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

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

TESTOVÁNÍ BEZPEČNOSTI

Autopsy pro vyhledávání artefaktů Windows

Metodický list

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

Recenzent: Ing. Vladimír Šulc Ph.D.

Rok vydání: 2023

Obsah

Cíle

Naučit se pracovat s free nástrojem Autopsy s profesionálními vlastnostmi pro forenzní analýzu artefaktů. Scénář navazuje na scénář „Základní seznámení s Autopsy“.

Dovednosti

Uvedení všech dovednosti, které by si žáci měli v rámci této úlohy osvojit

- Vytvoření nového forenzního případu
- Orientace ve zdrojích dat pro forenzní šetření
- Práce s časovou osou vyšetřování
- Prohlížení logů
- Zpracování výsledné zprávy o vyšetřování

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.

Časové kalkulace instalace Autopsy v prostředí Cylab JCEKB

1. Stažení souboru "Autopsy_workstation.ova"

   ~ 40 minut

2. Stažení VirtualBoxu, kliknutí na horní lištu kolonky "Soubor" a "Importovat applianci"

   ~ 5 minut

3. Zapnutí virtuálního počítač (Přihlášení)

   ~ 2 min

4. Hotovo

   Celkem: ~47 minut

Lze ale využít nainstalovaného systému v rámci scénáře scénář „Základní seznámení s Autopsy“

Průběh výuky

1 Forenzní artefakty systému Windows

Artefakty generované systémem Windows mohou zahrnovat několik aktivit, které lze číst jako systémové nebo uživatelské artefakty (ENISA 2013). Největší možnosti vyšetřovateli poskytují artefakty systému souborů, artefakty síťového sdílení, artefakty operačního systému, artefakty časového pásma, uživatelské účty a artefakty protokolů událostí Windows.

1.1 Artefakty souborového systému

Artefakty systému souborů obecně poskytují digitálnímu vyšetřovateli podrobnosti o odvozeném formátu souboru, svazku, vlastnostech souboru a oddílech pevného disku. Kromě toho informace, jako je typ systému souborů, historie volání, sériové číslo svazku, kapacita, informace o sektoru a clusteru a další známky související s případem vyšetřování.

Artefakty systému Windows obecně zahrnují několik vzorů dat a informací, které lze extrahovat ze systému souborů, informací o síti, podrobností o uživatelském účtu a vzorů odvozených z následujících artefaktů systému oken (plocha počítače, připnuté soubory, hiberfil.sys a pagefile.sys[1], Recycle Bin (odpadkový koš), registry, data aplikací, oblíbený a relevantní obsah, Swap soubory, Thumb cache[2], kořen třídy HKey (Hkey Class Root), soubory cookies, programové soubory, metadata, dokumenty, poslední složka (naposledy použitá), body obnovení, Print Spooler, logo, Nabídka Start, seznamy odkazů a kořenová uživatelská složka

Oprávnění přístupu jsou velmi důležité při soudním vyšetřování. Vyšetřovatel si proto musí být vědomi právních problémů spojených s přístupovými oprávněními. Z technického hlediska by se digitální vyšetřovatel měl dozvědět o konfiguraci přístupu a jejím dopadu na proces vyšetřování.

1.2 Artefakty síťového sdílení

Digitální forenzní vyšetřovatelé mohou získat informace o síťovém sdílení a použít je jako silný důkaz. Informace, které lze získat z umístění registru, jako jsou soubory .REG a podregistr registru, mohou využít k obnovení mnoha síťově sdílených připojených dat uživatelem. Ve většině případů však forenzní vyšetřovatel potřebuje používat forenzní nástroje. Například poskytnutím relevantních síťových sdílení digitálním vyšetřovatelům pro každého uživatele sítě mohou odhalené informace podporovat další zdroje potenciálních důkazů, které mohou být uloženy v jiném systému v síti.

[1] pagefile.sys je swapovací soubor, takže leda ho vypnout (nedoporučuji), nebo ho změnit na nižší hodnotu.hiberfil.sys je soubor režimu spánku

[2] ThumbCache je funkce v operačních systémech Windows dostupná počínaje Windows Vista, která se používá k ukládání miniatur obrázků souborů do mezipaměti pro zobrazení Průzkumníka Windows. Když otevřete Průzkumníka Windows v zobrazení miniatur, soubory ve složce se zobrazí jako malé obrázky, které představují obsah souborů.

1.3 Artefakty operačního systému

Podrobnosti získané z použitého operačního systému jsou pro digitální vyšetřovatele obrovským zájmem, aby mohly být použity jako důkaz, jako je verze systému, ID produktu a klíče, aktualizace service pack, časová razítka a další tisky pro používaný operační systém. Význam artefaktů operačního systému je prezentovat podrobnosti o tom, co se přesně děje v systému, stejně jako o aktivitě uživatele.

Existuje řada cenných scénářů, které lze vzít v úvahu z několika stop systému, například když byl systém jednoduše vypnut nebo odpojen. Nejzajímavější jsou však následující systémové artefakty: datum instalace systému, čas vypnutí, časová osa událostí, čas posledního přihlášení, kdy byl naposledy systém vypnut, datum instalace systému.

1.4 Informační artefakty časového pásma

Registr Windows ukládá informace o časovém pásmu a řadu časových razítek v místním i UTC čase. Pro forenzního vyšetřovatele je životně důležité, aby hluboce porozuměl vztahu mezi razítky a systémovými událostmi a jak souvisejí s formátem místního času a času UTC. Vyšetřovatel může například použít časové razítko k určení správného pořadí uživatelských událostí, a tudíž určit posloupnost událostí.

Obecně jsou informace o časovém pásmu uloženy v SYSTEM HIVE nebo obrazu systému, nicméně forenzní vyšetřovatel musí používat vyspělé forenzní nástroje, jako je Autopsy[3], aby mohl zobrazit časová razítka ve vztahu k časové ose incidentů nebo forenzním událostem.

1.5 Artefakty uživatelských účtů

Informace o uživatelských účtech jsou uloženy v podregistru, ve kterém budeme moci vypsat všechny výchozí systémové účty a účty vytvořené uživateli. Pomocí forenzních specializovaných nástrojů, jako je Autopsy, mohou digitální vyšetřovatelé získat zajímavé informace o uživatelských účtech, jako jsou: název účtu, typ účtu, skupiny účtů, přihlášení k účtu a poslední přihlášení, zakázané účty, hesla a časová razítka, nesprávná přihlášení a uživatelé domény.

Tyto informace mohou být velkou hodnotou pro digitálního vyšetřovatele při hledání jakéhokoli druhu vniknutí do nastavení uživatelského účtu.

1.6 Artefakty protokolů událostí systému Windows

Protokoly událostí systému Windows ukládají spoustu informací o systému a jeho uživatelích. Tyto informace však lze získat s ohledem na úroveň protokolování (tj. místní vs. síť) a verzi nainstalovaného systému Windows. Artefakty protokolů událostí systému Windows mohou poskytnout digitálním zkoušejícím následující základní podrobnosti o artefaktech: administrativní akce a jejich relevantní systémová razítka zájmu, aplikační a servisní deníky, záznamy o úspěchu a neúspěchu, bezpečnostní protokoly, protokoly nastavení, předané protokoly událostí a protokoly subscripce.

[3] Autopsy umožňuje od verze 4.13.

Typicky může digitální vyšetřovatel vytáhnout tóny událostí z uložených okenních protokolů, ale zaměřit se musí pouze na ty, které mají přímý nebo nepřímý vztah k incidentu. Forenzní vyšetřovatel proto může potřebovat filtrovat tyto protokoly pomocí forenzních nástrojů, aby určil konkrétní aktivace a silný seznam důkazů.

V reálném světě musí forenzní vyšetřovatel korelovat činnost uživatele systému s běžnými systémovými aktivitami. To může zahrnovat uživatelská oprávnění, systémové podmínky použití, umístění a tak dále. Ačkoli se tento typ korelace zdá být odlišný, každá událost v počítačovém systému ve skutečnosti koreluje s konkrétní aktivitou uživatele. Ve skutečnosti záleží na typu uživatele a příslušném nastavení účtu. To znamená, že každá událost je výsledkem toho, zda se jeden konkrétní uživatel podílel nebo nepodílel na tom, co je evidentní a vhodně odpovídá forenznímu případu. Forenzní vyšetřovatel proto potřebuje prozkoumat konkrétní podrobnosti o činnosti uživatele, zjednodušit události a předložit podrobnosti o důkazech.

Zkoumání uživatelských aktivit pomocí artefaktů Windows zahrnuje charakteristiky, které se přímo vztahují k uživateli a dalším osobám spojeným se systémem. Následující seznam obsahuje základní artefakty, které kombinují artefakty zaměřené na systém i uživatele.

- Informace o souborovém systému a přímé odkazy na spustitelné soubory poskytující důkaz o tom, jak jsou data skutečně uložena a načtena v systému.
- Funkce seznamů odkazů umožňuje vyšetřovateli prohlížet poslední dokumenty v programu a rychle prezentovat nejnovější uživatelské události.
- Síťové sdílení informací pro sdílení zdrojů nebo umožnění přístupu k informacím prostřednictvím více než jednoho zařízení.
- Informace o operačním systému poskytující jasné informace o schopnostech systému.
- Shellbags (klíče registru) a položky při spuštění, abyste mohli využít nastavení registru. Tyto klíče jsou užitečné pro forenzního vyšetřovatele, aby přesně určili, která složka byla použita, a hluboce analyzovali, co se přesně dělo.
- Informace o časovém pásmu k identifikaci informací o časovém pásmu na podezřelém počítači, o vyšetřování historie zařízení USB, o uživatelských účtech k identifikaci podrobností, o smazaných uživatelských účtech a k určení, kdo se přihlásil do systému.
- Protokoly událostí systému Windows a soubory předběžného načtení systému Windows k určení, které aplikace byly spuštěny v počítači, a ke shromažďování cenných dat o historii aplikací uživatele.

Digitální vyšetřovatel může použít přímo systémem extrahované artefakty z operačního systému Windows nebo použít specifické forenzní nástroje pro stejný účel. Forenzní nástroje pomáhají vyšetřovatelům získat úplný přehled o podrobnostech o systému a jeho uživatelích. Celkově může digitální vyšetřovatel odvodit spoustu informací o uživatelích a aktivitách systému s odkazem na výše uvedené artefakty. Digitální vyšetřovatel proto musí shromáždit a konsolidovat shromážděná data a informace, aby poskytl jasnou platformu o forenzním případu. Jako takový by byl vyšetřovatel schopen předložit silný a úplný obraz forenzních důkazů.

2 Hledání artefaktů v Autopsy

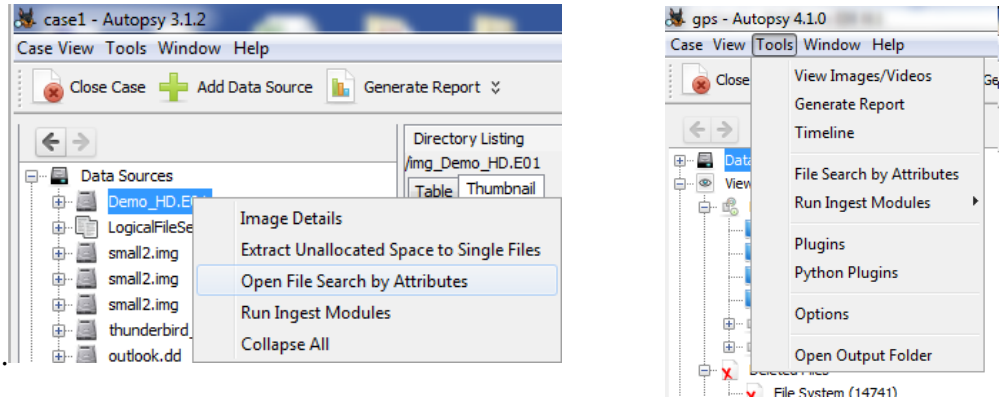
2.1 Artefakty souborového systému

K nástroji File Search lze přistupovat buď z nabídky Tools, nebo kliknutím pravým tlačítkem myši na uzel zdroje dat v Data Explorer / Directory Tree. Pomocí vyhledávání souborů můžete určit, filtrovat a zobrazit adresáře a soubory, které chcete vidět z obrázků v aktuálně otevřeném případě. Výsledky vyhledávání souborů se vyplní ve zcela novém prohlížeči výsledků tabulky na pravé straně.

Poznámka: Vyhledávání souborů v současné době nepodporuje regulární výrazy. Funkce vyhledávání klíčových slov (Key Search) aplikace Autopsy podporuje regulární výrazy a lze ji použít pro vyhledávání souborů a/nebo adresářů podle názvu.

2.1.1 Jak otevřít hledání souborů

Chcete-li otevřít vyhledávání souborů (File Search), můžete provést jednu z následujících věcí: Klepněte pravým tlačítkem na zdroj dat a vyberte „Open File Search by Attributes“ nebo vyberte „Tools“, "File Search by Attributes" (Obr. 2.1.1.)



Obr. 2.1.1.1 Dva možné způsoby otevření souboru.

2.1.2 Jak použít vyhledávání souborů

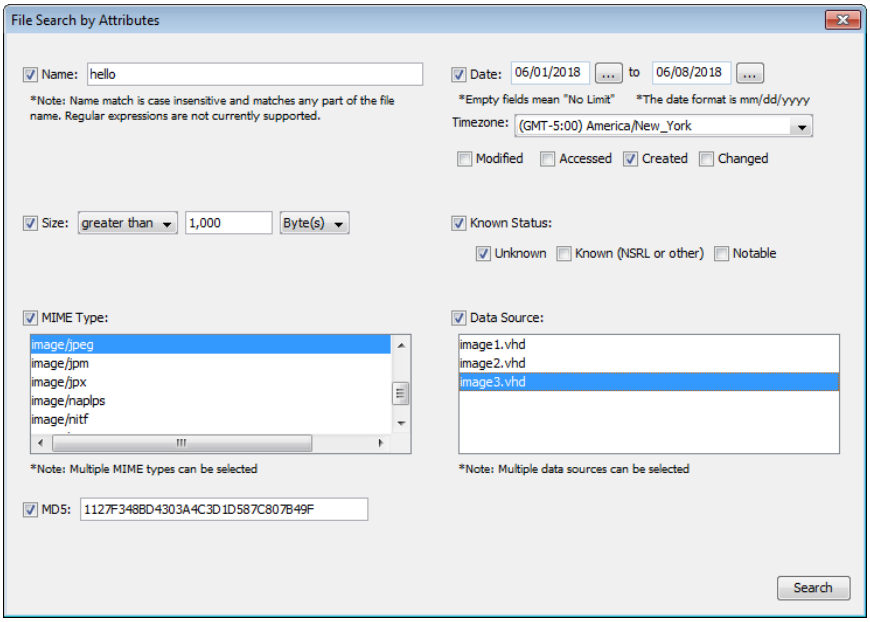
Existuje několik kategorií, které můžete použít k filtrování a zobrazení adresářů a souborů v obrázcích v aktuálně otevřeném případě. Kategorie jsou:

- *Název*: Vyhledejte všechny soubory a adresář, jejichž název obsahuje daný vzor. Poznámka: Nepodporuje regulární výrazy a shodu klíčových slov.
- *Velikost*: Vyhledá všechny soubory a adresáře, jejichž velikost odpovídá danému vzoru. Vzor může být „rovná se“, „greater than“ a „less than“. Jednotkou velikosti může být Byte(y), KB, MB, GB a TB.
- *Typ MIME*: Vyhledá všechny soubory s vybraným typem MIME. Více typů lze použít podržením SHIFT nebo CTRL při výběru.

- *MD5*: Vyhledá všechny soubory s daným hashem MD5.
- *Datum*: Vyhledejte všechny soubory a adresáře, jejichž „date property“ je v daném časovém rozmezí. „Date property“ jsou „Modified Date“, „Accessed Date“, „Changed Date“, a „Created Date“. Musíte také zadat časové pásmo pro dané datum.
- *Známý stav*: Vyhledejte všechny soubory a adresáře, jejichž známý stav je rozpoznán jako Unknown, Known, nebo Known Bad. Další informace o známém stavu najdete v modulu pro vyhledávání hashů. Chcete-li použít některý z těchto filtrů, zaškrtněte políčko vedle kategorie a kliknutím na tlačítko „Find“ spusťte proces vyhledávání. Výsledek se zobrazí v " Result Viewer".

Zdroj dat: Hledat pouze v rámci zadaného zdroje dat namísto celého případu. Všimněte si, že více zdrojů dat lze vybrat podržením SHIFT nebo CTRL při výběru.

Zde je vymyšlený příklad, kdy se snažíme získat všechny adresáře a soubory, jejichž název obsahuje „hello“, má velikost větší než 1000 bajtů, je ve formátu JPEG, byl vytvořen mezi 6. 1. 2018 a 6. 8. 2017 (v GMT-5 timezone), je neznámý soubor, má hash 1127F348BD4303A4C3D1D587C807B49F a objevuje se ve zdroji dat „image3.vhd“:



2.2 Artefakty síťového sdílení

Autopsy je schopno pracovat v klusteru, ke kterému mohou přistupovat jeho klienti Autopsy a server Solr[4]. Toto sdílené úložiště bude použito pro zdroje dat i výstupy případu, takže bude zapotřebí spousta místa. Konkrétní konfigurace sdíleného úložiště bude záviset na tom, jaký typ sdílení souborů je k dispozici. Může být sdílení souborů ve Windows, Linux Sambě nebo NAS využívajícím FibreChannel. Pro daný typ laboratoří jde o příliš náročnou kategorii artefaktů.

[4] Solr je platforma pro vyhledávání v textu, včetně fasetového vyhledávání, distribuovaného vyhledávání a vyhledávání v dokumentech typu PDF nebo ODT. Jedná se o svobodný software dostupný pod licencí Apache License, který je napsaný v Javě.

2.3 Artefakty operačního systému

Prohledání artefaktů operačního systému i událostí nejlépe zabezpečí klíčová časová osa – Timeline.

Funkce časové osy může pomoci odpovědět na otázky, jako jsou tyto:

- Kdy došlo v systému k velké webové aktivitě?
- Kdy byla externí zařízení zapojena do systému?
- Kdy byly přidány obrázky s informacemi EXIF?
- Jaké webové stránky byly navštíveny, které vedly k úpravám souborového systému bezprostředně poté?

Chcete-li otevřít časovou osu, použijte tlačítko „Timeline“ nebo přejděte v nabídce na „Tools“ a poté na „Timeline“. Během zpracování obrázku můžete otevřít časovou osu, ale data nebudou kompletní, dokud nebude dokončena. Časová osa začne v zobrazení *count view* s grafem zobrazujícím počet událostí v každém časovém období.

Kliknutím na jeden ze segmentů grafu zobrazíte seznam událostí vlevo dole. Kliknutím na jednotlivou událost se v pravé dolní části zobrazí podrobnosti. Režim zobrazení můžete změnit pomocí tlačítek v horní střední části okna. Druhý režim zobrazení, zobrazení *detail view*, zobrazuje informace o událostech, které se staly v určitém časovém období. Tento režim se nejlépe používá po odfiltrování na malé časové okno.

Posledním režimem zobrazení je zobrazení *list views*. Toto zobrazení zobrazuje každou událost v pořadí, v jakém se vyskytla. To může být užitečné, abyste viděli, které další události se staly ve stejném časovém rámci jako událost zájmu. Stejně jako u režimu podrobností se tento režim nejlépe používá s filtry ke snížení počtu zobrazených událostí.

2.4 Artefakt časového pásma

Uživatel si může vybrat mezi zobrazením událostí v místním časovém pásmu nebo v univerzálním koordinovaném čase.

2.5 Artefakty uživatelských účtů

Uživatelský účet, pod kterým Autopsy běží, bude potřebovat přístup ke sdílenému úložišti. Existují tři obecné možnosti:

- *Doménové účty*: Pokud je cluster v doméně Windows, lze Autopsy spustit pomocí doménového účtu.
- *Jedinečné místní účty*: Některé clustery nejsou v doméně Windows a mají jedinečné účty pro každého analytika/uživatele.
- *Sdílený místní účet*: A konečně, některé clustery používají jeden místní účet.

2.6 Artefakty protokolů událostí

Nástroj časové osy timeline je uspořádán podle událostí. Událost má časové razítko, typ a popis. Poznámka: Všechny události jsou samostatné, ale mohou být seskupeny do shluků s délkou trvání v zobrazení podrobností v závislosti na úrovni popisu, která je povolena v uživatelském rozhraní.

