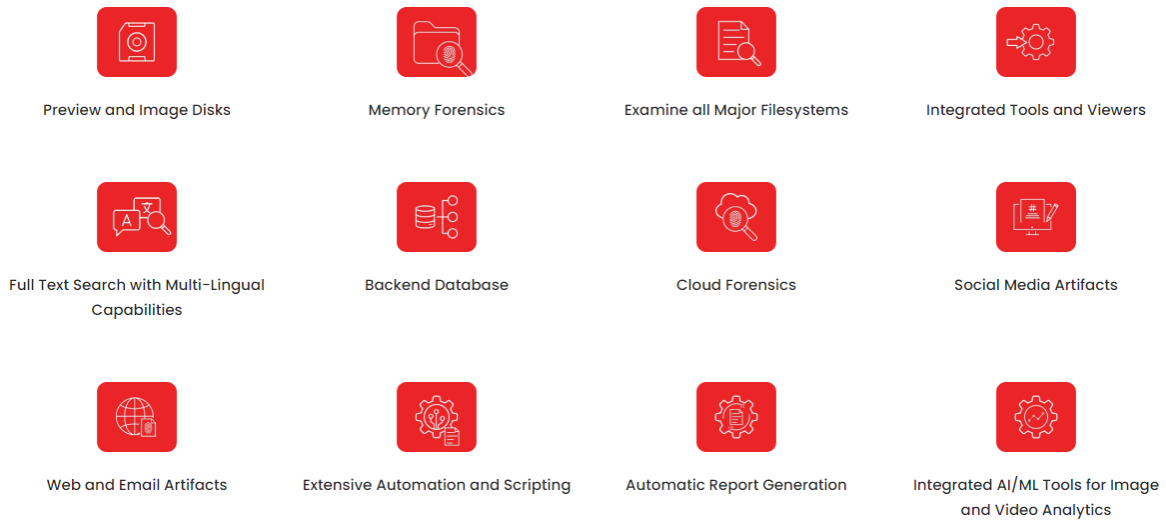
Jeden z nejvíce používaných a nejkomplexnějších nástrojů pro forenzní analýzu vůbec. Jedná se o přední zcela zdarma open-source software, který má využití pro kybernetiku. Hlavními přednostmi jsou obrovské množství funkcí, které lze být ještě rozšířeno placenou, ale cenově dostupnou verzí. Takové funkce jsou i rozšiřitelné a uživatel si tak může vytvořit nové funkce pomocí zásuvných modulů. Základní jádro funkcionality ale tvoří trojice pro skenování, průzkum a následné zobrazení výsledků pomocí reportů. Dále dokáže analyzovat souborové systémy, hashovat či extrahovat soubory nebo obnovit smazané soubory. Další výhody tohoto programu jsou rychlost, spolehlivost, přehledné uživatelské rozhraní či snadnost používání. Společnost *Basis Technology* krom poskytování tohoto software, nabízí i placené školení pro používání produktu. [32]

5.4.2 FTK Imager

FTK je toolkit od značky AccessData, který se skládá z několika nástrojů pro forenzní analýzu dle využití. Z důvodu že Autopsy je navržen spíše pro zkoumání, tak bohužel nemá žádnou funkcionalitu, díky které by dokázal vytvořit obraz disku. Z tohoto důvodu je vhodné využít nejprve nástroj FTK Imager pro vytvoření například obrazu disku, z kterého se následně bude zkoumat pomocí programu Autopsy. FTK Imager dokáže vytvářet obrazy disků, CD, DVD, flash disků, složek i souborů pomocí perfektní kopie, která je neroznatelná od originálu. I tento program dokáže vytvářet hash pro prokázání neporušené integrity pomocí bitových kopií. [33]

5.4.3 ProDiscover Forensics

Jedná se o velmi komplexní software pro forenzní analýzu, který dokáže zachytit všechny klíčové důkazy. Jeho hlavní výhodou pokud pomineme vysokou cenu, je schopnost zvládnout všechny aspekty hloubkové forenzní analýzy až do posledního detailu. Jeho funkcionalita je velmi topologicky široká a kromě základních funkcí má například integrovanou umělou inteligenci, umožňuje automatizaci včetně skriptování, či práci s libovolným jazykem. Nutno ale podotknout, že taková funkcionalita lze být rozšířena ještě více PRO verzí, která dokáže například upozornit a reagovat ihned při narušení systému. [34] Zde obrázek pro ilustraci základních funkcí:



Obrázek 5 Funkcionalita ProDiscover. [34]

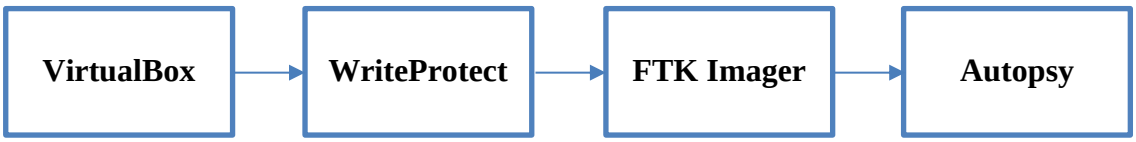
Další nejpoužívanější programy:

- Pro Linux – CAINE
- Pro síťovou analýzu – Wireshark
- Pro mobilní zařízení – Cellebrite UFED
- Pro paměti – Volatility / Magnet RAM Capture
- Pro registry – Registry recon

6 Video tutoriály

Veškeré videomateriály probíhaly pořizováním skrze program OBS (https://obsproject.com) a jejich úprava proběhla skrze Windows editor videí + Clipchamp video editor (https://clipchamp.com/en/)

Za účelem demonstrace nástrojů pro forenzní analýzu byly vytvoření video tutoriály, pokrývající základní operace forenzní analýzy – sběr obrazu disku a jeho zkoumání.



Obrázek 6 Topologie videí. Zdroj: vlastní

6.1 Nastavení virtuálního prostředí a instalace Windows

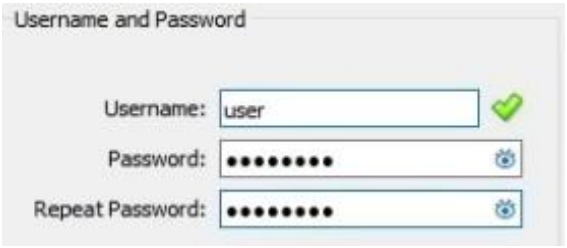
První fáze se zabývá vytvořením virtuálního prostředí pro provádění forenzní analýzy, zahrnuje tedy stažení a instalaci Oracle VM VirtualBox, přípravu Windows ISO, tvorbu a nastavení virtuálního počítače včetně následné instalace systému. Každý forenzní analytik by měl pracovat s virtuálním zařízením, aby nedošlo k ohrožení ztráty dat.

