|  |
| --- |
|  |
| **Windows İşletim Sisteminde Kullanılan Jumplist Bilgilerinin Adli Bilişim Analizi** |
| Bengü Çağla SARI |
| Adli Bilişim Mühendisliği, Teknoloji Fakültesi, Elazığ, Türkiye |

**Özet**

*Bu projede amaç Windows işletim sistemleri tarafından kullanıcı isteğine bağlı olarak oluşturulan jumplist dosyalarının adli bilişim analizini gerçekleştirmektir Jumplist dosyaları bilgisayar kullanıcısı tarafından son açılan belge, doküman gibi dosyaların sistemde kaydedilmesi sonucu oluşur. Oluşan bu dosyalar sistemde dosya silinse dahi kalır. Tutulan dosya bilgileri adli bilişim açısından çok önemlidir. Davaya kanıt olabilecek dosyanın dizin yolu, boyutu gibi verilere erişilir. Windows tarafından tutulan jumplist dosyalarına manuel yol ile erişim mümkündür. Manuel yol ile erişilen veriden bilgi elde etmek için analiz araçları kullanılır. Analiz araçları ile dosya hakkında bilgi elde edilir.*

**Anahtar Kelimeler:** jumplist, windows, adli bilişim

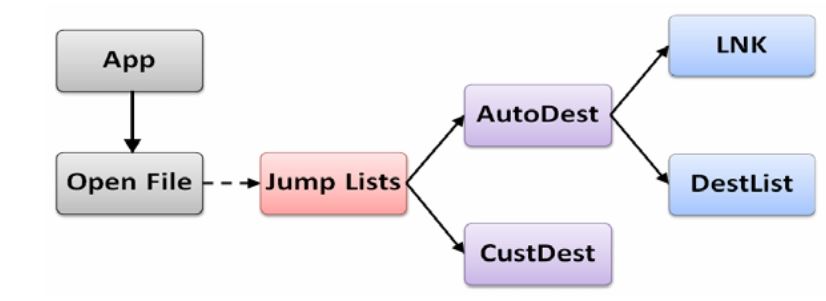
**Giriş**

Windows işletim sistemlerinde açılan her dosya sonrası oluşturulan jumplist dosyaları adli bilişim açısından incelenmesi gereken önemli alanlardandır. Sistemde hali hazırda var olan veya kullanıcı tarafından önceden açılıp sonrasından silinen dosyalara erişmek için kullanılır. Dosyalar Windows’da AppData\Microsoft\Windows\Recent dizini içinde tutulur. Bu dosyalara manuel olarak erişim mümkündür, analiz için gerekli olan araçlar tercih edilir. Bu araçlar vasıtasıyla dosya hakkında bilgilere ulaşılır.

**JUMPLİST**

Jumplist(atlama dosyaları) bir bilgisayar kullanıcısının açtığı son dosyaları gösterir. Kullanıcı açtığı son dosyayı tekrar açmak istediğinde dosya ile bilgileri gösterir. Jumplist dosyaları aynı zamanda saklı olan jumplist dosyalarını da gösterir. Bu dosyalar adli bilişim açısından çok önemlidir. Saklı olan jumplist dosyaları bir dolandırıcının sahte belgelerini, yasa dışı faaliyetler ile uğraşırken kullandığı belgeleri ortaya çıkarır. Dosyayı inceleyen adli bilişim uzmanı tarafından araştırılan davada kanıt olarak kullanılabilir. Jumplist dosyaları açılan belge, doküman silinse bile sistemde kaldığı için gösterir.