Časová osa shromažďuje data z více zdrojů a organizuje události do následující taxonomie:

- *Souborový systém* – Modified, Access, Created, Changed
- *Aktivita webu* – Web Downloads, Web Cookies, Web Bookmarks (creation), Web History, Web Searches, Web Form Auto Fill,Web Form Address
- *Různé* – Messages, GPS Routes, Location History, Calls, Email, Recent Documents, Installed Programs, Exif metadata, Devices Attached, Log Entry, Registry

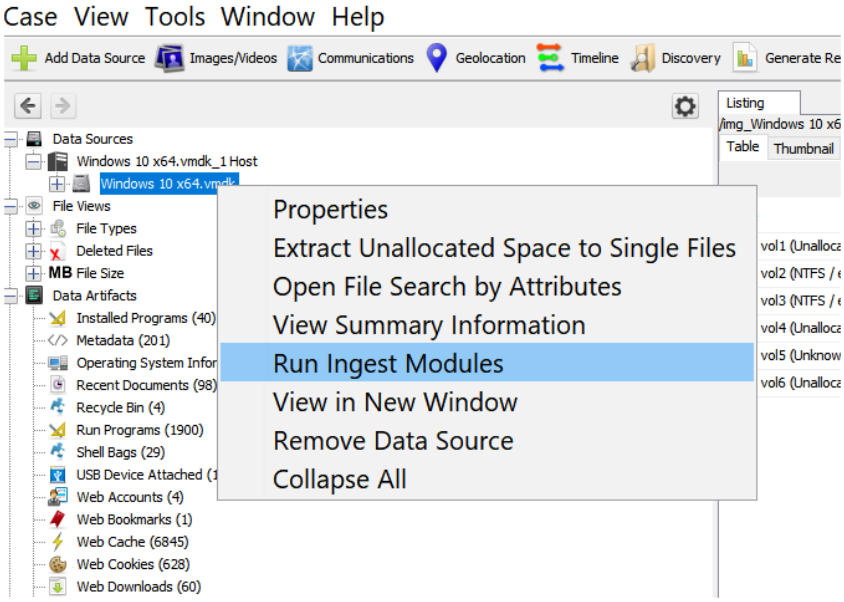
3 Praktická práce

3.1 Moduly Ingest

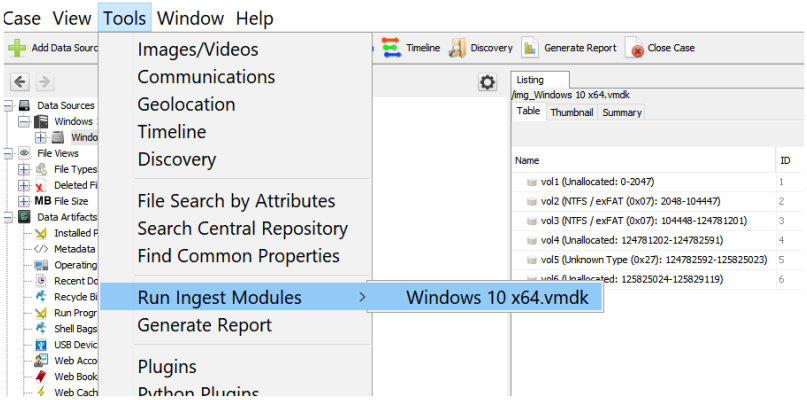
3.1.1 Využití automatizované analýzy

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.

1. První je v defaultním (výchozím) nastavení, což je bezprostředně po přidání zdroje dat.
2. Za druhé, kliknutím pravým tlačítkem na zdroje dat (Data Sources) ze stromu v hlavním rozhraní a výběrem *Tools*, *Run Ingest Modules* (Spustit modul příjmu). Tento proces se zobrazí na obrazovce a použije se, pokud se rozhodnete analyzovat data, která jste dříve nezahrnuli – – viz Obr. 3.1.1.1.
3. Nakonec můžete přejít na *Tools*, Run *Ingest Modules* a zde budete mít zdroje dat (např. Dropbox) – viz Obr. 3.1.1.2.

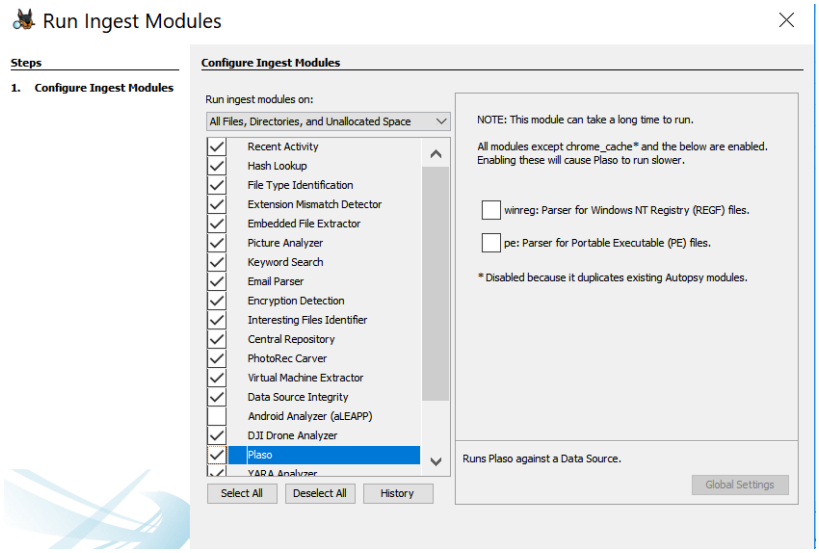


Obr. 3.3.1.1 Spuštění modulu *Ingest* ze stromu v hlavním rozhraní přes *Data Sources*



Obr. 3.3.1.2 Spuštění modulu *Ingest* z karty *Tools*

Při konfiguraci v modulech *Ingest* se vám zobrazí rozhraní pro výběr souborů, které chcete analyzovat, a povolení nebo zakázání pro každý modul – viz Obr. 3.1.1.3.



Obr. 3.1.1.3 Rozhraní pro výběr souborů v modulech *Ingest*

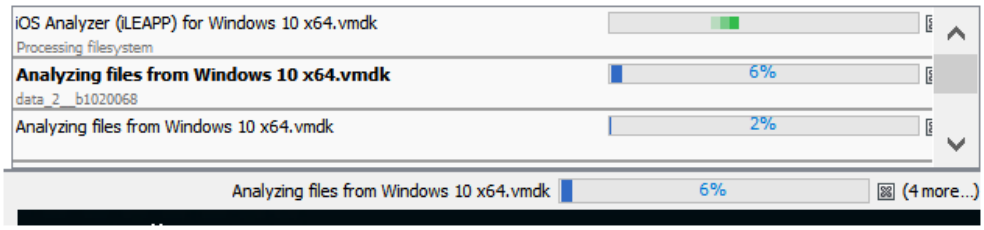
Například nemáme k dispozici obrázek z mobilního telefonu, takže nebudeme potřebovat modul analyzátoru Android (aLAPP). Pokud však později obdržíme tento důkaz jako součást jiného případu, můžeme pomocí tohoto procesu povolit, aby se modul spustil.

Pole výběru v horní části okna řídí, na kterých souborech poběží moduly *Ingest*. Obvykle necháme přednastavenou variantu *All Files, Directories, Unallocated Space*.

Nepřidělené místo (*Unallocated Space*) je oblast na pevném disku, kam lze ukládat nové soubory. To je důležité, protože některé soubory mohly být označeny ke smazání a mohou být pro vyšetřování zásadní. Takže nezahrnutí této možnosti může být pro vyšetřování škodlivé.

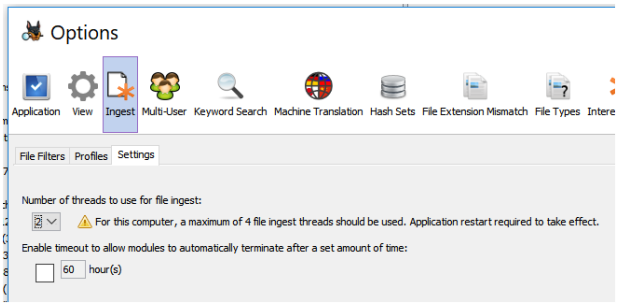
Existují dvě místa pro konfiguraci modulů *Ingest*. Když vyberete název modulu, můžete mít některá obecná nastavení, která lze změnit obrázek od obrázku nebo podle případu. Například jedno vyšetřování se týká případu zneužívání dětí a jiné se týká případu exfiltrace dat a není vhodné používat stejné moduly pro podporu každého incidentu. V dolním rohu je tlačítko *Global Settings* (Globální nastavení) a lze globální nastavení měnit. K tomuto panelu pokročilé konfigurace lze přistupovat také prostřednictvím panelu nástrojů *Selecting Options*.

Je třeba také poznamenat, že spuštění mnoha modulů zpomalí počítač a také bude trvat déle, než Ingest dokončí jejich zpracování. Např. na co spouštět modul *Android Analyzer*, pokud analyzujete PC? Při vlastním výběru je třeba mít na paměti dobu zpracování, a že ta může být při neuvážené konfiguraci značně dlouhá, viz obr. 3.1.1.4.



Obr. 3.1.1.4 Takto dopadl autor scénáře po dvou hodinách analýzy souborů při konfiguraci typu „velké oči“

Při analýze je třeba optimalizovat výkon počítače: Doporučuje se spustit Autopsy z plochy nebo z nabídky *Start*. Druhou možností je potvrdit použití maximálního počtu vláken pro soubory *Ingest*. K tomu je třeba přejít na *Tools*, *Options*, pak *Ingest* (viz Obr. 3.1.1.5), na něm jsou tři karty *File Fiber*, *Profiles*, *Settings*), pak je třeba přejít *na Settings* umístěné úplně vpravo. Pod ním je rozevírací seznam. A vedle něj je žlutý vykřičník a vedle něj doporučení pro konkrétní počítač (v tomto případě maximálně čtyři vstupní vlákna). Stačí kliknout na *Apply* a poté *OK*.



Obr. 3.1.1.5 Nastavení zdrojů pro vstupní zpracování

Po kliknutí na OK je třeba zavřít Autopsy a restartovat, aby se změna projevila. Pro zajištění optimálního výkonu je rozumné použít pro obraz disku případu jiný disk. To není totéž jako zdroj dat. Pokud jsou například uloženy podrobnosti o případu v počítači, ale obraz disku na externí pevný disk, je umožněno čtení a zápis maximálního množství dat současně. Navíc je špatným postupem mít své důkazy uloženy v počítači, protože by to mohlo poškodit soubor, což je přesně důvod, proč jsou vyžadovány blokátory zápisu, aby byla zajištěna integrita důkazů.

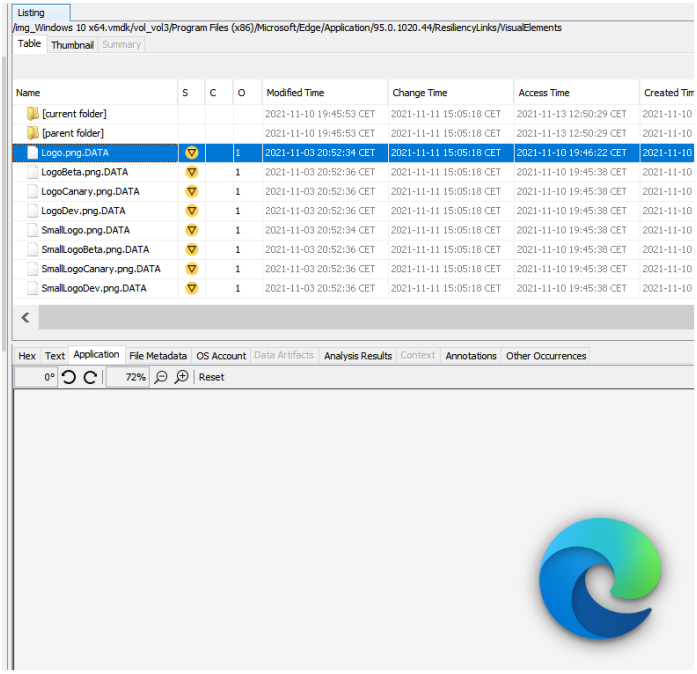
3.1.2 Moduly Extension Mismatch a USB zařízení

Autopsy má řadu základních modulů. Moduly nejsou seřazeny podle priority, protože každý případ bude jiný. Při každém spuštění ingestu budou výsledky přidány ke stávajícím výsledkům.

Na panelu stromového prohlížeče lze nalézt strom *Extension Mismatch Detected*. Pro něj dodává výsledky modul *Extension Mismatch Detector*. Modul je důležitý, protože někteří podezřelí se mohou pokusit skrýt své soubory změnou této přípony. Pokud by vyšetřovatel soubor otevřel, došlo by k vygenerování chyby poškozeného souboru a soubor by se zdál být zbytečným. To však nemusí platit vždy.

Pro potvrzení toho, co je povoleno je třeba přejít na *Tools*, pak dolů na *Ingest Modules* a *Extension Mismatch Detector*. Zobrazí se také možnosti kontroly všech typů souborů, kontroly všech typů souborů kromě textových souborů a kontroly pouze multimediálních a spustitelných souborů. Lze také přeskakovat soubory bez přípon a známé soubory a *Finish*.

Po potvrzení, že se tento modul spustil lze přejít do stromu *Extension Mismatch Detect* na panelu stromového prohlížeče. Bude vidět spoustu jmen, která vypadají podezřele – viz obr. 3.1.2.1. Vyloučit je ale třeba případy false positives.



Obr. 3.1.2.1 Příklad nesouladu v příponách souborů

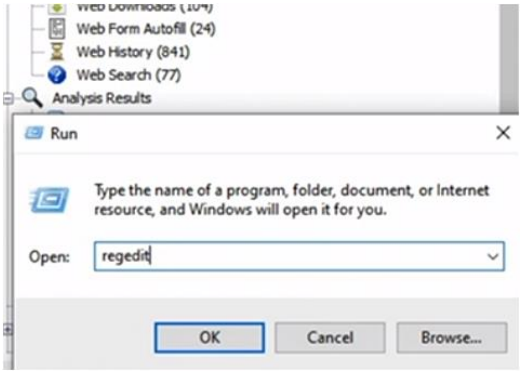
3.1.3 Moduly Recent Activity a Interesting Files

Podívejme se na několik dalších důležitých modulů Autopsy. *Recent activity* module (modul nedávné aktivity) extrahuje aktivity uživatelů, jako jsou informace uložené webovými prohlížeči, včetně vyhledávání na webu a spouštění programů a například operačního systému. Také používá *RegRipper* na podregistry registru.

RegRipper (RegRipper 2023) je open source nástroj, který se používá pro extrakci a korelaci dat. Používá pluginy k načtení často potřebných informací během vyšetřování na zařízení se systémem Windows. Posuzuje soubory s vysokým obsahem registru pro extrahování konkrétních klíčů, hodnot a dat.

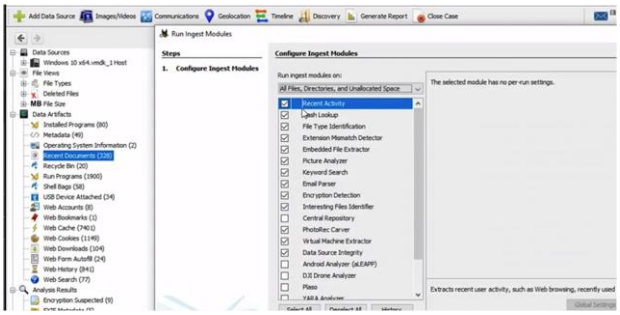
Registr je databáze, která ukládá nízkoúrovňová nastavení pro operační systém Windows. Jeho účelem je pomoci programům využívat prostředky počítače a obsahuje komplexní informace o aplikacích, vytvořených dokumentech hardwaru a mnoho dalšího. Tyto funkce jsou důvodem, proč Autopsy tyto nástroje do sebe začlenila. Neexistuje žádná lepší databáze pro zařízení se systémem Windows, a pokud byste chtěli vidět registraci pro lepší pochopení, lze to provést pomocí vyhledávacího pole.

Stačí jednoduše zadat REGEDIT a pak jednoduše kliknout na enter (Obr. 3.1.3.1) a v tomto okamžiku budete moci vidět svůj registr. Je to velmi nízká úroveň a neměli byste měnit žádná zařízení, protože je to velmi důležité pro daný počítačový systém.



Obr. 3.1.3.1 Regedit

Takže teď, když víte, odkud všechny tyto informace pocházejí, se lze vrátit zpět k modulu nedávných aktivit (*Recent Activity*) – Obr. 3.1.3.2. To umožní vidět, k jaké aktivitě došlo v posledním týdnu používání, jaké webové stránky byly navštíveny, co dělal samotný stroj a jaká zařízení k němu byla připojena. Pro testovaný případ není co konfigurovat, protože se jedná o výchozí nastavení.

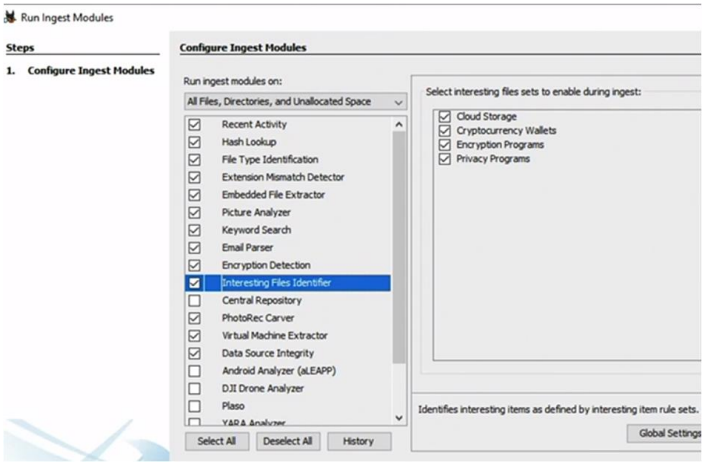

Obr. 3.1.3.2 K nejdůležitějším částem analýzy patří vyšetřování nedávných aktivit

Výsledky se zobrazí ve stromovém prohlížeči pod datovými artefakty. Vzhledem k množství informací, které tento modul poskytuje, zkoumání nedávných aktivit patří k nejdůležitějším částem analýzy. Pod tím uvidíte nejnovější dokumenty, webovou historii, stahování z webu a další – viz Obr 3.1.3.3.

Obr. 3.1.3.3 Zajímavé dokumenty

Další je zajímavý modul pro identifikaci souborů – viz Obr. 3.1.3.4. To vám umožní automaticky označit soubory a adresáře, které odpovídají sadě pravidel. To může být užitečné, pokud vždy potřebujete zkontrolovat určité soubory, ať už se jedná o konkrétní typ nebo identifikovaný název souboru. Pomocí vlastní sady pravidel vám tento modul

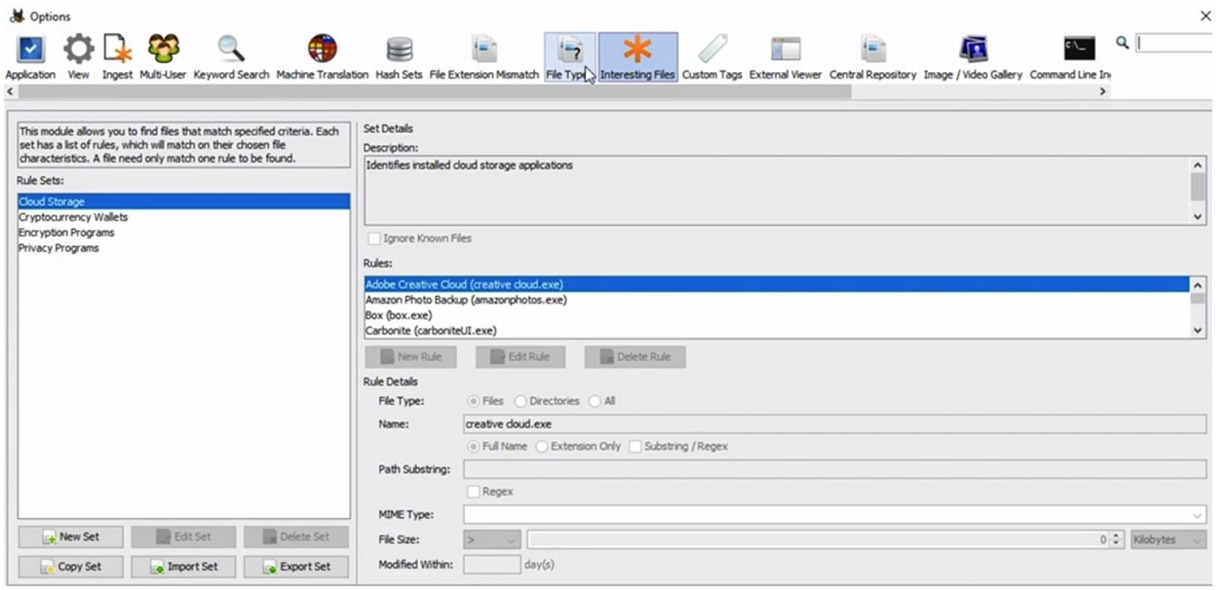
umožňuje spouštět je proti každému zpracovávanému souboru. Pokud soubor odpovídá některému z pravidel, uvidíte pro něj záznam ve stromovém prohlížeči. Svá pravidla můžete také sdílet s ostatními uživateli a importovat sady vytvořené ostatními do vaší kopie Autopsy.