1. **Stažení instalačního souboru pro Oracle VM VirtualBox a jeho instalace**
   - https://www.virtualbox.org/wiki/Downloads
2. **Stažení nástroje Media Creation Tool a jeho následná instalace**
   - https://www.microsoft.com/cs-cz/software-download/windows10
3. **Tvorba ISO souboru Windows 10 skrz Media Creation Tool**
   - V první fázi souhlas s podmínkami
   - Následně zvolení „Vytvořit instalační médium“
   - Výběr edice Windows 10 a volba architektury (32/64 bitů) četně jazyka
   - Jako médium vybereme Soubor ISO
   - Vybereme místo v počítači pro uložení ISO souboru

4. **Vytvoření nového virtuálního počítače**
    - V prostředí Oracle VM VirtualBox klikneme na: **Vytvořit nový stroj**
    - Dle obrázku 8 nastavit **Název** virtuálního stroje, **složku** pro uložení počítače a přiřazení **Windows ISO**, který automaticky nastaví **Typ** a **Verzi** Windows

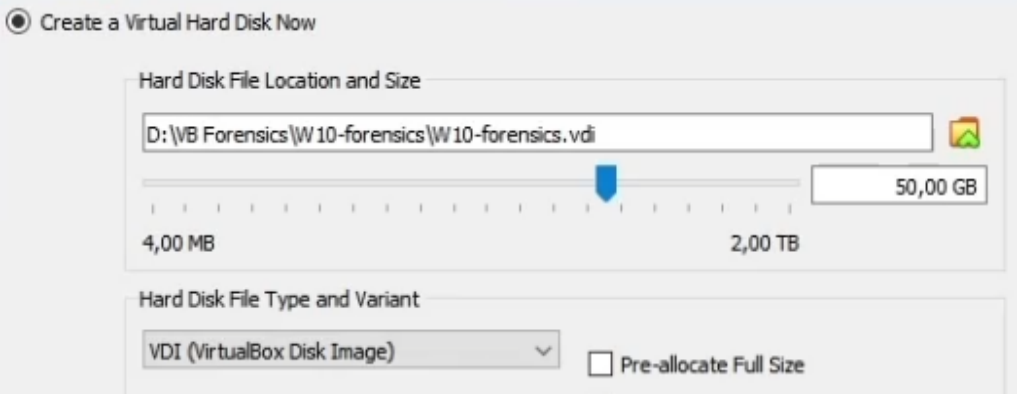
Obrázek 7 Tvorba stroje. Zdroj: vlastní

- Nová verze virtualboxu již umožňuje **vytvoření uživatele včetně hesla** přímo při vytváření virtuálního počítače, dle obrázku 8 a případně upravit název pro hostname



Obrázek 8 Tvorba uživatele. Zdroj: vlastní

- **Přidělení operační paměti a počet jader CPU** (čím více, tím lépe; nutnost být v zelených hodnotách; minimálně 2 GB RAM, doporučeno alespoň 4 GB RAM) a vytvoření dynamicky alokovaného **virtuálního pevného disku**, zvolí se tedy velikost a umístění (velikost se odvíjí od operačního systému a další práce na něm; v případě Windows 10 dle systémových požadavků minimálně 20 GB)

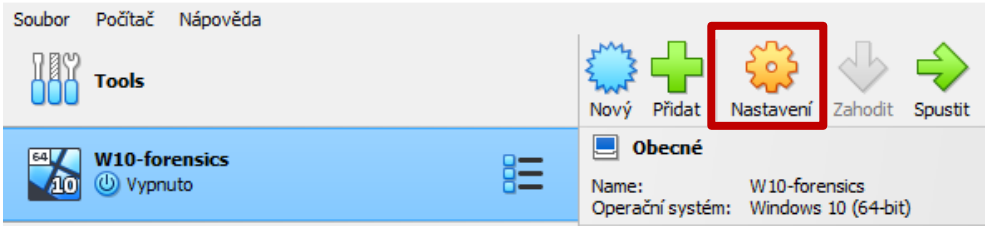


Obrázek 9 Tvorba disku. Zdroj: vlastní

- Kliknutí na tlačítko „Dokončit“
- Ihned po kliknutí na tlačítko „Dokončit“ se zapne virtuální počítač, nejdříve je třeba ale virtuální počítač nastavit, proto je virtuální počítač třeba vypnout pomocí křížku „Vypnout počítač“

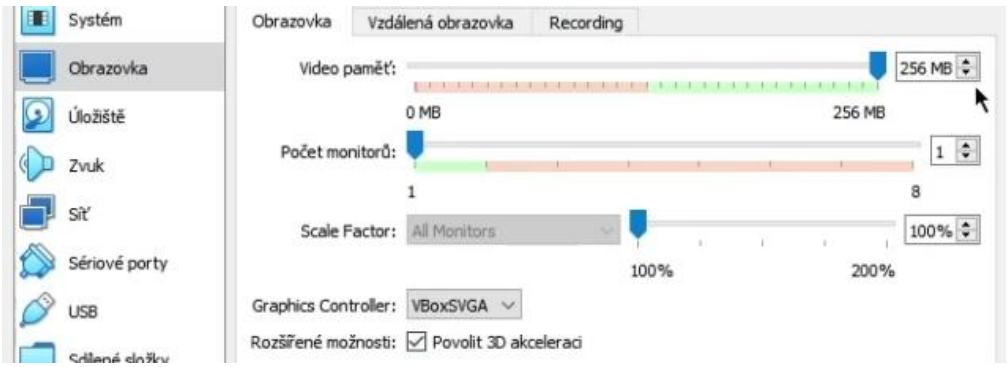
5. Nastavení virtuálního počítače

- Volba nově vytvořeného virtuálního PC **a kliknutí na „nastavení“**



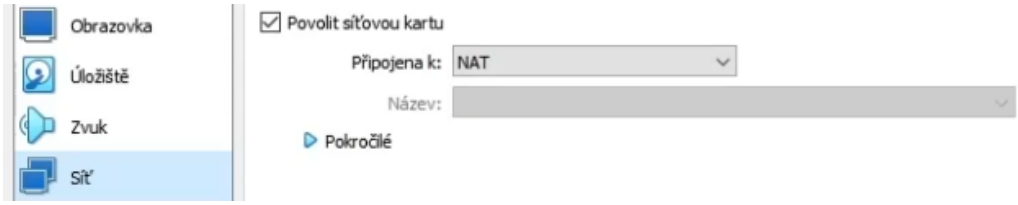
Obrázek 10 Nastavení virtuálního PC. Zdroj: vlastní