# JUMPLİST DOSYALARININ YAPISI

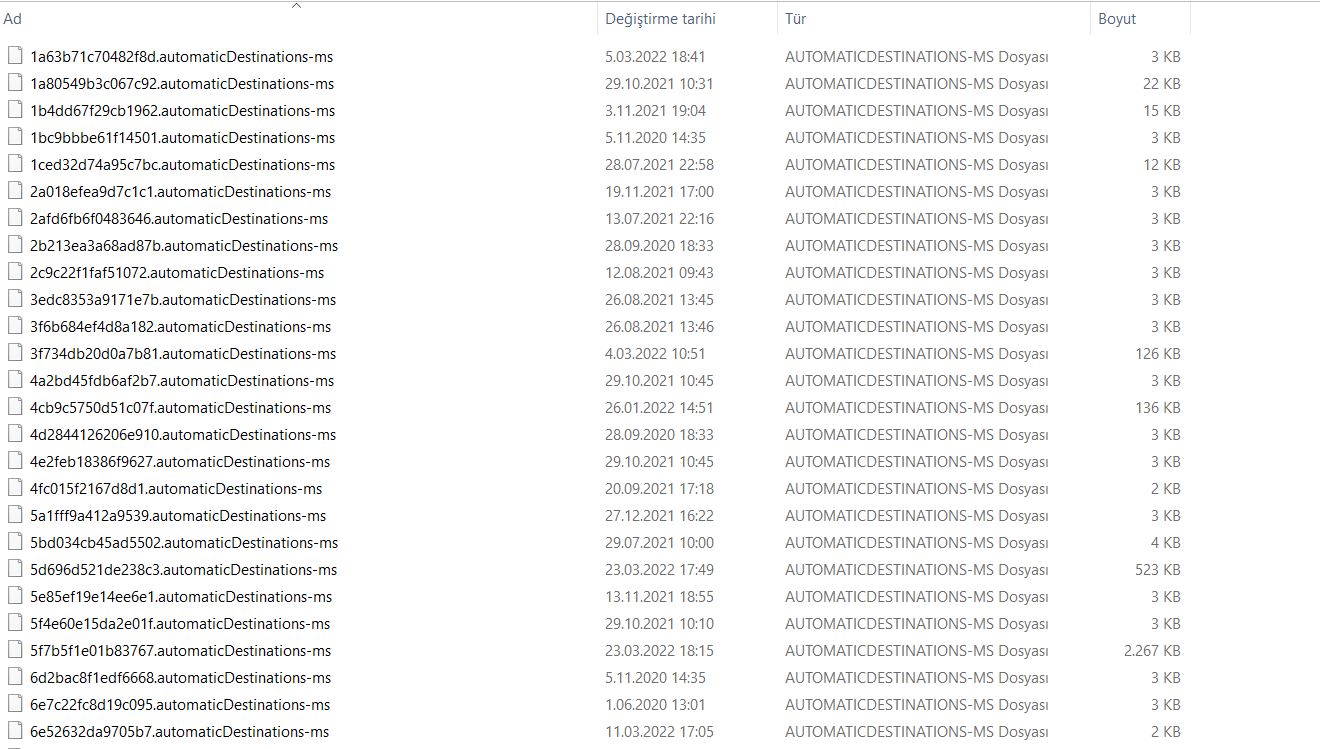


Şekil 1. Jumplist dosya yapısı

Her Jumplist dosyası AppID(Uygulama Tanımlayıcı) ve uzantısı .ms olan 16 basamaklı sayıdan oluşur. AppID’ler tüm Windows sistemlerinde evrensel olan benzersiz tanımlayıcılardır. Uygulama belirli eylemler gerçekleştirdiğinde iki tür dosya oluşur:

1. **AutomaticDestinations-ms files:**

%AppData%\Microsoft\Windows\Recent\AutomaticDestinations dosyalarına erişmek için üstteki dizin yolu kullanılır. İşletim sistemleri tarafından oluşturulan dosyalardır. Dosyaya ait zaman damgası, uygulama kimliği ve dosya yolunu içerir. Kullanıcı bir dosya veya uygulama açtığında otomatik olarak oluşturulan jumplist dosyalarıdır.



Şekil 2. AutomaticDestinations -msfiles

1. **CustomDestinations-ms files:**

C:\Users\%username%\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

User name kısmına kullanıcıya ait olan kullanıcı adı girilir. CustomDestinations dosyaları kullanıcı tarafından bir dosyayı görev çubuğuna veya başlat menüsüne sabitlenmesi ile oluşur.