Obr. 3.1.3.4 K nejdůležitějším částem analýzy patří vyšetřování zajímavých souborů

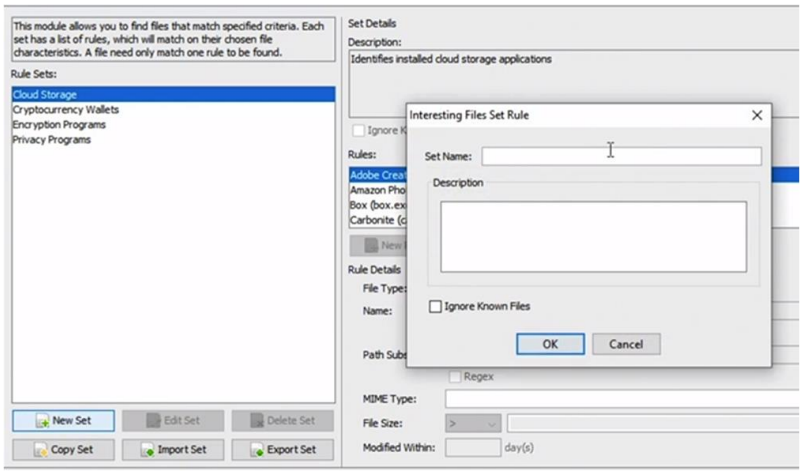
Pokud soubor odpovídá některému pravidlu v sadě přijatých pravidel, bude označen jako odpovídající pro tuto sadu pravidel. Sady pravidel lze povolit a zakázat v době příjmu.

Chcete-li tedy vytvořit úpravu vlastní sady pravidel, můžete přejít na *Tools*, *Options*, přejít na kartu *Interesting Files*, v oblasti na levé straně vám zobrazíme seznam sad pravidel, které jsou aktuálně k dispozici (Obr. 3.1.3.5). Výběrem sady pravidel se zobrazí její popis a informace. Sadu pravidel můžete kopírovat, importovat, exportovat, vytvářet nové, upravovat a mazat. Nemůžete však odstranit ani upravit ty, které jsou přítomny, jak je nastaveno v defaultním nastavení.



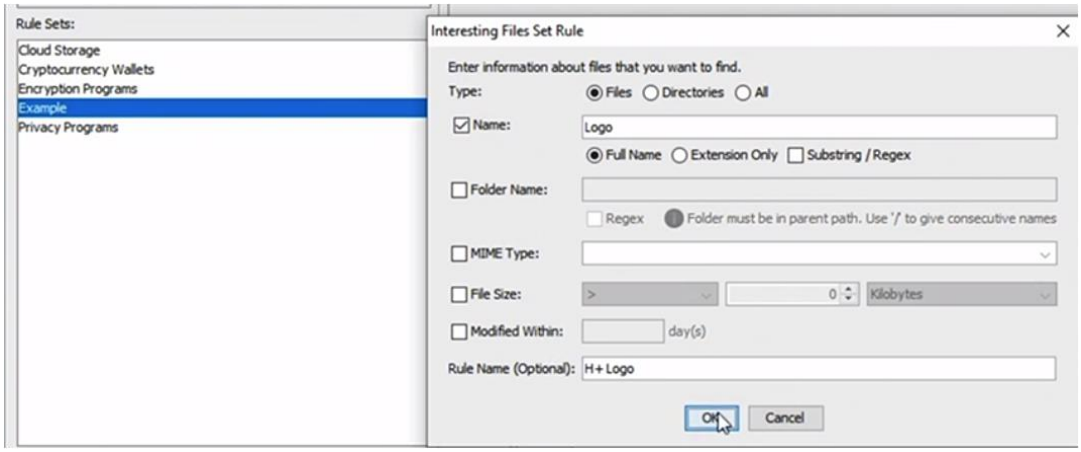
Obr. 3.1.3.5 Prohlížení zajímavých souborů (Interesting Files)

Pojďme si však projít proces tvorby nového pravidla (Obr. 3.1.3.6). Otevře se nové okno, takže můžete zadat informace o svých ideálních souborech. Uveďme tedy název případu jako příklad.

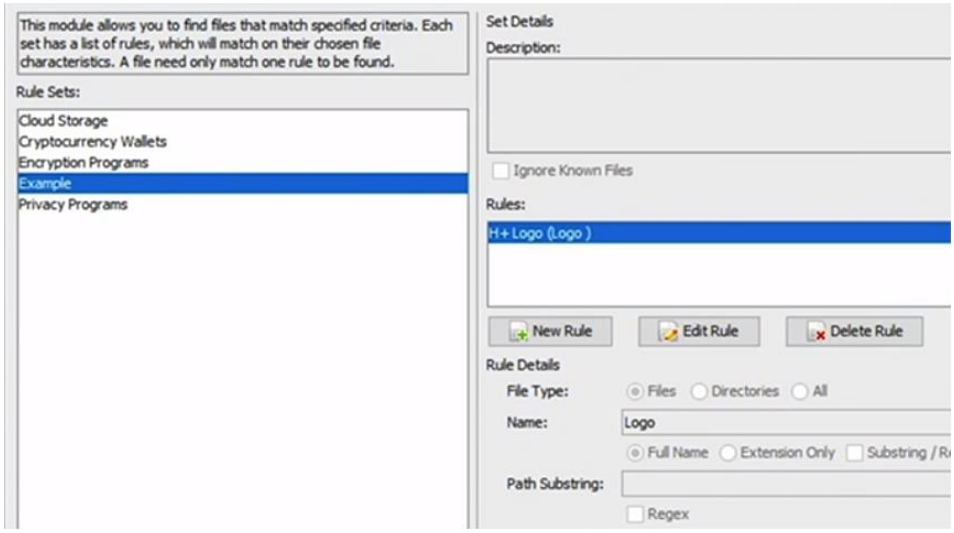


Obr. 3.1.3.6 Vytváření nového pravidla

Horní řádek umožňuje vybrat jeden ze tří typů, soubory, adresáře nebo všechny, což jednoduše znamená obojí. Uvědomte si, že některé typy podmínek se vztahují pouze na soubory a nebudou dostupné, pokud vyberete možnost adresáře nebo všechny. Každé pravidlo musí mít alespoň jednu podmínku. Toto nově vytvořené pravidlo můžete uložit pod libovolným názvem, pojmenování je samozřejmě zcela volitelné. Definujme například pravidlo H+Logo pro nalezení souboru Logo (Obr. 3.1.3.7 a Obr. 3.1.3.8).

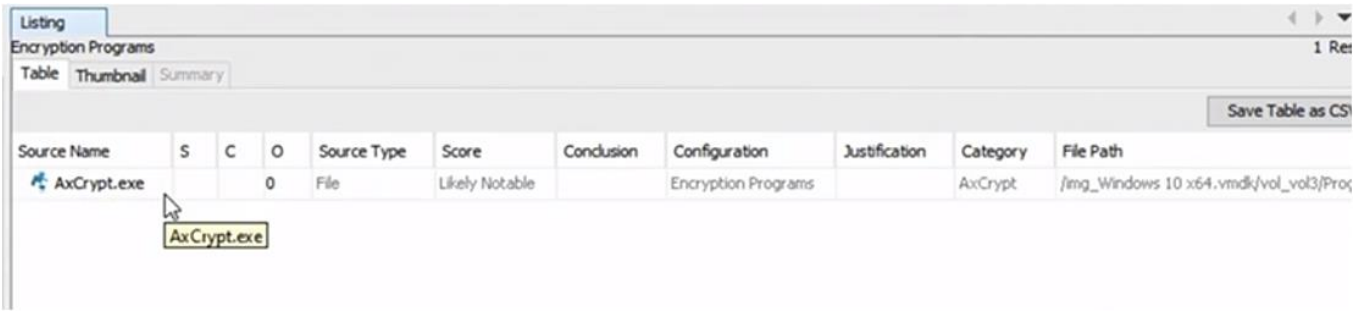


Obr. 3.1.3.7 Vytvoření pravidla H+Logo pro soubor se jménem Logo



Obr. 3.1.3.8 Pravidlo H+Logo pro soubor se jménem Logo v seznamu pravidel

S logem se pracuje v rámci programu AxCrypt.exe – viz Obr. 3.1.3.9.



Obr. 3.1.3.9 Program AxCrypt.exe pracující s logem

Pravidlo práce se souborem Logo bylo nalezeno, přestože takový soubor ve skutečnosti nemusí existovat, jen se na něj program AxCrypt odvolává – běžným voláním souboru by to volání nebylo zchyceno.

3.1.4 Instalace modulů třetích stran

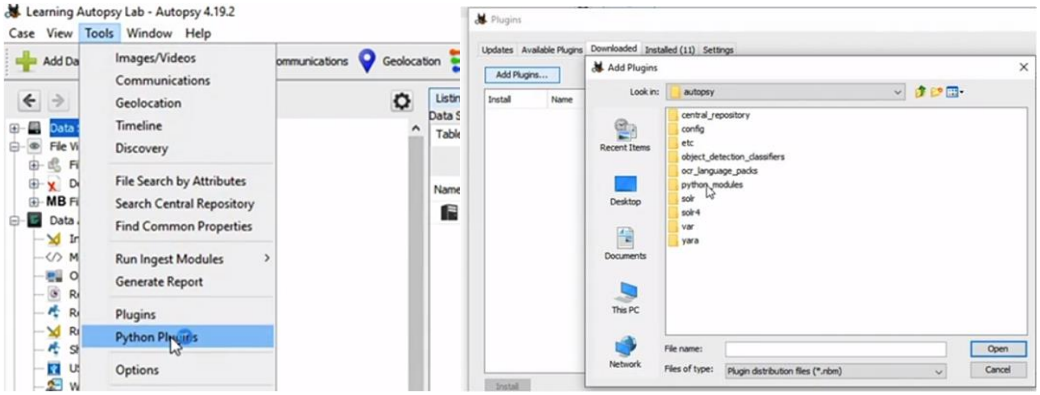
Autopsy má mnoho ingestových modulů, které analyzují data, ale někdy jsou zapotřebí funkce, které ještě nebyly začleněny. Zde přicházejí na řadu moduly třetích stran. Toto je ošemetné téma, protože pro jakýkoli digitální forenzní případ musí být metody extrakce dat forenzně správné, tj. bez jakýchkoliv změn v datech nebo metadatech.

Aby byl proces shromažďování dat forenzně správný, musí být obhajitelný, což znamená, že musí být konzistentní, opakovatelný a dobře zdokumentovaný. Za předpokladu, že modul třetí strany to dodržuje, zde bude poskytnut návod, jak nainstalovat modul do případu.

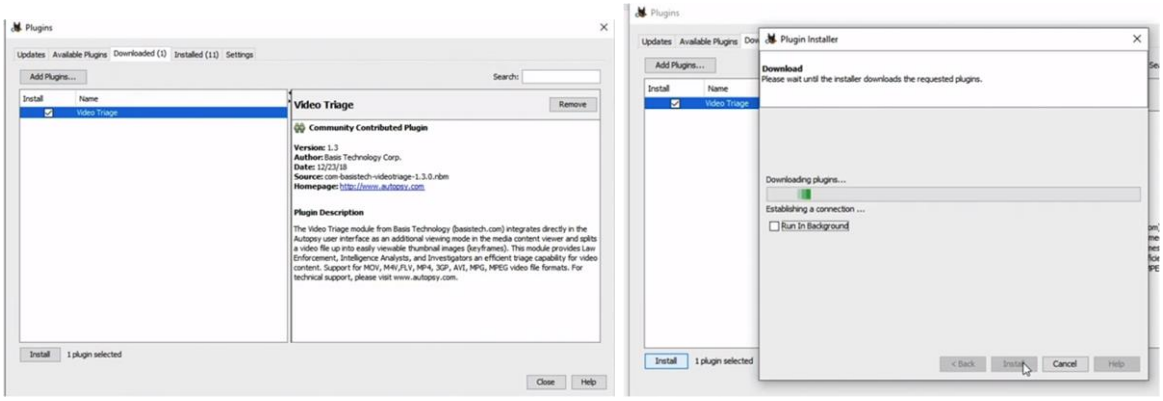
Pro příklad bude použit modul od samotné Autopsy. Je třeba přejít do prohlížeče a zadat autopsy.com a pak přejít ku přidání modulů. Modul, který bude použit, se nazývá VIDEO TRIAGE (Obr. 3.1.4.1). Tento modul efektivně třídí obsah videí jejich rozdělením do snadno zobrazitelných miniatur.

Obr. 3.1.4.1 Volba VIDEO TRIAGE

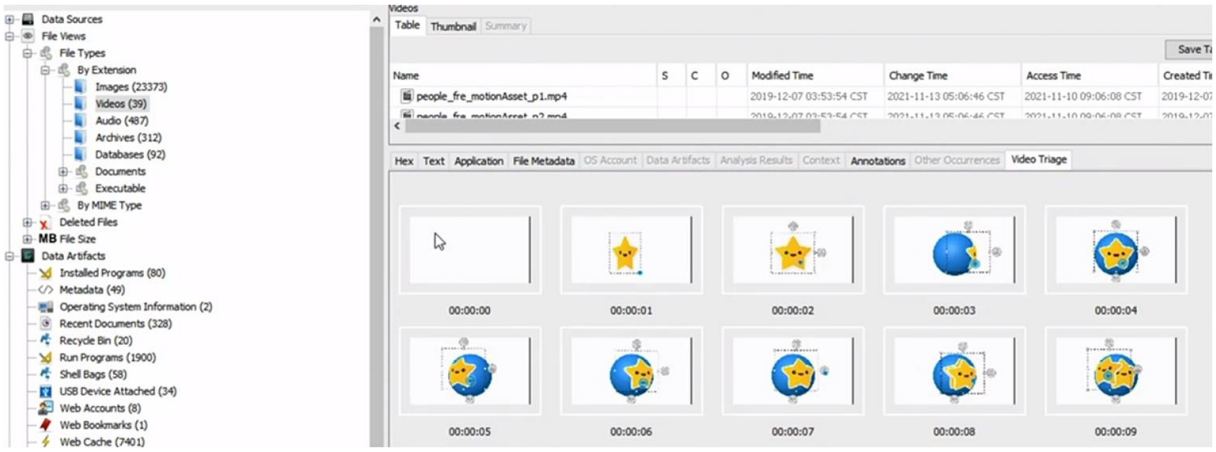
Po instalaci se je třeba vrátit do okna Autopsy, přejít na *Tools, Python Plugins* – Obr. 3.1.4.2 a instalovat Video Triage – Obr. 3.1.4.3. V rámci instalace proběhne restart aplikace a pak lze přejít na libovolné video Obr. 3.1.4.4.



Obr. 3.1.4.2 Volba Python Plugins, a modulů Pythonu.



Obr. 3.1.4.3 Instalace Video Triage



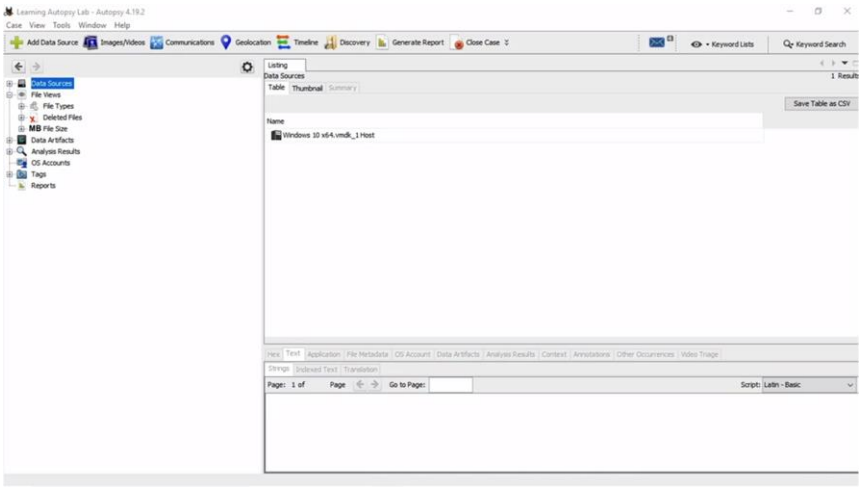
Obr. 3.1.4.4 Výsledek instalace

Výsledkem jsou miniatury každou sekundu, každých pár sekund, v závislosti na tom, o jaký soubor se jedná. A obdobně se instalují všechny moduly třetích stran.

3.2 Prohlížení výsledků

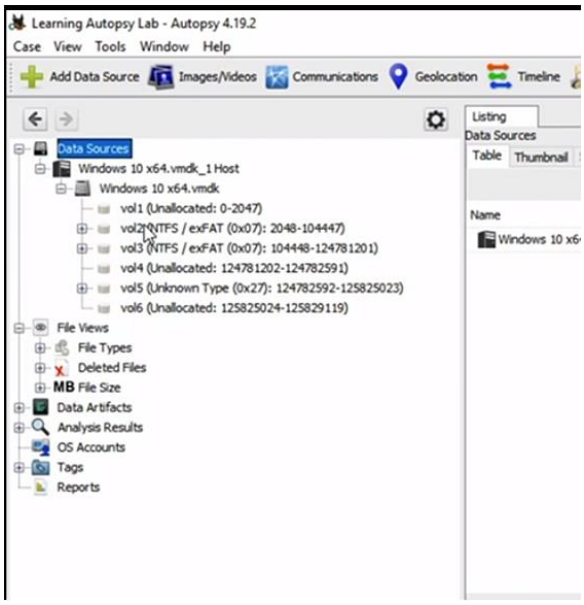
3.2.1 Popis uživatelského rozhraní

Uživatelské rozhraní Autopsy má pět hlavních oblastí, stromový prohlížeč (*tree viewer*), prohlížeč výsledků (*results viewer*), prohlížeč obsahu (*content viewer*), klíčové vyhledávání (*key search*), vyhledávání klíčových slov (*keyword search*) a stavovou oblast (*status area*) viz Obr. 3.2.1.1.



Obr. 3.2.1.1 Uživatelské rozhraní Autopsy

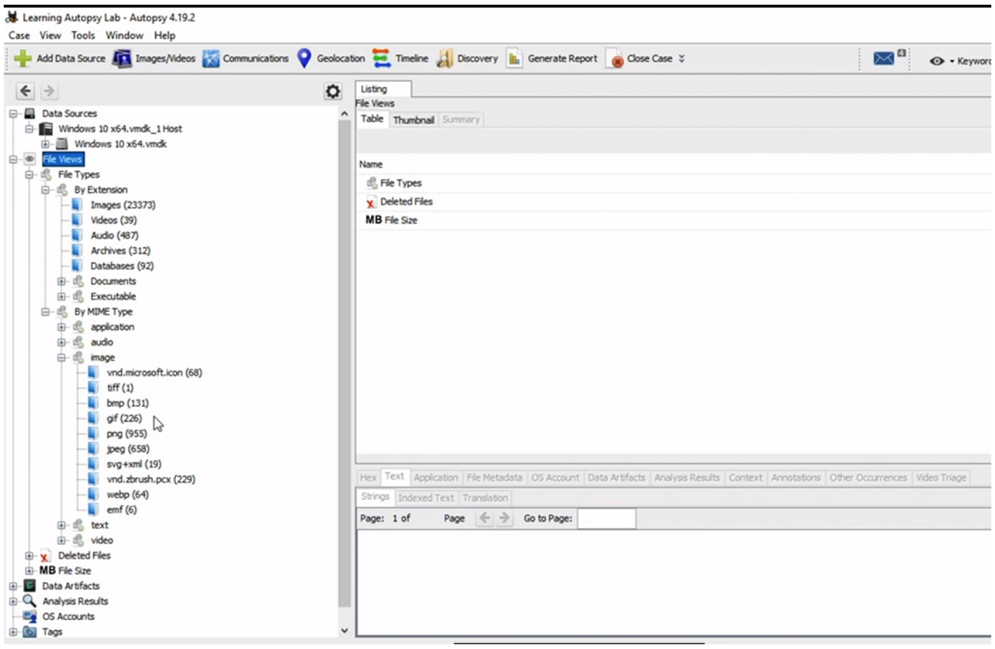
Na levé straně hlavního okna je panel, kde lze procházet soubory zdroje dat daného případu. Tento panel stromového prohlížeče (tree viewer panel) má také pět hlavních oblastí – viz Obr. 3.2.1.2.



Obr. 3.2.1.2 Panel stromového prohlížeče (tree viewer panel)

První částí panelu stromového prohlížeče jsou soubory zdroje dat (*Data Sources*), které zobrazí hierarchii stromu adresářů. Lze procházet konkrétními cestami, protože po výběru mohou obsahovat odlišné podstromy. Pokud bychom například měli obraz disku plochy (*desktop disk image*), obraz virtuálního disku a obraz USB, tak budou všechny umístěny zde.