- **V menu „Obrazovka“** zakřížkovat „Povolit 3D akceleraci“ a přidělit nejvyšší možnou video paměť pro vyšší výkon



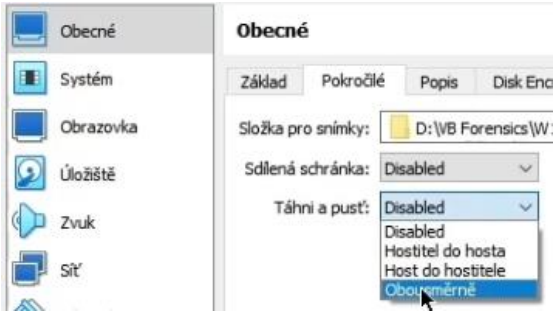
Obrázek 11 Nastavení virtuálního PC – část 1. Zdroj: vlastní

- **V menu „Síť“** zakřížkovat „Povolit síťovou kartu“ a nastavit připojení na NAT z důvodu nejvyšší bezpečnosti



Obrázek 12 Nastavení virtuálního PC – část 2. Zdroj: vlastní

- **Volitelné:** V menu „Obecné“ -> „Pokročilé“ nastavit „Táhni a pusť“ obousměrně pro lepší práci při přesouvání souborů mezi virtuálním a reálným systémem



Obrázek 13 Nastavení virtuálního PC – část 3. Zdroj: vlastní

6. Spuštění virtuálního stroje a instalace systému

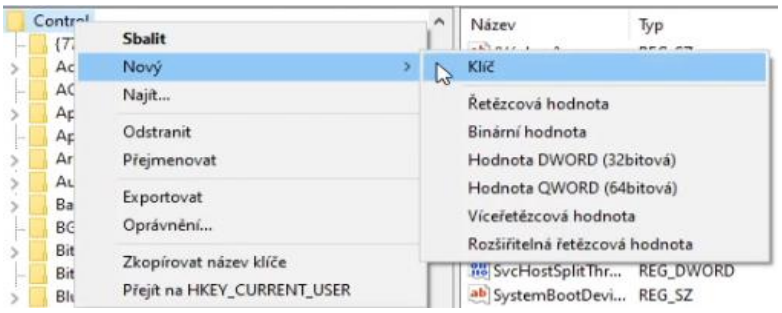
- Zvolení nově vytvořeného virtuálního počítače a **kliknutí na „spustit“**
- Vyčkání na instalaci systému v řádu desítek minut

Obrázek 14 Spuštění virtuálního PC. Zdroj: vlastní

6.2 WriteProtect

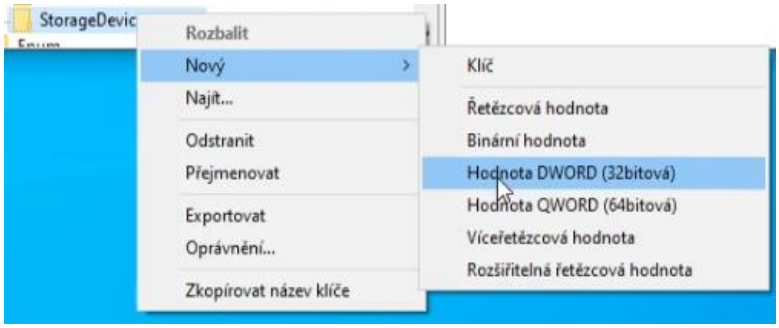
Jednoduchá druhá část pro přípravu na práci s FTK Imagerem. WriteProtect umožňuje chránit jakékoliv USB zařízení před změnou (přidání, odebrání i jakékoli úpravy dat), díky tomu, že nastaví USB zařízení po připojení na read-only. Tato část není nutná, zato je velmi užitečná v rámci další práce s programem FTK Imager.

1. Zadání příkazu **„regedit“** do Windows vyhledávání
2. Přesunutí do části **CONTROL** skrze:
   HKEY_LOCAL_MACHINE -> SYSTEM -> CurrentControlSet -> Control
3. Kliknutí pravým tlačítkem na Control a následně **vytvoření nového klíče** s názvem **StorageDevicePolicies** podle obrázku 15



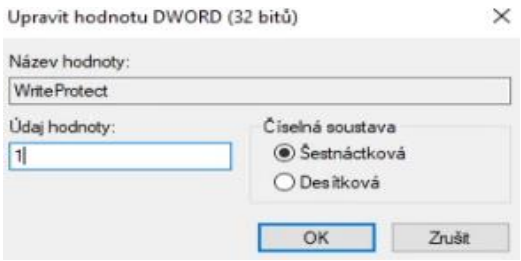
Obrázek 15 Tvorba klíče. Zdroj: vlastní

4. Kliknutí pravým tlačítkem na **StorageDevicePolicies** a **vytvoření nové 32bitové hodnoty (DWORD)** s názvem **WriteProtect** dle obrázku 16



Obrázek 16 Tvorba DWORD-32bit. Zdroj: vlastní

5. **Nastavení hodnotu WriteProtect na 1** (zapnuto) a uložení, WriteProtect tedy funguje od momentu připojení USB zařízení



Obrázek 17 WriteProtect. Zdroj: vlastní

Pozn. V případě potřeby vypnutí WriteProtectu, je třeba přepsat hodnotu na výchozí číslo 0 – vypnuto, pokud tak nebude učiněno, WriteProtect bude automaticky nastavovat každé připojené USB diskové zařízení na read-only; netestovánu u rozhraní SATA ani M.2, u takových rozhraní by WriteProtect neměl fungovat

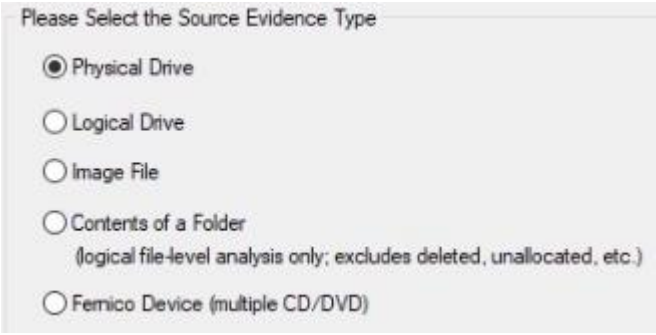
6.3 Tvorba obrazu disku přes FTK Imager

Třetí fáze se zabývá programem FTK Imager a jeho využitím pro vytvoření obrazu disku. Pro tuto část je třeba mít vytvořený a zapnutý WriteBlocker na zdrojovém USB zařízení, z kterého se bude obraz disku vytvářet (viz. předchozí část). Takovýto obraz disku je nutnou částí pro další zkoumání a budoucí analýzu bitové kopie skrze program Autopsy.