Şekil 3. CustomDestinations –msfiles

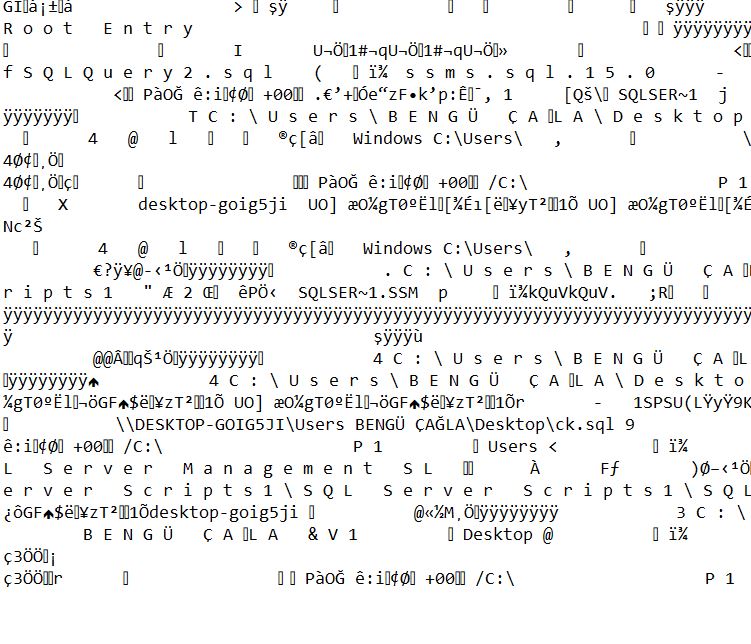
# 

# 

Şekil 3. CustomDestinations-ms files

# JUMPLİST DOSYALARININ ANALİZİ

Jumplist dosyalarını normal bir text editör ile incelemeyiz. Not defteri ile açılan dosyalarda yazılar okunaklı halde görünmez.



Şekil 4. Not defteri aracılığı ile jumplist analizi

Yazıları detaylı bir şekilde incelemek için jumplist analiz aracı kullanılması gerekir. Woanware tarafından geliştirilmiş olan JumpLister aracı ile jumplist dosyaları analizi yapılabilir.



Şekil 5: Jumplister aracı kullanımı

Uygulama ekranı bu şekildedir. File içinde load, export ve exit menüleri bulunur. Load menüsü ile incelenmek istenen jumplist dosyası yüklenir. Export ile incelenen jumplist dosyası dışarı aktarılır. Exit menüsü ile uygulamadan çıkılır. Tools içinde use decimal to represent HEX values menüsü bulunur. Bu menü ile HEX değerlerini temsil etmek için ondalık sayı kullanılır.

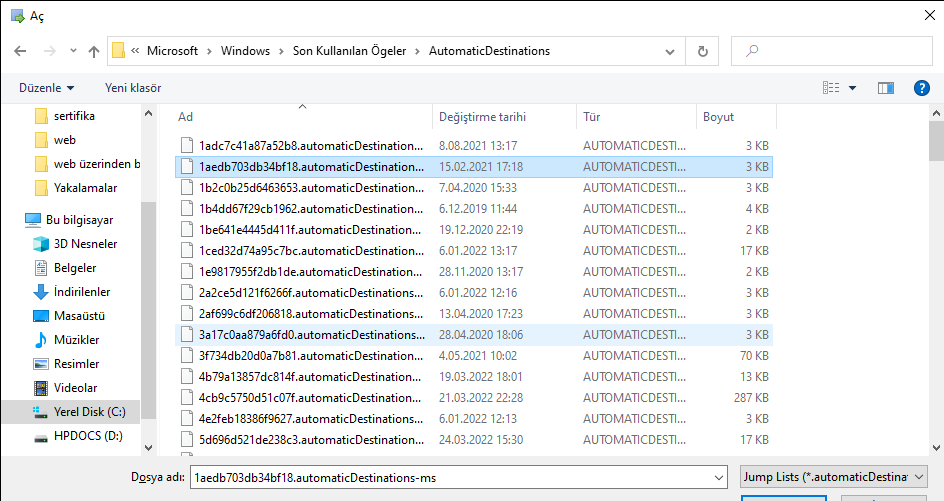
Bu ekranda sol kısımda açtığımız jumplist dosyasının açılan verilerini görebiliriz.

