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

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

TESTOVÁNÍ BEZPEČNOSTI

Základní seznámení s Autopsy

Metodický list

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

Recenzent: Ing. Vladimír Šulc Ph.D.

Rok vydání: 2023

Obsah

Cíle

Seznámit se s free nástrojem Autopsy s profesionálními vlastnostmi pro forenzní analýzu artefaktů. Scénář vytváří předpoklady pro úspěšnou práci se scénářem „Autopsy pro vyhledávání artefaktů Windows“.

Dovednosti

Uvedení dovednosti, kterou by si žáci měli v rámci této úlohy osvojit: Seznámit se se systémem Autopsy. Systém je free, ale má vlastnosti a složitost těch nejnáročnějších profesionálních systémů.

Pracovní prostředí

Úlohu lze realizovat v prostředí:

- Cylab JCEKB
- Offline Security Classroom

Pro práci budeme potřebovat následující nástroj:

- Autopsy 4 (pro Windows) – autopsy.ova 804 160 kB
- Image Windows 10 – 10 345 849 kB
- VideoTriageModule-1.3 – rozděluje video soubor na snadno zobrazitelné miniatury (klíčové snímky) – 45 573 kB.

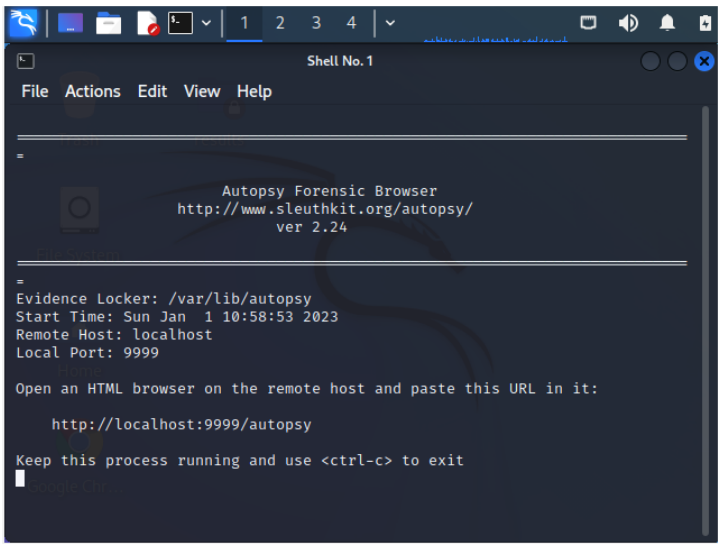
Průběh výuky

1 Charakteristika Autopsy

Autopsy[1] je grafické rozhraní pro The Sleuth Kit a další open source digitální forenzní nástroje. Autopsy 3 byl kompletní přepis z Autopsy 2, aby byl založen na Javě. Autopsy 4 vylepšuje Autopsy 3 tím, že podporuje spolupráci na jednom případu více uživateli. Přestože je Autopsy navrženo jako multiplatformní (Windows, Linux, MacOSX), aktuální verze je plně funkční a plně testovaná pouze na Windows (pustit ji lze na kterékoliv verzi Windows počínajíc Windows XP), a proto se zde budeme věnovat verzi pro Windows.

Autopsy je určen k provádění forenzních operací s obrazem disku důkazů. Získané výsledky pomáhají prozkoumat a najít relevantní informace. Autopsy se může pochlubit funkcemi, které se běžně vyskytují v komerčních digitálních forenzních nástrojích. Nástroj používají orgány činné v trestním řízení, policejní vyšetřovatelé a lze jej použít také pro interní firemní šetření k vyšetřování důkazů nalezených při počítačovém zločinu. Může být také použit k obnovení informací, které byly vymazány.

Autopsy je rovněž součástí vybavení systému Kali, který používá starší verzi 2 s menšími možnostmi – viz obr. 1.1. Výhodou je, že v jednom virtuálním stroji je celá škála nástrojů, což se hodí pro operativní šetření. Pro hlubší poznání Autopsy je ale přesto vhodnější verze pro Windows.



Obr. 1.1 Autopsy Forensic Browser pro Kali

V tomto modulu budeme používat verzi 4.19.3. Instalace vyžaduje oprávnění správce. Když soubor otevřete, váš antivirus se může zeptat, zda důvěřujete softwaru. Je to proto, že prodejce z nějakého důvodu nepodepsal tuto kopii Autopsy. Je však důvěryhodný, pokud je získán z webu Autopsy.

[1] https://www.hackingarticles.in/comprehensive-guide-on-autopsy-tool-windows/

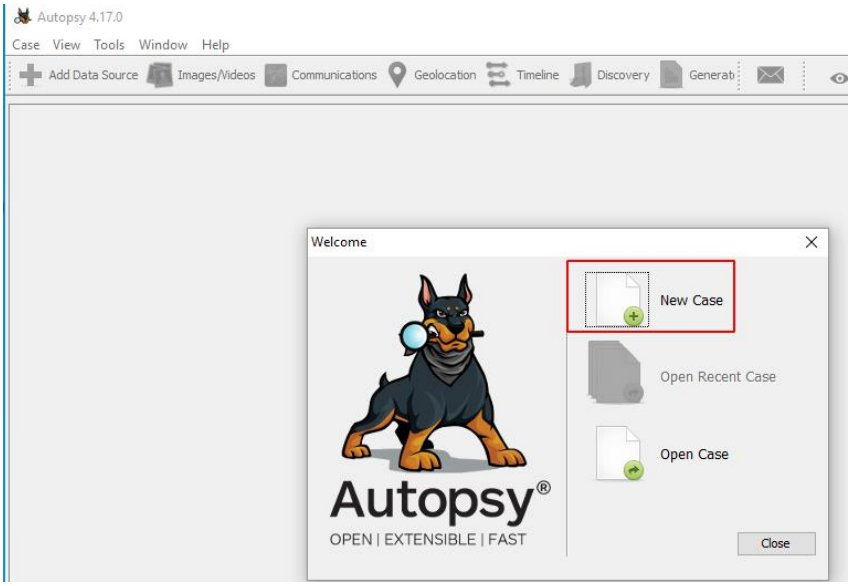
Existují dva způsoby nasazení Autopsy: single user and multi-user. Hlavním rozdílem je, že případy pro jednoho uživatele jsou jedinou instancí Autopsy v jeden daný okamžik a jeho instalace je snadná. Zatímco pro více uživatelů je otevřeno více uživatelů, kteří mohou vidět, co jeden druhý dělá a spolupracovat, a vyžaduje instalaci a konfiguraci dalších síťových služeb. Může se také zobrazit výzva systému Windows, že Autopsy chce komunikovat s ostatními zařízeními ve vaší síti. Aby to bylo možné, Autopsy chce otevřít některé porty firewallu. Lze to povolit nebo zakázat. Samo o sobě je to ale v pořádku.

2 Vlastnosti Autopsy

Pro seznámení s vlastnostmi Autopsy byl použit zdroj (Vaghela 2020). Obsahem další kapitoly (3. kapitoly) bude praktické ověření jednotlivých funkcí systému s využitím image Windows 10 převzatého z kurzu (Hendrix 2022).

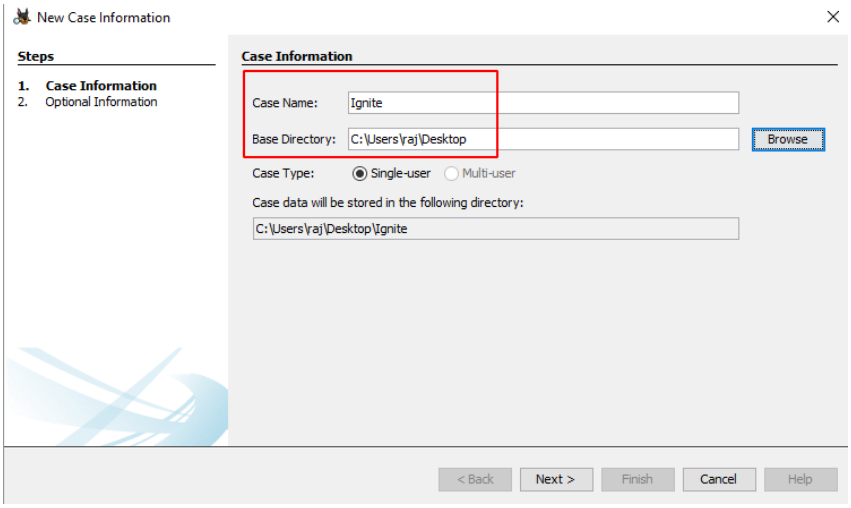
2.1 Vytvoření nového případu (New Case)

Nástroj Autopsy se spouští v operačním systému Windows kliknutím na „New Case“ – viz obr. 2.1.1, kdy se vytváří nový případ.



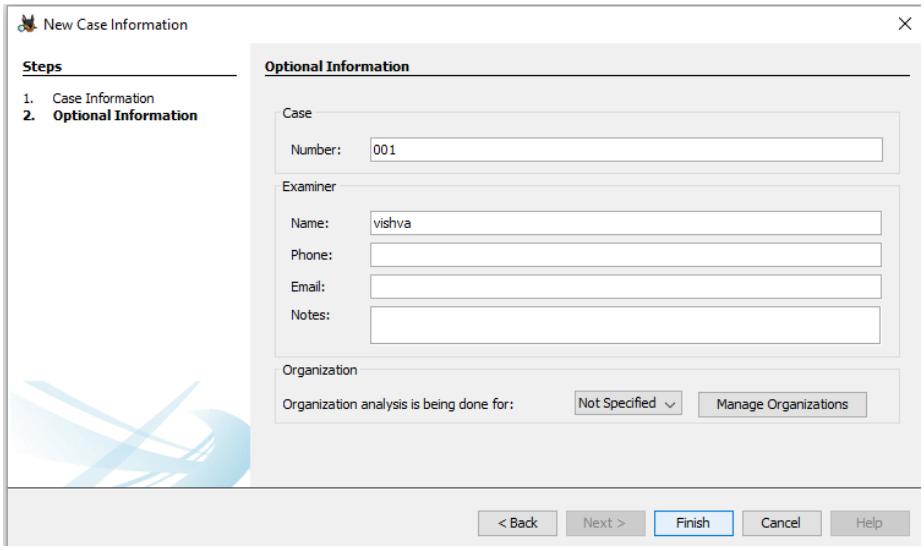
Obr. 2.1.1 Vytvoření nového případu – New Case

Poté je třeba vyplnit všechny potřebné informace o případu, jako je název případu, a vybrat základní adresář – viz obr. 2.1.2, aby byla všechna data případu uložena na jedno místo.



