LNK File Forensics

Čo sa skrýva za príponou .LNK

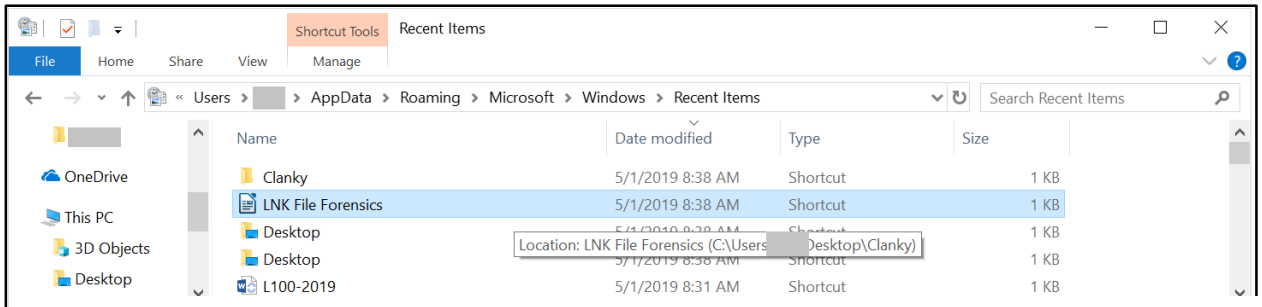
So súborovým typom .lnk sa stretáva každý používateľ OS Windows na dennej báze. Najznámejším zástupcom LNK súborov sú odkazy – shortcuts, ktoré slúžia na rýchly prístup k najpoužívanejším programom, súborom či lokalitám. Takéto odkazy buď vytvárame ručne, alebo sa generujú pri inštalácií programu. LNK súbory, oficiálne Windows Shortcut Files, však vznikajú pri mnohých iných udalostiach a akciách v systéme, spravidla transparentne. Niektoré zo situácií, pri ktorých vznikne LNK file, popíšeme v tomto článku.

Windows Shortcut Files sú v podstate metadátovými súbormi, špecifickými pre platformu Windows. Interpretuje ich Windows Shell. Preto sa tieto aj ďalšie špecifické štruktúry s formátom podobným LNK súborom označujú ako tzv. Shell Items.

LNK súbory sú identifikovateľné na základe magic number 0x4C (4C 00 00 00) na ich začiatku. Ďalším rozlišovacím znakom je GUID (CLSID) 00021401-0000-0000-c000-000000000046, ktorý možno nájsť na offsete 4 (bajty).

Kde ich hľadať?

%userprofile%\AppData\Roaming\Microsoft\Windows\Recent



Obrázok 1- Recent Items

%userprofile%\AppData\Roaming\Microsoft\Office\Recent

Forenzný význam

Tak ako mnohé iné forenzne významné artefakty OS, aj LNK súbory slúžia na optimalizáciu práce používateľa so systémom. Urýchľujú prístup k programom a lokalitám. OS tiež uchováva informácie o naposledy otvorených súboroch – práve vo forme LNK súborov – aby ich vedel používateľovi opäť rýchlo

sprístupniť pri nasledujúcej relácií. Preto napríklad textový editor, programy MS Office či prehrávače zvuku pri otvorení umožňujú výber z posledných spracúvaných súborov.

Aby bola táto funkcionalita možná, Windows automaticky generuje LNK súbory pri každom otvorení súboru. V skutočnosti sú vytvorené 2, resp. až 3 LNK súbory: jeden pre súbor samotný, jeden pre adresár, v ktorom sa súbor nachádza, a, od operačného systému Windows 10, vznikne tretí LNK file s dátami o prarodičovskom adresári súboru. Od OS Windows 10 takisto platí, že LNK file vzniká už pri vytvorení nového súboru na disku, a že prípona originálneho súboru je súčasťou názvu LNK súboru.

Tieto súbory sú uložené v používateľskom adresári „Recent Documents“, ku ktorému existuje skratka vo Windows Exploreri: pri otvorení nového okna môžete vidieť „Quick Access“, zoznam „Recent files“ a „Frequent folders“. Skutočnou lokalitou, kde možno súbory nájsť, je adresár %userprofile%\AppData\Roaming\Microsoft\Windows\Recent. Jeho kapacita je 149 LNK súborov.

Informácie o súboroch naposledy otvorených/editovaných programami MS Office možno nájsť v LNK súboroch v osobitnej lokalite %userprofile%\AppData\Roaming\Microsoft\Office\Recent.

Z forenzného hľadiska vieme z existujúcich LNK súborov zistiť:

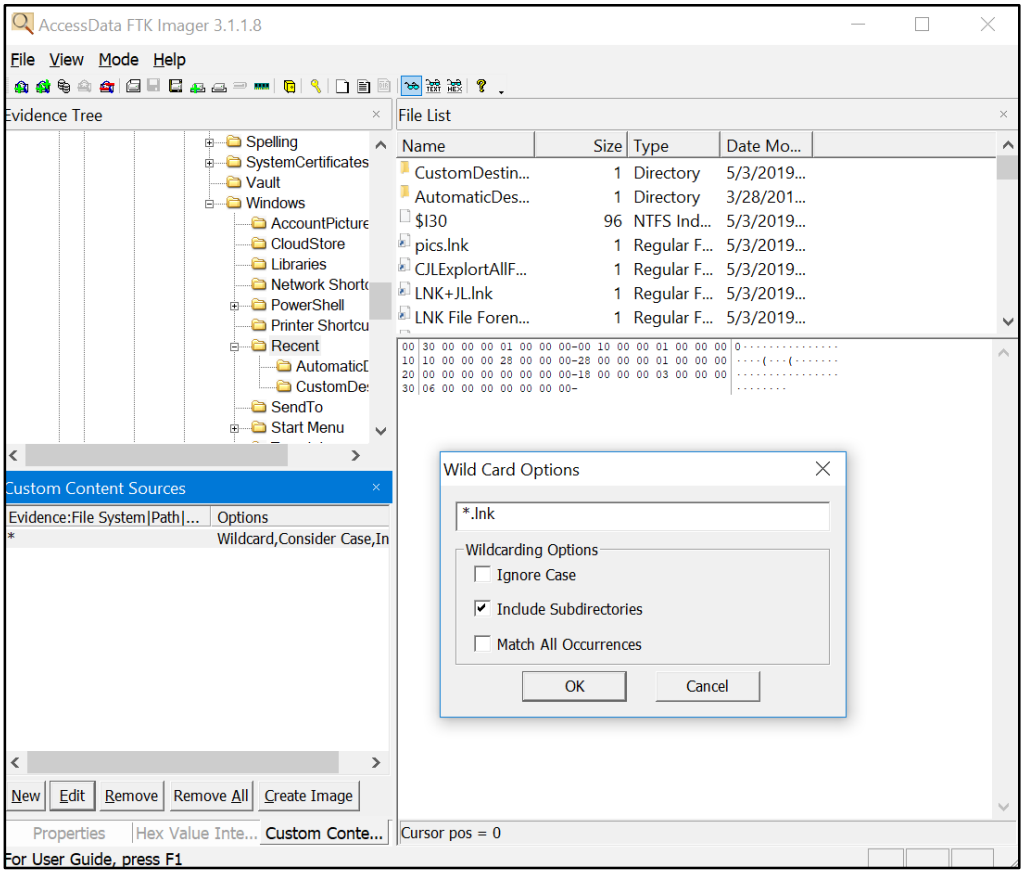
- MACB časové pečiatky súboru, na ktorý LNK súbor ukazuje. Môžeme ich interpretovať nasledovne:
  - Creation Date = čas, kedy bol cieľový súbor 1.krát otvorený, pretože vtedy sa LNK súbor vytvára
  - Last Modification Date = čas, kedy bol target naposledy otvorený, pretože LNK súbor sa aktualizuje pri každom dvojkliku na súbor, ktorý popisuje
  - Aj ak bol súbor zmazaný, LNK file bude naďalej existovať
- Informácie o pamäťovej jednotke (volume), na ktorej bol súbor zapísaný (názov, typ, sériové číslo).
- Na akom type zariadenia bol súbor zapísaný – na pevnom či vymeniteľnom disku, alebo na sieťovom umiestnení.
- Pôvodnú cesta k súboru – relatívna i absolútna.
- MAC adresu zariadenia, odkiaľ cieľový súbor pochádza (nie vždy).