1. **Příprava flashdisku**
   - Sehnání flashdisku pro instalaci FTK Imageru (alespoň 2 GB) z případných akutních důvodů pro vytvoření okamžitého obrazu disku
2. **Stažení nástroje FTK Imager a jeho následná instalace na flashdisk**
   - https://www.exterro.com/ftk-imager
3. **Tvorba obrazu disku skrze program FTK Imager**
   - Spuštění programu FTK Imager
   - Kliknutí na „**File -> Create Disk Image**“ nebo na **ikonu** dle obrázku 18

Obrázek 18 Tvorba obrazu. Zdroj: vlastní

   - **Zvolení typu zdroje evidence** (fyzický disk) podle obrázku 19 a kliknutí na tlačítko „**Další**“

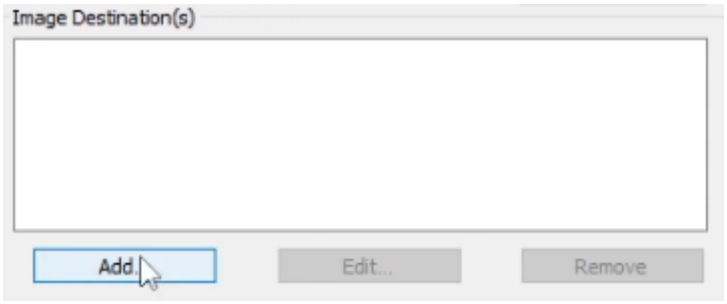


Obrázek 19 Zdroje evidence. Zdroj: vlastní

- Rozkliknutí nabídky připojených zařízení a **výběr zdrojového zařízení** pro tvorbu obrazu, ilustrace znázorněna na obrázku 20

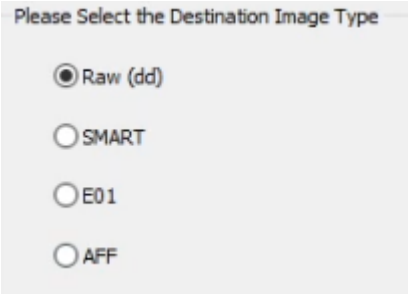
Obrázek 20 Výběr zařízení pro obraz. Zdroj: vlastní

- Kliknutí na tlačítko „**ADD**“ pro přidání destinace obrazu podle obrázku 21



Obrázek 21 Tvorba destinace obrazu. Zdroj: vlastní

- Zvolení **typu obrazu** dle obrázku 22 (RAW-dd) a kliknutí na tlačítko „**Další**“ **SMART** – Linux; **E01** – EnCase; **AFF** – starší formát -> kompatibilita

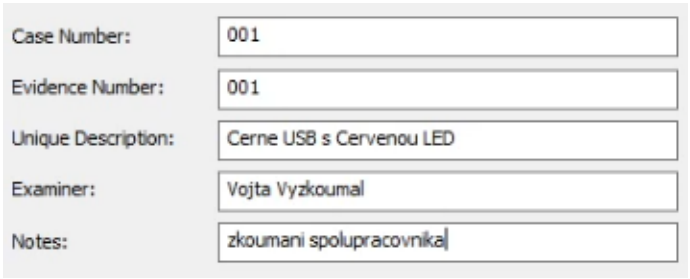


Obrázek 22 Volba typu obrazu. Zdroj: vlastní

- **Vyplnění informací k evidenci** příklad na obrázku 23**:**
  Case Number – číslo zkoumaného případu
  Evidence Number – podčíslo zkoumaného případu tzv. evidenční číslo
  Description – unikátní popis pro identifikaci

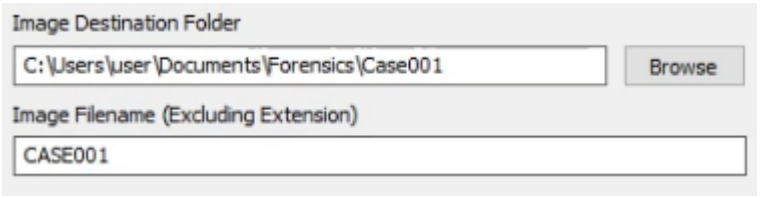
Examiner – celé jméno zkoumajícího člověka

Notes – dodatečné poznámky k případu



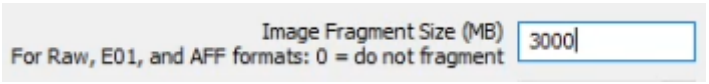
Obrázek 23 Evidenční informace. Zdroj: vlastní

- V následujícím vyskakovacím okně **výběr cesty pro uložení obrazu** a zvolení intuitivní a logický **název souboru**, znázorněno na obrázku 24



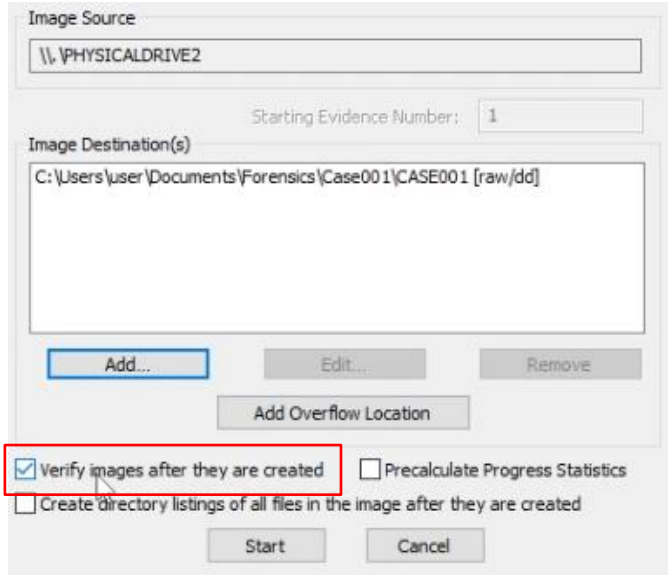
Obrázek 24 Cesta a název obrazu. Zdroj: vlastní

- V poslední části doplnit **velikost fragmentu**, pro pouze jeden nerozdělený soubor, je potřeba zvolení velikost větší, než je celková velikost zdrojového disku (nebo zadání čísla 0); pro rozdělení obrazu na více částí, zvolení menší velikosti



Obrázek 25 Velikost fragmentu. Zdroj: vlastní

- Kliknutí na tlačítko „**Finish**“ pro dokončení nastavení destinace obrazu
- V původním okně **je vhodné zkontrolovat** vyplněné informace a **zaškrtnout** tlačítko pro ověření obrazů, následně kliknutí na tlačítko „**Start**“, ilustrace znázorněna na obrázku 26