Obr. 2.1.2 Uložení povinných informací případu

V případě potřeby lze také přidat volitelné informace o případu – viz obr. 2.1.3.

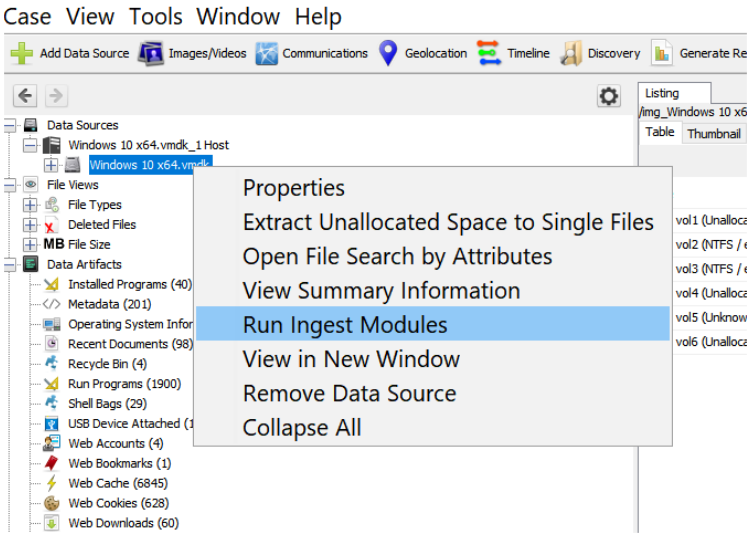


Obr. 2.1.3 Uložení volitelných informací případu

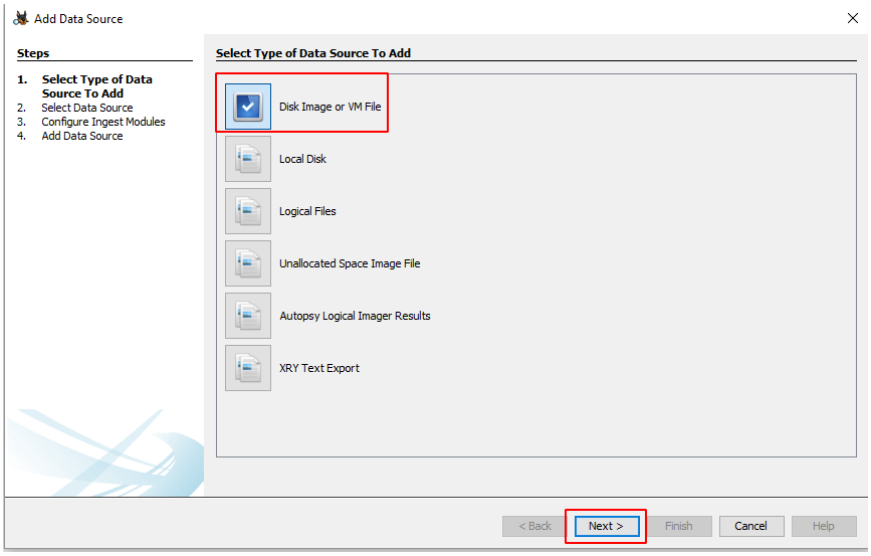
2.2 Určení typu zdroje dat

Nyní je třeba přidat typ zdroje dat – *Select Type of Data Source to Add*. Moduly *Ingest* analyzují data a zdroj dat, čímž provádějí veškerou analýzu souborů a analyzují jejich obsah. Po přidání zdroje dat do případu se zobrazí dialog, který umožní nakonfigurovat, co by se mělo na těchto datech analyzovat. To bude spuštěno na pozadí a poskytne výsledky v reálném čase. Tyto moduly lze spustit třemi způsoby.

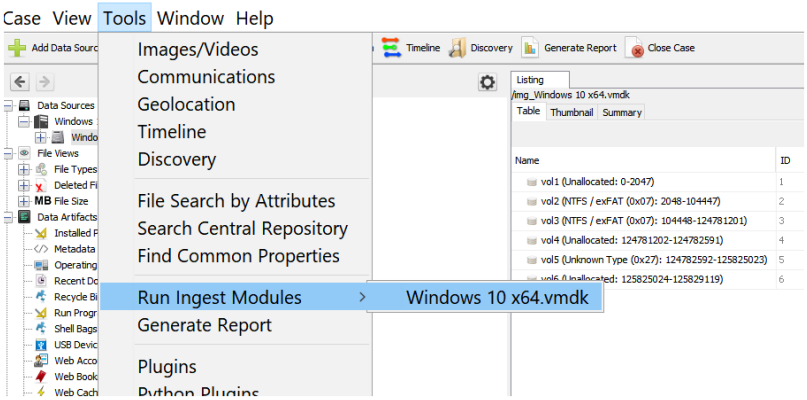
- První je v defaultním (výchozím) nastavení, což je bezprostředně po přidání zdroje dat – obr. 2.2.1.
- Za druhé, kliknutím pravým tlačítkem na zdroje dat (Data Sources) ze stromu v hlavním rozhraní a výběrem *Tools*, *Run Ingest Modules* (Spustit modul příjmu) – obr. 2.2.2. Tento proces se zobrazí na obrazovce a použije se, pokud se rozhodnete analyzovat data, která jste dříve nezahrnuli.
- Nakonec můžete přejít na *Tools* (obr. 2.2.3), *Run Ingest Modules* a tam možnosti zdroje dat, např. Dropbox.



Obr. 2.2.1 Spuštění modulu příjmu v defaultním nastavení



Obr. 2.2.2 Spuštění modulu příjmu přes *Data Sources* a výběr *Tools*



Obr. 2.2.3 Spuštění modulu příjmu přes výběr *Tools*

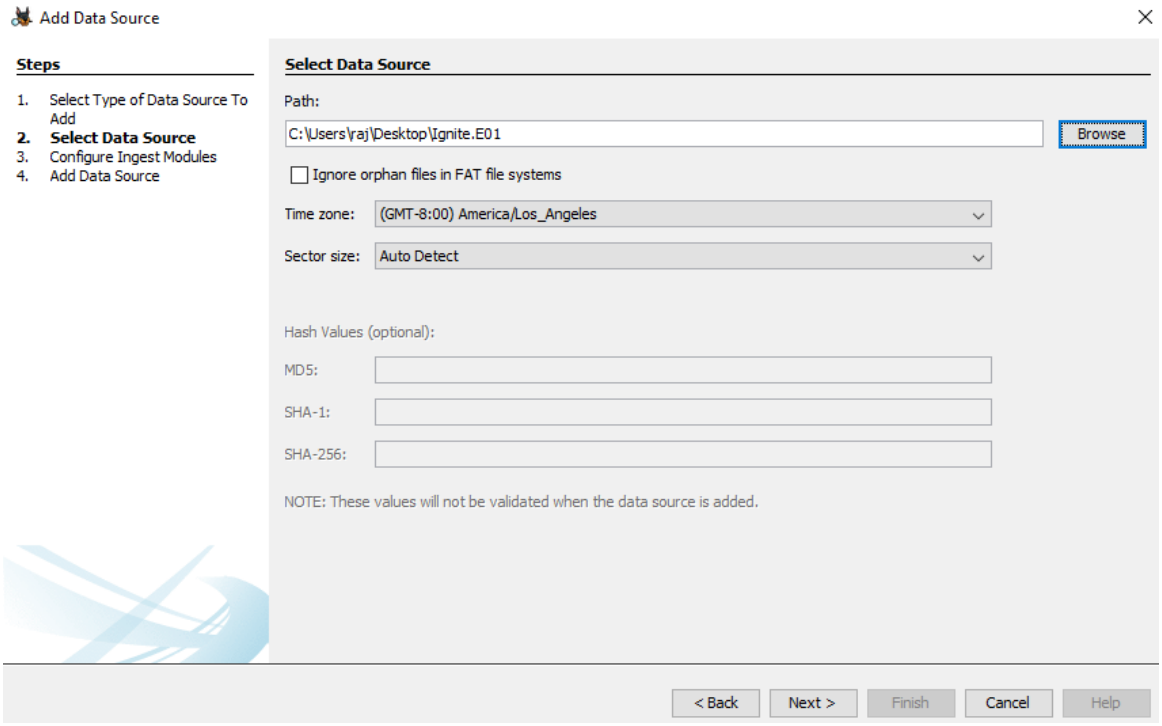
Na výběr jsou různé druhy příjmu:

- *Disk Image or VM file*: Zahrnuje soubor image, který může být přesnou kopií pevného disku, paměťové karty nebo dokonce virtuálního počítače.
- *Local Disk*: Tato možnost zahrnuje zařízení jako pevný disk, jednotky pera, paměťové karty atd.
- *Logical Files*: Obsahuje image všech místních složek nebo souborů.
- *Unalocated Space Image File*: Zahrnují soubory, které neobsahují žádný souborový systém a spouštějí se pomocí modulu ingest.
- *Autopsy Logical Imager Results*: Zahrnuje zdroj dat ze spuštění logického imageru.
- *XRY Text Export*: To zahrnuje zdroj dat z exportu textových souborů ve formátu .xry[2].