Poznámka: v dokumente budeme súbor, o ktorom obsahuje LNK súbor informácie, označovať ako cieľový (Target File) súbor. Zdrojovým súborom (Source File) budeme rozumieť konkrétny LNK súbor.

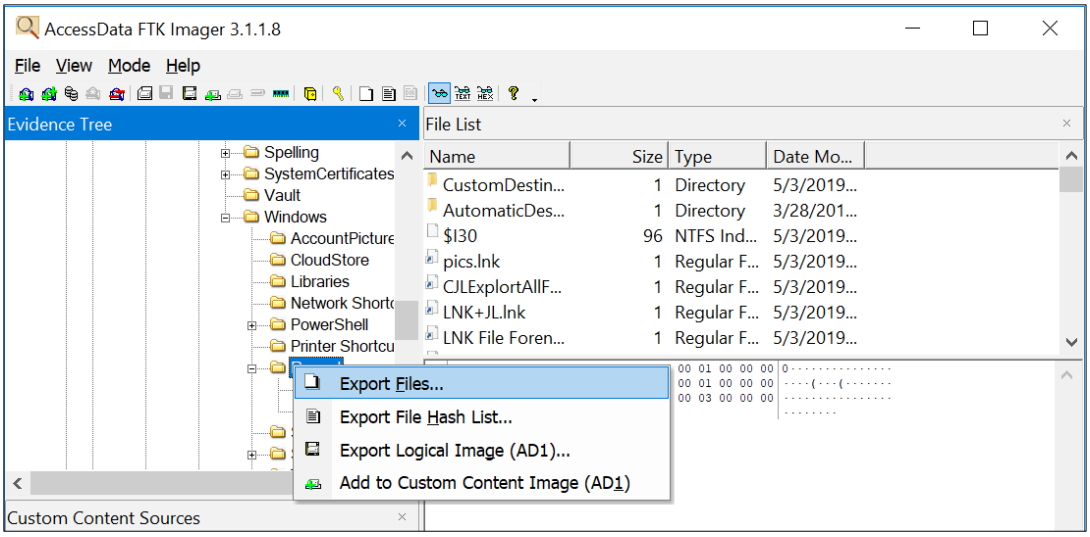
Ako získať .LNK súbory z analyzovaného zariadenia

Na získanie súborov z bežiaceho systému alebo z pripojeného image disku je možné použiť napríklad nástroj FTK Imager. Z namountovaného disku vieme pomocou vytvorenia wildcard vzoru *.lnk získať

všetky súbory s príponou .LNK z analyzovaného pamäťového zariadenia a pridať ich na tzv. Custom Content Image. Alternatívne možno exportovať LNK súbory priamo z lokality, kde sú uložené.



Obrázok 2 - Vytvorenie WildCard v FTK Imageri

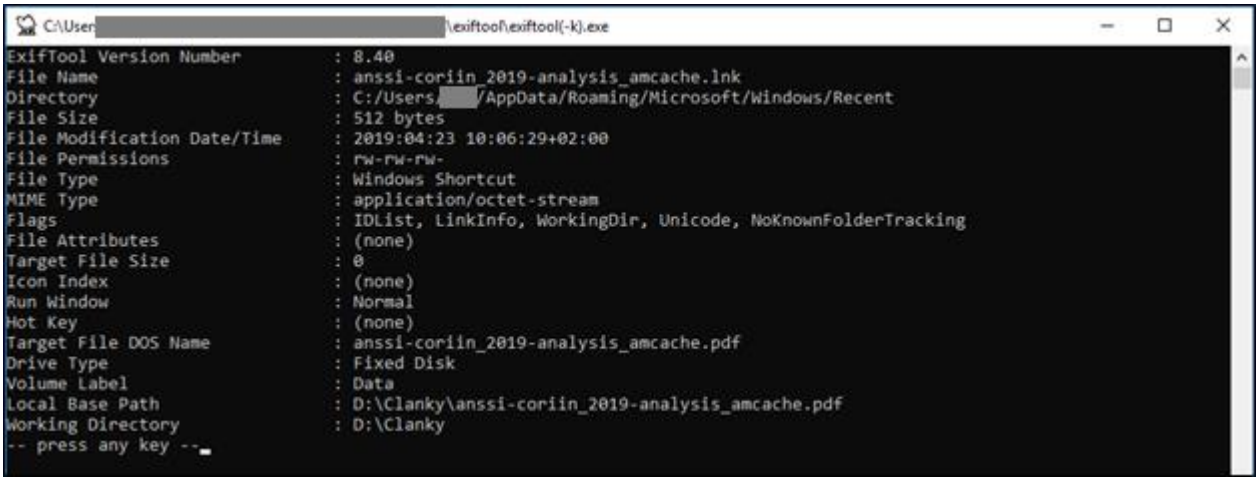


Obrázok 3 - Export súborov z FTK Imagera

Ako analyzovať .LNK súbory

Existuje viacero nástrojov, pomocou ktorých dokážeme LNK súbory analyzovať.

Keďže ide o metadátové súbory, môžeme ich na začiatok preskúmať napríklad pomocou nástroja Exiftool:



Obrázok 4 - LNK súbor a Exiftool

Vo výstupe vidíme informácie o umiestnení súboru na disku, nie však všetky informácie. Použijeme preto ďalší nástroj - LECmd, alebo LinkfileExplorer vo verzii pre príkazový riadok.

```
C:\Forensic Program Files\Zimmerman>LECmd.exe -f
C:\Users\XXX\AppData\Roaming\Microsoft\Windows\Recent\pestudio.zip.lnk
LECmd version 1.1.0.3

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd

Command line: -f
C:\Users\XXX\AppData\Roaming\Microsoft\Windows\Recent\pestudio.zip.lnk

Processing
'C:\Users\XXX\AppData\Roaming\Microsoft\Windows\Recent\pestudio.zip.lnk'

Source file:
C:\Users\XXX\AppData\Roaming\Microsoft\Windows\Recent\pestudio.zip.lnk
  Source created:  2019-04-08 14:58:09
  Source modified: 2019-04-08 14:58:09
  Source accessed: 2019-05-02 14:43:22

--- Header ---
  Target created:  2019-04-08 14:19:09
  Target modified: 2019-04-08 14:19:10
  Target accessed: 2019-04-08 14:58:09
```

```
File size: 937,581
  Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, IsUnicode,
DisableKnownFolderTracking
  File attributes: FileAttributeArchive
  Icon index: 0
  Show window: SwNormal (Activates and displays the window. The window is
restored to its original size and position if the window is minimized or
maximized.)

Relative Path: ..\..\..\..\..\Downloads\pestudio.zip

--- Link information ---
Flags: VolumeIdAndLocalBasePath

>>Volume information
  Drive type: Fixed storage media (Hard drive)
  Serial number: 0CF98FE5
  Label: (No label)
  Local path: C:\Users\XXX\Downloads\pestudio.zip

--- Target ID information (Format: Type ==> Value) ---

  Absolute path: My Computer\Desktop\pestudio.zip

  -Root folder: GUID ==> My Computer

  -Root folder: GUID ==> Desktop

  -File ==> pestudio.zip
    Short name: pestudio.zip
    Modified: 2019-04-08 14:19:12
    Extension block count: 1

    --------- Block 0 (Beef0004) ---------
    Long name: pestudio.zip
    Created: 2019-04-08 14:19:10
    Last access: 2019-04-08 14:19:12

--- End Target ID information ---

--- Extra blocks information ---

>> Tracker database block
   Machine ID: sans-sift
   MAC Address: 00:0c:29:be:ef:fe
   MAC Vendor: VMWARE, INC.
   Creation: 2019-04-02 14:40:20
```

```
   Volume Droid: aa5b055a-2d19-4986-b630-35ada5326569
   Volume Droid Birth: aa5b055a-2d19-4986-b630-35ada5326569
   File Droid: 3d8d4c73-5555-11e9-b549-000c29e8c9be
   File Droid birth: 3d8d4c73-5555-11e9-b549-000c29e8c9be

>> Property store data block (Format: GUID\ID Description ==> Value)
   446d16b1-8dad-4870-a748-402ea43d788c\104    (Description not available)
==> Unmapped GUID: e20c140e-0000-0000-0000-100000000000


---------- Processed
'C:\Users\XXX\AppData\Roaming\Microsoft\Windows\Recent\pestudio.zip.lnk' in
0.11539360 seconds ----------
```