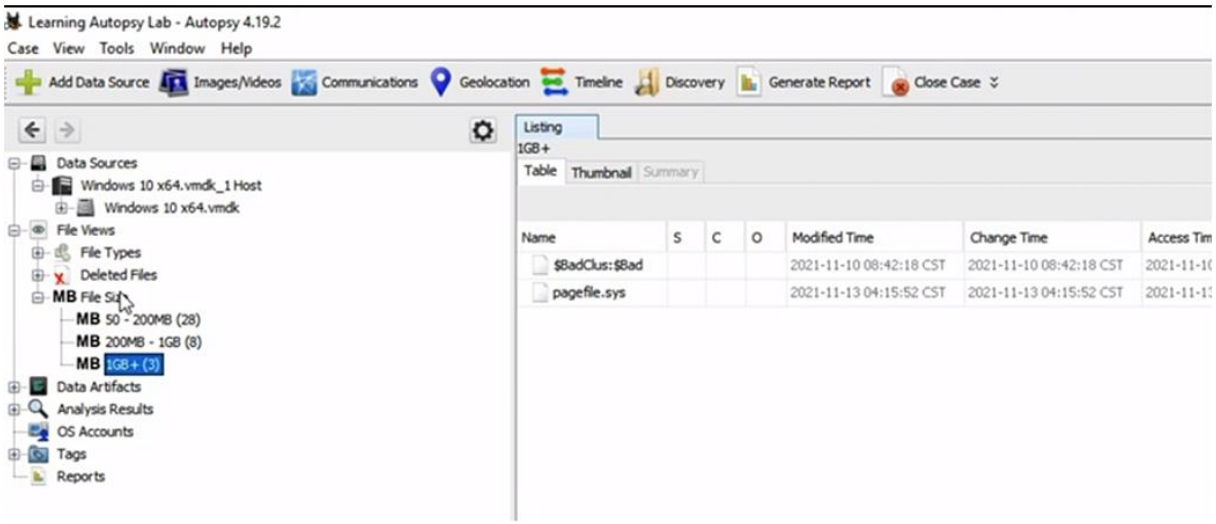
Pod *Data Sources* je umístěn přehled souborů (*File Views*) – viz Obr. 3.2.1.3. Toto je oblast seznamu souborů, které lze seskupit podle typu nebo jiných vlastností ve všech zdrojích dat. To vám jednoduše umožní přejít na konkrétní typ média. Lze tedy například procházet typy souborů, přípony či přejít na obrázky. Nebo lze postupovat podle konkrétního rozšíření, Přípony souborů se běžně používají pro operační systém k rozhodování o tom, jaké programy otevřít a který typ MIME používá prohlížeč k rozhodnutí, jak prezentovat některá data.



Obr. 3.2.1.3 přehled souborů (File Views)

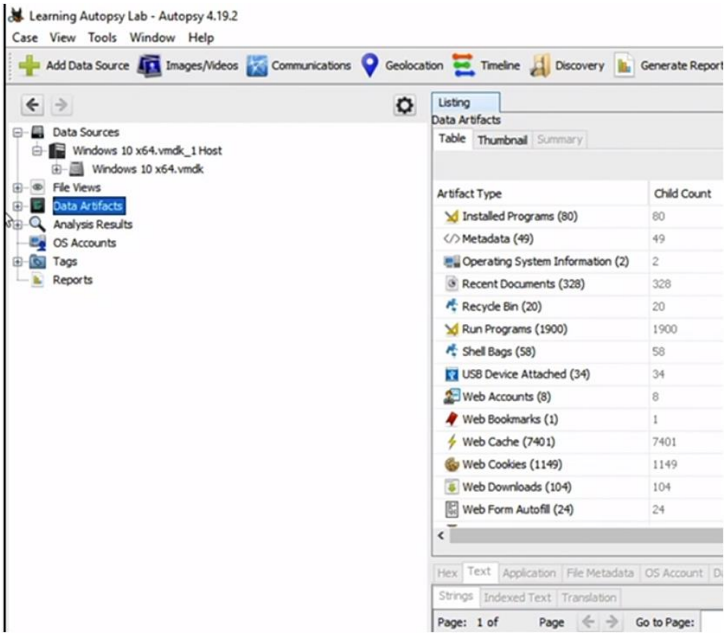
Po typech souborů jsou zde smazané soubory (deleted files), těch může být velké množství a řada z nich může být pro konkrétní vyšetřování irelevantní. Je-li třeba zjistit, co vlastně uživatele iniciovalo ke smazání, lze navštívit sekci s výsledky odpadkového koše.

A nakonec je dole uvedena velikost souboru (**MB** File Sizes) – viz Obr. 3.2.1.4. To může být užitečné v případě, že na zařízení bylo uloženo velké množství médií anebo pokud je známa velikost příslušného souboru. Např. pokud je hledán zip soubor o velikosti 2 GB, pak ho lze hledat odtud.



Obr. 3.2.1.4 Místo, odkud lze zahájit vyšetřování rozsáhlých souborů

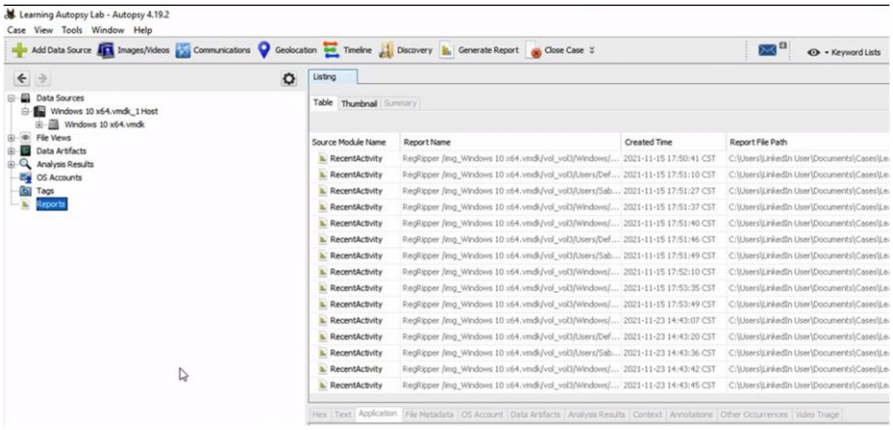
Dále zde máme datové artefakty (Data Artefacts) – Obr. 3.2.1.5. Zde lze nalézt výsledky z ingestů (příjem dat) a výsledků vyhledávání. Zde vyšetřovatel tráví většinu času, protože je zde shromážděno nepřeberné množství informací.



Obr. 3.2.1.5 Datové artefakty

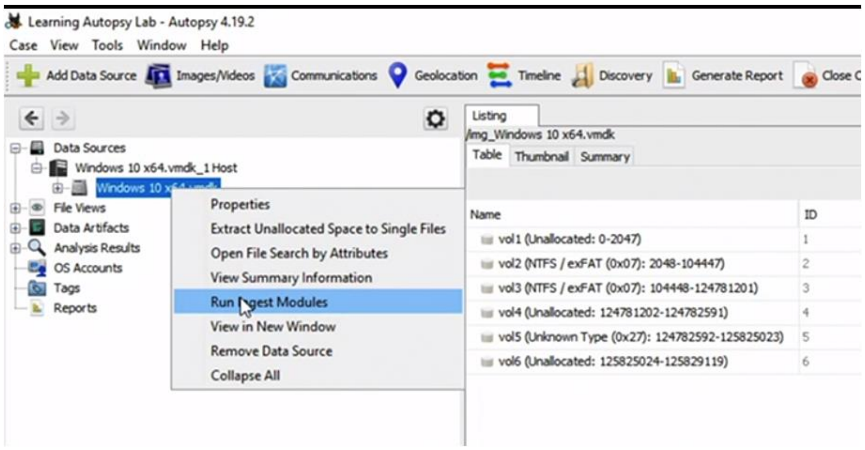
V další hlavní oblasti ve stromovém prohlížeči jsou soubory, které budou mít značky (tagy).

A poslední shora jsou zprávy (reports) – Obr. 3.2.1.6, které mohou být automaticky generovány ingestovými moduly anebo ručně vytvořeny. Použity budou samozřejmě až v průběhu šetření.



Obr. 3.2.1.6 Hlášení (reports)

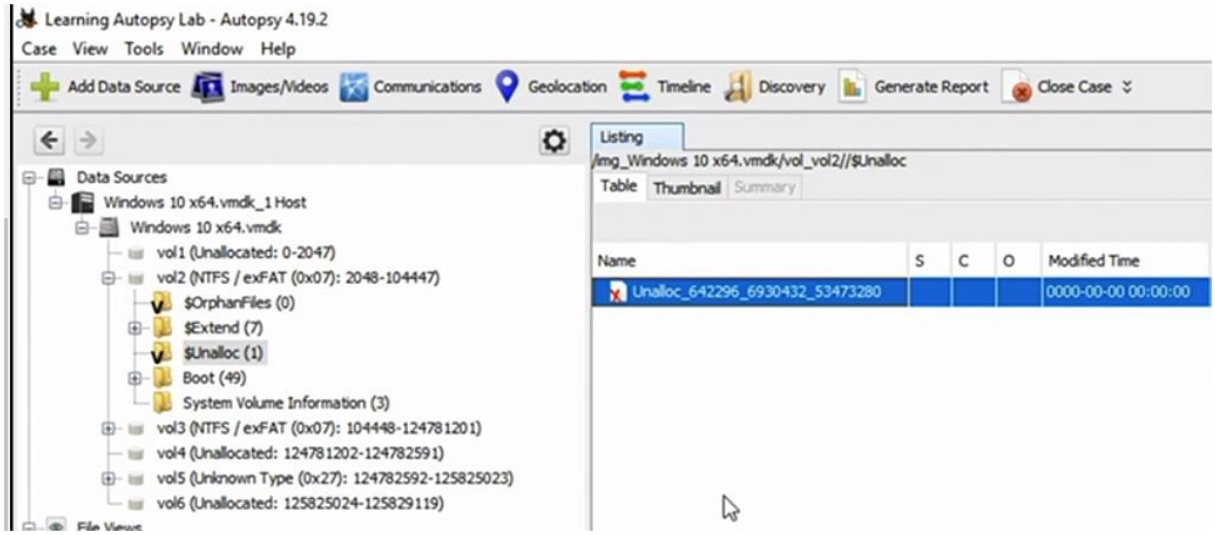
Pokračujme ve vyšetřování souborů dat kliknutím na ně pravým tlačítkem. Co s nimi vše můžeme dělat? Jsme například schopni restartovat ingestové moduly – Obr. 3.2.1.7.



Obr. 3.2.1.7 Restart ingestových modulů

Jsme schopni extrahovat přidělený prostor do jednotlivých souborů a prohlížet nepřidělená místa, bloky souborového systému, které se k ničemu nepoužívají.

V obrazu zařízení (*device image*) má přidělený prostor uložení odlišná umístění v systému souborů, proto by bylo lépe je spojit do jednoho většího souboru. Autopsy umožňuje použití obou metod současně. Pokud se rozhodnete metody používat odděleně, bude daná složka označena jako Unaloc a označena znakem $ – viz Obr. 3.2.1.8.



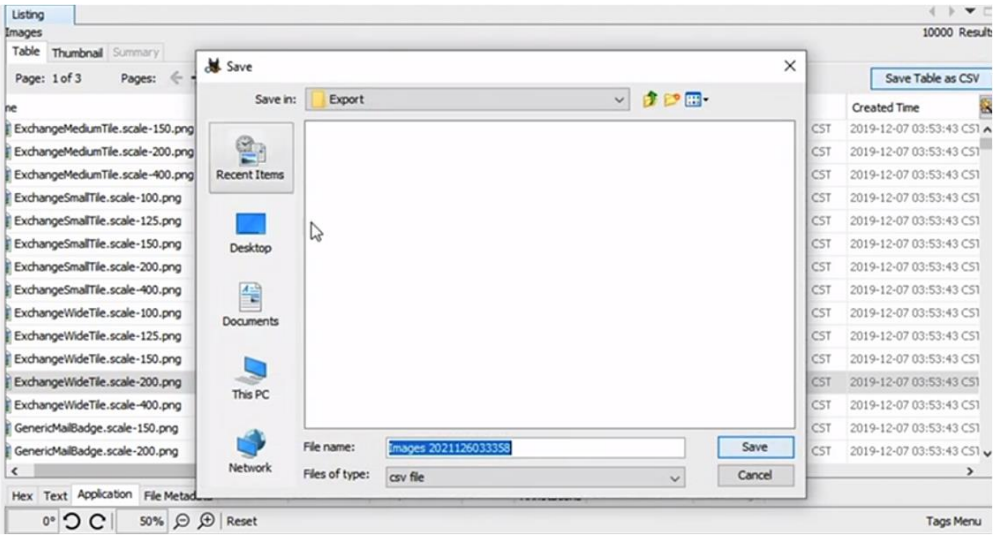
Obr. 3.2.1.8 Unaloc označuje nepřidělený prostoru

Když se přesunete do prohlížeče výsledků (*results viewer*), vaše výsledky se budou lišit a neměly by být zaměňovány s oblastí výsledků ve stromovém prohlížeči (*tree viewer*). *Results viewer* se nachází v pravé horní části hlavní obrazovky a zobrazuje obsah toho, co bylo vybráno ve stromovém prohlížeči. Obvykle se skládá z prohlížeče tabulek (*Table*) a miniatur (*Thumbail*). Je-li zvolen konkrétní soubor, je o něm získána řada informací. A u souborů uvidíte data úprav, časová razítka vytvoření, velikost a další informace o souboru.

Sloupce označené písmeny S C O mají tento význam:

- S znamená sloupec skóre a označuje, zda je tato položka zajímavá.
  - Červený vykřičník pak znamená, že tento soubor odpovídá hashi.
  - Žlutá ikona znamená, že tento soubor je zajímavý.
- C znamená, že položka má komentář v centrálním úložišti[5] (central repository).
- O udává, kolik dalších zdrojů dat obsahuje tuto položku.

Existují však případy, kdy jej můžete vidět, pokud jej máte otevřený. Je zde možnost exportování souborů i obsahu *Table* do souboru ve formátu CSV. Na soubor je třeba kliknout pravým tlačítkem, uložit jako tlačítko CSV a vybrat cíl (Obr. 3.2.1.9). Lze vybrat určité řádky nebo zvýraznit všechny řádky.

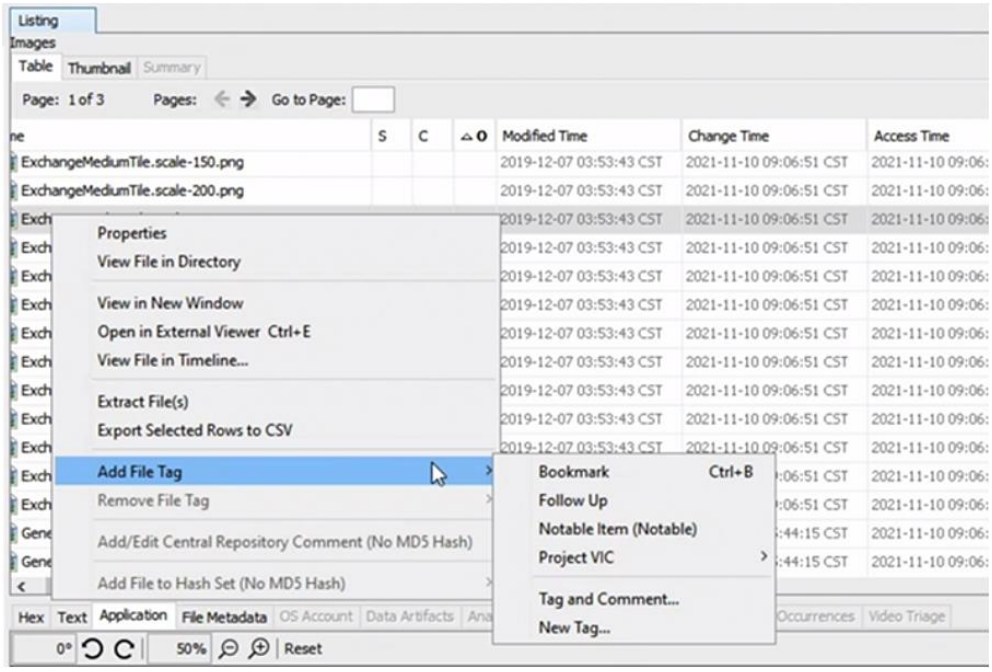


Obr. 3.2.1.9 Export souborů *table viewer* do CVS souboru

Kliknutí pravým tlačítkem navíc umožňuje provádět více akcí, než je přístup k souboru v externím prohlížeči. Lze například otevřít HTML soubor v Chrome nebo dokumentu v textovém editoru, jako je Poznámkový blok. Lze extrahovat soubory, což může umožnit uložení místní kopie pro další analýzu a pak ji zahrnout do dokumentace, případně ji analyzovat pomocí jiného forenzního programu. Výsledek lze zobrazit v novém okně.

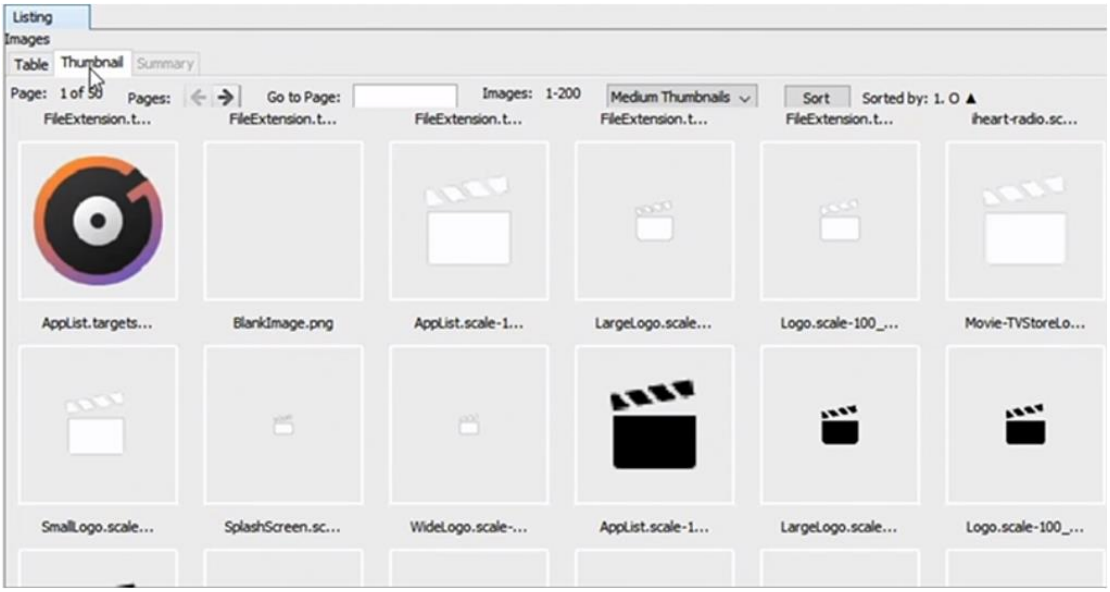
A nakonec lze přidat značku souboru (File Tag) – viz Obr. 3.2.1.10, která pomůže správně kategorizovat informace a umožní je později zkontrolovat, pokud je třeba podpořit nějakou teorii nebo se k ní jen vrátit.

[5] Umožňuje spolupracovat s dalšími analytiky ve vaší síti a tyto sloupce se pak používají v tomto kolaborativní prostředí.



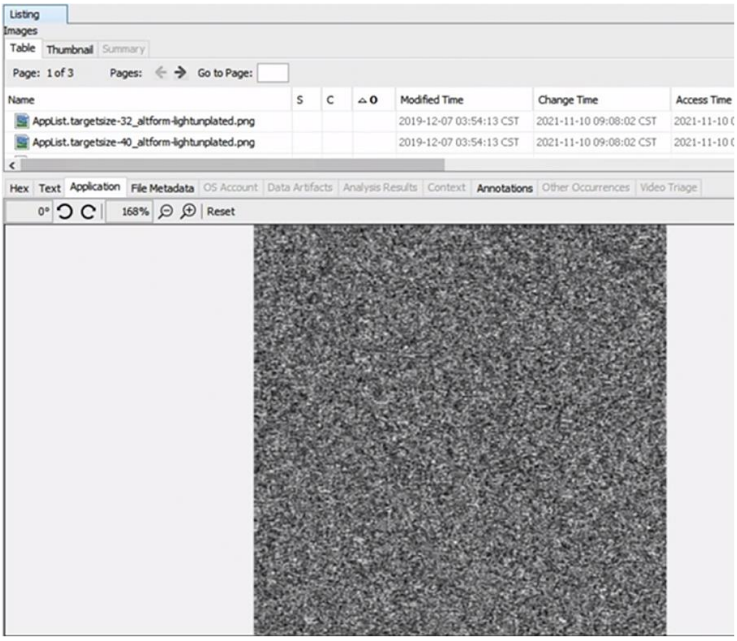
Obr. 3.2.1.10 Přidání značky souboru (File Tag)

Pro prohlížeč miniatur, který se nachází v prohlížeči výsledků, se položky zobrazí jako tabulka miniatur – Obr. 3.2.1.11. Tento prohlížeč zobrazuje pouze určité soubory obrázků, jako jsou soubory gif, PNG a soubory ve formátu JPEG.