V druhém kroku je třeba specifikovat zdroj dat – *Select Data Source* (obr. 2.2.4). Pro cvičení máme k dispozici dříve vytvořený image, takže přidáme umístění tohoto souboru. V šabloně pro výběr datového zdroje se také zobrazí možnost ignorovat osiřelé soubory a systémy souborů FAT – *Ignore orphan files in FAT file systems*. Osiře-

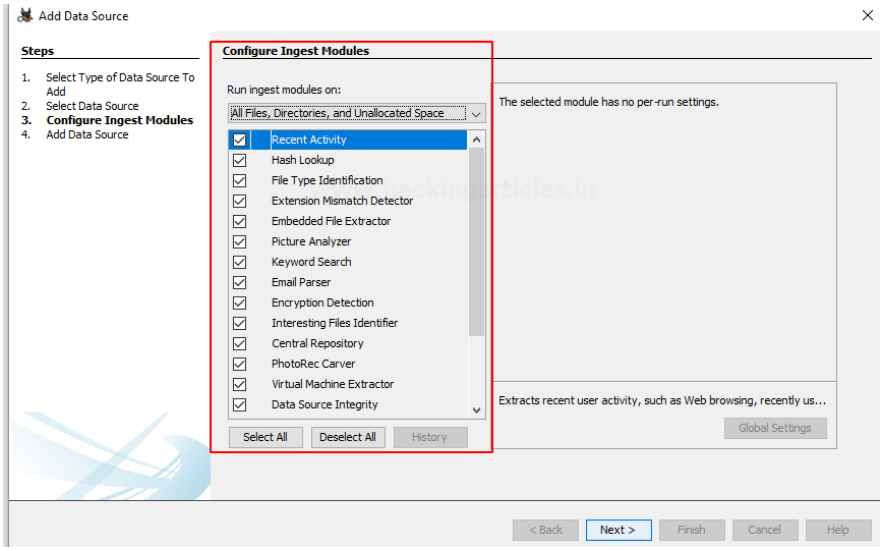
[2] XRY slouží k analýze a obnově informací z otevřených zařízení, jako je GPS, tablet, mobilní telefony atd.

lý soubor je soubor, který již nemá účel. Podezřelý může mít například odinstalovanou aplikaci, ale ta přesto zůstává na tomto pevném disku. Nevýhodou této možnosti je, že pokud je vybrána, doba zpracování se prodlouží a může dojít k pádu počítače.



Obr. 2.2.4 Specifikace zdroje dat – *Select Data Source*

Dále budete vyzváni ke konfiguraci modulu příjmu (*Configure Ingest Module*)**.** Zaškrtnutí všech modulů (obr. 2.2.5) vede k časově náročnému zpracování, zde je třeba být uvážlivý a střídmý.



Obr. 2.2.5 konfiguraci modulu příjmu – *Configure Ingest Module*

Ve verzi 3.1[3] Autopsy disponoval těmito moduly:

- *Recent Activity Module* extrahuje aktivitu uživatele uloženou webovými prohlížeči a operačním systémem. Také spustí Regipper[4] na podregistru registru.
- *Hash Lookup Module* používá hash databáze k ignorování známých souborů z NIST (National Institute of Standards and Technology) NSRL (National Software Reference Library)[5] a označení známých špatných souborů. Pomocí tlačítka *Advanced* v nabídce Tools lze přidat a nakonfigurujte hašovací databáze, které se mají během tohoto procesu používat. Jakmile dojde ke zpracování, budou přicházet aktualizace o známých chybných souborech. Hash databáze můžete později přidat prostřednictvím nabídky *Tools -> Options* v hlavním uživatelském rozhraní.
- *File Type Identification Module* určuje typy souborů na základě podpisů a hlásí je na základě typu MIME. Výsledky ukládá do tabulky. Využívá open source knihovnu Tika[6]. V nabídce *Tools, Options, File Types* lze definovat své vlastní typy souborů.
- *Embedded File Extraction Module* otevírá ZIP, RAR, další archivní formáty, Doc, Docx, PPT, PPTX, XLS a XLSX a odesílá odvozené soubory z těchto souborů zpět přes ingest pipeline k analýze.
- *Picture Analyzer Module* (ve verzi 3 zvaný EXIF Parser Module) extrahuje informace EXIF[7] ze souborů JPEG a zveřejňuje výsledky do stromu v hlavním uživatelském rozhraní.
- *Keyword Search Module* používá seznamy klíčových slov k identifikaci souborů s konkrétními slovy. Můžete vybrat seznamy klíčových slov, které se mají automaticky vyhledávat, a pomocí tlačítka *Advanced* lze vytvářet nové seznamy. Vyhledávání klíčových slov lze provádět např. po dokončení zpracování. Seznamy klíčových slov, které vyberete během příjmu, budou prohledávány v pravidelných intervalech a výsledky získáte v reálném čase.
- *Email Parser Module* identifikuje soubory Thunderbird MBOX a soubory ve formátu PST na základě podpisů souborů, extrahuje z nich e-maily a výsledky přidá na tabuli.
- *Extension Mismatch Detector Module* používá výsledky z Identifikace typu souboru a označí soubory, které mají příponu, která není tradičně spojena s detekovaným typem souboru. Ignoruje „známé“ (NSRL) soubory. Typy MIME a přípony souborů podle typu MIME můžete přizpůsobit v nabídce Tools, Options, Discord přípon souborů.
- *E01 Verifier Module* vypočítá kontrolní součet souborů E01 a porovná je s interním kontrolním součtem souboru E01, aby se ujistil, že se shodují. Soubor E01 (Encase Image File Format) uchovává zálohu různých typů získaných digitálních důkazů, které zahrnují zobrazování disků, ukládání logických souborů atd. Když vyšetřovatel (nebo soudní znalec) použije Encase k vytvoření zálohy dat dostup-

[3] https://sleuthkit.org/autopsy/docs/user-docs/3.1/quick_start_guide.html

[4] RegRipper je open source nástroj napsaný v Perlu pro extrakci resp. analýzu informací (klíče, hodnoty, data) z registru a jejich prezentaci pro analýzu.

[5] Index NIST NSRL si lze stáhnout z http://sourceforge.net/projects/autopsy/files/NSRL/

[6] Apache Tika je knihovna, která se používá pro detekci typů dokumentů a extrakci obsahu z různých formátů souborů. Interně používá Tika existující různé analyzátory dokumentů a techniky detekce typů dokumentů k detekci a extrakci dat.

[7] E*xif* (zkratka z anglického Exchangeable image file format) je specifikace pro formát metadat, vkládaných do souborů digitálními fotoaparáty.

ných v pevný disk, vytvoří se fyzický bitový tok dat. Tento postup je známý jako Disk Imaging. Základní teorií vztahu mezi formátem souborů Encase a E01 je, že při vytváření obrázků dat dostupných na pevném disku Encase rozděluje kompletní data do 640 MB datových bloků. Díky tomuto rozdělení dat při pauze 640 MB vzniká více datových souborů, ve kterých jsou uloženy zásadní informace o pevném disku. Nejzvláštnější vlastností těchto souborů je, že názvy souborů zůstávají stejné (jak je pojmenoval uživatel), zatímco přípona souboru se mění.

- *Android Analyzer Module* umožňuje analyzovat běžné položky ze zařízení Android. Umístí artefakty na BlackBoard.
- *Interesting Files Identifier Module* vyhledává soubory a adresáře na základě pravidel zadaných uživatelem v nabídce Tools -> Options -> Interesting Files. Funguje jako „File Alerting Modul“ (modul generování varovných zpráv).
- *PhotoRec Carver Module* vyřezává soubory z nepřiděleného prostoru a posílá je do řetězce zpracování souborů.

Moduly Ingest[8] byly v aktuální verzi 4.19.3 doplněny o:

- *Extension Mismatch Detector Module* využívá výsledky z Identifikace typu souboru a označuje soubory, které mají příponu, která není tradičně spojena s detekovaným typem souboru. Ignoruje „známé“ (NSRL – National Software Reference Library) soubory. Typy MIME a přípony souborů podle typu MIME lze přizpůsobit v *Tools, Options, File Extension Mismatch*.
- *Data Source Integrity Module* má dva účely: Pokud má zdroj dat přidružen nějaký hash (buď zadaný uživatelem nebo obsažený v souboru E01), ověří jej. Pokud zdroj dat nemá žádný přidružený hashe, vypočítá jej a uloží do databáze.
- *Central Repository Module* je zodpovědný za přidávání vlastností do databáze a porovnávání každé vlastnosti se seznamem pozoruhodných vlastností. Aby se z Correlation Engine vytěžilo maximum, je třeba spustit všechny ingestové moduly. Pokud například není spuštěno *Hash Lookup,* modul *Central Repository* nevloží do databáze žádné soubory.
- *Encryption Detection Module* vyhledává soubory, které by bylo možné zašifrovat jak pomocí obecného výpočtu entropie, tak pomocí specializovanějších testů pro určité typy souborů.
- *Virtual Machine Extractor Module* přidá všechny virtuální stroje, které najde ve zdroji dat, do případu jako nové zdroje dat. To zahrnuje soubory disku virtuálního počítače (.vmdk) a soubory virtuálního pevného disku (.vhd).
- *Plaso* je rámec pro spouštění modulů pro extrahování časových razítek pro různé typy souborů.
- *DJI Drone Analyzer* umožňuje analyzovat soubory z dronu.
- *GPX Analyzer* umožňují importovat data GPS ze souboru GPX (GPS Exchange).
- *iOS Analyzer (iLEAPP)* spouští iLEAPP (https://github.com/abrignoni/iLEAPP) a převádí výsledky na výsledky, které lze zobrazit v Autopsy.