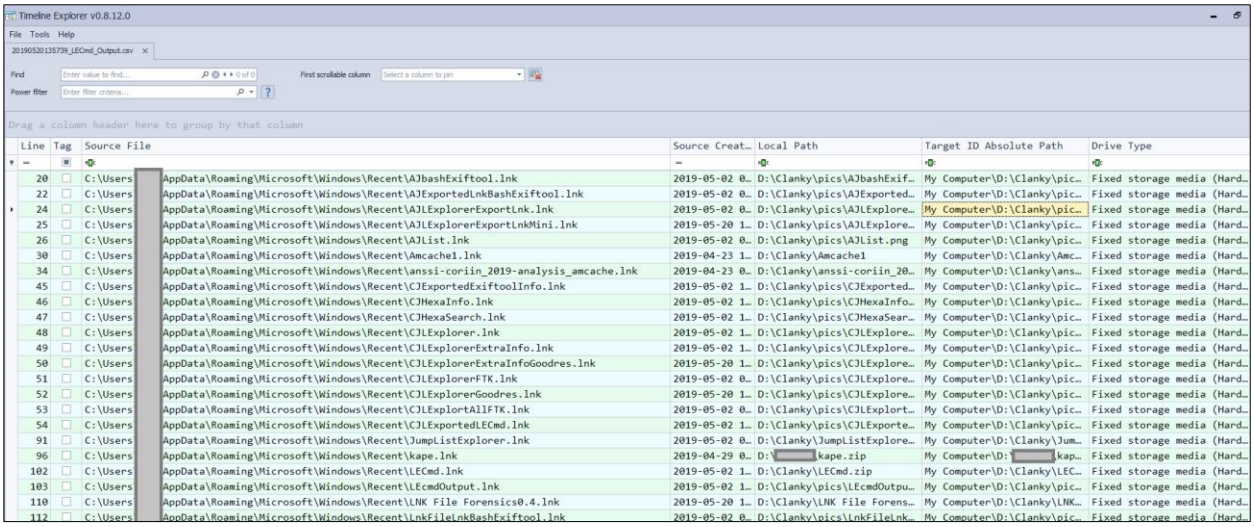
Zo súboru pestudio.zip.lnk môžeme vyvodiť nasledovné závery:

Keďže Create Time LNK súboru je 2019-04-08 14:58:09, v tomto čase sa súbor PEStudio.zip po prvý krát otvoril. Čas posledného prístupu k LNK súboru je rovnaký, vtedy sa teda s cieľovým .zip archívom naposledy manipulovalo. Informácie o cieľovom súbore hovoria, že pestudio.zip bol vytvorený 8.4.2019 o 14:19:09 a modifikovaný o sekundu neskôr. Ak sa ďalej pozrieme na lokalitu, v ktorej sa súbor nachádzal – Downloads – dáva sekundový odstup zmysel: súbor bol pravdepodobne stiahnutý z internetu, pričom sťahovanie začalo o 14:19:09 a trvalo (necelú?) sekundu. So súborom sme začali manipulovať v ten istý deň o 14:58:09 – mohlo ísť o rozpakovanie súboru, čo spôsobilo vytvorenie LNK súboru v priečinku Recent. (*V adresári by sa mal nachádzať aj LNK file s údajmi o rodičovskom adresári Downloads.)

Autor nástroja Eric Zimmerman pridal funkcionalitu spracovania adresára, obsahujúceho JumpListy, a exportovania spracovaných dát do súboru. Hlavičky stĺpcov špecifikujú, aké informácie môžeme z jediného LNK súboru získať:

- SourceFile
- SourceCreated
- SourceModified
- SourceAccessed
- TargetCreated
- TargetModified
- TargetAccessed
- FileSize
- RelativePath
- WorkingDirectory
- FileAttributes
- HeaderFlags
- DriveType
- VolumeSerialNumber
- VolumeLabel
- LocalPath
- CommonPath
- Arguments
- TargetIDAbsolutePath
- TargetMFTEntryNumber
- TargetMFTSequenceNumber
- MachineID
- MachineMACAddress
- MACVendor
- TrackerCreatedOn
- ExtraBlocksPresent

V ukážke nižšie vidíme príklad výstupu v CSV formáte, s viacerými skrytými stĺpcami. Dáta v CSV môžeme ďalej sortovať, filtrovať etc.



Obrázok 5 - Výstup LEcmd

JumpLists

JumpListy je hodno spomenúť súčasne s LNK súbormi z jednoduchého dôvodu: JumpListy obsahujú jeden alebo viacero LNK súborov, v závislosti od typu JumpListu rôzne usporiadaných. Môžeme ich pozorovať od verzie OS Windows 7, kedy pribudla funkcionalita panelu úloh: ak pravým tlačidlom myši klikneme na ikonu programu či súboru/adresára, môže si používateľ vybrať – „skočiť“ na posledné použité súbory, adresáre, ale i posledné vykonané úlohy.

JumpListy môžu byť dvoch typov: Automatic (ďalej len AJL) a Custom jumplists (ďalej CJL). Ani pri jednom z nich nejde o klasické LNK súbory.

V prípade AJL ide o súbory v OLECF formáte – proprietárna technológia Microsoftu, ktorá umožňuje prítomnosť viacerých dátových streamov v jednom súbore (a.k.a. Compound binary file, známe aj napr. z MS Office súborov). Každý stream v Automatic Destinations obsahuje vnorený LNK súbor, ktorý stade vieme extrahovať a parsovať. Ako napovedá názov, Automatic Destinations JL sú automaticky vytvárané operačným systémom pre každú aplikáciu, ktorá používa spoločné Windows API. Preto je ich formát štandardizovaný, a AJL sú preto jednoduchšie na parsovanie.

Custom JL sú definované vývojárom aplikácie: vývojári používajú JL ako mini-start menu na pridanie nejakých základných úloh - napr. po inštalácii programu 7zip s potvrdením defaultných volieb (asociácie súborov, vytvorenie odkazov a pod.), ktoré inštalátor ponúka, sa pri kliknutí pravým tlačidlom myši na súbor/archív zobrazia 7zipom poskytované úlohy.

Nad vznikom Custom JumpListov už nemá kompletnú kontrolu OS. Preto je ich interpretácia zložitejšia a spoľahlivosť z forenzného hľadiska nižšia. Záznamy v CustomDestinations sa vytvárajú, keď používateľ pripne program na panel úloh alebo k menu Štart. Každý takýto súbor obsahuje reťaz LNK súborov, zoradených za sebou – viď obrázky nižšie, ako vyzerajú v hexadecimálnom editore.