Ekranın sağ kısmında ise veri ile ilgili detaylar bulunmaktadır. Burada açtığımız uygulamanın yolunu, uygulamanın içinde nerelere girdiğimizi, oluşturulma değiştirilme zamanlarını, hangi kullanıcı tarafından açıldığı gibi kritik olabilecek veriler bulunmaktadır.

# CUSTOMDESTINATIONS VE AUTOMATICDESTINATIONS ANALİZ

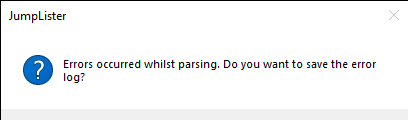
Az önce de bahsettiğimiz gibi bu verileri JumpLister uygulaması ile incelemeye çalışalım.

Adım.1: Uygulama arayüzünden file seçeneğine tıklayıp load dediğimizde bize –ms uzantılı dosya seçmemiz gerektiğini belirtiyor.



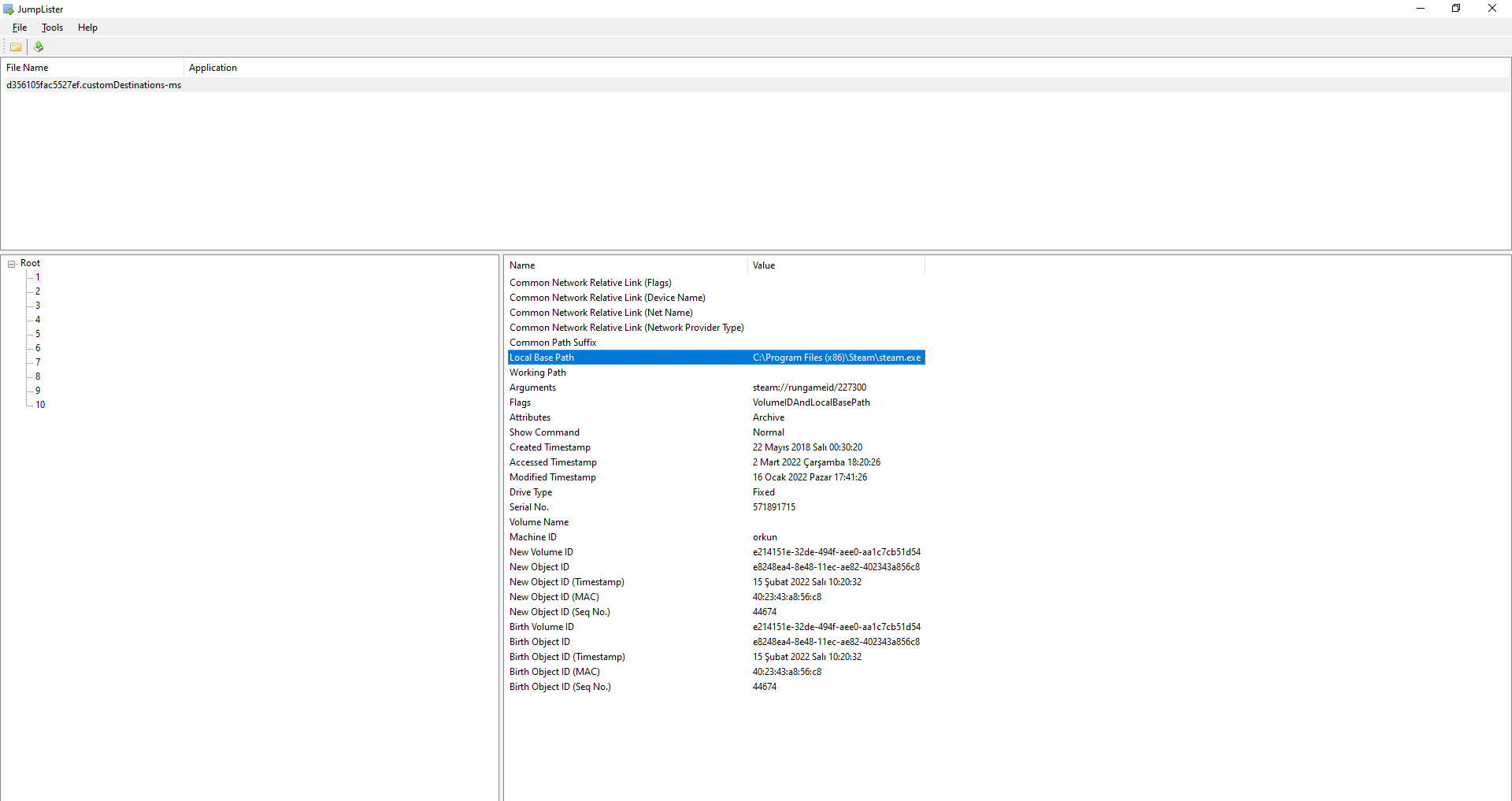
Şekil 6. AutomaticDestinations dosyaları jumplister ile analizi