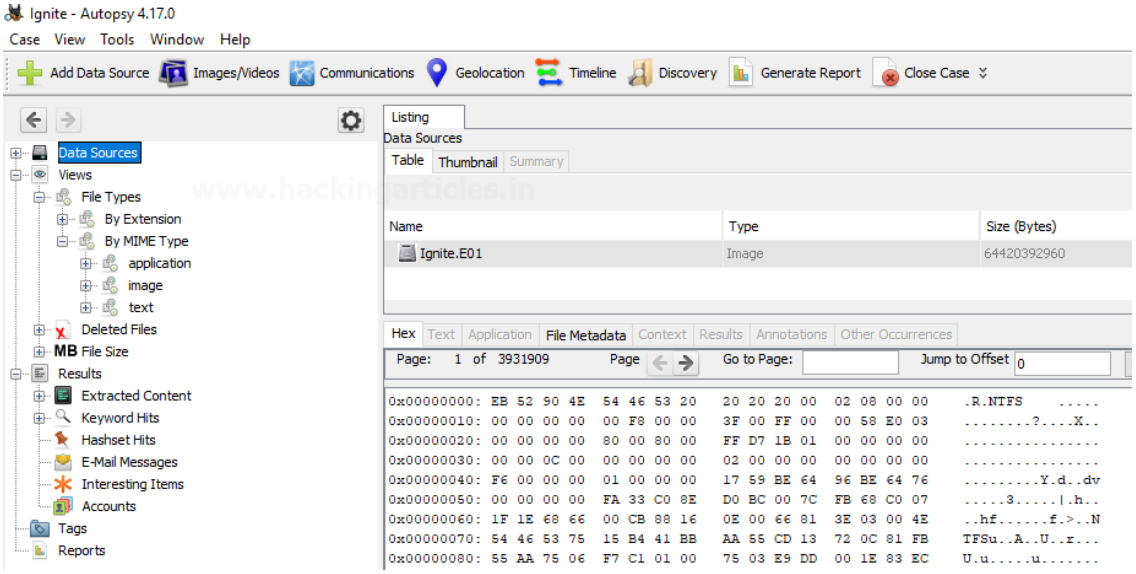
8 https://sleuthkit.org/autopsy/docs/user-docs/4.19.3/

- *Android Analyzer (aLEAPP)* spouští LEAPP (https://github.com/abrignoni/aLEAPP) a převádí výsledky na výsl*edky, které lze zobrazit v Autopsy.*
- *YARA Analyzer* používá sadu pravidel pro vyhledávání souborů pro textové nebo binární vzory. YARA (https://virustotal.github.io/yara/) byla sice navržena pro analýzu malwaru, ale lze ji použít k vyhledávání jakéhokoli typu souborů.

2.3 Práce se zdroji dat

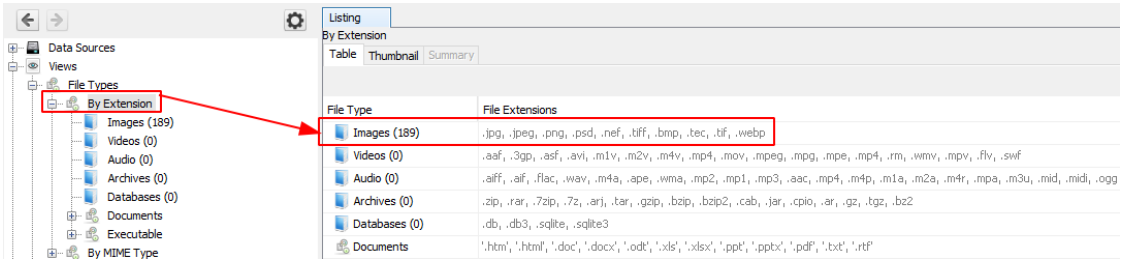
Informace o zdroji dat zobrazují základní metadata ve stromové struktuře. Jejich podrobná analýza je zobrazena ve spodní části. Lze jej extrahovat jeden po druhém shora dolů ve sloupci na levé straně obrazovky. V horní části stromu jsou *Views* (pohledy) vhodné pro přehledové prohlížení, v dolní *Results*, *Tags* a *Reports*. V dolní části jsou *Results* ve kterých získáváme informace o obsahu, který byl extrahován. Nakonec jsou *Tags* a *Reports* (hlášení).

Views tvoří *File Types* (typy souboru), *Deleted Files* (smazané soubory) a *MB FileSize* – viz obr. 2.3.1.



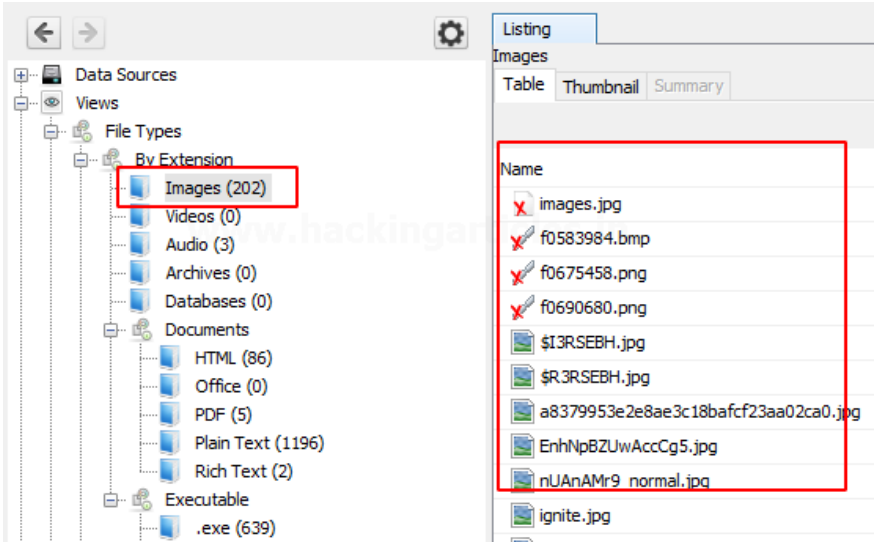
Obr. 2.3.1 Informace o zdroji dat (*Data Sources*) obsahují některé formy náhledů na metadata.

File Types mohou být tří kategorií: *By Extensions*, *Documents* a *Executable*. Kategorie *By Extensions* je rozdělena na *Images*, *Videos*, *Audio*, *Archives*, Databases – viz Obr. 2.3.2.



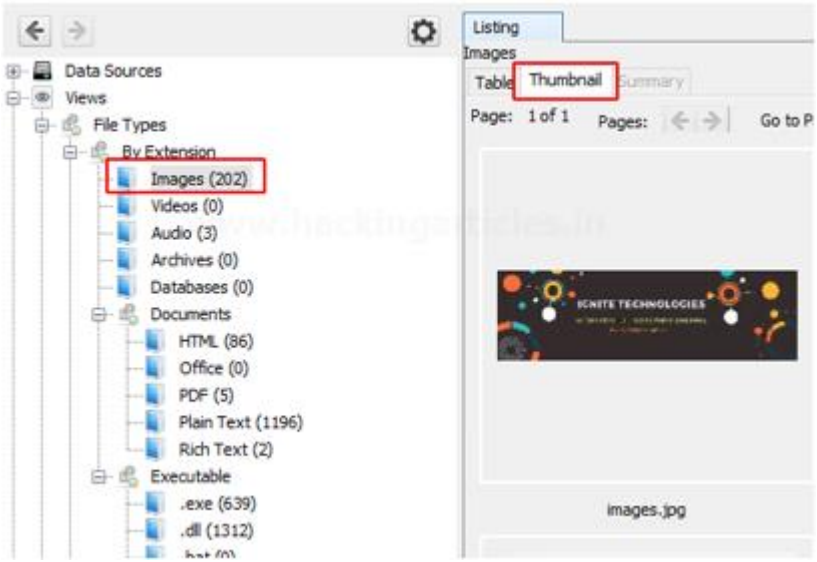
Obr. 2.3.2 Rozdělení kategorie *By Extensions*.

Klikněme na obrázky a prozkoumejme obrázky, které byly obnoveny – Obr. 2.3.3.



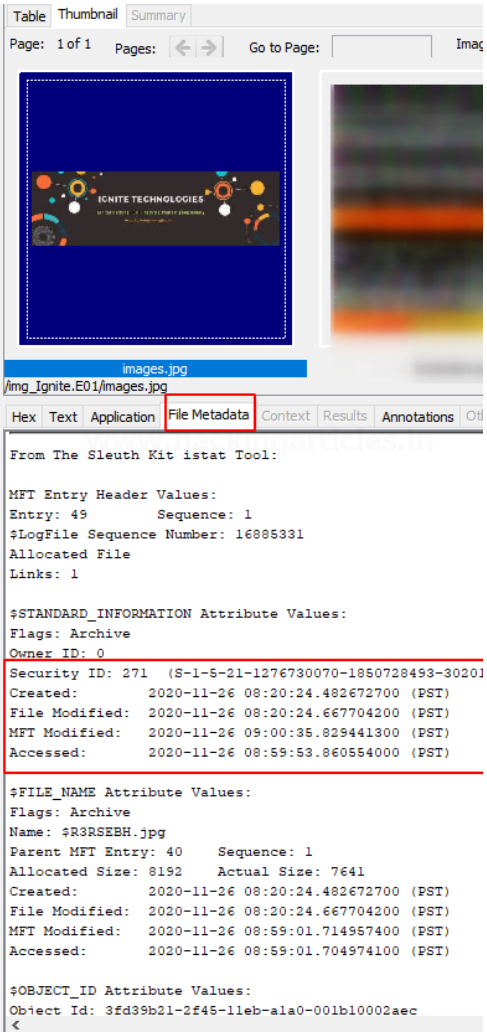
Obr. 2.3.3 Obnovené obrázky.

Lze si také prohlédnout náhledy (*Thumbnail*) obrázků – obr. 2.3.4.