Položky automatických aj customizovaných JL môžeme deliť na

- **Destinations**: položky vo Frequent (Časté položky), Recent (Nedávne položky) a customizovaných kategóriách. Tieto zoznamy sú generované na základe použitia konkrétneho používateľa, ktorý ich vie mazať a pridávať; príkladom sú zoznamy posledných otvorených súborov v textovom editore, či posledných navštívených stránok/dokumentov webového prehliadača.
- **Tasks:** Zvyčajné akcie, ktoré možno s aplikáciou vykonať, spoločné pre všetkých používateľov (bez ohľadu na spôsob, akým oni konkrétne aplikáciu používajú); úlohy nemôže používateľ meniť. Takéto JumpListy sú vlastne LNK súbormi – odkazmi - k príkazom. Príkladom je napríklad spustenie prehliadača v privátnom móde alebo rozpakovanie .7zip archívu.

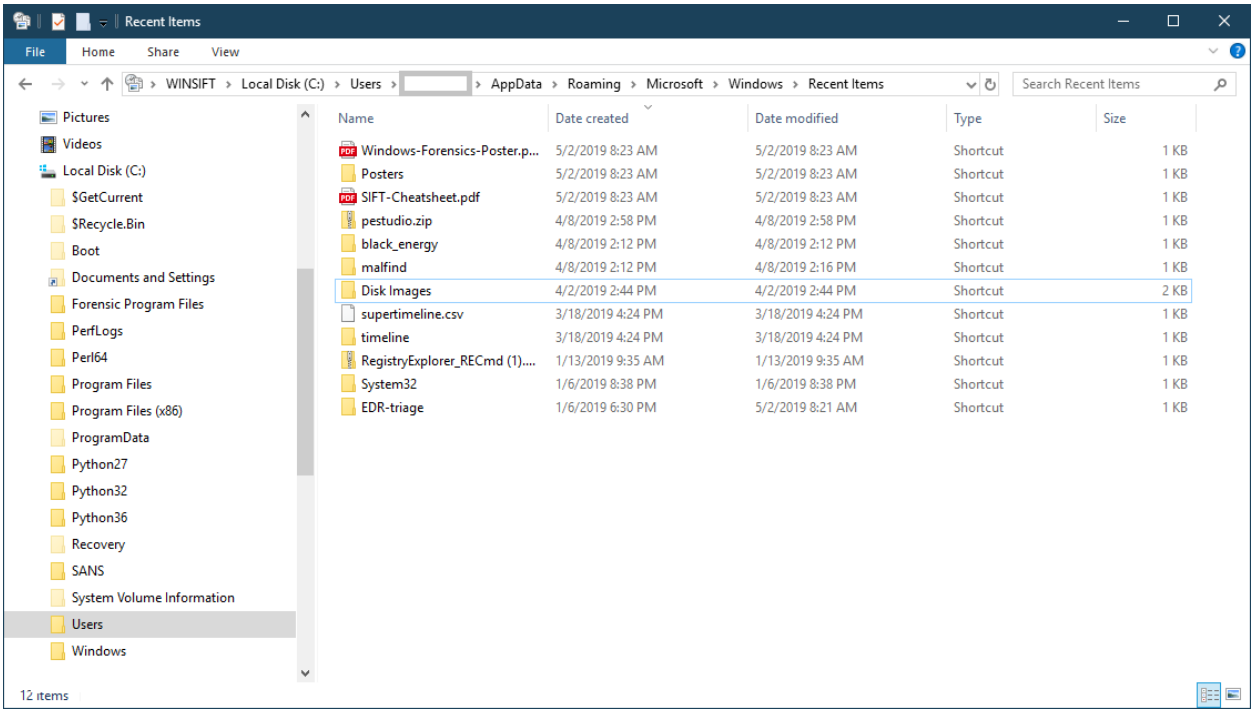
V oboch druhoch JumpListov možno nájsť identifikátor aplikácie, ku ktorej JumpList prislúcha – podľa AppID sú LNK súbory zoskupené do jedného JumpListu. Tieto ID sú jedinečné na danom zariadení,

pričom online sú udržiavané zoznamy ID známych programov. Napríklad https://www.forensicswiki.org/wiki/List_of_Jump_List_IDs a https://github.com/EricZimmerman/JumpList/blob/master/JumpList/Resources/AppIDs.txt.

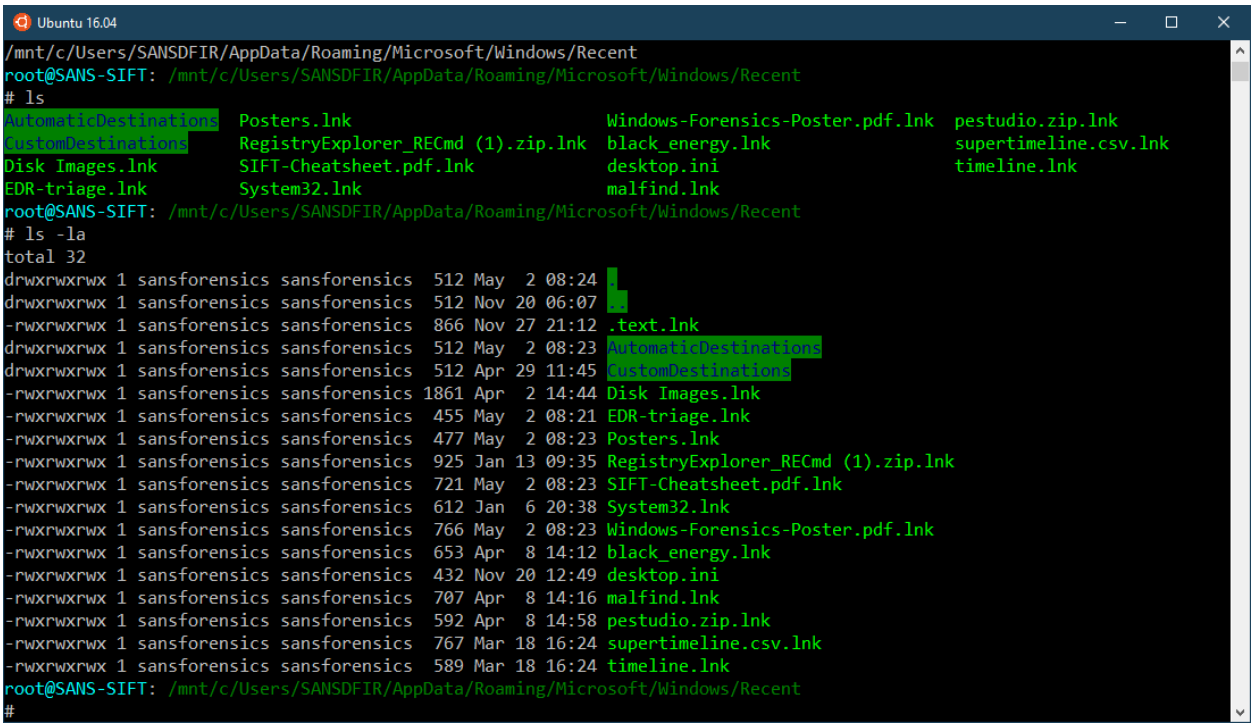
Kde ich hľadať?

%userprofile%\AppData\Roaming\Microsoft\Windows\Recent\ - adresáre AutomaticDestinations a CustomDestinations

Ak vo Windows Exploreri otvoríme príslušnú lokalitu na bežiacom systéme, neuvidíme tam adresáre AutomaticDestinations ani CustomDestinations. Adresáre sú viditeľné len pri vylistovaní obsahu adresára v príkazovom riadku alebo v bashi (pri použití Windows Subsystem for Linux).