Obrázek 26 Finalizace obrazu. Zdroj: vlastní

- **Vyčkání** na tvorbu obrazu a jeho ověření v rámci několika minut, doba závisí na velikosti zdrojového USB zařízení neboli velikosti obrazu disku a hardwarovém vybavení fyzického počítače

4. **Kontrola shodnosti hashů a chyb**
   - Ve vyskakovacím okně zobrazeném na obrázku 27 je potřeba **zkontrolovat shodnost hashů** a zda nedošlo k nějakým **blokacím** během tvorby obrazu

MD5 Hash	
Computed hash	cfbd6b77a1a2a5f69899d03f971bebfa
Report Hash	cfbd6b77a1a2a5f69899d03f971bebfa
Verify result	Match
SHA1 Hash	
Computed hash	64c04f8f09306199a306c6ef0b69cd49b44b07b1
Report Hash	64c04f8f09306199a306c6ef0b69cd49b44b07b1
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Obrázek 27 Kontrola hashů a bloků. Zdroj: vlastní

- **Volitelné:** zkontrolovat informace (základní, fyzické, obrazu, verifikace) u vygenerovaného .txt souboru dle nastavené cesty

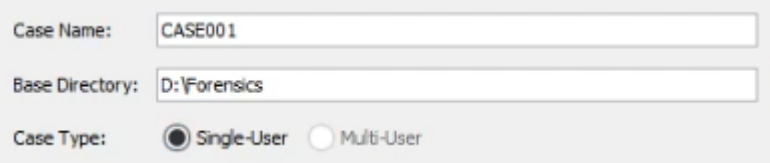
6.4 Základy Autopsy

Čtvrtá a poslední část se zabývá základy programu Autopsy a využitím tohoto programu pro zkoumání obrazu disku vytvořeného dle minulé části pomocí FTK Imageru.

1. **Stažení nástroje Autopsy a jeho následná instalace**
   - https://www.autopsy.com/download/
2. **Otevření programu Autopsy a příprava případu**
   - Vytvoření nového CASE neboli případu (Case -> New Case)

Obrázek 28 *Tvorba Case*. Zdroj: vlastní

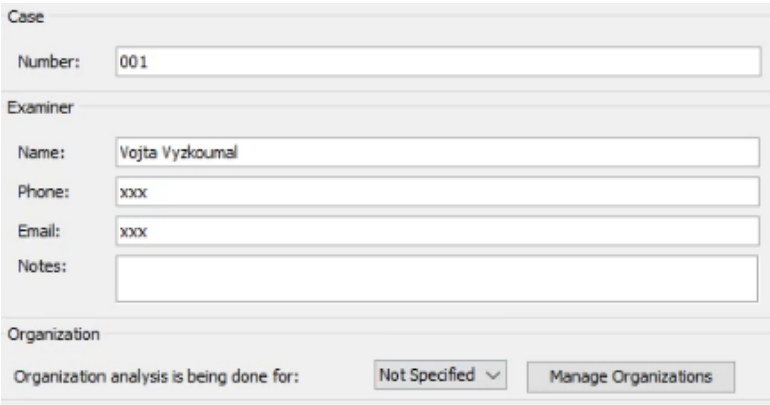
   - Vyplnění základních informací k případu z obrazu disku (jméno případu; složka kde se případ vytvoří; zvolení Sigle/Multi-User dle počtu lidí, kteří mají přístup)



Obrázek 29 Základní infromace případu. Zdroj: vlastní

Pozn. nastavení Multi-User:
https://sleuthkit.org/autopsy/docs/user-docs/4.0/install_multiuser_page.html

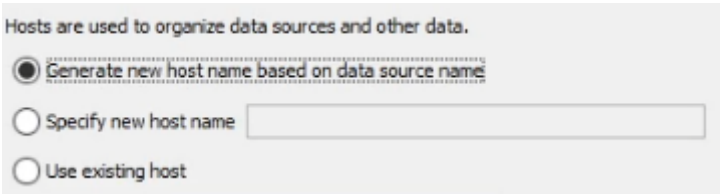
   - Vyplnění čísla případu a dodatečných informací (číslo případu; informace o zkoumající fyzické osobě; informace o organizaci)



Obrázek 30 Doplňující informace případu. Zdroj: vlastní

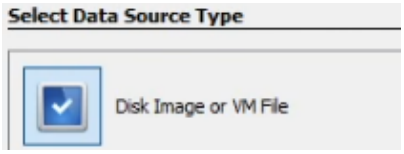
3. **Přidání zdroje k případu**

- **Vybrání názvu hosta** – automatické vygenerování na obrázku 31 / vlastní specifikování / použití existujícího (host je buď fyzický PC nebo server k analýze dat)



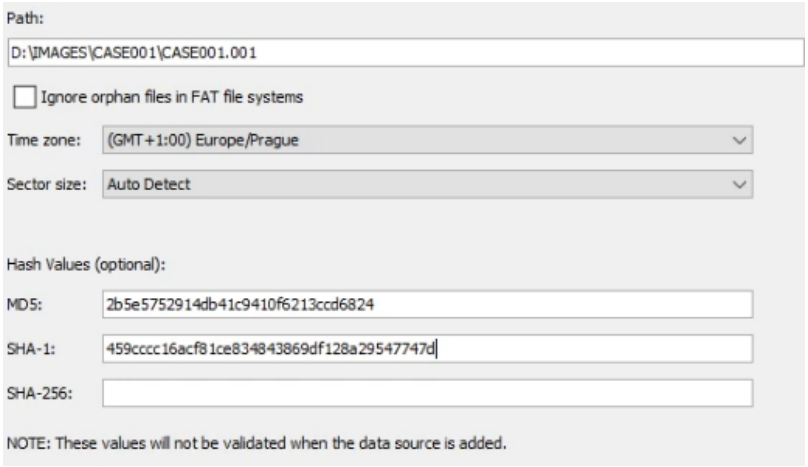
Obrázek 31 Výběr názvu hosta. Zdroj: vlastní

- **Vybrání typu zdroje** podle obrázku 32 **–** program Autopsy vyzve k vybrání typu zdroje **(obraz disku)**, následně kliknutí na tlačítko „Další“



Obrázek 32 Typ zdroje. Zdroj: vlastní

- **Nastavení zdroje** – Autopsy zobrazí tabulku pro vybrání cesty k cílovém soboru (obrazu disku), nastavení správné časové zóny a v poslední části doplnění hashů z vygenerovaného .txt soboru (viz. video FTK Imager) – příklad na obrázku 34



Obrázek 34 Nastavení zdroje. Zdroj: vlastní

- Poslední část je vybrání pluginů, doporučení je všechny ponechat zakřížkované kromě pluginů pro Android, iOS a DJI drony, následně započne analýza obrazu