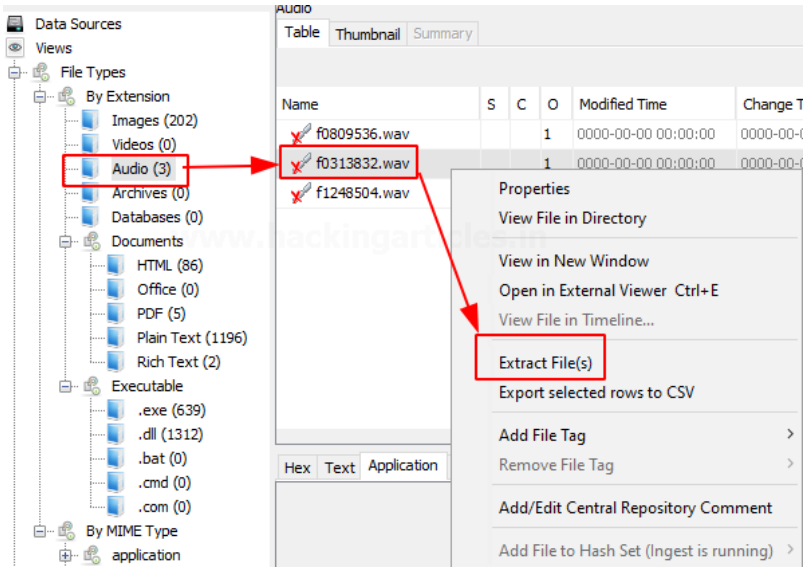
Obr. 2.3.4 *Thumbnail* (náhledy) obrázků

Při zobrazení náhledu lze zobrazit metadata souboru a podrobnosti o obrázku – Obr. 2.3.5.



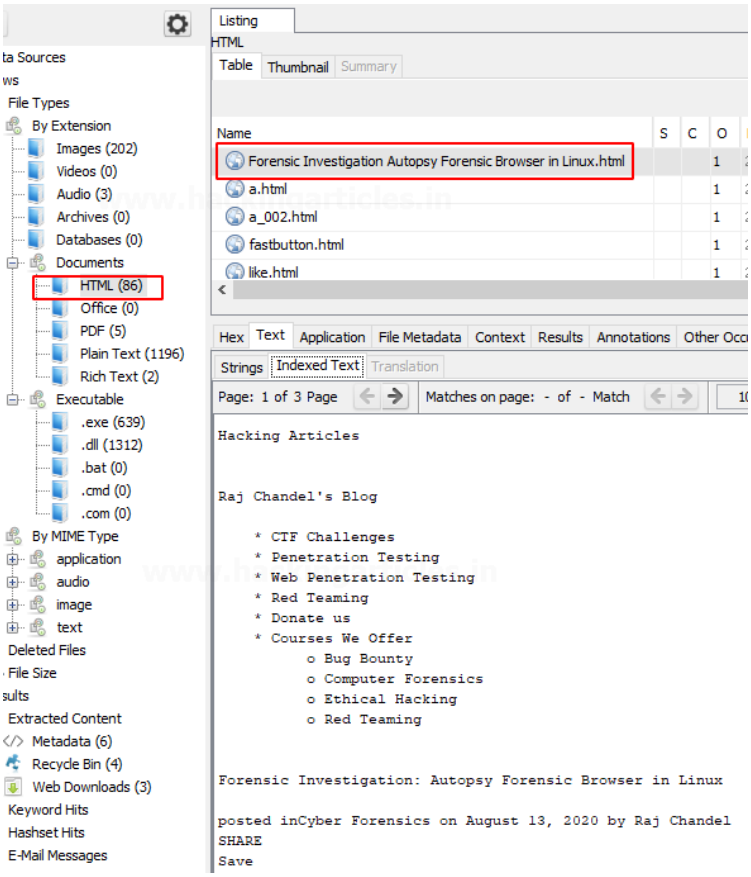
Obr. 2.3.5 Zobrazení metadat souboru a podrobnosti o obrázku

Můžeme také zobrazit několik zvukových souborů, které byly obnoveny. Tyto soubory lze extrahovat ze systému – Obr. 2.3.6 – a slyšet je pomocí různého softwaru.



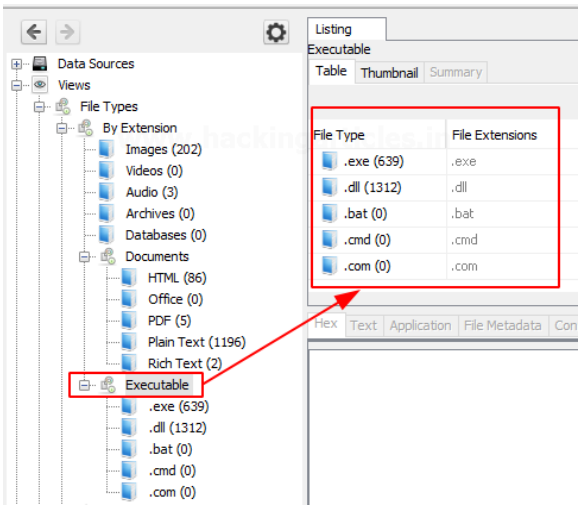
Obr. 2.3.6 Zobrazení zvukových souborů

Dokumenty jsou rozděleny do pěti typů: *HTML*, *Office*, *PDF*, *Plain Text*, *Rich Text*. Při prohlížení dokumentů lze vidět všechny přítomné HTML dokumenty s pak lze kliknout na ty důležité a zobrazit si je – viz Obr. 2.3.7.



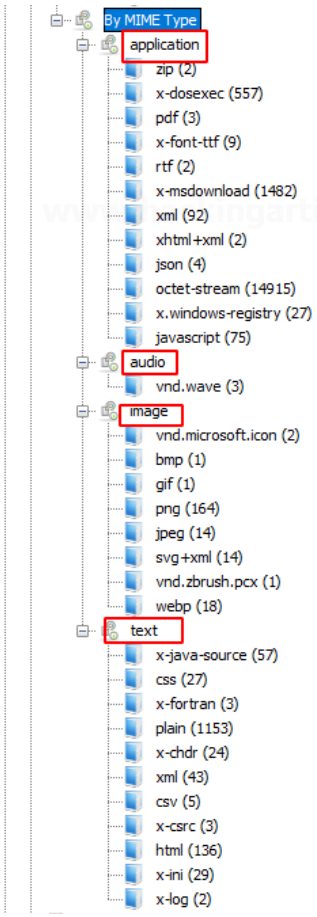
Obr. 2.3.7 Prohlížení HTML dokumentů

Podobně lze také prohlížet různé soubory ve formátu prostého textu (*Plain Text*). Lze také obnovit smazané soubory ve formátu prostého textu anebo formátu *Rich Text* (RTF). Typy souborů *Executable* jsou pak dále rozděleny na .exe, .dll, .bat, .cmd a .com – příklad viz Obr. 2.3.8.



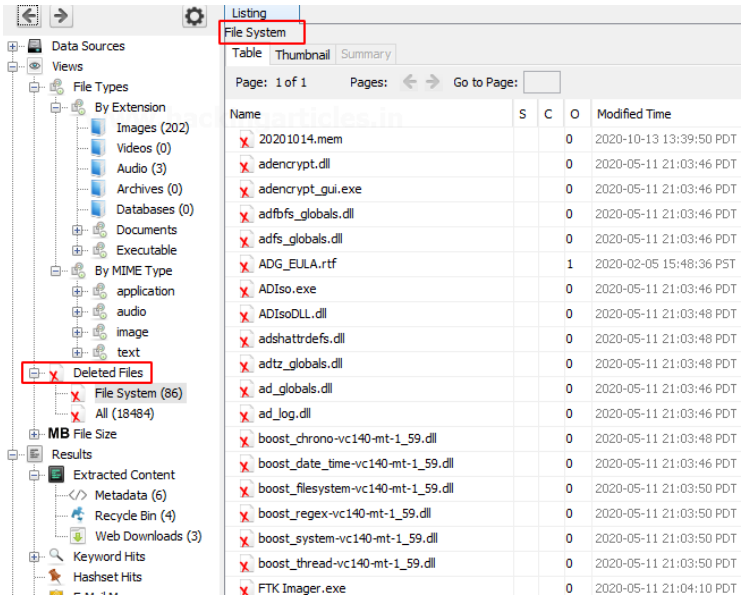
Obr. 2.3.8 Příklad prohlížení vykonavatelných souborů (typu *Executable*)

V typu *By MIME Type* existují čtyři podkategorie, jako je application, audio, image a text. Tyto podkategorie se dále dělí na více sekcí a typů souborů – viz obr. Obr. 2.3.9.



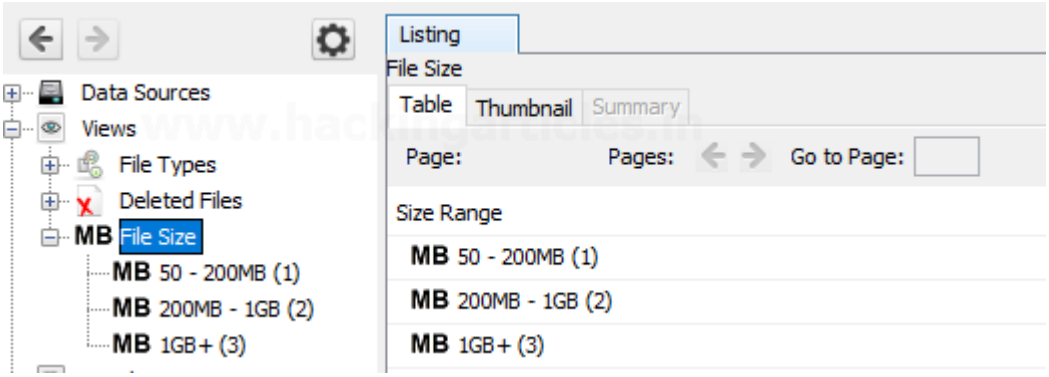
Obr. 2.3.9 Podkategorie typu *By MIME Type*

V typu *Deleted Files* **se z**obrazí informace o smazaném souboru, který lze poté obnovit – viz Obr. 2.3.10.