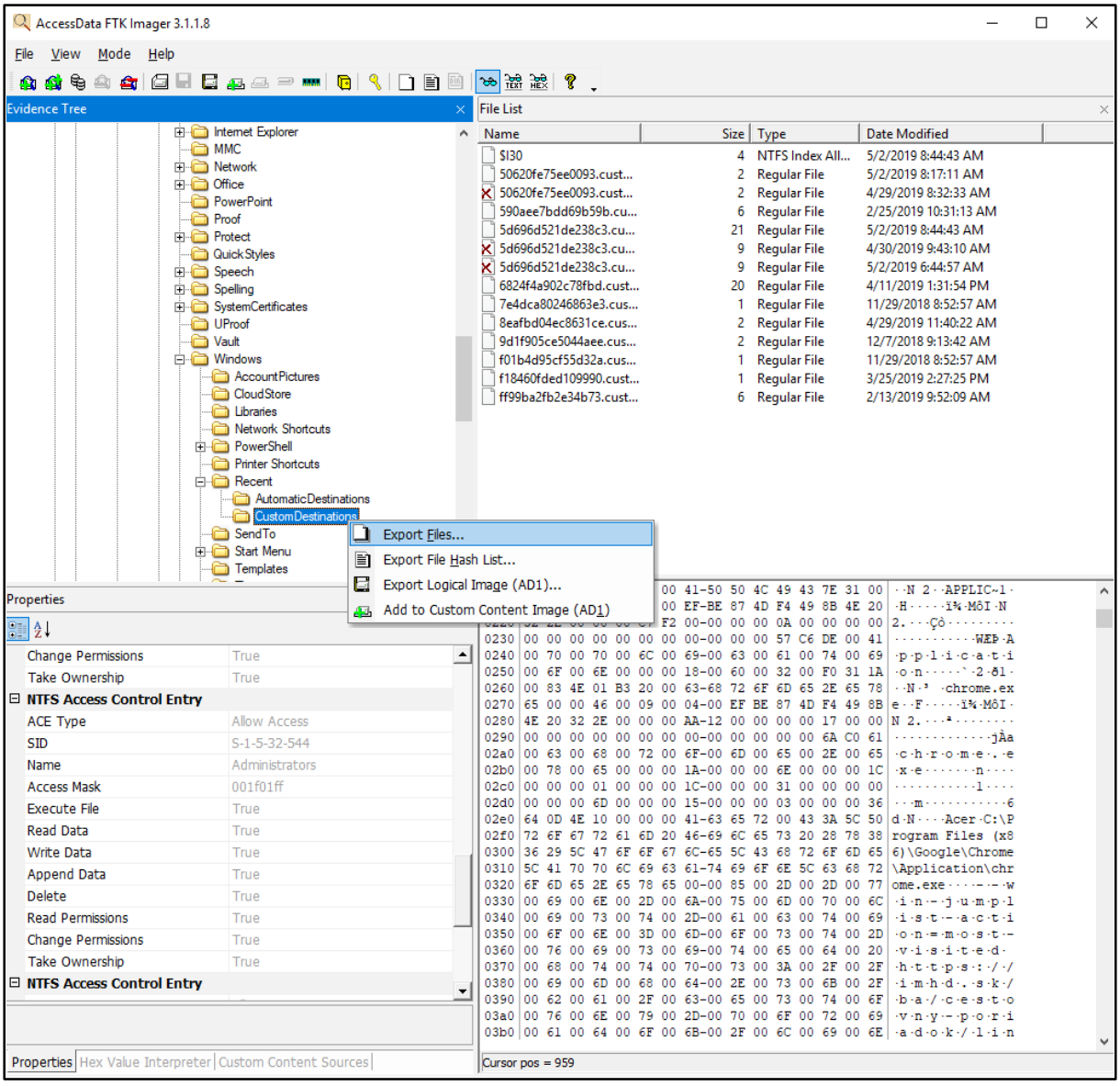
Obrázok 6 - lokality s JumpListami nie sú v Exploreri viditeľné



Obrázok 7 - Automatic a Custom Destinations v adresári

Ako získať súbory s JumpListami

Podobne ako v prípade LNK súborov, môžeme použiť napríklad nástroj FTK Imager. Na namountom image, alebo lokálneho logického disku, sú lokality Automatic a Custom destinations viditeľné a možno ich z nástroja exportovať. Jumplisty pre potreby neskoršej analýzy zaisťuje aj nástroj KAPE.



Obrázok 8 - Export adresárov s JumpListami

Forenzný význam

Keďže AJL aj CJL sa nachádzajú v používateľskom adresári, umožňujú koreláciu aktivity používateľa s programom a súborom. Ak napríklad v JumpListe programu Windows Explorer existuje zmienka o súbore/adresári, môžeme z toho vyvodiť, že daný používateľ vedel o existencií súboru a otváral/vytvoril ho. I v prípade, že súbor bol medzitým zmazaný, zmienka v JumpListe nám poskytuje dôkaz o existencií súboru, jeho časové pečiatky, lokalitu, kde sa súbor na disku/sieti nachádzal, či veľkosť súboru. Tieto informácie je v JumpListoch možné dohľadať aj spätne (potenciálne od prvého spustenia príslušnej aplikácie na systéme), hoci od zmazania/modifikácie súboru ubehlo pomerne veľa času. Aj v prípade použitia niektorých antiforenzných techník je možné stopy dohľadať práve v JumpListoch.

Interpretácia dát v JumpListoch:

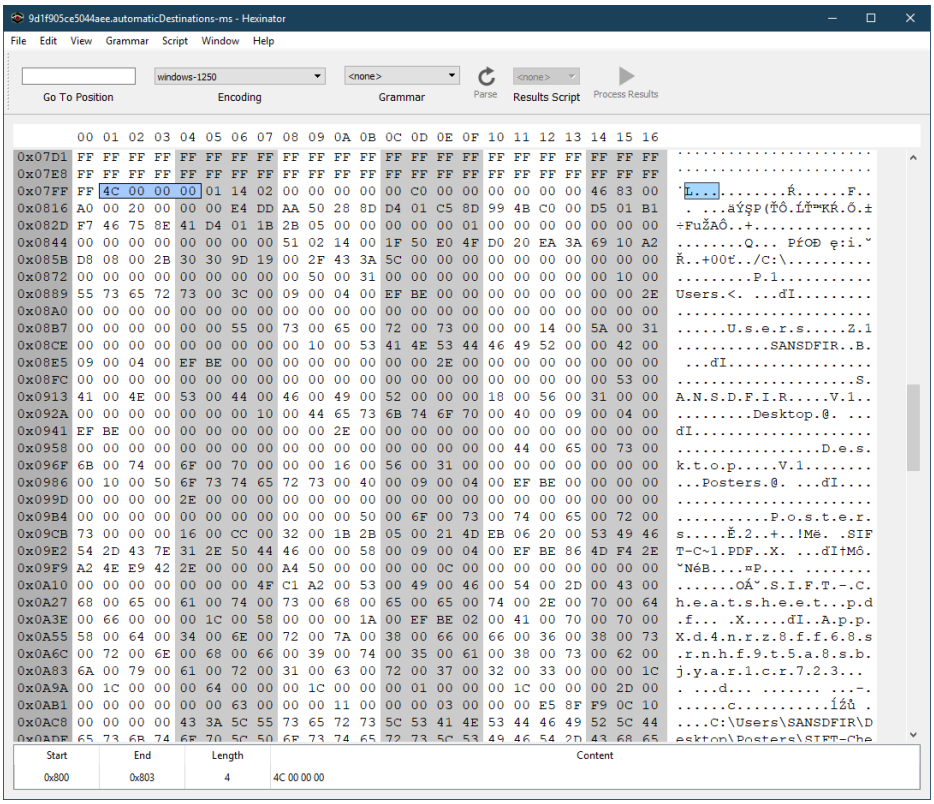
- **Automatic** JL:
  - Creation Time JumpListu – čas prvého pridania položky do JL aplikácie, teda čas jej **prvého** spustenia s otvorením súboru
  - Modification Time - čas posledného pridania položky do JL aplikácie, teda čas jej **posledného** spustenia s otvorením súboru
- **Custom** JL:
  - Creation Time – čas prvého pridania položky do JL aplikácie, teda čas jej **prvého** spustenia
  - Modification Time - čas **posledného** pridania položky do JL aplikácie

Z JumpListov je možné parsovať jednotlivé LNK súbory, v ich analýze pokračujeme rovnako ako pri ostatných LNK súboroch z priečinka Microsoft\{Windows|Office}\Recent.