4. **Zkoumání případu**

- V první části zkoumání je třeba vyčkat na **dokončení analýzy případu systémem**, dokud analýza nebude na 100 %. Není to však podmínkou, jelikož lze i zkoumat během analýzy. Obecně osobní zkoumání případu během analýzy programem není doporučeno, jelikož program není příliš stabilní a je zpomalený

Obrázek 35 Průběh analýzy. Zdroj: vlastní

- **Zkoumání případů** je velmi individuální a proto neexistuje žádný konkrétní postup, osobní analýza ale probíhá v levém okně příklad na obrázku 36, kde program Autopsy rozdělil strukturu do několika částí:

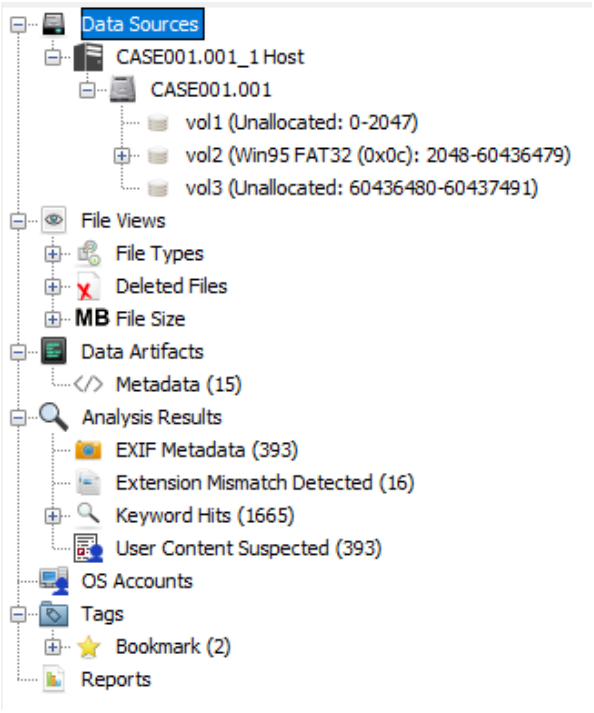
  Data Sources – zobrazuje hierarchii nahraného zdroje (obrazu disku) a jeho logické rozdělení na svazky a nealokovaná místa, dále zobrazuje konkrétní složky a soubory i včetně těch nedávno smazaných

  File Views – tato hierarchie se používá k třídění a vyhledávání konkrétních dat, rozděluje soubory dle velikosti, typu, přípon souborů a zobrazuje všechny smazané soubory

  Data Artifacts – slouží k nalezení metadat souborů na zdroji, zobrazuje tedy metadata typu kdo soubor vytvořil, kdy vytvořil, datum poslední změny, kdo je vlastníkem,... Dále podávají informace o typu OS a jeho účtech, instalovaných souborech, webové informace (vyhledávání, historii, účty, cookies, stažené soubory), připojené USB zařízení i koš.

  Analysis Results – jedná se o výsledky analýzy pomocí zmiňovaných pluginů, tato část zobrazuje například všechny nalezené emailové adresy, podezřelý či zašifrovaný obsah, EXIF Metadata (obrázků), neshodnosti přípon soborů a vyfiltrované zajímavé soubory či klíčová slova (například Tor)

  Tags – zobrazuje veškerá člověkem označená data, které jsou předpokládány jako podezřelé či průkazné a budou využity například jako podklad při soudním řízení pomocí reportů



Obrázek 36 Základní zkoumání. Zdroj: vlastní

Pokročilé zkoumání s ilustrací na obrázku 37 **pomocí horní navigace:**

Add Data Source – položka pro přidání dalších zdrojů k případu

Images/Videos – položka zobrazující hierarchickou strukturu zaměřenou na obrázky a videa, včetně základních informací ohledně těchto souborech

Communications – položka poskytuje pohled na všechny komunikační události pro daný případ (zejména telefon, emaily a sociální sítě)

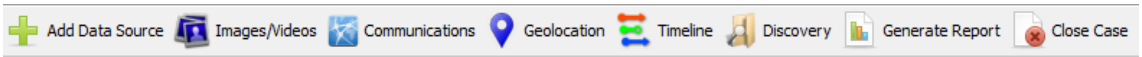
Geolocation – položka zobrazuje artefakty, které mají zaznamenanou polohu neboli atributy zeměpisné délky a šířky jako body na mapě

Timeline – položka zobrazuje časovou osu používání zdrojového zařízení a jeho celkových změn, úprav a tvorby souborů

Discovery – položka zobrazuje obrázky, videa, dokumenty nebo domény, které odpovídají sadě filtrů nakonfigurovaných uživatelem

Generate report – položka pro generování report, viz. další bod

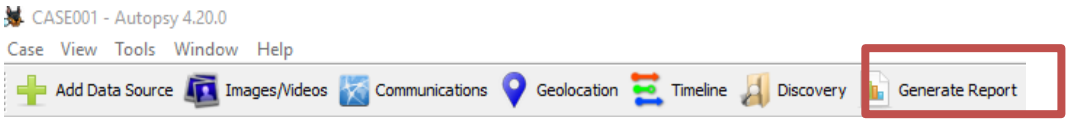
Close Case – položka pro uzavření případu



Obrázek 37 Pokročilé zkoumání

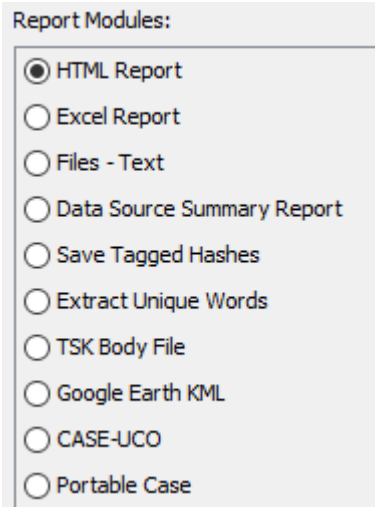
5. Generování reportu

- V horním menu kliknutí na položku „Generate report“ podle obrázku 38



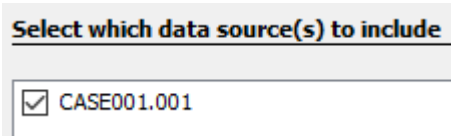
Obrázek 38 Generování reportu. Zdroj: vlastní

- Program zobrazí nové vyskakovací okno pro výběr formy reportu (nejčastěji HTML/Excel report) následně kliknutí na tlačítko „Další“