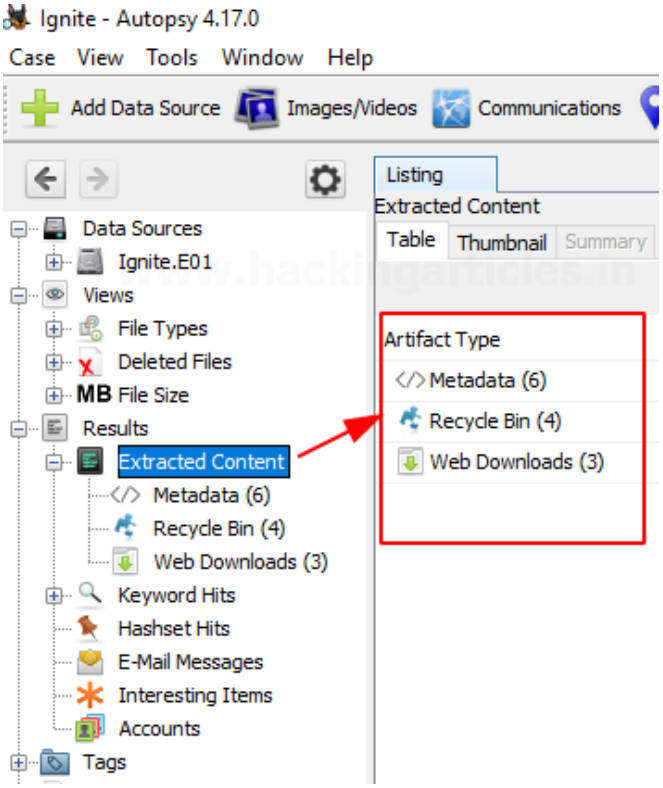
Obr. 2.3.10 Příklad zobrazení smazaných souborů

Pomocí typu *MB File Size* jsou soubory kategorizovány na základě jejich velikosti počínaje 50 MB – viz Obr. 2.3.11. To umožňuje vyšetřovateli hledat velké soubory.



Obr. 2.3.11 Kategorizace souborů na základě velikosti

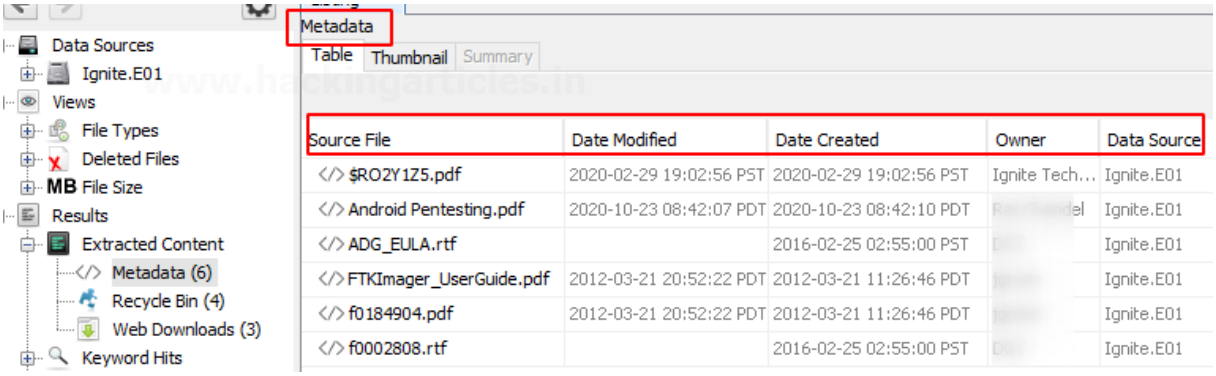
Typ *Results* tvoří *Extracted Content* (extrahovaný obsah), neboli artefakt[9]. Veškerý obsah, který byl extrahován, je dále podrobně segregován. Jsou zde *Metadata*, *Recycle Bin* (koš) a *Web Downloads* – viz Obr. 2.3.12.



Obr. 2.3.12 Zobrazení artefaktů

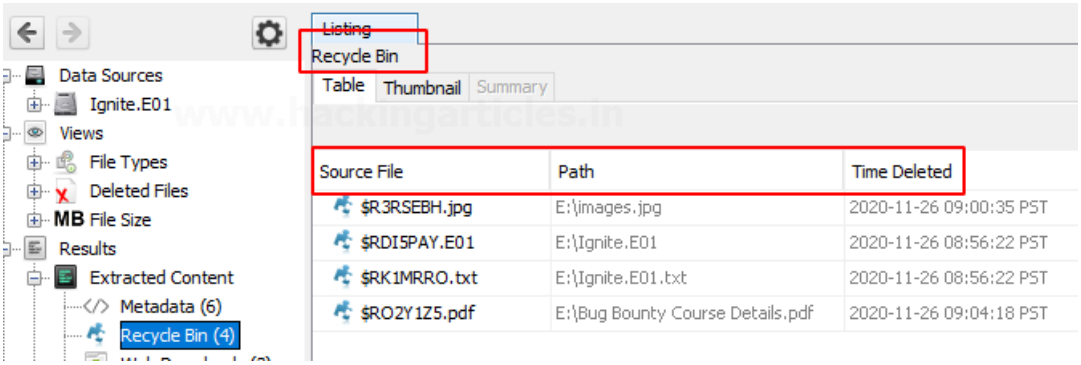
Pomocí metadat můžeme zobrazit všechny informace o souborech, jako je datum modifikace, úprava, vlastník souboru atd. – viz obr. Obr. 2.3.13. Soubory, které byly vloženy do koše zobrazuje Obr. 2.3.14, soubory, které byly staženy z internetu, zachycuje Obr. 2.3.15.

[9] Artefakt je dle Wikipedie jedním z mnoha druhů hmotných vedlejších produktů vzniklých během vývoje softwaru. Některé artefakty pomáhají popsat funkci, architekturu a design softwaru. Další artefakty se týkají samotného procesu vývoje – jako jsou projektové plány, obchodní případy a hodnocení rizik.



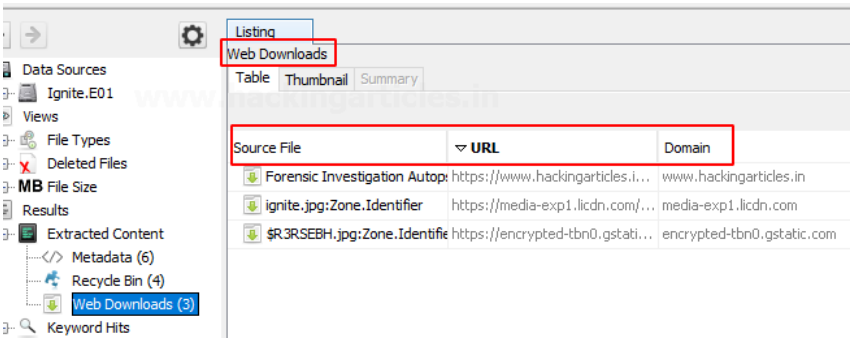
Obr. 2.3.13 Zobrazení tabulky metadat

Recycle Bin se nacházejí v seznamu *Extracted Content* pod Metadaty.



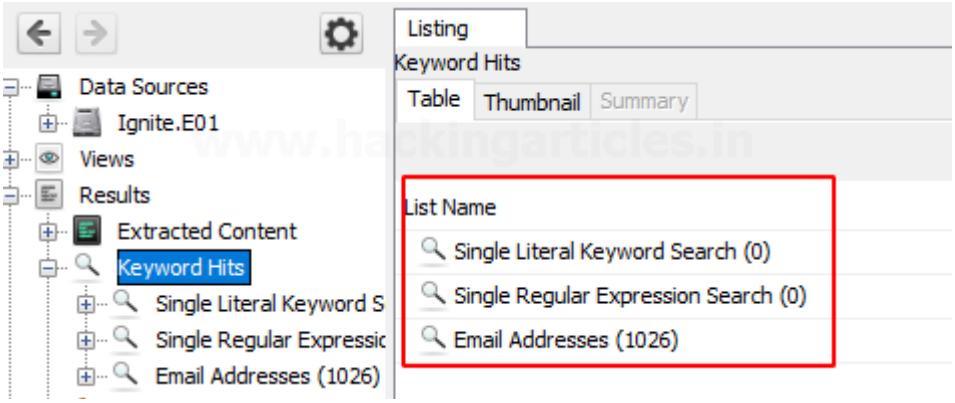
Obr. 2.3.14 Zobrazení smazaných souborů

Web Downloads: Zde vidíte soubory, které byly staženy z internetu.