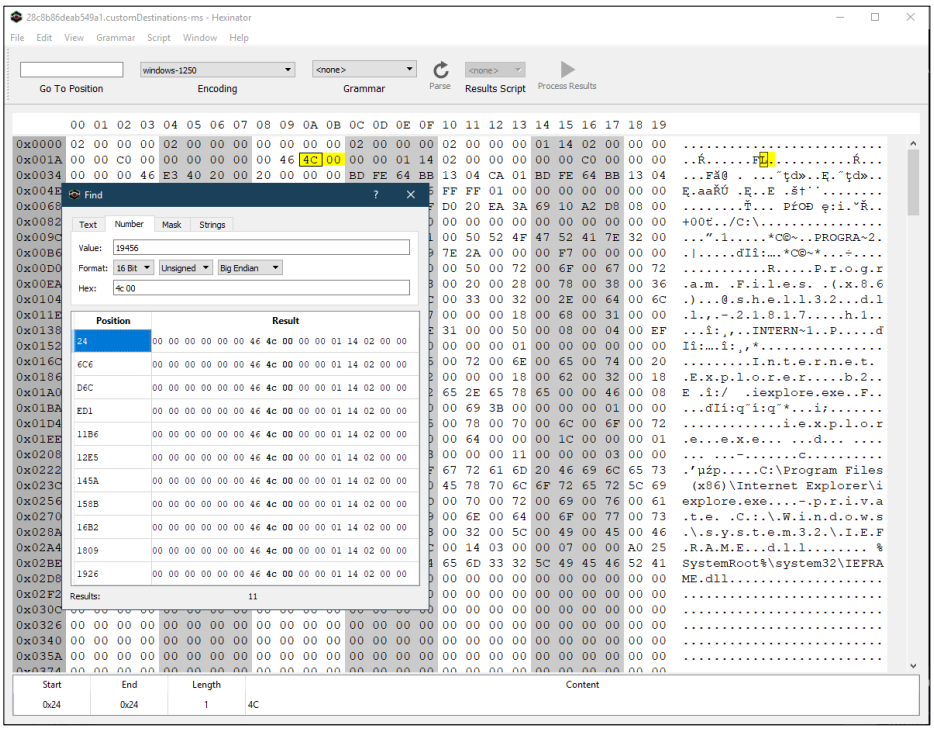
Analýza JumpListov

Jumplisty obsahujú LNK súbory. Aby sme sa o tom presvedčili, otvoríme ich v hexadecimálnom editore. Ak vyhľadáme magic number 4C 00 00 00, uvidíme, koľko LNK súborov sa reálne v JumpListe nachádza.

Custom Destinations – podľa magic number možno rozlíšiť jednotlivé LNK súbory. Na druhom obrázku sú jasne čitateľné informácie v LNK súbore – v tomto prípade je zvýraznená lokalita http://sourceforge.net/projects/pidgin/files/Pidgin/2.10.7/pidgin-2.10.7.exe/download… na základe čoho vieme potvrdiť návštevu tejto lokality a potenciálne stiahnutie chatovacieho programi pidgin. Informácia bude prítomná v systéme, aj ak by bol stiahnutý súbor i príslušný LNK file z lokality Recent zmazaný.

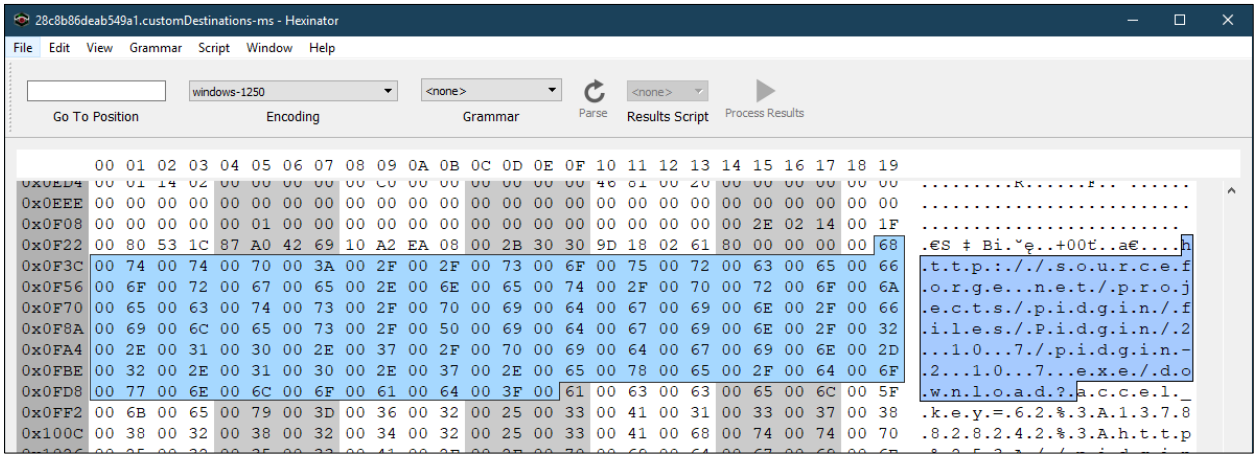


Obrázok 9 - Automatic Destinations: vidíme cestu k súboru – jeho umiestnenie na disku