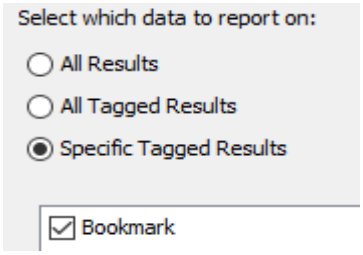


Obrázek 39 Forma reportu. Zdroj: vlastní

- Další vyskakovací okno vyzve k **vybrání zdroje** pro zahrnutí do reportu a **vybrání dat** pro reportování

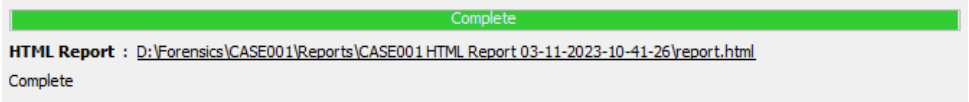


Obrázek 41 Výběr zdroje.
Zdroj: vlastní



Obrázek 40 Výběr dat.
Zdroj: vlastní

- Dokončení reportu pomocí tlačítka **FINISH**, forma dokončení na obrázku 42



Obrázek 42 Vygenerovaný report. Zdroj: vlastní

7 Závěry a doporučení

Práce jako taková představuje souhrn teoretických i praktických poznatků pro forenzní analýzu zejména diskových úložišť, jelikož je tato problematika stále se rozšiřující, stejně jako počítačová kriminalita a její návaznost na zjišťování důkazů. Teoretická část je zaměřena na operační systém Windows, zejména na jeho historické i momentální verze, bezpečnost, možné zranitelnosti a základní principy ochrany. V další kapitole již práce uvádí přesunem do kyberkriminality a její návazností do teoretické části forenzní analýzy v operačním systému Windows. Zde se práce věnuje základům forenzní analýzy, jejím postupům, principům a zásadám s dalším případným využitím u soudního řízení.

Praktická část poukazuje na průběh možného fiktivního forenzního případu s úvodem základních programů pro práci s forenzní analýzou – VirtualBox, WriteProtect, FTK Imager, Autopsy. Pro lepší pochopení byla vytvořena videa s komentářem, která kopírují praktickou část pro lepší pochopení funkcionality.

V úvodu práce byly formulovány následující výzkumné otázky:

1) Jaké jsou hlavní typy (jádra) operačních systémů?
2) Kolik, či jaké hrozby a zranitelnosti existují u OS Windows?
3) Co všechno lze zkoumat pomocí forenzní analýzy?
4) Jaké jsou nejpoužívanější nástroje forenzní analýzy a jejich odlišnosti?

Výzkumná otázka číslo 1 potvrdila předpoklady v existenci sady operačních systémů a několika typů jader.

Výzkumná otázka číslo 2 identifikovala množství hrozeb a zranitelností specifických pro OS Windows, jejichž počet se nedá kvalifikovaně odhadnout, ale sledujeme exponenciální růst.

Výzkumná otázka číslo 3 identifikovala následující oblasti, které mohou být zkoumány pomocí forenzní analýzy: forenzní analýza pro zachycení disku a dat, forenzní analýza pro souborové systémy, forenzní analýza pro analýzu registrů, forenzní analýza pro dočasné paměti (RAM), forenzní analýza pro síťovou analýzu (včetně firewallu) a forenzní analýza pro mobilní zařízení (zařízení založené na GPS).

Výzkumná otázka číslo 4 potvrdila sadu nástrojů využitelných pro forenzní analýzu OS Windows se zaměřením na forenzní analýzu diskových úložišť. Jednalo se o nástroje: FTK Imager, Autopsy a WriteProtect. Celková odlišnost nástrojů pro forenzní analýzu je odlišná zejména zaměřením programu, při stejném zaměření je funkcionalita velmi podobná.

Možná rozšiřitelnost práce je vskutku možná, jelikož tato bakalářská práce se zabývala především forenzní analýzou diskových úložišť ve Windows. V rámci dalšího výzkumu v oblasti forenzní analýzy OS Windows je vhodné se zaměřit na oblasti registrů, dočasných pamětí a analýzu síťového provozu. Další více rozšiřitelnou částí by mohlo být poukázání a zaměření na forenzní analýzu v operačním systému Linux.

8 Seznam použité literatury

[1] LARVIČNÍK, Jan Ph.D. PhDr. OPERAČNÍ SYSTÉMY. Mvso [online]. internet: Moravská vysoká škola Olomouc, 2018 [cit. 2023-03-26]. Dostupné z: https://www.mvso.cz/files/operacni-systemy.pdf

[2] VANĚK, Libor. Historie operačních systémů: se zaměřením na jiné OS než Windows a UNIX. FI.MUNI [online]. internet: Masarykova Univerzita, 2016 [cit. 2022-10-02]. Dostupné z: https://www.fi.muni.cz/usr/jkucera/pv109/2002/xvanek.html

[3] MILLS, Matt. Všechny verze Windows v celé historii. Itigic.com [online]. internet: ITIGIC, 2020 [cit. 2022-10-02]. Dostupné z: https://itigic.com/cs/all-versions-of-windows-throughout-history/

[4] PEKAŘ, Lukáš. HISTORIE WINDOWS V KOSTCE. Bonsai-development.cz [online]. internet: Bonsai Development, 2019 [cit. 2022-10-02]. Dostupné z: https://bonsai-development.cz/clanek/historie-windows-v-kostce

[5] Jádro (operační systém). Wikijii [online]. internet: Wikimedia Foundation, 2021 [cit. 2022-10-02]. Dostupné z: https://wikijii.com/wiki/Kernel_(operating_system)#Kernel-wide_design_approaches

[6] PROVOST, Ariel. Jádro operačního systému. Frwiki [online]. internet: Wikipedia FR, 2022 [cit. 2022-10-02]. Dostupné z: https://cs.frwiki.wiki/wiki/Noyau_de_système_d%27exploitation

[7] POHL, Marek. Bezpečnost operačního systému Windows. internet, 2008. Diplomová práce. Univerzita Pardubice. Vedoucí práce Ing. Lukáš Slánský. Dostupné z: https://dk.upce.cz/bitstream/handle/10195/29101/PohlM_Bezpecnost%20operacniho_LS_1%20cast_2008.pdf?sequence=3&isAllowed=y

[8] MANDA, Ing. David. FORENZNÍ ANALÝZA V OPERAČNÍCH SYSTÉMECH WINDOWS. internet, 2016. Diplomová práce. Vysoké učení technické v Brně. Vedoucí práce Ing. Pavel Otčenášek, Ph.D. Dostupné z: https://theses.cz/id/0r763c/diplomova_prace.pdf?zpet=%2Fvyhledavani%2F%3Fsearch%3Dforenzní%20analýza%20windows%26start%3D1