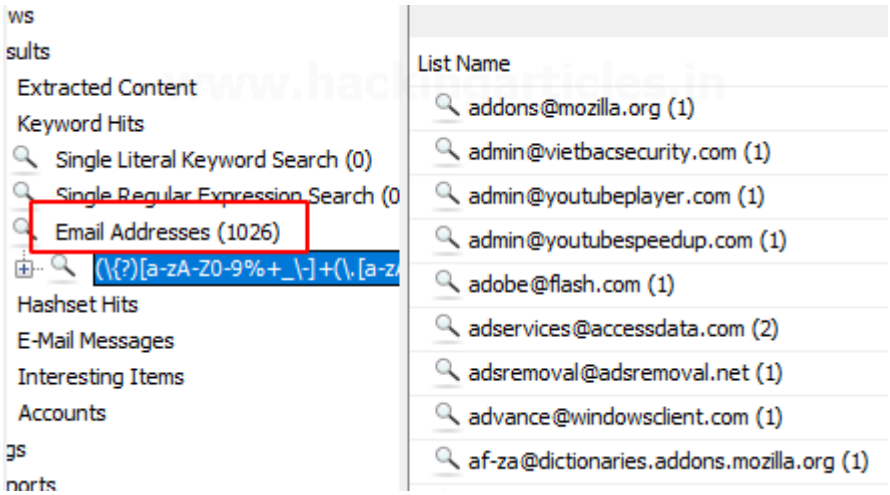


Obr. 2.3.15 Příklad souborů stažených z internetu

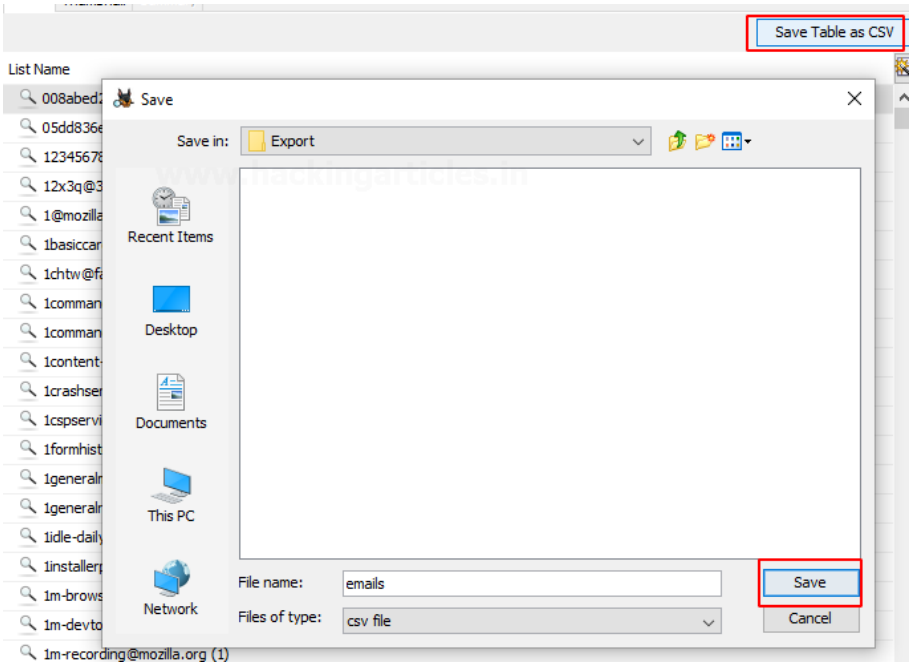
Pomocí typu *Keyword Hints* – Obr. 2.3.16 – lze v obrazu disku vyhledat jakákoli konkrétní klíčová slova. Vyhledávání lze provádět s ohledem na přesnou shodu, shodu podřetězců, e-maily, doslovná slova, regulární výrazy atd. Lze také zobrazit dostupné e-mailové adresy – Obr. 2.3.17. Tabulku údajů lze exportovat do formátu CSV – Obr. 2.3.18.



Obr. 2.3.16 Hledání konkrétních klíčových slov

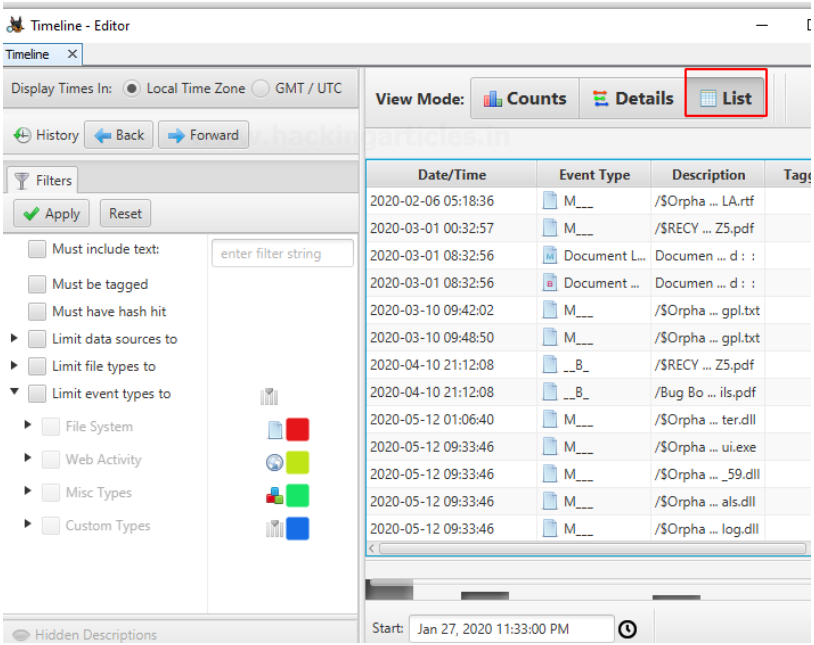


Obr. 2.3.17 Zobrazení dostupných e-mailových adres



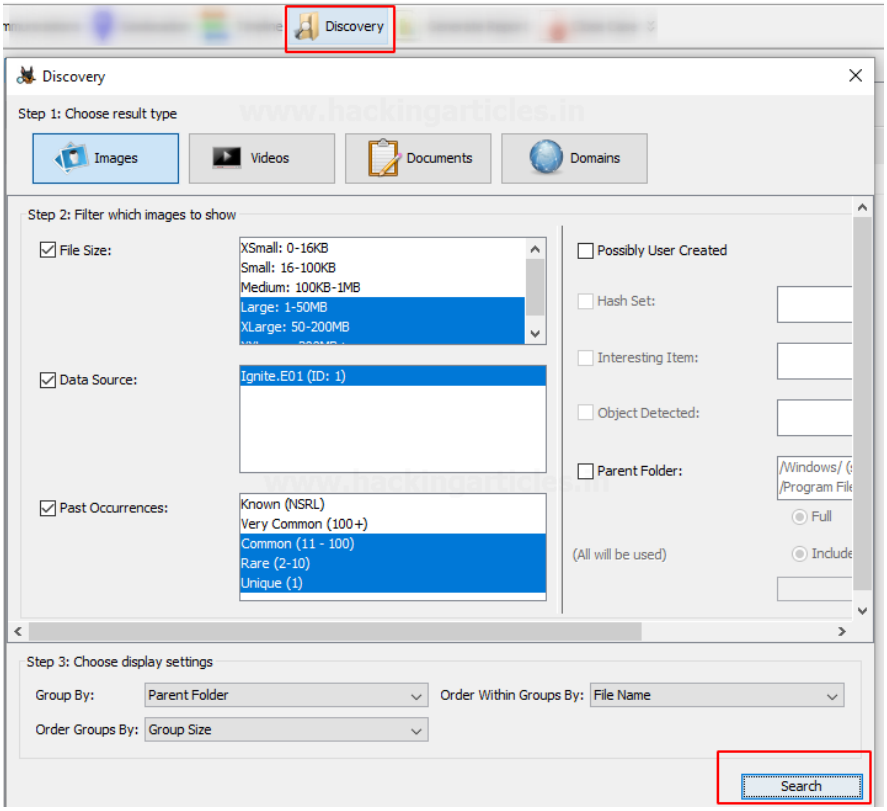
Obr. 2.3.18 Export tabulky údajů do formátu CSV

Pomocí funkce Timeline (časová osa) lze získat informace o využití systému ve statistické, podrobné nebo seznamové podobě (nejběžnější) – viz Obr. 2.3.19.

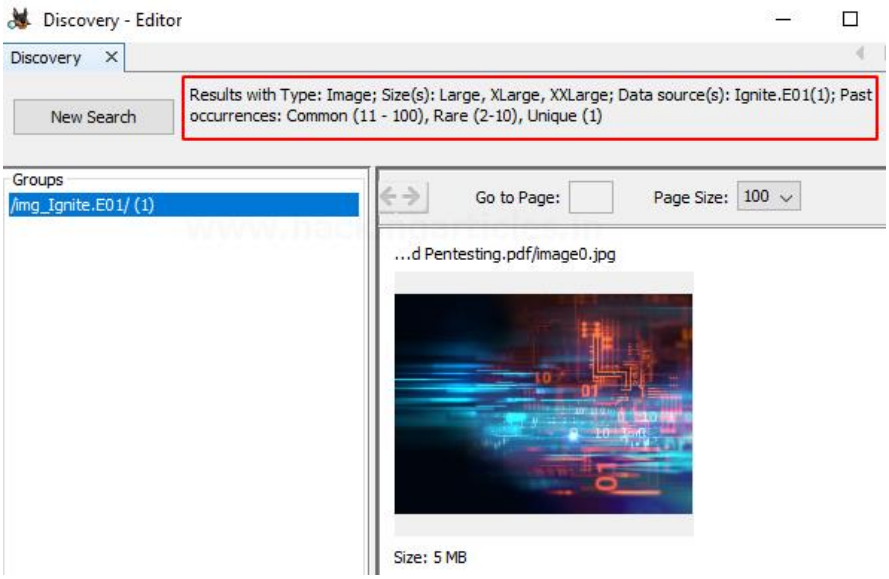


Obr. 2.3.19 Zobrazení časové osy v módu List (seznam)

Vyhledání média lze provést pomocí různých filtrů, které jsou přítomny v obrazu disku. Tato možnost umožňuje volba *Discovery* – viz Obr. 2.3.20. Podle zvolených možností lze získat požadované výsledky – Obr. 2.3.21. Lze rovněž vyhledávat obrázky a videa prostřednictvím různých možností a více kategorií – příklad viz Obr. 2.3.22.