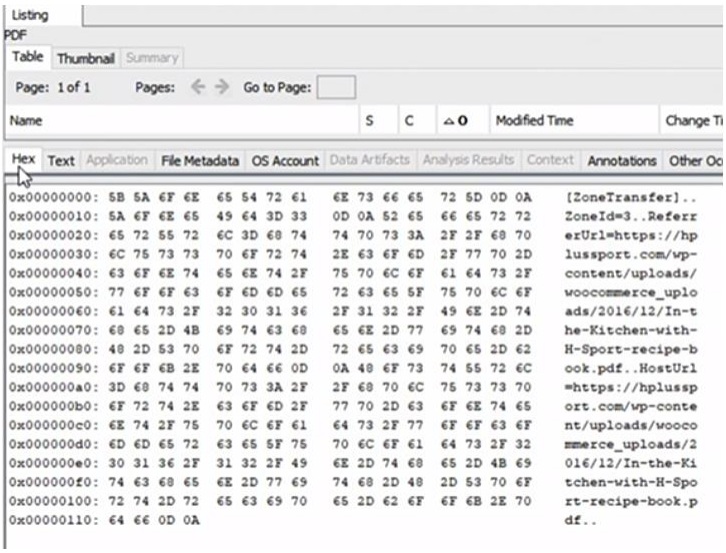
Obr. 3.2.1.11 Tabulka miniatur (Thumbnail)

Pokud je třeba prohlížet soubory v jiných formátech, pravděpodobně bude třeba použít funkci přístupu k souboru a externího prohlížeče kliknutím pravým tlačítkem na samotný soubor. Prohlížeč obsahu (*Content Viewer*) se nachází v pravé dolní části hlavní obrazovky Autopsy. Tento prohlížeč se generuje, když je vybrána daná položka tabulky – viz Obr. 3.2.1.12.



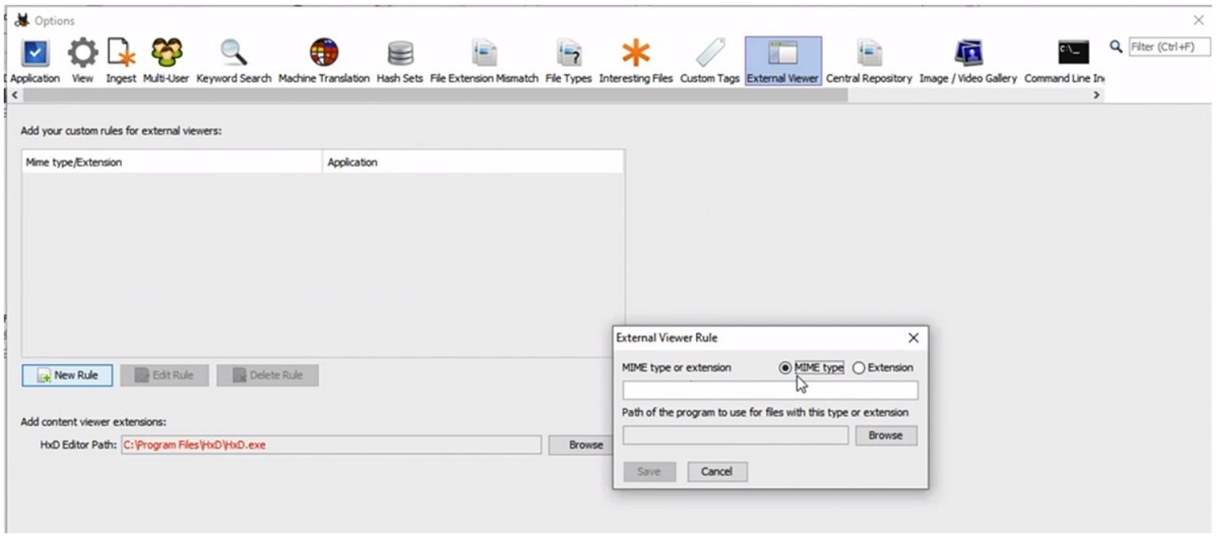
Obr. 3.2.1.12 Výběr obsahu JPG souboru

Díky tomu, že je to vpravo dole, lze obsah zvětšit na velikost podle daných preferencí. Samotný prohlížeč obsahu zobrazuje obrázky, videa, text, metadata, operační systém, informace o účtu a mnoho dalšího. Obvykle je k dispozici karta *Hex* (Obr. 3.2.1.13), která zobrazuje nezpracovaný a extrahovaný obsah souboru. To nás ušetří od nezbytnosti otevírat samostatný hexadecimální prohlížeč.



Obr. 3.2.1.13 Prohlížení HTML souboru pomocí karty Hex

Totéž lze ale udělat pomocí okna *Options* (možnosti), které se nachází v části *Tools*. Po odkliknutí karty *Tools* na horní liště je třeba přejít na kartu *Options* – viz Obr. 3.2.1.14, a poté kliknout na externí prohlížeč a vybrat nové pravidlo. Lze si ho přitom přizpůsobit podle potřeby. Lze si např. vybrat typ MIME nebo příponu, nebo jednoduše procházet soubor.



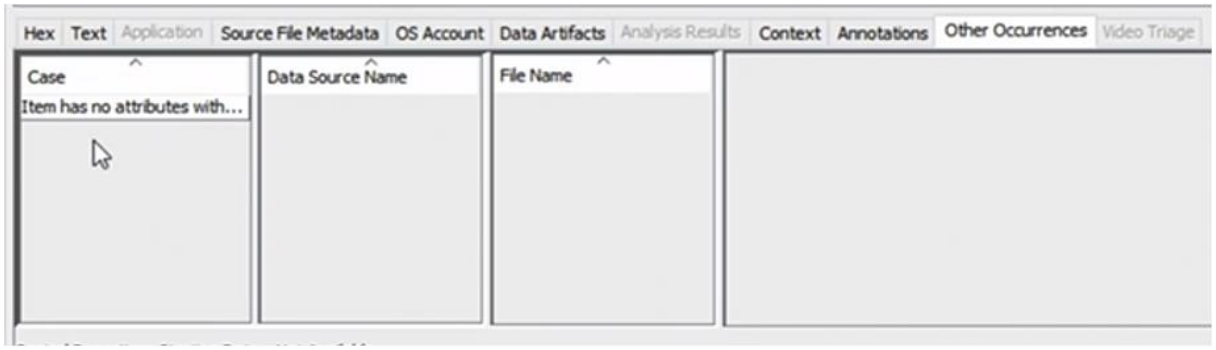
Obr. 3.2.1.14 Volba pravidla pro výběr zkoumaného objektu

Záložka *Text* má tři podzáložky. Řetězce vrátí všechny textové řetězce nalezené v souboru, což lze použít k zobrazení čitelných řetězců uvnitř typů souborů. Mohou mít také mnoho dalších informací.

Je zde k dispozici indexovaný text, který zobrazuje text, který byl indexován modulem pro vyhledávání klíčových slov. A samozřejmě je zde překlad, který v podstatě překládá nebo překládá tyto informace do jakéhokoli jazyka, který používáte. Aplikace sama o sobě zobrazí soubory přátelským způsobem, pokud se jedná o běžný typ souboru. Funguje to například pro videa, obrázky, databáze SQL a soubory HTML, ne pro soubory PDF.

Karta *Context* (obsah) zobrazuje zdroj připojeného souboru a umožňuje zobrazit původní cestu. Může se to týkat například obrázku z řetězce e-mailů.

Karta *Other Occurrences* (další výskyt) zobrazuje seznam míst, kde jinde byl daný soubor ještě umístěn – viz Obr. 3.2.1.15. Poznámky zobrazují karty a komentáře, které jste jako analytik vytvořili.



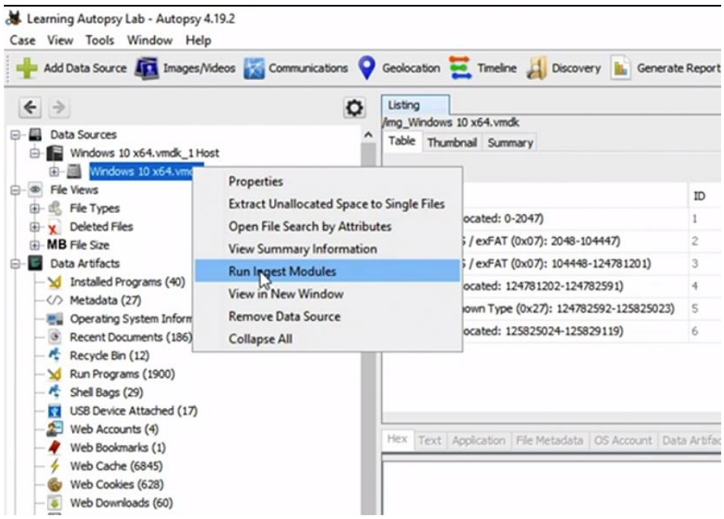
Obr. 3.2.1.15 Příklad karty *Other Occurrence*

Zbývá popsat stavovou oblast, tento pruh ukazuje průběh toho, co se děje. Kliknutím na tuto lištu lze zobrazit další podrobnosti anebo zrušit jakékoli právě probíhající zpracování.

3.2.2 Galerie obrázků a videí

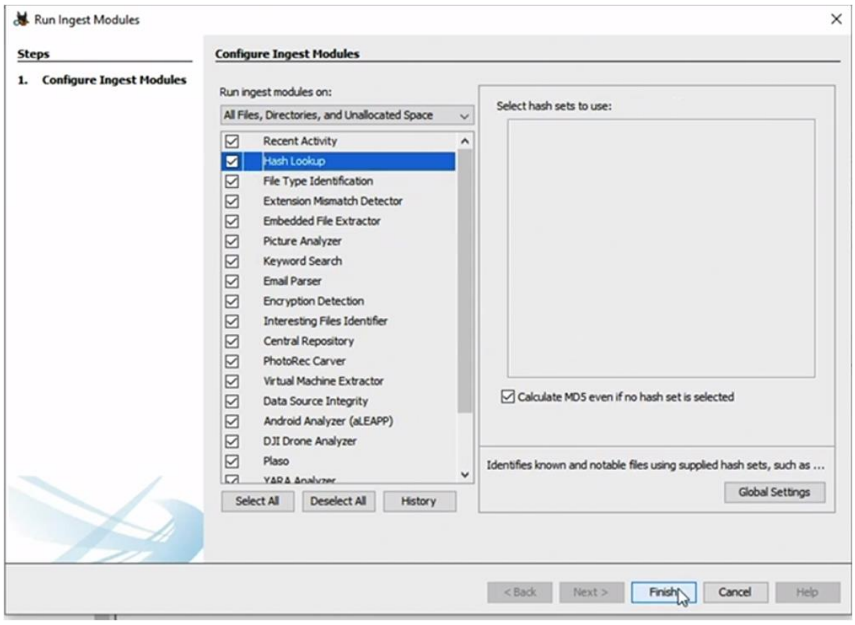
Galerie obrázků (*Image Gallery*) je funkce, byla speciálně navržena pro případy zneužívání dětí v rámci vymáhání práva, ale lze ji použít i pro jiná vyšetřování. Seskupuje obrázky pomocí složek, které analytikovi pomáhají dále oddělovat fotografie a soustředit se na klíčové obrázky. To také umožňuje vyšetřovateli prohlížet si snímky okamžitě po přidání do případu, na rozdíl od čekání na jejich požití.

Chcete-li Galerii obrázků použít, musíte se ujistit, že jsou povoleny konkrétní moduly. Potvrzuje se to kliknutím pravým tlačítkem na příslušný zdroj dat a spuštěním modulu příjmu – položka rolety *Run Ingest Modules* (Obr. 3.2.2.1).



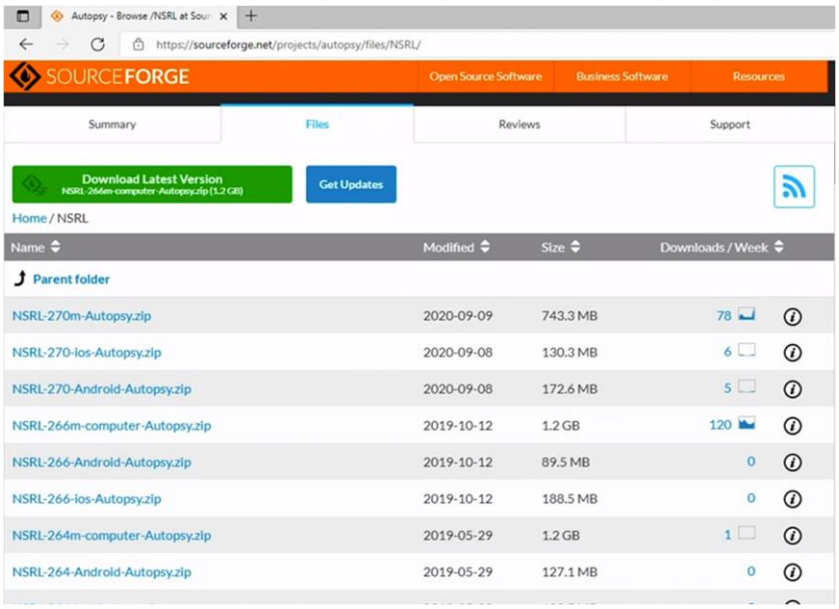
Obr. 3.2.2.1 Výběr zdroje dat pro *Picture Gallery* (galerii obrázků)

Dále je třeba potvrdit výběr identifikace typu souboru, výběr analyzátoru obrázků a výběr způsobu vyhledávání hashe (zakliknout *File Type Identification*, *Picture Analyzer* a *Hash Lookup* na obr. 3.2.2.2). Pro jistotu je samozřejmě zapotřebí kliknout na *Finish* a tím uzavřít výběr.



Obr. 3.2.2.2 Výběr identifikace typu souboru, analyzátoru obrázků a způsobu vyhledávání hashe

Hash Lookup vyžaduje přítomnost *Hash Setů* [6] . Ty se obvykle vytvářejí pomocí importu z sourceforge.net/projects/autopsy/files/NSRL – Obr. 3.2.2.3. Seznamy v knihovně NSRL[7] (National Software Reference Library) jsou navrženy tak, aby shromažďovaly software z různých zdrojů a začleňovaly profily souborů vypočítané z tohoto softwaru do referenční datové sady informací.



Obr. 3.2.2.3 Zdroje na sourceforge.net/projects/autopsy/files/NSRL

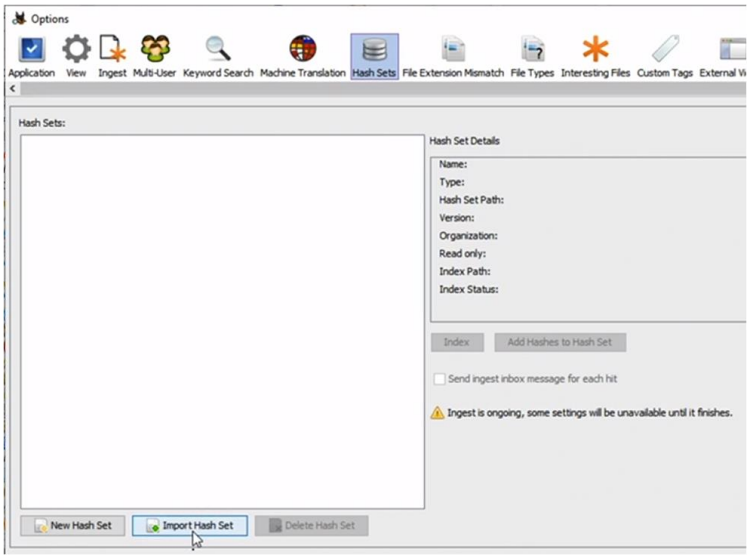
Reference *Data Set* (RDS) je sbírka digitálních podpisů známých sledovatelných softwarových aplikací. Mohou ji používat orgány činné v trestním řízení, vládní a průmyslové organizace k revizi souborů v počítači porovnáním profilů souborů v RDS. To ulehčuje určení, které soubory jsou důležité jako důkazy v počítačích nebo souborových systémech, které mohly být zabaveny v rámci vyšetřování trestných činů.

V hash setu jsou hodnoty hash aplikací, které mohou být považovány za škodlivé, jako jsou jiné nástroje pro hacking, síťové sniffery a další nástroje. Nejsou k dispozici žádné hashovací hodnoty nezákonných dat, tedy například obrázky zneužívání dětí nebo cokoliv podobného. I když NSRL nelze použít pro původní účel, ale pro další použití ano.

Pokud je zapotřebí z jakéhokoli důvodu použít podklady z NSRL, je třeba přejít na *Tools*, *Options*, *Hash Sets*, a poté kliknout na *Import Hash Set* (Obr. 3.2.2.4) a potřebné zdroje stáhnout z sourceforge.net/project/autopsy/files/NSRL.

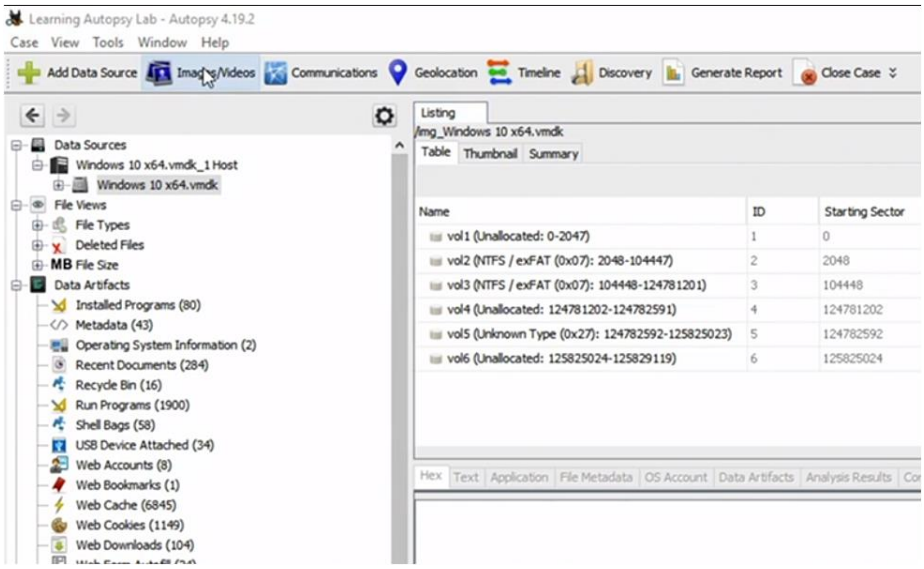
[6] Hash set je sada kolekcí, které neobsahují duplicitní prvky a uložené prvky nemají konkrétní pořadí. Představuje soubor hodnot a poskytuje vysoce výkonné operace.

[7] Projekt podporovaný americkým National Institute of Standards and Technology (NIST). Blíže https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl

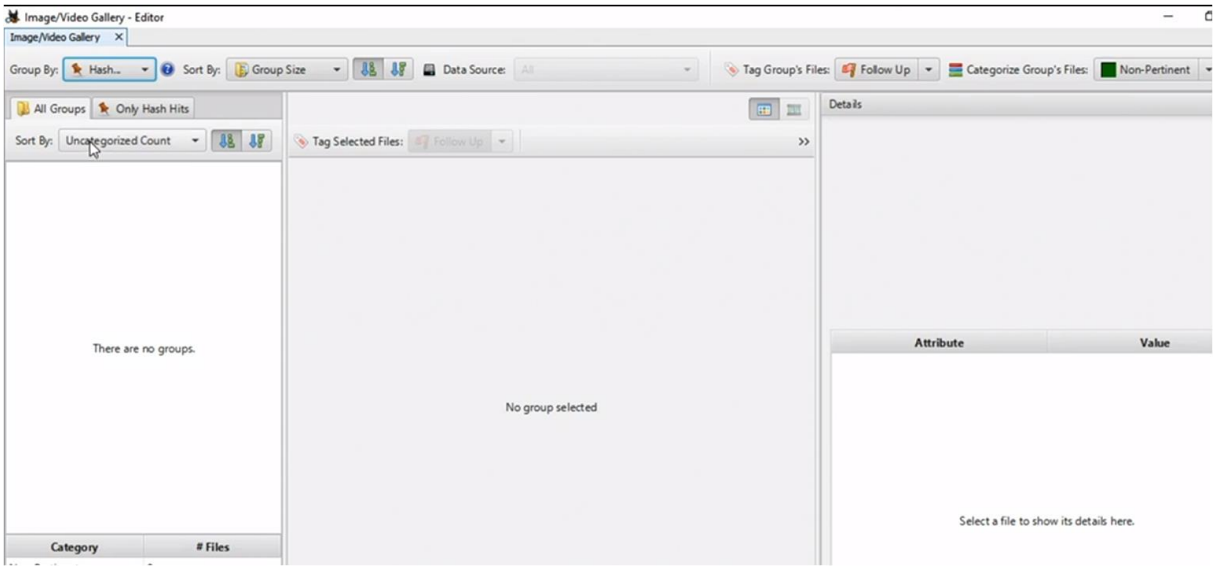


Obr. 3.2.2.4 *Import Hash Set* z sourceforge.net/projects/autopsy/files/NSRL

Chcete-li však použít Galerii obrázků, můžete kliknout na *Image/Videos* (obr. 3.2.2.5). Autopsy otevře nové okno. V levém panelu si všimnete, že jsou zde dvě karty, *All Groups* a *Only Hash Hits* – viz Obr. 3.2.2.6. Zde bude zahrnuta již zmíněná sada hashů.