Adım.2: Raporun başlarında belirttiğimiz dosya yolunu kopyalayıp yapıştırdıktan sonra herhangi bir –ms uzantılı dosyayı seçebiliriz veya ctrl+a diyerek hepsini de ekleyebiliriz. Tabi ki içlerinde silinmiş olan veya bozuk olan veriler de olabiliyor ve uygulama bunları açamıyor bunlar için log oluşturmak ister misin diye bize soruyor.

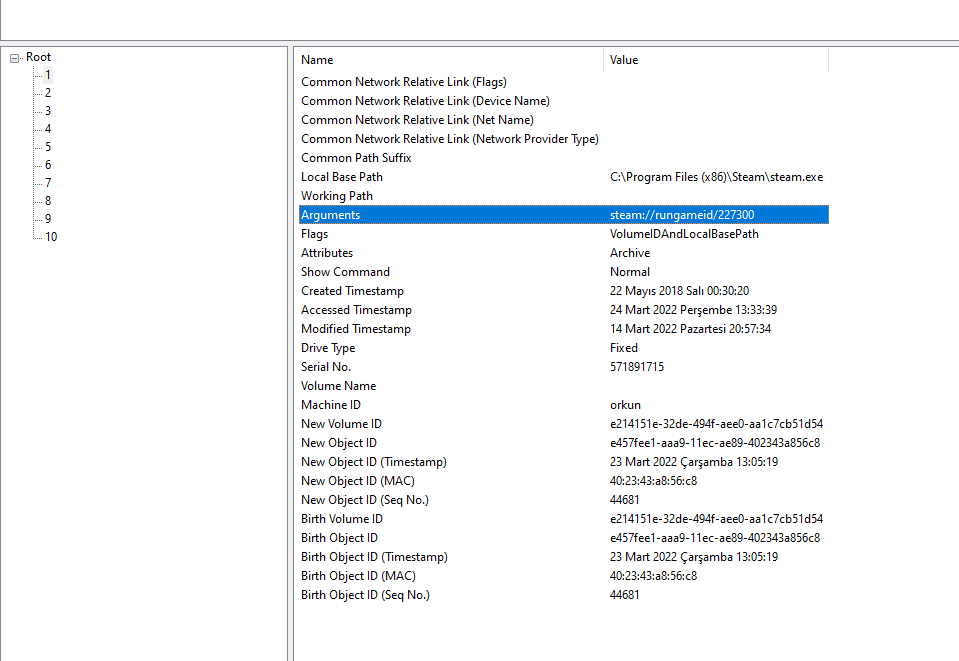