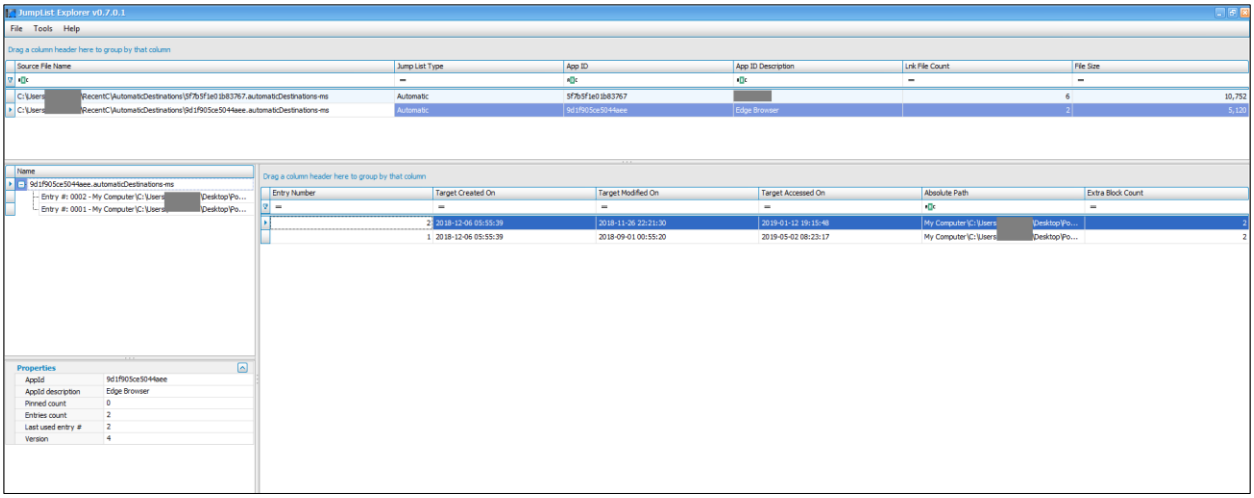


Obrázok 10 - LNK súbory v CustomDestinations

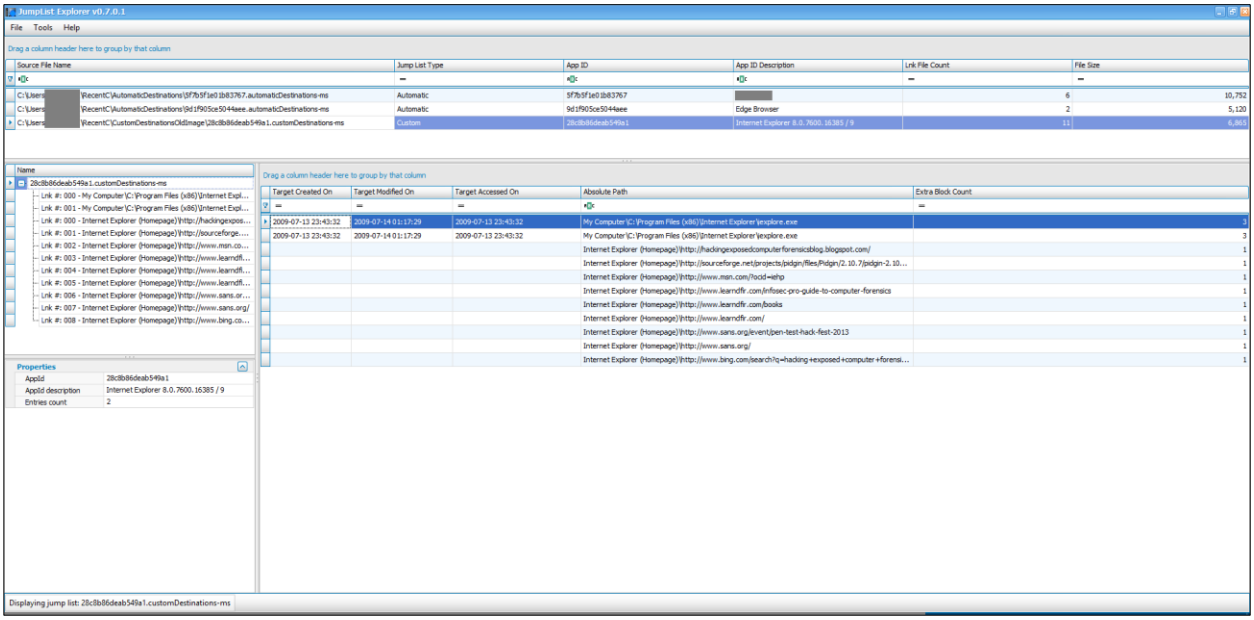
Na parsovanie JumpListov existuje viacero špecializovaných nástrojov. JumpListExplorer, autorom ktorého je Eric Zimmerman, od ktorého pochádzajú aj spomínané tooly LECmd a KAPE, je grafickým nástrojom na skúmanie Automatic aj Custom JumpListov. Umožňuje detailný pohľad na obsah JumpListov a zobrazenie podrobných informácií o jednotlivých referencovaných súboroch.



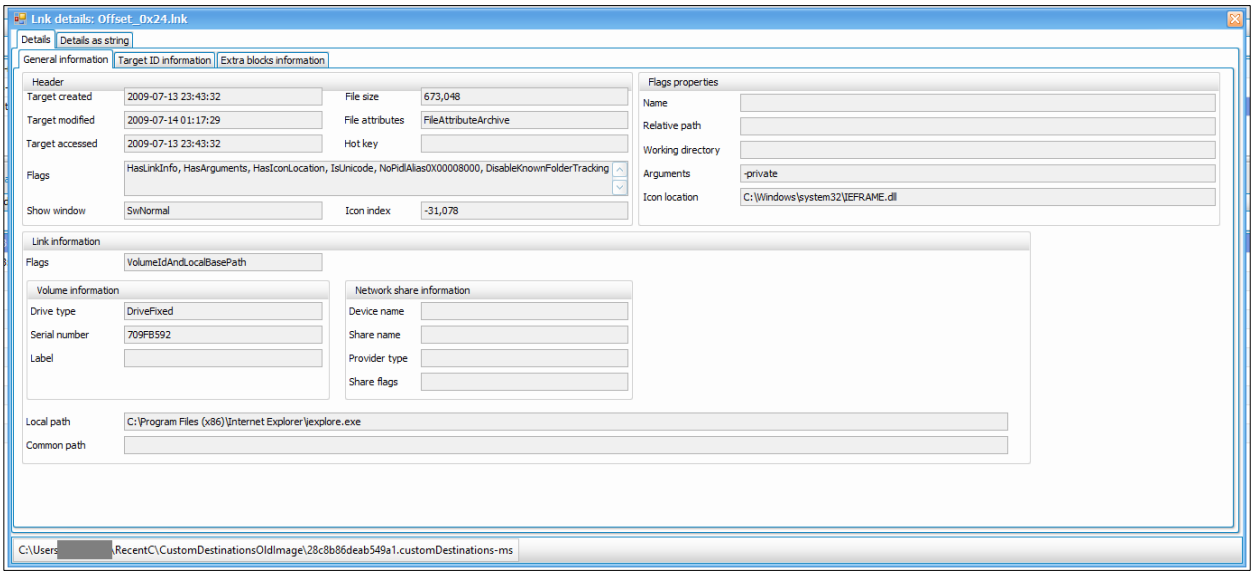
Obrázok 11 - navštívená URL v CustomDestinations Jumpliste