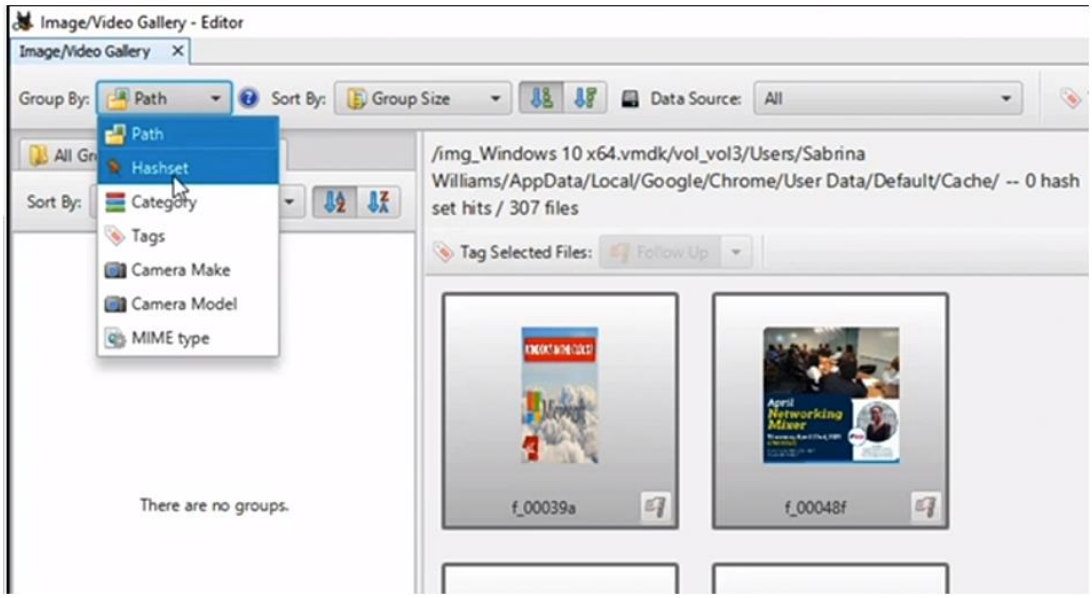


Obr. 3.2.2.5 Spuštění Galerie obrázků přes kartu *Images/Videos*



Obr. 3.2.2.6 Karty *All Groups* a *Only Hash* v rámci editoru *Image/Video Gallery*

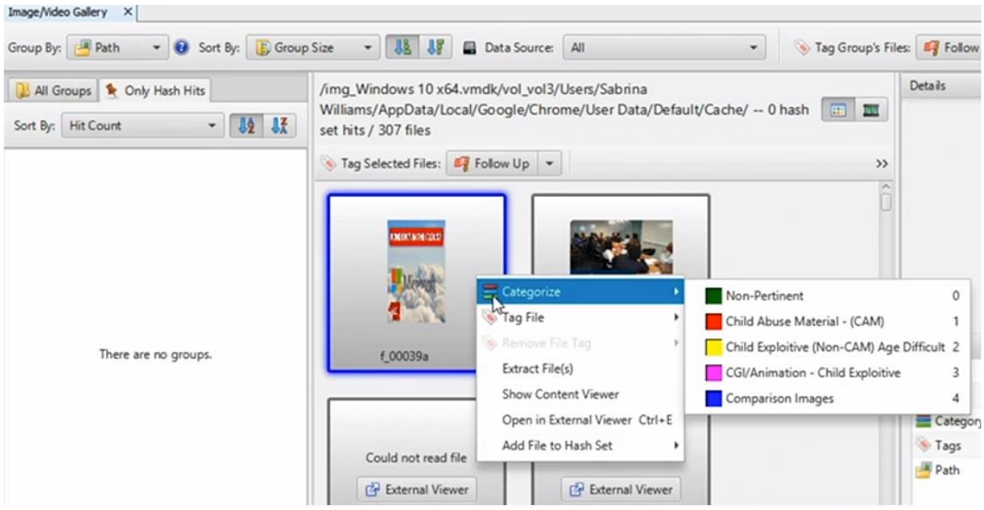
Protože však pro školní laby nebudeme mít k dispozici hash set, je třeba se podívat na cesty stahování (Obr. 3.2.2.7), které jsou velmi důležité právě kvůli snadnosti jejich analýzy. Lze například přejít do části *Downloads* a přesně vidět, co bylo staženo. Je to také důležité, protože zobrazuje umístění obrázku, které může odhalit něco zajímavého, například pokud se uživatel pokusí skrýt soubor ve složce s daty programu.



Obr. 3.2.2.7 Prohlídka cesty stahování

Při kontrole každé skupiny se zobrazí další skupina s nejvyšší prioritou podle kritérií řazení a výchozí je obvykle hustota zásahů sady hashů. Obrázky, které byly skryty, budou mít obvykle kolem sebe čárkovaný okraj.

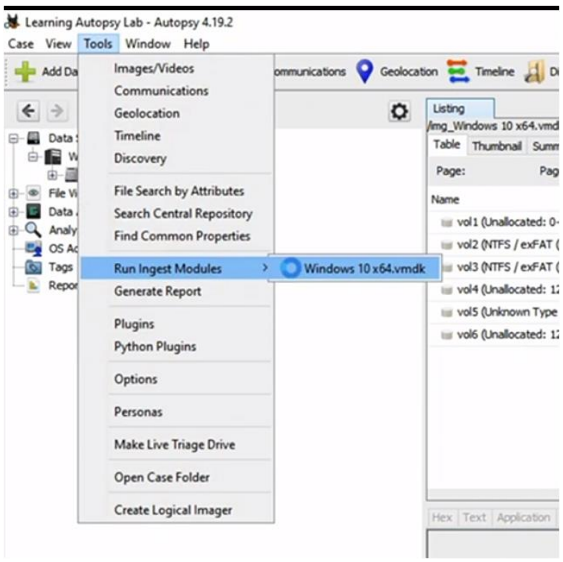
Pro kategorizaci celé skupiny lze rovněž použít panel nabídek v horní části skupiny. Kliknutím pravým tlačítkem na obrázek lze jednotlivé obrázky roztřídit nebo označit podle důležitosti. Můžete kliknout pravým tlačítkem v *Category* podle toho, co je prospěšné, nebo jednoduše přidat text, označující např. *Notable Item* (pozoruhodná položka). Obrázek může být zařazen pouze do jediné kategorie, ale může mít více tagů.



Ob. 2.5.2.8 Kategorizace obrázků

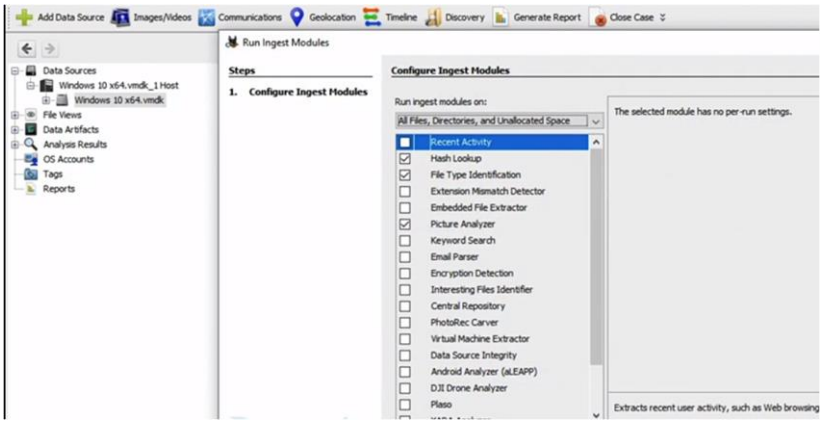
3.2.3 Funkce Timeline

Dalším specializovaným prohlížečem je funkce Časová osa (*Timeline*)[8]. Existuje několik modulů, které je třeba povolit. Nejprve přejděte na *Tools*, klikněte na *Run Ingest Modules* (Obr. 3.2.3.1) a ujistěte se, že jsou vybrány všechny potřebné položky.



Obr. 2.5.3.1 Spouštění vstupních modulů

[8] Verze 4.13 a starší tuto možnost nemají.



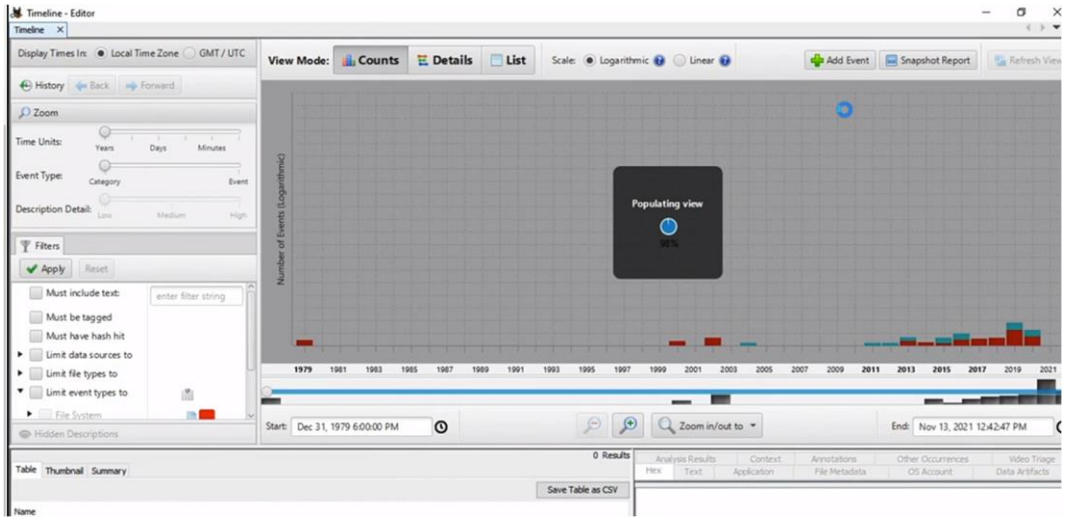
Obr. 3.2.3.2 Výběr vstupních modulů

Moduly, které je účelné spustit (obr 2.5.3.2):

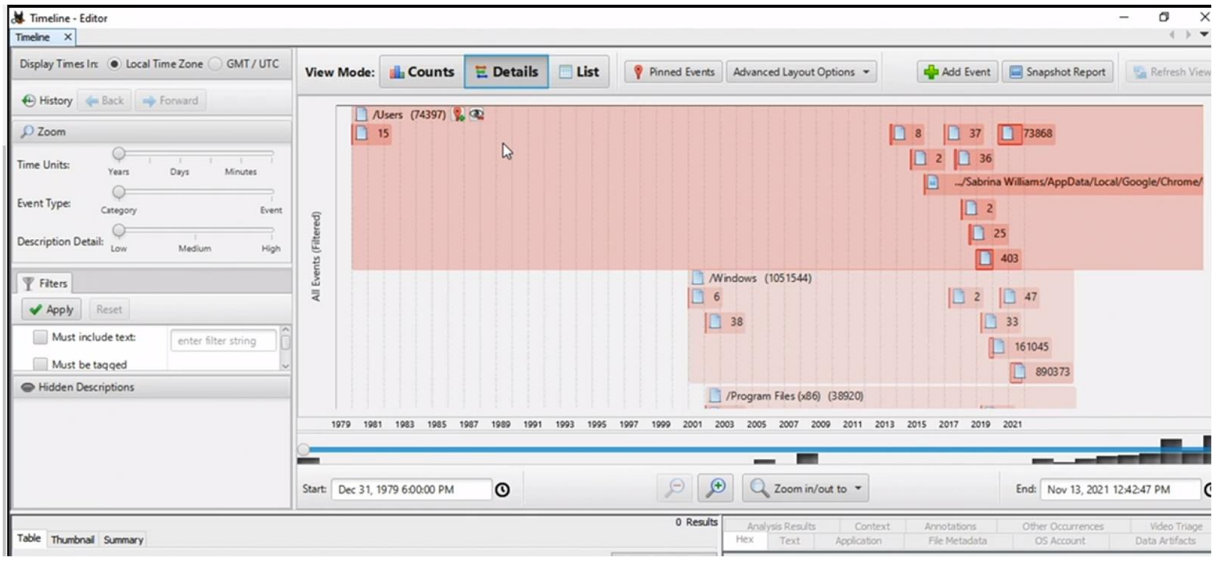
- *Hash Lookup*, protože používá NSRL k ignorování známých souborů.
- *Recent Activity*, ten generuje události související s webem.
- *exif-parser*.
- *Picture Aanalyzer*, aby bylo zajištěno, že budou zahrnuty i události založené na uložených metadatech.
- jakékoli další zpracování, o kterém si myslíte, že by mohlo být užitečné. Pokud bychom tedy například analyzovali tablet, chceme povolit modul Android Analyzer.

Chcete-li tuto funkci otevřít, musíte přejít na nástroje a přejít na časovou osu, nebo můžete jednoduše vybrat funkční tlačítko časové osy.

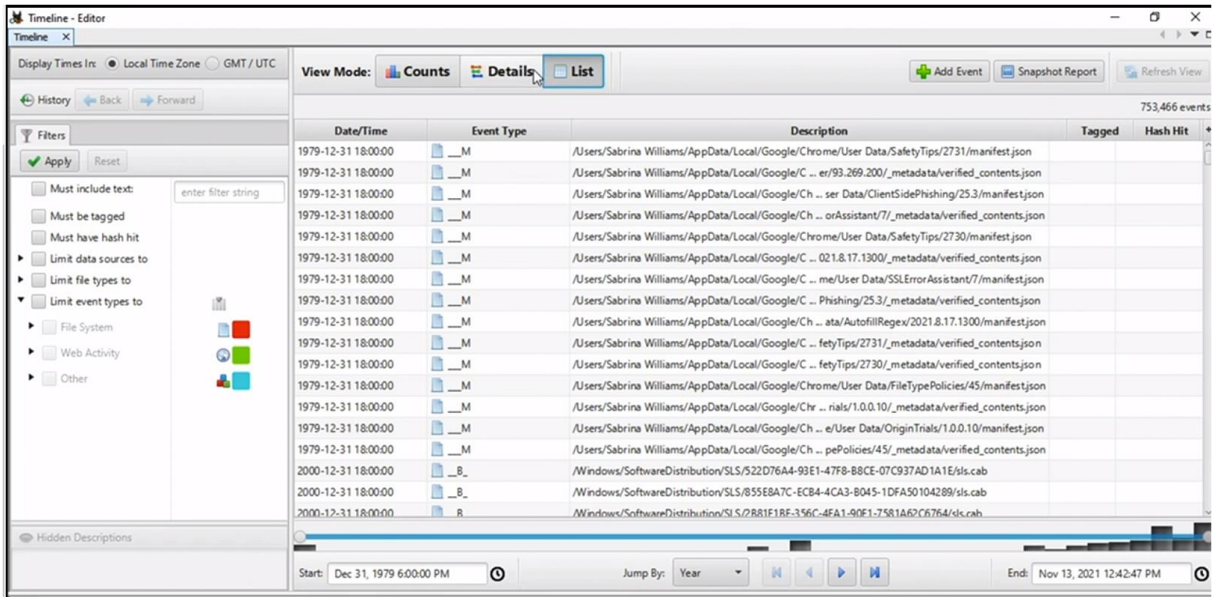
Abyste získali úplnou časovou osu, budete muset počkat, až bude zpracování vstupních dat dokončeno. Tyto informace budou prezentovány ve sloupcovém grafu zvaném *Counts* (viz Obr. 3.2.3.4), který používá počet událostí. Toto zobrazení můžete použít k zobrazení množství aktivity v daném časovém rámci. Pokud například podezřelý tvrdí, že zařízení nepoužil, natož aby jej vlastnil, lze použít funkci *Counts* k podpoře nebo zamítnutí jeho tvrzení. Toto zobrazení lze změnit na zobrazení podrobností (*Details* – Obr.3.2.3.4) nebo seznamu (*List* – Obr. 3.2.3.5) nastavením v horní části.



Obr. 3.2.3.3 Zobrazení časové osy při nastavení *Count*



Obr. 3.2.3.4 Zobrazení časové osy při nastavení *Details*

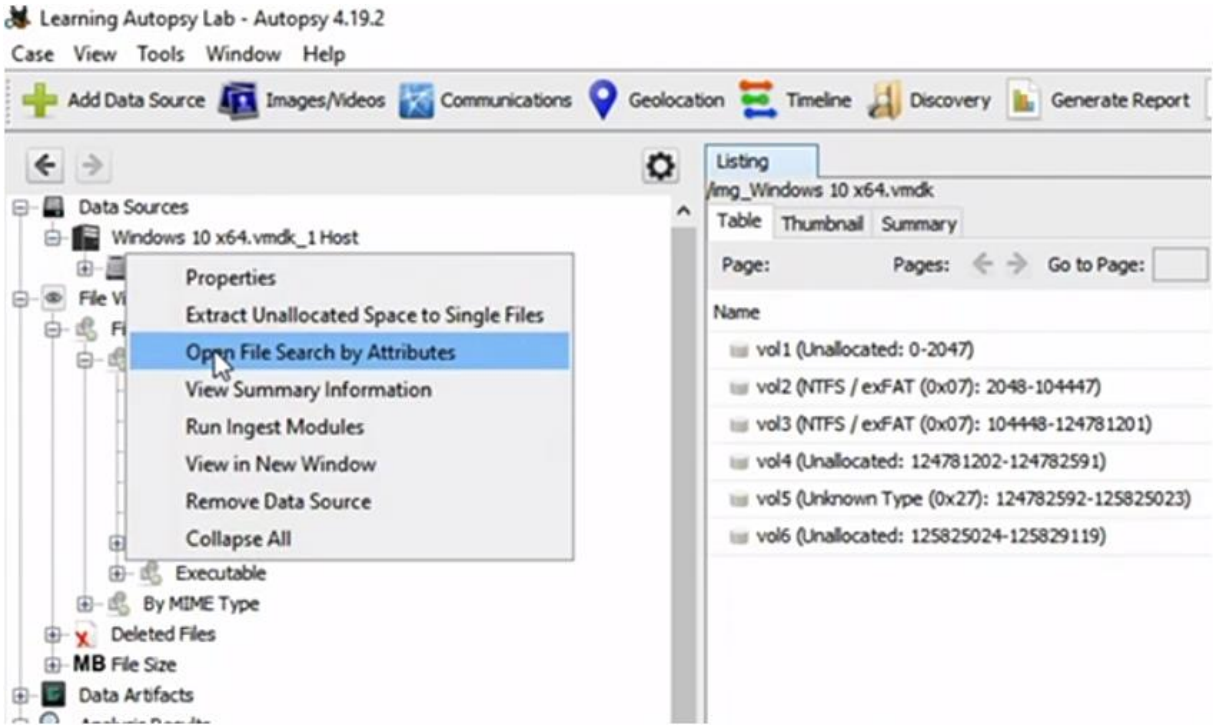


Obr. 3.2.3.5 Zobrazení časové osy při nastavení *List*

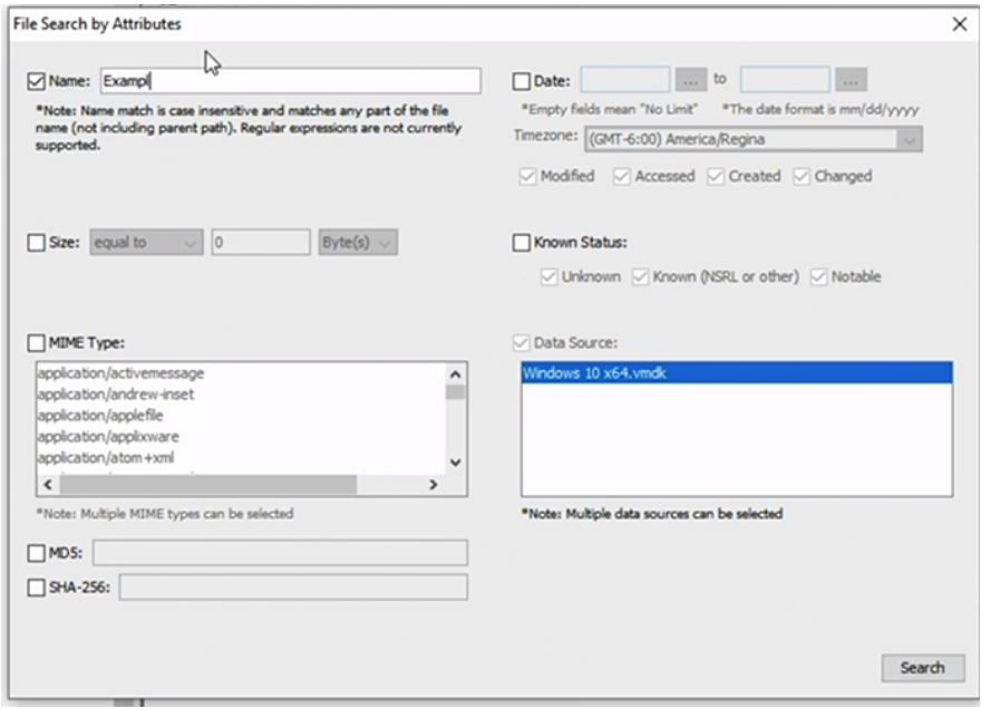
3.3 Vyhledávání a hlášení

3.3.1 Vyhledávání klíčových slov a souborů

Autopsy může ze souborů extrahovat řadu informací. Nástroj pro vyhledávání souborů je přístupný z nabídky nástroje Tools nebo kliknutím pravým tlačítkem myši na uzel zdroje dat v adresářovém stromu, soubory pak lze hledat podle atributů (klik na *Open File Search by Attributes* – Obr. 3.3.1.1 a získáte okno z Obr. 3.3.1.2.