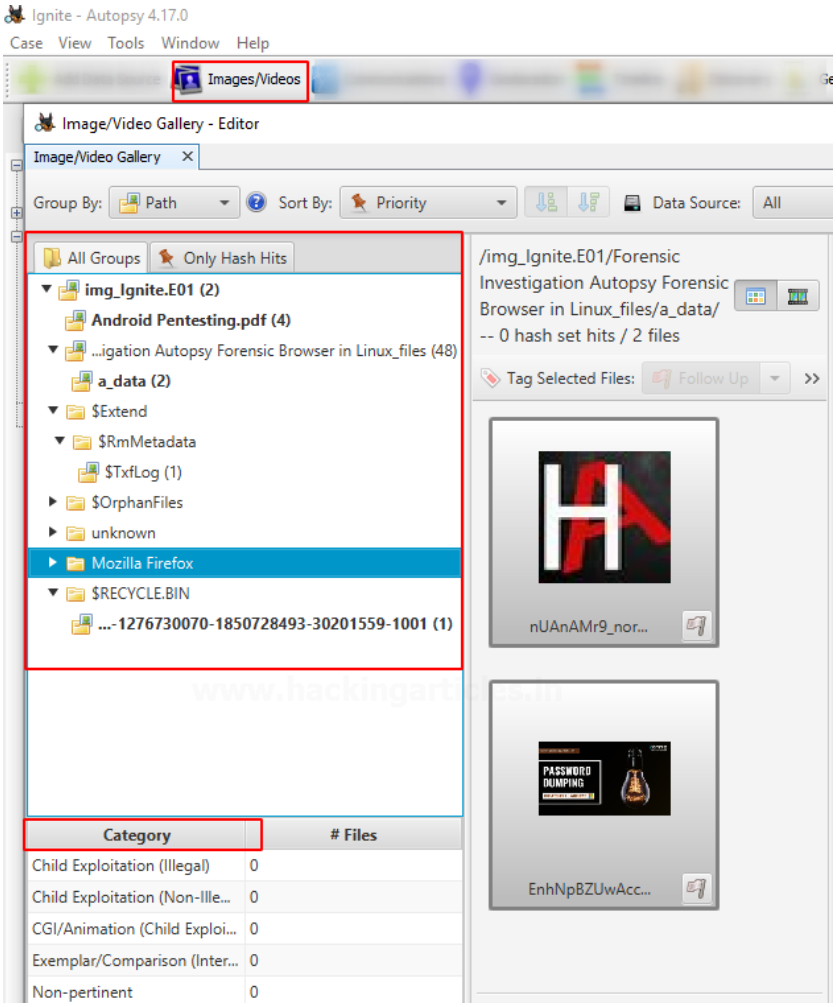


Obr. 2.3.20 Příklad hledání obrázků dané velikosti z daného zdroje pomocí volby *Discovery*.



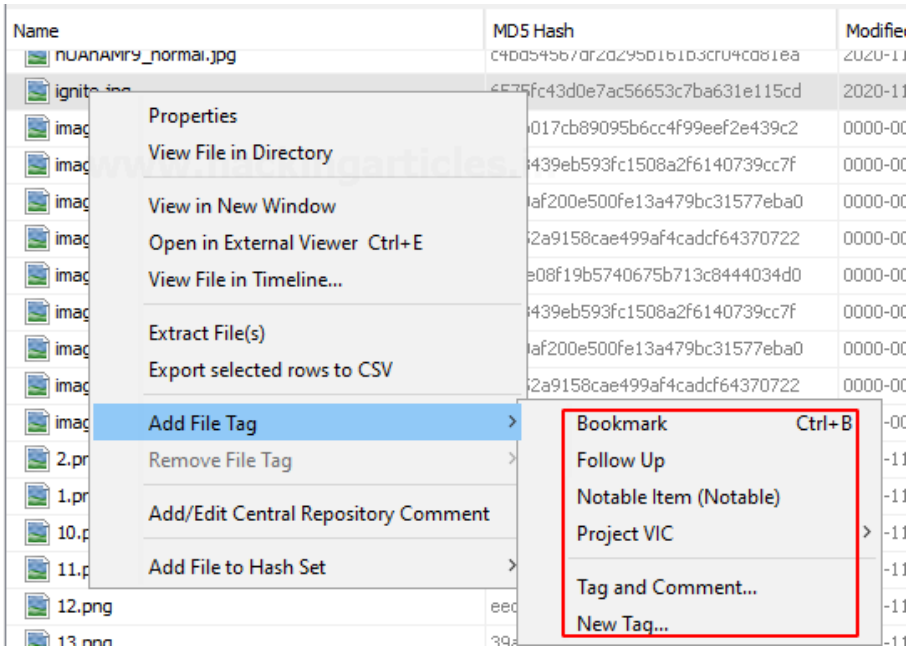
Obr. 2.3.21 Výsledek hledání

Obrázky hledáme pod *Images/Videos*.



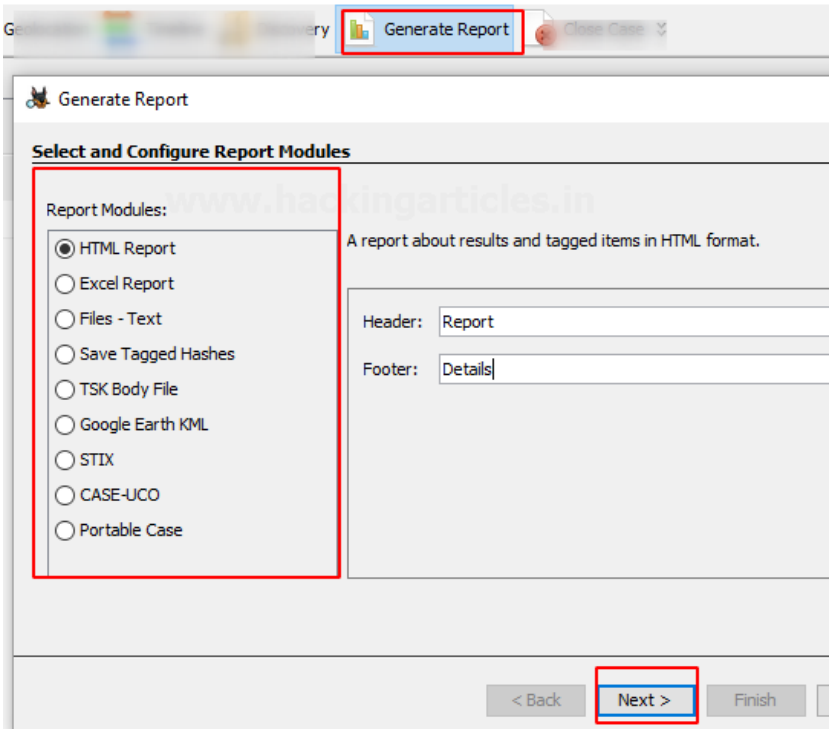
Obr. 2.3.22 Jiný způsob hledání souboru

K vytvoření záložek pro sledování zajímavých položek lze použít Tagy (přidání značky souboru) – Obr. 2.3.23.



Obr. 2.3.23 Přidání značky/záložky vhodného typu

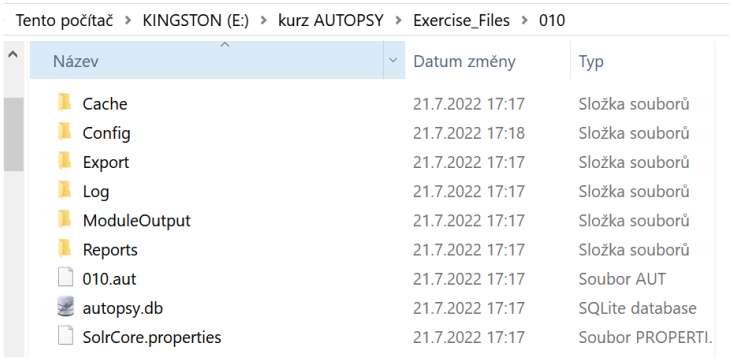
Po dokončení vyšetřování může zkoušející vygenerovat zprávu resp. report v různých formátech podle svých preferencí – viz Obr. 2.3.24.



Obr. 2.3.24 Příklad vygenerování hlášení v HTML tvaru

2.4 Prohlížení logů případů a výstup

Chcete-li zobrazit výstup případů, přejdeme do nabídky *Tools* v pruhu nabídek. Přejdeme dolů do složky *Open Case Folder* – viz Obr. 2.4.1.



Obr. 2.4.1 Zobrazení výstupu případů

V adresáři nalezneme především tyto složky:

- *Export* – obsahuje všechny informace od exportovaných souborů.
- *Log* – umístění, které použité pro základní adresář. Alternativou by tedy bylo přejít na tuto cestu ručně.
- *ModuleOutput* – jediná věc, která obsahuje složky a soubory.
- *Reports* – existuje jednodušší způsob, který nevyžaduje více kroků. Lze přejít na Help v pruhu nabídek a potom se posunout dolů na Open Log. Tím se otevře stejná složka Log z předchozí obrazovky, ale vše je provedeno zhruba v jednom kroku.

3 Zadání úkolu

3.1 Instalace Autopsy

- Stáhněte soubor "Autopsy_workstation.ova" (~ 40 minut)
- Stáhněte VirtualBox kliknutím na horní lištu kolonky "Soubor" a "Importovat applianci" (~ 5 minut)
- Zapněte virtuálního počítač (Přihlášení) (~ 2 min)
- Instalujte VideoTriageModule-1.3 – rozděluje video soubor na snadno zobrazitelné miniatury (klíčové snímky) – 45 573 Kb (~ 10 minut)
- Hotovo (Celkem: ~47 minut)

Seznam použitých zdrojů

(Hendrix 2022) Bennett Hendrix. Learning Autopsy for Digital Forensics. LinkedIn course Feb 2022. Dostupné z: https://www.linkedin.com/learning/learning-autopsy-for-digital-forensics

(Vaghela 2020) VAGHELA, Vishva. Comprehensive Guide on Autopsy Tool (Windows). Hacking Articles. December 14, 2020. Dostupné z: https://www.hackingarticles.in/comprehensive-guide-on-autopsy-tool-windows/