[9] RAFFER, Dan. What is the difference between black, white and gray hat hackers?. Norton.com [online]. internet: NortonLifeLock, 2022 [cit. 2022-10-02]. Dostupné z: https://us.norton.com/blog/emerging-threats/black-white-and-gray-hat-hackers#

[10] Ochrana před hrozbami na internetu. Avast.com [online]. internet: AVAST Software, 2022 [cit. 2022-10-02]. Dostupné z: https://www.avast.com/cs-cz/c-online-threats

[11] Typy detekovaných síťových útoků. Helpmax.com [online]. internet: Internet Security, 2019 [cit. 2022-10-02]. Dostupné z: http://internetsecurity.helpmax.net/cs/rozsirena-nastaveni-aplikace/ochrana-site/blokovani-sitovych-utoku/typy-detekovanych-sitovych-utoku/

[12] BEZPALEC, Pavel. Útoky na sítě. Publi.cz [online]. internet: ČVUT, 2021 [cit. 2022-10-02]. Dostupné z: https://publi.cz/books/223/02.html

[13] SOJKA, Michal. Operační systémy: Bezpečnost. Cvut.cz [online]. internet: FEL, 2018, 26.11.2018 [cit. 2022-10-06]. Dostupné z: https://cw.fel.cvut.cz/b181/_media/courses/b4b35osy/osy8_2018.pdf

[14] Pojem bezpečnostní služby. In: Cvut.cz [online]. internet: FEL, 2019 [cit. 2022-10-06]. Dostupné z: http://techpedia.fel.cvut.cz/html/frame.php?oid=76&pid=1005&finf=&fp=

[15] Co je triáda CIA?. Tombouctou-food.com [online]. internet: TOMBOUCTON, 2021, 12.1.2021 [cit. 2022-10-06]. Dostupné z: https://tombouctou-food.com/cs/co-je-triada-cia/

[16] ČERMÁK, Miroslav. CIA: Důvěrnost-Integrita-Dostupnost. Cleverandsmart.cz [online]. internet: ISSN 2694-9830, 2021, 19.6.2010 [cit. 2022-10-06]. Dostupné z: https://www.cleverandsmart.cz/duvernost-integrita-dostupnost/

[17] CHAI, Wesley. Confidentiality, integrity and availability (CIA triad). Techtarget.com [online]. internet: TechTarget, 2022, 28.6.2022 [cit. 2022-10-06]. Dostupné z: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

[18] SCHON, Otakar. Microsoft se snaží v oblasti bezpečnosti. Zive.cz [online]. internet: zive.cz, 2005, 8.4.2005 [cit. 2022-10-06]. Dostupné z: https://www.zive.cz/clanky/microsoft-se-snazi-v-oblasti-bezpecnosti/sc-3-a-123926/default.aspx

[19] 8 bezpečnostních chyb, kterých se možná dopouštíte. Dvojklik.cz [online]. internet: ESET, 2017, 29.6.2017 [cit. 2022-10-06]. Dostupné z: https://www.dvojklik.cz/8-bezpecnostnich-chyb-kterych-se-mozna-dopoustite/

[20] MALINA, Patrik. Zabezpečení Windows: ACL a Active Directory. Computerworld.cz [online]. internet: Internet Info DG, 2010, 15.4.2010 [cit. 2022-10-06]. Dostupné z: https://www.computerworld.cz/clanky/zabezpeceni-windows-acl-a-active-directory/

[21] Kyberkriminalita. Policie [online]. internet: Policie České Republiky, 2022 [cit. 2023-02-10]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[22] Jednotlivé druhy kyberkriminality. Policie [online]. internet: Policie České Republiky, 2022 [cit. 2023-02-10]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspxf

[23] DLUBALOVÁ, Klára. Na nebezpečí kyberkriminality upozorní Den bezpečnějšího internetu. Mvcr [online]. internet: Ministerstvo vnitra České republiky, 2023 [cit. 2023-04-01]. Dostupné z: https://www.mvcr.cz/clanek/na-nebezpeci-kyberkriminality-upozorni-den-bezpecnejsiho-internetu.aspx

[24] MORAVČÍK, Ondřej. Vývoj registrované kriminality v roce 2022. Policie [online]. internet: Policie ČR, 2023 [cit. 2023-04-01]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx

[25] BAKER, Kurt. Cyber Espionage. *WHAT IS CYBER ESPIONAGE?* [online]. internet: CROWDSTRIKE, 2022 [cit. 2023-02-10]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

[26] BREZINSKI, D. a T. KILLALEA. Guidelines for Evidence Collection and Archiving. Evidence Collection and Archiving [online]. neart.org: In-Q-Tel, 2002 [cit. 2023-02-10]. Dostupné z: https://www.rfc-editor.org/rfc/rfc3227.html#section-2

[27] KADLEC, Josef. Forenzní analýza (1). Root.cz [online]. internet: ROOT, 2005 [cit. 2023-02-10]. Dostupné z: https://www.root.cz/clanky/forenzni-analyza-1/

[28] KADLEC, Josef. Forenzní analýza (2). Root.cz [online]. internet: ROOT, 2005 [cit. 2023-02-10]. Dostupné z: https://www.root.cz/clanky/forenzni-analyza-2/

[29] HOWARD, Poston. 7 best computer forensics tools. INFOSEC [online]. internet: Infosec Institute, 2021 [cit. 2023-03-24]. Dostupné z: https://resources.infosecinstitute.com/topic/7-best-computer-forensics-tools/

[30] WILLIAMS, Lawrance. 15 BEST Computer (Digital) Forensic Tools & Software in 2023. GURU99 [online]. internet: GURU99, 2023 [cit. 2023-03-24]. Dostupné z: https://www.guru99.com/computer-forensics-tools.html

[31] CUMAR, Chandan. 22 FREE Forensic Investigation Tools for IT Security Expert. GEEKFLARE [online]. internet: GeekFlare, 2023 [cit. 2023-03-24]. Dostupné z: https://geekflare.com/forensic-investigation-tools/

[32] CARRIER, Brian. Autopsy. Sleuthkit [online]. internet: The Sleuth Kit, 2023 [cit. 2023-03-24]. Dostupné z: https://www.sleuthkit.org/autopsy/

[33] FTK Imager. Exterro [online]. internet: Exterro, 2023 [cit. 2023-03-24]. Dostupné z: https://www.exterro.com/ftk-imager

[34] ProDiscover - computer forensics [online]. internet: ProDiscover, 2023 [cit. 2023-03-24]. Dostupné z: https://prodiscover.com

9 Přílohy

1) **USB FLASHDISK** – video tutoriály

Příloha č. 1

Oskenované zadání práce