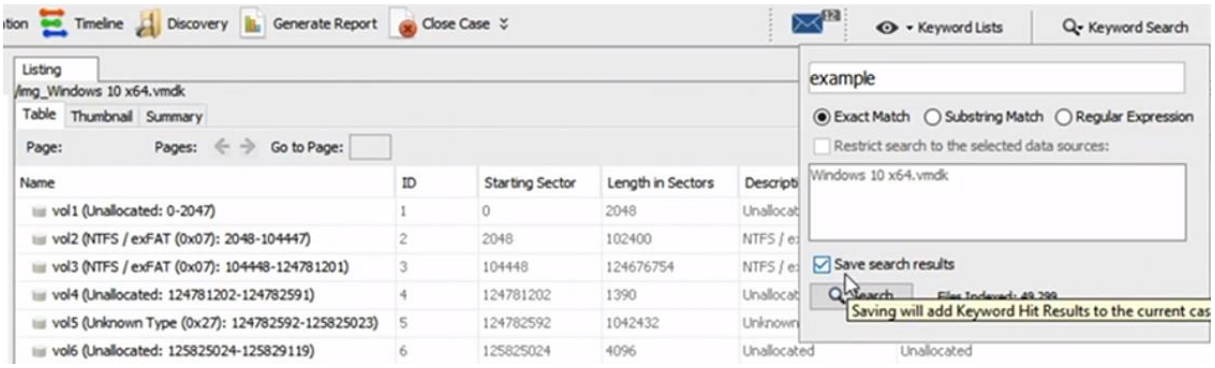
Obr. 3.3.1.1 Cesta z nabídky Tools k Open File Search by Attributes



Obr. 3.3.1.2 Vyhledávání v souborech podle atributů (*Open File Search by Attributes*)

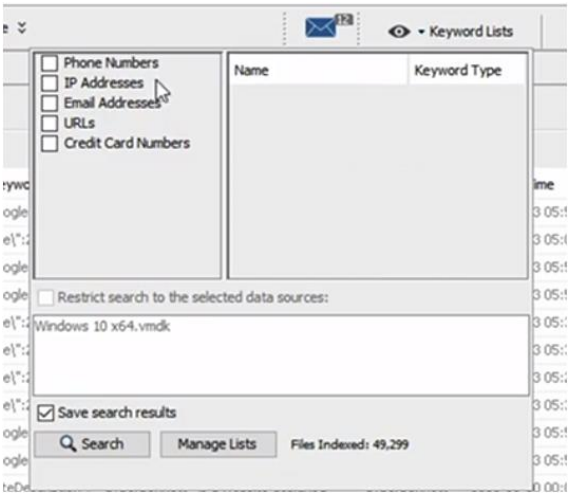
Existuje několik kategorií, které lze použít k vyhledání souborů a adresářů. Poblíž textového pole jsou poznámky s hvězdičkou – ty si je třeba pečlivě pročíst. Název například rozlišuje velká a malá písmena a shoduje se s jakoukoli částí názvu souboru. V tomto místě nejsou regulární výrazy podporovány.

Druhý způsob vyhledávání je v pravém rohu obrazovky – podle jednoho klíčového slova (*Keyword Search*) nebo seznamu klíčových slov (*Keyword List*)[9], viz Obr. 3.3.1.3. Zde regulární výrazy podporovány jsou a lze u nich použít pro specifické vzory a podporu mnoho druhů zástupných karet[10]. Pravidla pro tvorbu regulárních výrazů lze nalézt např. na ttp://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html, např. po sobě jdoucí skupiny pěti a šesti číslic oddělené mezerou (např. 01234 567890) lze zapsat pomocí výrazu `[0-9]{5}[ ][0-9]{6}`



Obr. 3.3.1.3 Vyhledávání podle klíčového slova (*Keyword Search*) nebo seznamu klíčových slov (*Keyword List*)

V seznamech klíčových slov (*Keyword Lists*) lze vybírat podle telefonního čísla, IP adresy, e-mailové adresy, URL a čísla kreditní karty – viz obr. 3.3.1.4.



Obr. 3.3.1.4 Výběr v seznamech klíčových slov (*Keyword Lists*)

3.3.2 Značkování (Tagging)

Značování (tagging) je jiný název pro záložky a umožňuje vám označit a odkazovat na soubor, který vás zajímá, pro pozdější použití. Můžete to udělat kliknutím pravým tlačítkem myši na objekt a výběrem příslušné značky.

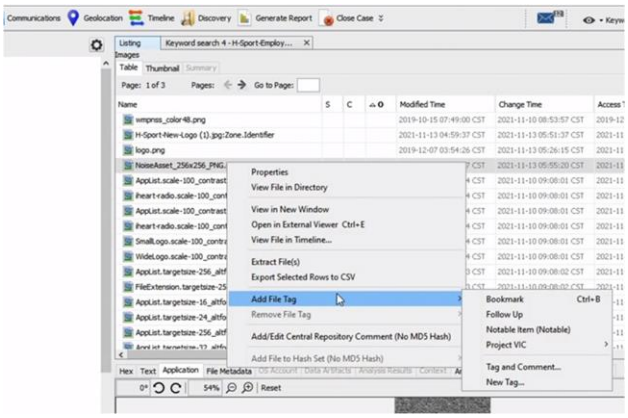
Existují dva různé typy značek

[9] https://sleuthkit.org/autopsy/docs/user-docs/4.4.1/ad_hoc_keyword_search_page.html

[10] https://www.youtube.com/watch?v=yvAMu6h7bnQ

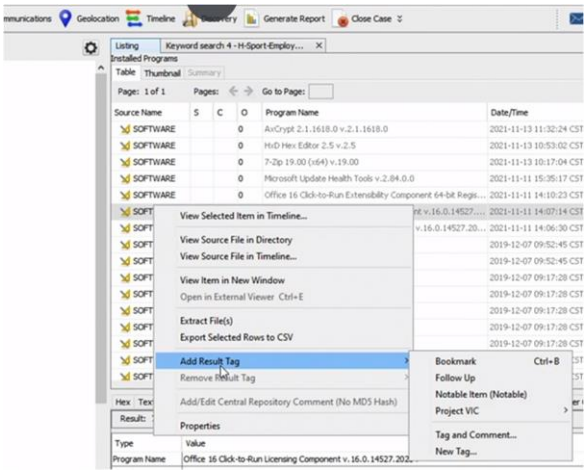
- značka výsledku (*result tag*).
- značka zajímavého souboru (*file tag*).

Na obr. 3.3.2.1 je ukázka přidání značky *file tag*, např. při vyšetřování manželské nevěry lze pomocí tagu označit fotky, na kterých je někdo jiný než manžel.



Obr. 3.3.2.1 Přidání značky souboru

Na obr. 3.3.2.2 je jiný příklad použití značky *Result Tag*. V tomto případě jsou výsledky generovány ze samotných modulů. Již existující názvy značek budou mít svůj popis. Komentář je zde něco dodatečného, co je třeba zaznamenat, např. místo nálezu.



Obr. 3.3.2.2 Použití značky *result tag*

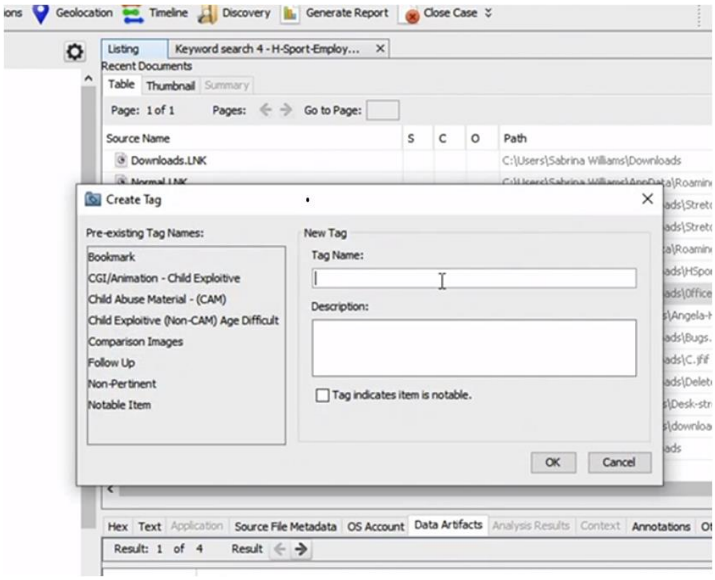
Existuje několik výchozích názvů značek:

Bookmark (záložka), což je defaultní značka pro označování souborů, které uživatele zajímají.

- *follow-up* (následující)
- *Notable items* (pozoruhodné položky)

Project VIC je mezinárodní kategorizace s ohledem na případy zneužívání dětí. Jednotlivé kategorie mají přidělené barvy od zelené po červenou (materiál zneužívání dětí). V budoucnu tuto kategorizaci autoři Autopsy hodlají zaměnit na vlastní.

Samotného značkování se bezprostředně týkají další tři možnosti. Lze použít existující tag, k tagu přidat komentář *Tag and Comment* a vytvořit nový tag (kliknout *New Tag* – viz Obr. 3.3.2.3).



Obr. 3.3.2.3 Vytvoření nové značky (Tagu)

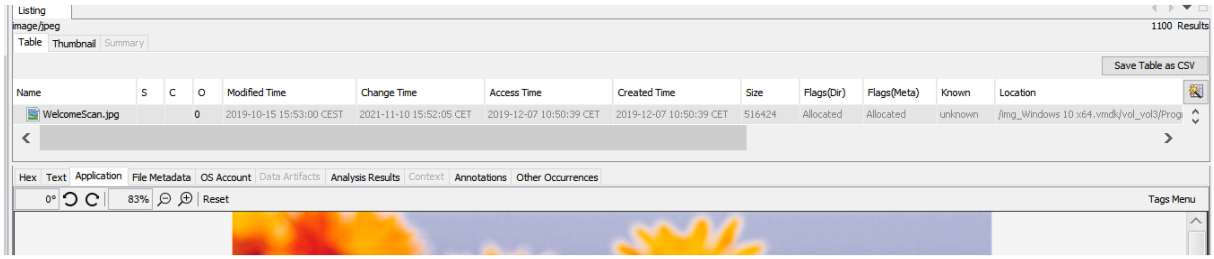
Již existující názvy značek budou mít popis, komentář musí být tím pádem něčím dodatečným, co by bylo také zapotřebí zaznamenat, jako je například místo, kde byl soubor nalezen. Možná byl soubor smazán, aby se zničil důkaz, což ukazuje, že uživatel si byl vědom jeho existence.

Defaultní značka by měla být označena v centrálním úložišti jako notable (pozoruhodná). Vytvoření vlastního názvu značky bude automaticky uloženo nad výchozími značkami a je určeno pro případné budoucí použití. Existuje také možnost označit skupinu položek. Jako kontextní odkaz zde slouží žlutý vykřičník.

Lze zvýraznit všechny položky, které je třeba označit, a to kliknutím na první z nich a poté přejitím na další soubory. Po kliknutí pravým tlačítkem myši můžete kliknout na *Add Results* a přidat je k čemukoli, co je zapotřebí. Poté si lze značku prohlédnout ve stromovém prohlížeči ve složce Tagy.

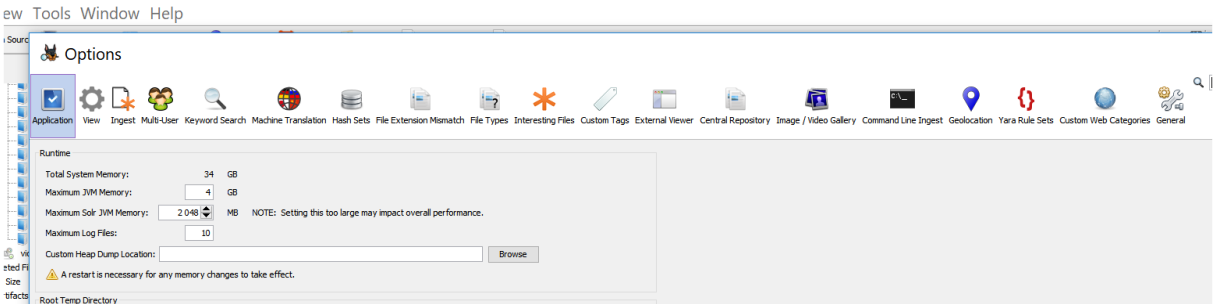
Další funkce značkování se nazývá image tagging (označování obrázků). Umožňuje označit část obrázku prohlíženou v *Content Viewer*. Tato funkce je dostupná pouze pro Windows[11]. K provedení této akce musí být obrázek vybrán v prohlížeči výsledků (Results Viewer). Tato funkce bude užitečná např. tehdy, když je třeba identifikovat konkrétní objekt na různých obrázcích a pak se na něj je třeba odkazovat později. Manipulaci s tagy obrázků zajišťuje *Tag Menu* v pravé horní části obrázku (*Create, Delete, Hide, Export*) – viz Obr. 3.3.2.4.

[11] Windows jsou zde preferovaný systém.



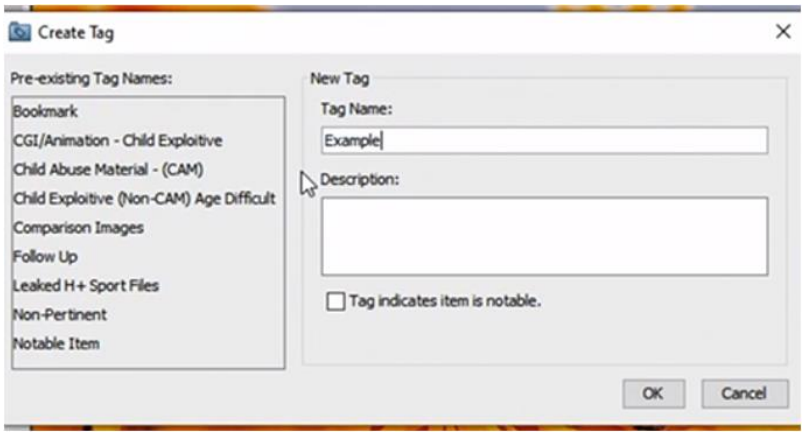
Obr. 3.3.2.4 Tag Menu obrázku

Seznam tagů lze spravovat prostřednictvím karty Tags v nabídce Options (možnosti). Cesta je z *Tools* přes *Options* na *Custom Tags* – viz Obr. 3.š.2.5). Je třeba také poznamenat, že smazáním tagu nedojde k jeho odstranění z žádných označených položek. A tato značka bude také použitelná v každém případě, ve kterém byla použita.



Obr. 3.3.2.5 Z nabídky Tools se dostanete přes *Options* k *Custome Tags*

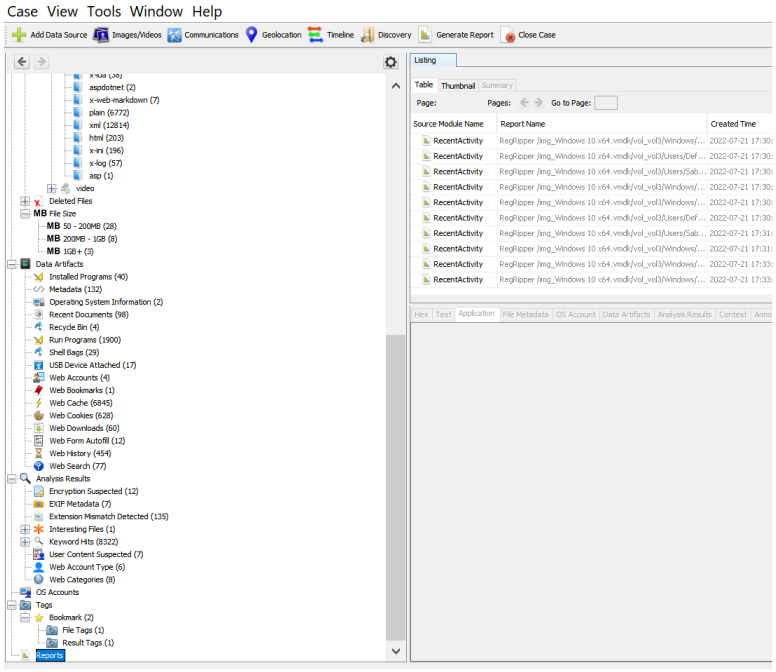
Řekněme například, že shromažďujete data o podezřelém z vraždy. Podezřelý je viděn s jinou osobou na několika různých fotografiích. Takže je třeba označit jeho i komplice. Později se zjistí, že se jedná o jeho bratra, a tyto informace lze poskytnout právníkům v dané zprávě. Označením obou jedinců není třeba znovu hledat obě osoby na fotkách. Obrázek lze vybrat, změnit jeho velikost a případně zase odstranit značku obrázku. Dvojím pokliknutím poblíž tagu obrázku ho lze znovu vyvolat a zařadit (kategorizovat) do některého z existujících názvů tagů a také lze přidat komentář (Obr. 3.3.2.6 ukazuje kategorizaci obrázku).



Obr. 3.3.2.6 Kategorizace obrázku pomocí vytvoření značky (tagu)

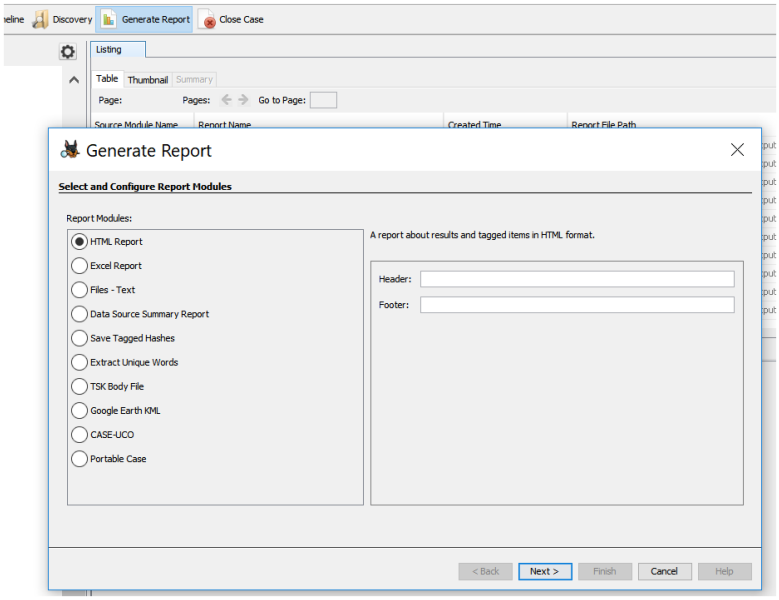
3.3.3 Generování hlášení (raportů)

Modul raportů umožňuje uživateli extrahovat klíčové informace z případu v různých formátech, které zahrnují např. HTML, Excel, Text, CSV. Většina typů sestav vyžaduje, abyste vybrali, který zdroj dat chcete zahrnout. Většina modulů raportů vygeneruje soubor sestav zobrazený pod poznámkou k sestavám ve stromovém prohlížeči – viz Obr. 2.6.3.1.

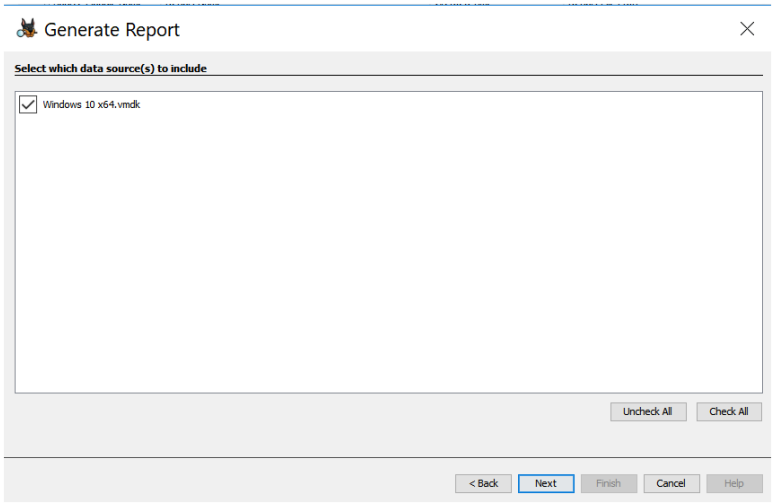


Obr. 3.3.3.1 Hlášení využívá záznamy z provedených aktivit

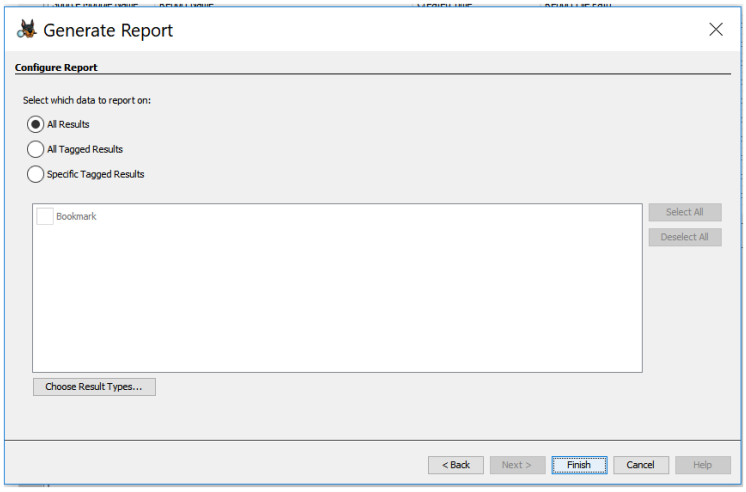
Na základě jednotlivých zjištění se vytváří základní zpráva, provede se to kliknutím na *Generate Report*. U zpráv HTML si lze vybrat záhlaví nebo zápatí, které se zobrazí s výsledky – příklad postupu je zachycen na obr. 3.3.3.2 až 3.3.3.6.