Obrázok 12 - JumpList Explorer a AJL

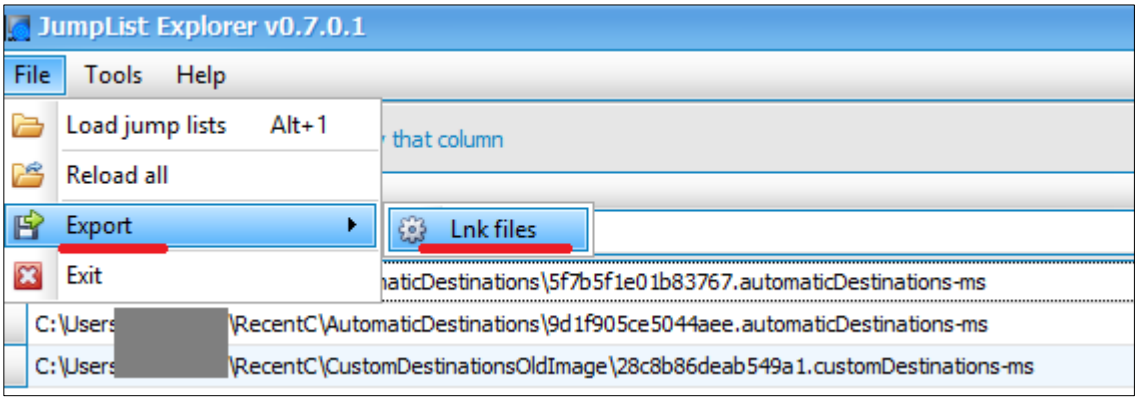


Obrázok 13 - JumpList Explorer a CJL



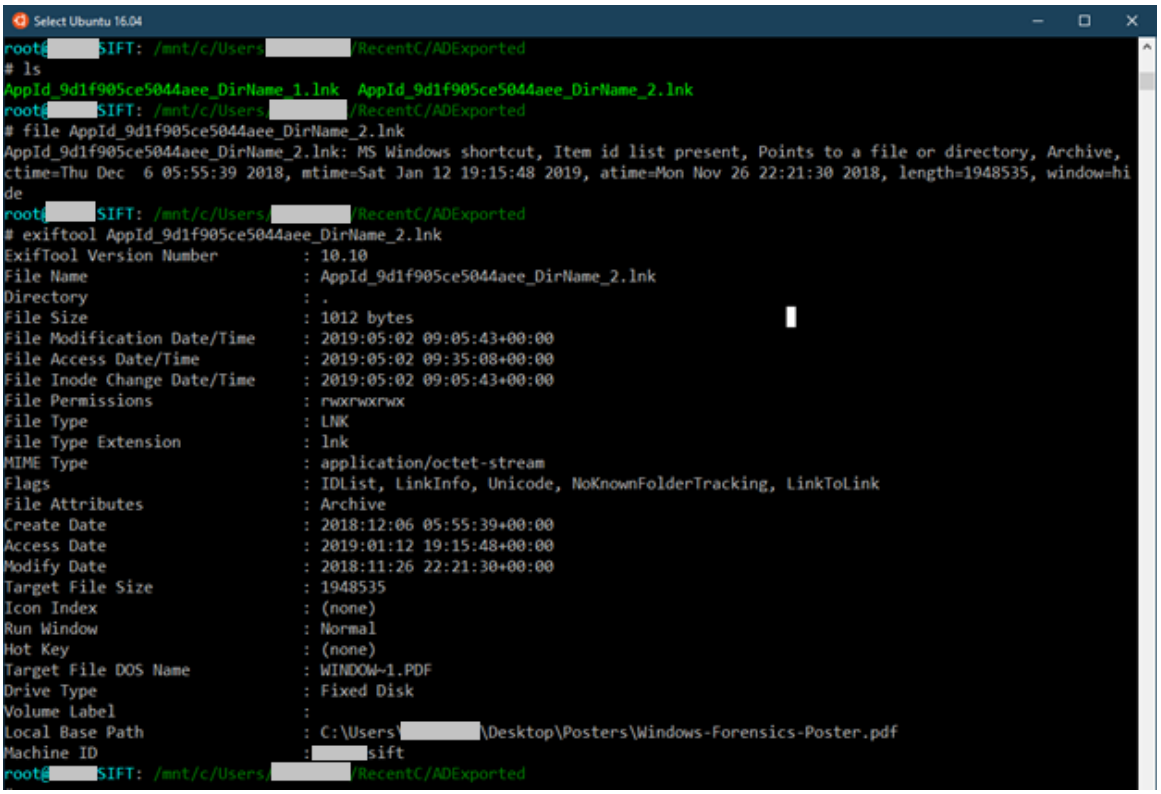
Obrázok 14 - detail položky JumpListu

Užitočnou funkcionalitou je možnosť exportu LNK súborov z jumplistov. Získané odkazy možno následne spracovať spolu s ostatnými LNK súbormi prostredníctvom LECmd a skonsolidovať stopy po používateľskej aktivite z týchto artefaktov na jedno miesto.

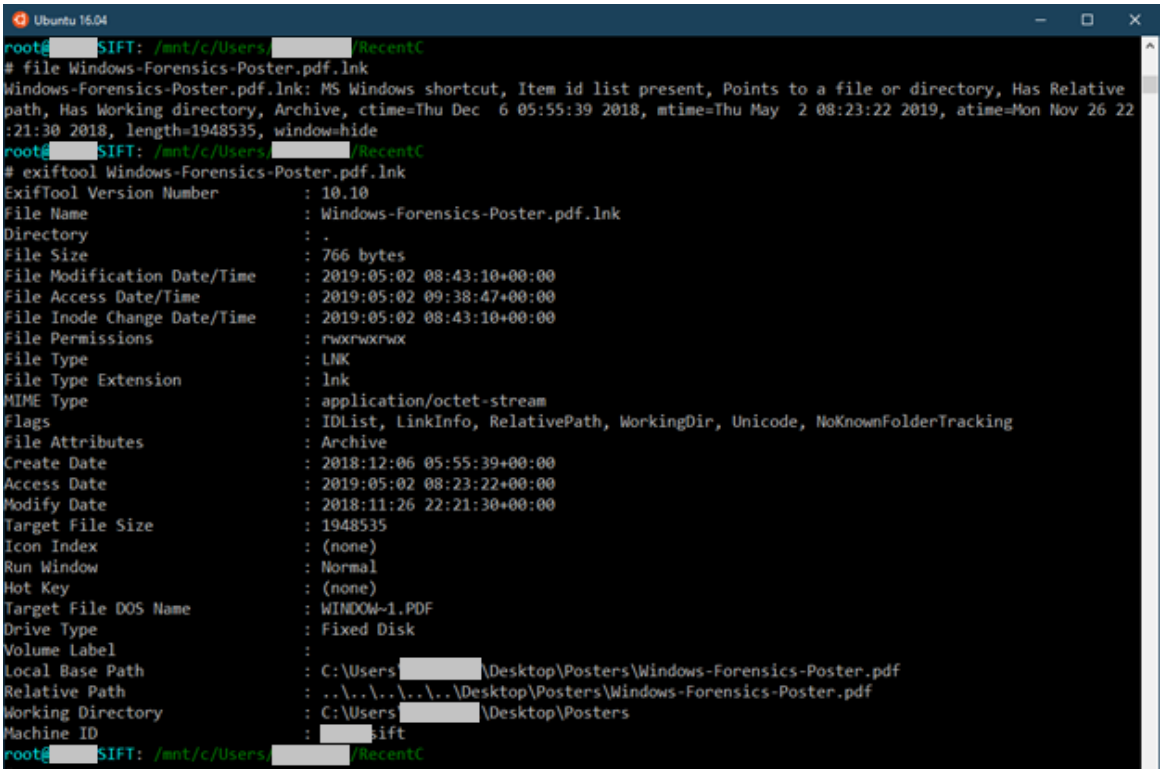


Obrázok 15 - Export LNK súborov z JumpListu

Po exporte jednotlivých LNK súborov môžeme porovnať informácie o položkách v JumpListe s tými, ktoré by sme získali analýzou štandardného LNK súboru v Recent adresári.



Obrázok 16 - Exportovaný LNK súbor



Obrázok 17 - LNK súbor zodpovedajúceho targetu

Keď porovnáme Create a Modify časové pečiatky cieľových súborov (v tomto prípade ide o plagát Windows-Forensics-Poster.pdf), vidíme, že časové pečiatky z LNK súboru v lokalite Recent súhlasia s časmi z LNK súboru exportovaného z JumpListu. Na základe toho je zjavný forenzný význam JumpListov: je možné z nich získať obdobné informácie, ako z LNK súborov. V prípade, že LNK súbor je zmazaný alebo prepísaný z dôvodu naplnenia kapacity 149 LNK súborov, je možné stopy získať analýzou Jumplistov (a mnohých iných artefaktov, ktoré budú predmetom nasledujúcich článkov :).

Záver

V článku sme popísali štruktúru LNK súborov a JumpListov. Uviedli sme, za akých okolností tieto artefakty vznikajú: pri interakcií používateľa so súbormi a programami, pri otváraní súboru či lokality, a pri používaní rôznych aplikácií. Venovali sme sa forenznému významu artefaktov – skutočnosti, že na základe časových pečiatok v súboroch je možné určiť časy prvého a posledného otvorenia nejakého súboru či použitia aplikácie. Uviedli sme príklady spracovania LNK súborov a JumpListov a ukázali, akými nástrojmi ich vieme analyzovať.

Na základe uvedených informácií je nesporné, že analýza LNK súborov a JumpListov je nevyhnutnou súčasťou podrobnej forenznej analýzy systémov s OS Windows.