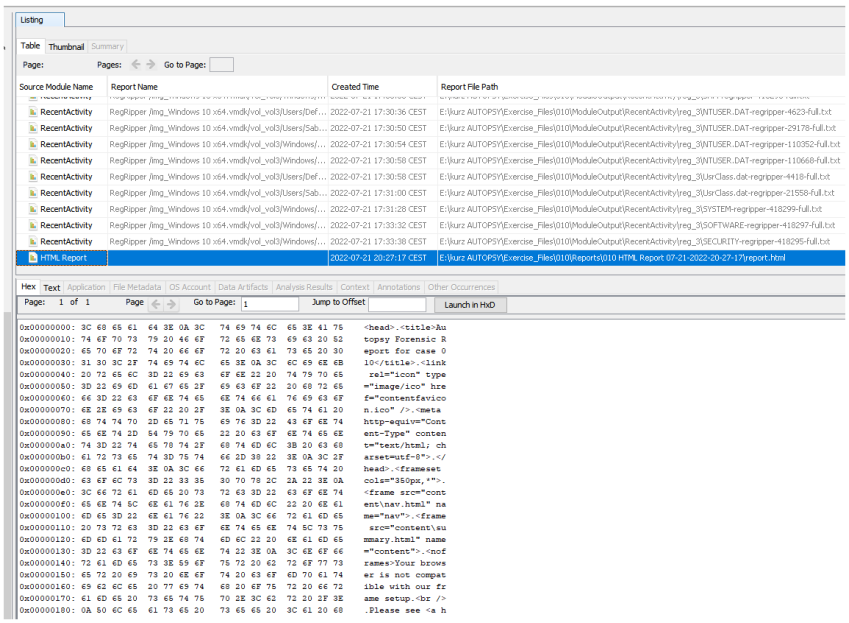
Obr. 3.3.3.2 Generování HTML zprávy se záhlavím a zápatím



Obr. 3.3.3.3 Výběr objektu hlášení



Obr. 3.3.3.4 Upřesnění typu výstupu



Obr. 3.3.3.5 Výstupní soubor hlášení

Autopsy Forensic Report

Warning, this report was run before ingest services completed!

HTML Report Generated on 2022/07/21 20:27:17

Case:	010
Case Number:	010
Number of data sources in case:	1
Examiner:	jarda

Image Information:

Windows 10 x64.vmdk

Timezone:	Europe/Prague
Path:	E:\kurz AUTOPSY\Exercise_Files\Windows 10 VM\Windows 10 x64.vmdk

Software Information:

Autopsy Version:	4.19.3
Central Repository Module:	4.19.3
DJI Drone Analyzer Module:	4.19.3
Data Source Integrity Module:	4.19.3
Email Parser Module:	4.19.3
Embedded File Extractor Module:	4.19.3
Encryption Detection Module:	4.19.3
Extension Mismatch Detector Module:	4.19.3
File Type Identification Module:	4.19.3
Hash Lookup Module:	4.19.3

Obr. 3.3.3.6 Text výstupného hlášení

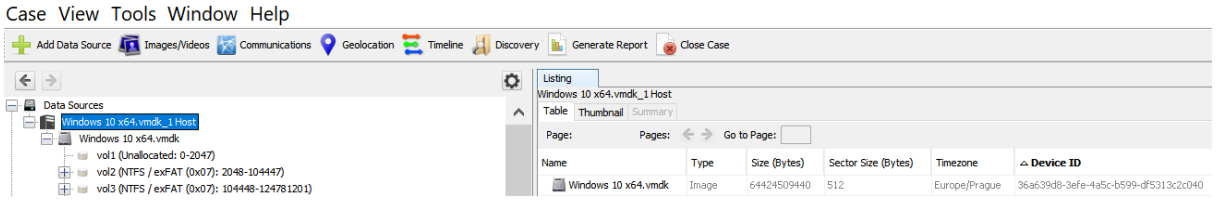
4 Zadání úkolů

4.1 Úkol 1

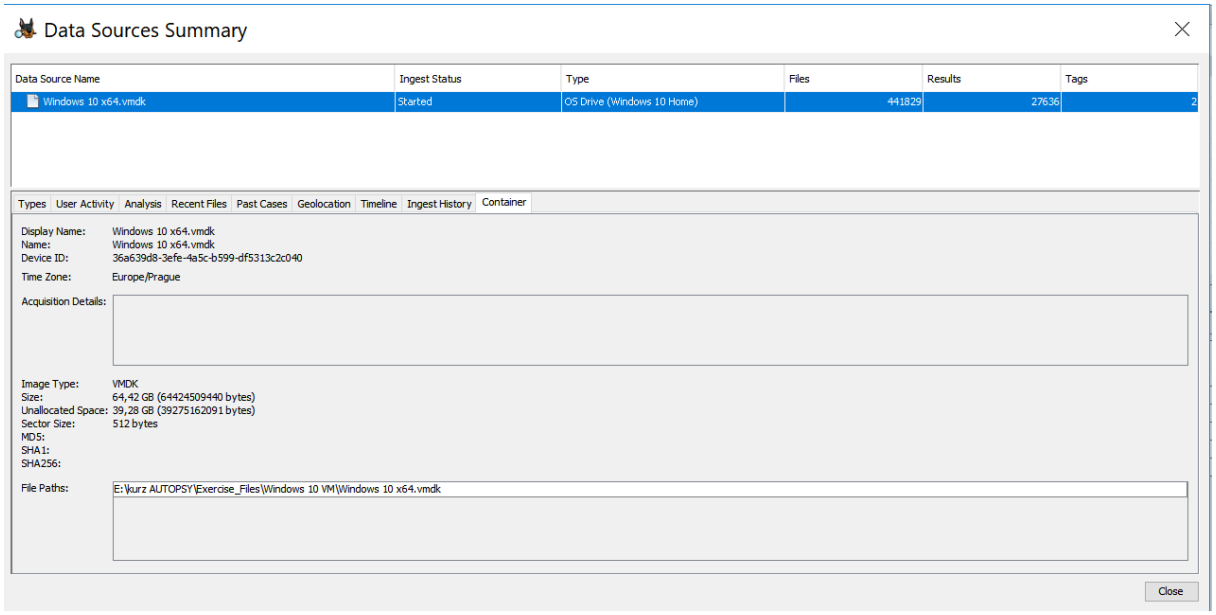
4.1.1 Zadání

Nalezněte ID zařízení pro poskytnutý obraz disku. Existuje několik způsobů, jak tyto informace najít (např. použít *Data Source Summary*).

4.1.2 Řešení



anebo



4.2 Úkol 2

4.2.1 Zadání

Analyzujte spustitelný soubor H+ a odpovězte na následující dvě otázky.

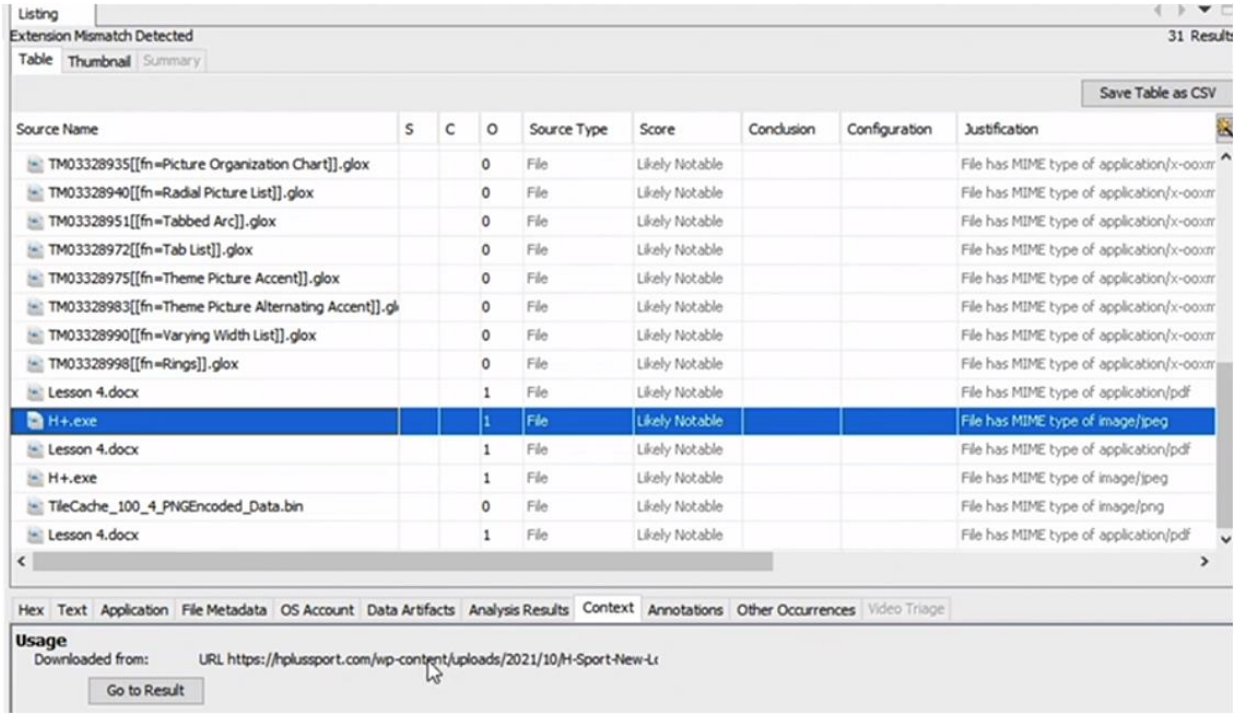
- Odkud to bylo staženo?
- Jaký typ souboru to byl původně?

4.2.2 Řešení

Přejděte do prohlížeče stromu *Tree Viewer*, skrolujte dolů a otevřete *Analyst Result* a vyberte *Extension Mismatch* Detected. Pak přejděte dolů, dokud se nenalezne spustitelný soubor H+, (na obrazovce jich je více, jen proto, že byl tento modul spuštěn několikrát. To nebude mít vliv na výsledky).

Takže první otázka zní, odkud byl stažen? Odpověď lze nalézt tak, že přejdete na kartu *Context* a zjistíte, že tento soubor samotný byl stažen z následující adresy URL. Tato adresa URL pochází z webu H+ Sports, takže vypadá legitimně.

Druhou odpověď lze nalézt posouváním vpravo v prohlížeči výsledků, kde můžeme vidět, že tento soubor je JPEG, ve dvou různých oblastech. První je Justification, druhý je typ MIME. Ať tak či onak, tento soubor byl původně souborem JPEG i přes jeho spustitelnou příponu.



4.3 Úkol 3

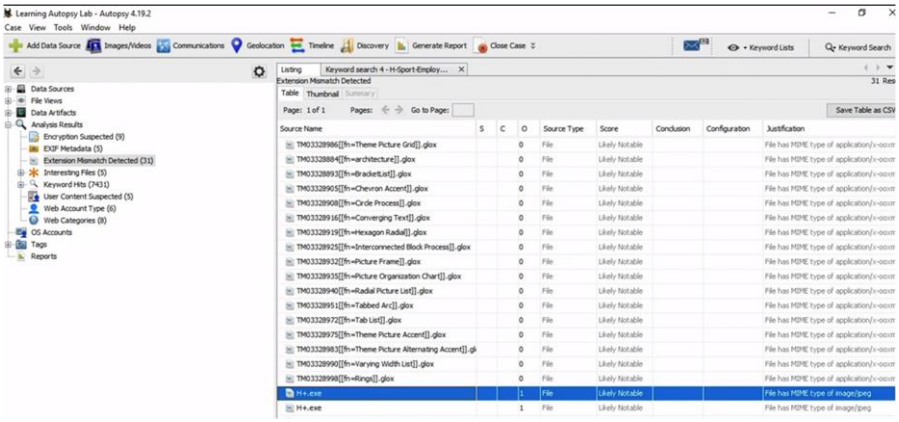
4.3.1 Zadání

Nalezněte nové logo, které uniklo. A jakmile jej najdete, vyhledejte všechny výskyty loga pomocí možnosti vyhledávání souborů a hash tohoto loga. Až s tím budete hotovi, přejděte na další video s naším řešením.

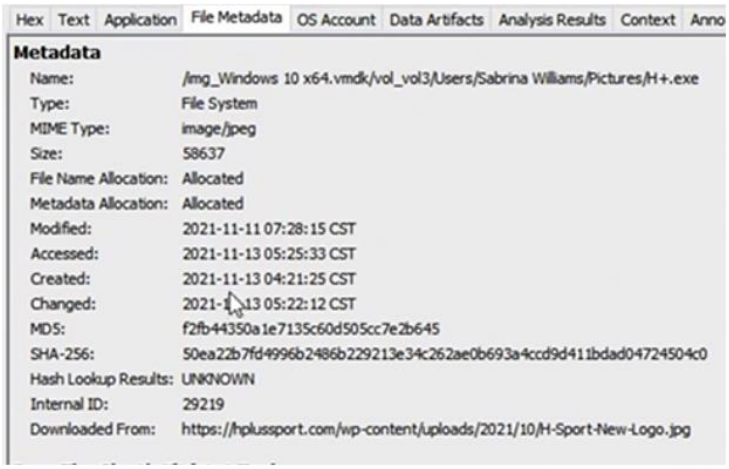
4.3.2 Řešení

Řešení této úlohy je postaveno na řešení druhé úloh. Pokud si pamatujete spustitelný soubor H+, který jsme analyzovali ve druhé kapitole, všimnete si, že na kartě aplikace jste viděli uniklé logo.

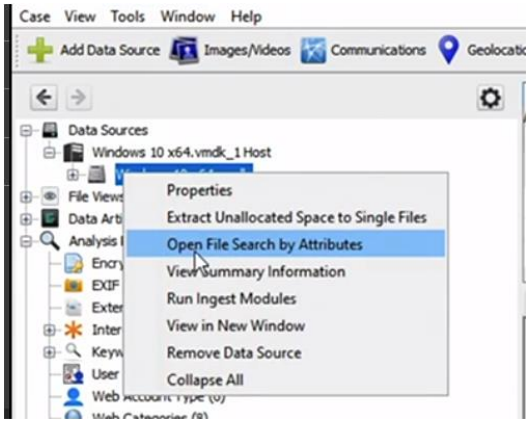
Vraťme se tam tedy rozbalením *Analysis Results, Extension Mismatch Detected*.



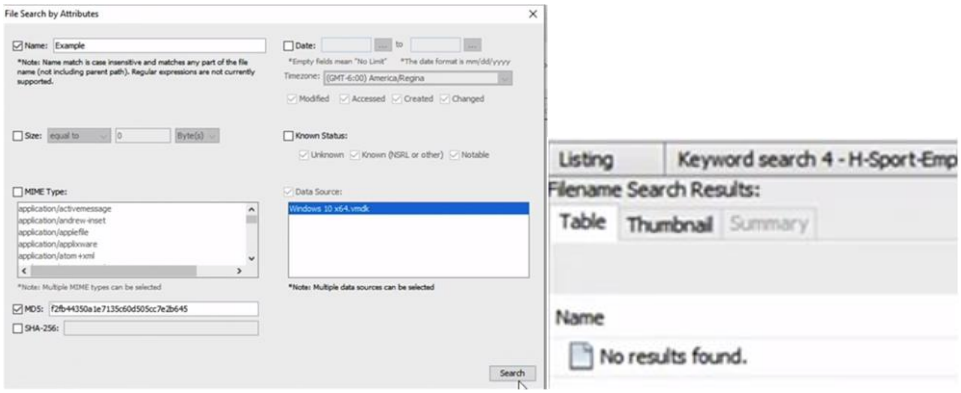
Náznak řešení je patrný podle přípony jpeg a typu MIME. Když soubor otevřete, uvidíte logo. A když přejdete na metadata souboru, můžete získat hash MD5.



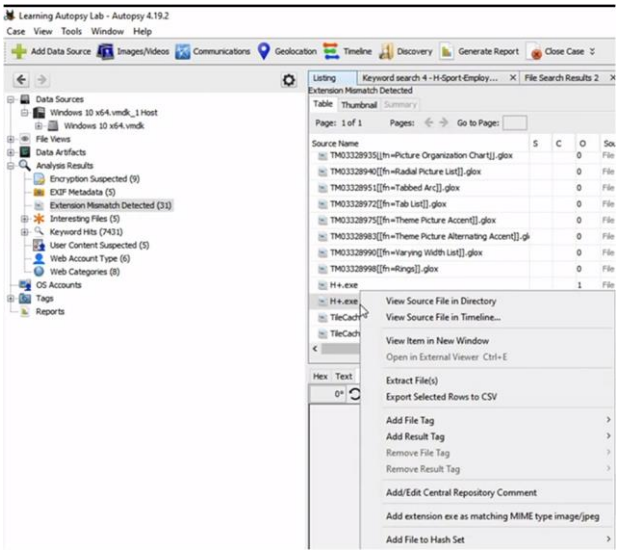
Kopírujte hash pomocí CTRL C, pak přejděte na *Data Sources*, kliknout pravým tlačítkem myši na *Open File Search by Attributes*.



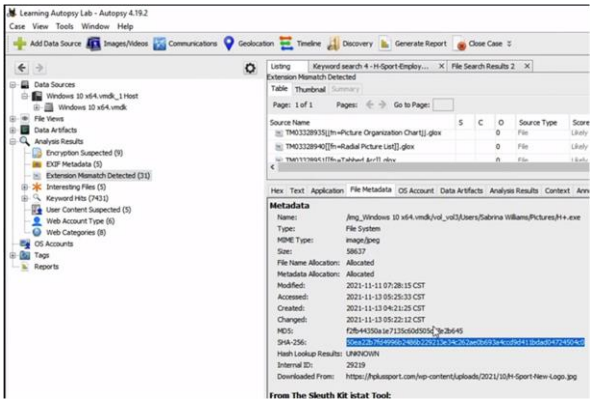
Pak přejdete na MD5, vložíte tam hodnotu a kliknete na Search… a nenajdete nic.



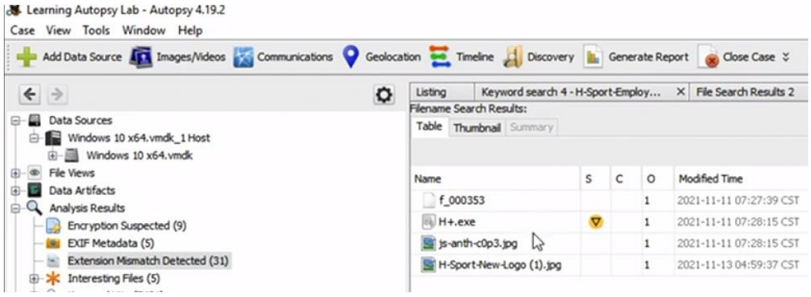
Takže krok zpět.



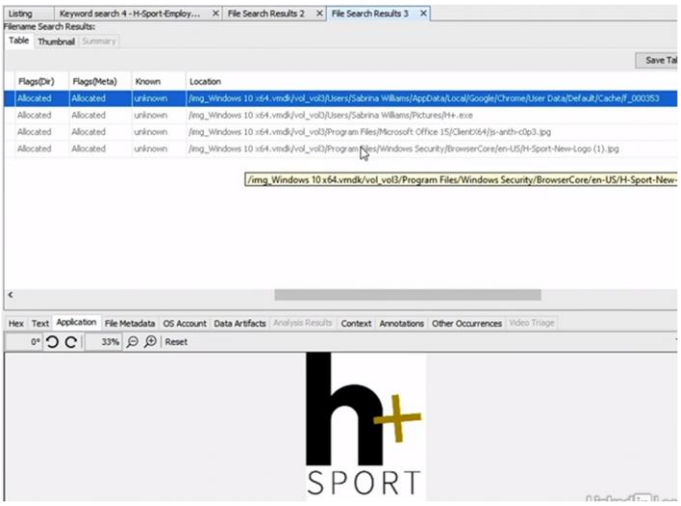
Zkusíme to znovu přes SHA256.



Vraťte se zpět do *File Search for Attributes*:



Všimněte si, že na této ploše máme čtyři různé instance souboru. Chcete-li o nich získat další informace, můžete se podívat na informace, čas úprav, časy změn a data, ke kterým byl přístup. Pokud je vyberete, všimnete si v aplikaci, že se skutečně jedná o identické kopie, navzdory samotným různým názvům souborů.



A konečně, pokud bychom chtěli jen potvrdit, abychom viděli, kde byly všechny tyto soubory umístěny, máte spustitelný soubor, který byl umístěn v adresáři *Pictures*. Všechno ostatní bylo nějak skryto v jiném, neznámém souboru programu. Nicméně zadaný úkol byl vyřešen.

Seznam použitých zdrojů

(ENISA 2013) Digital forensics Handbook, Document for teachers September 2013. ENISA September 2013. Dostupné z: https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/documents/digital-forensics-handbook

(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

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

(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/