Şekil 7. Jumplister log kaydı tutma

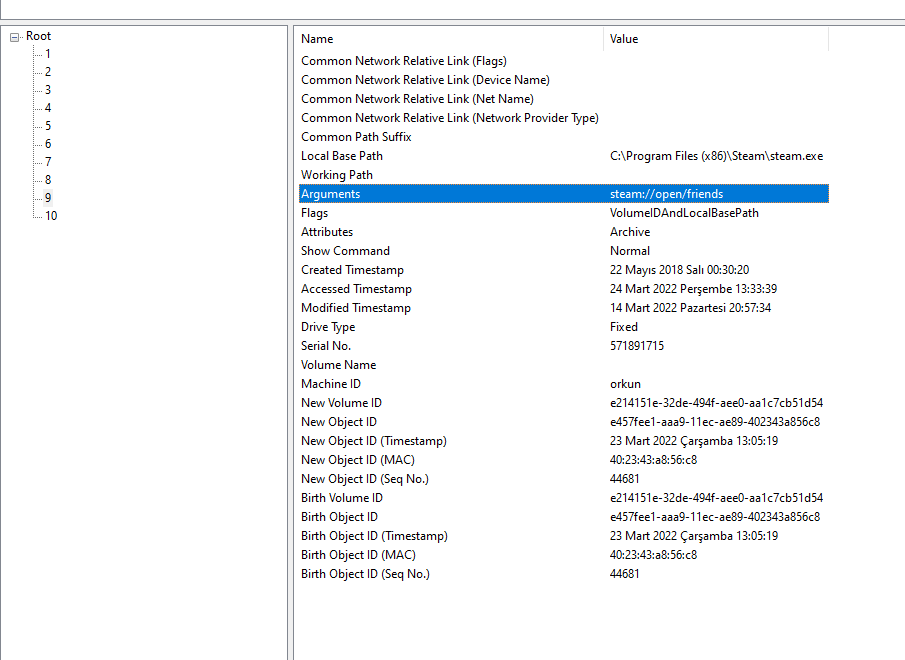
Adım.3: bu aşamada artık jumplist verilerini inceleyebiliriz. Açtığımız jumplistler uygulamada şu şekilde görünüyor;



Şekil 8. Jumplister aracı ile dosya bilgilerine ulaşma

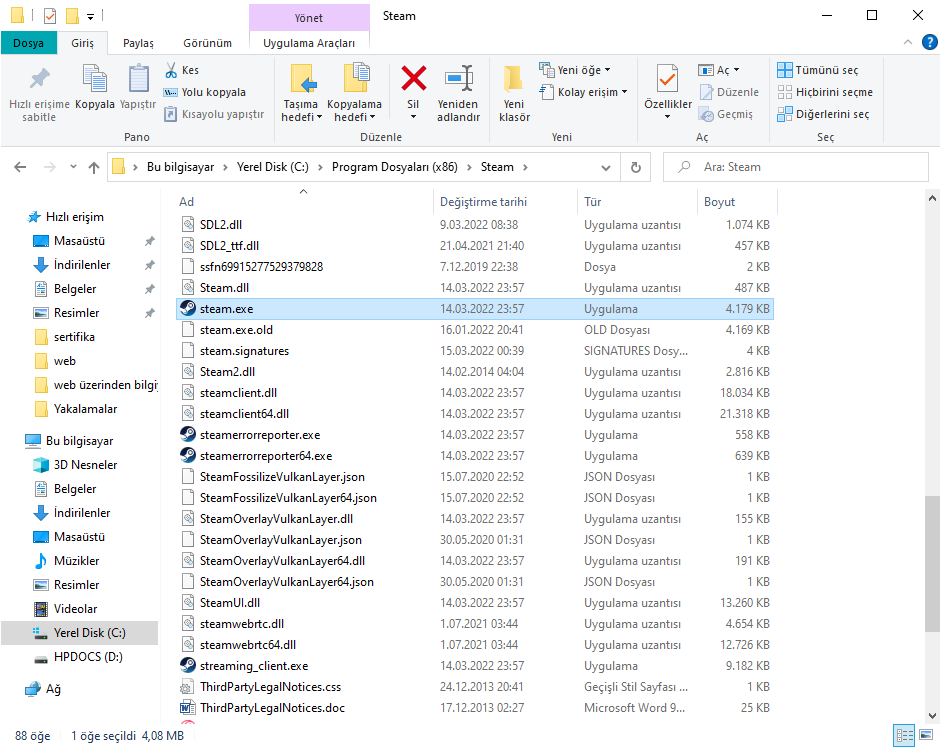
Örneğin açtığımız bu jumplist verisi steam uygulamasına ait bir dosya. Sol tarafta görünen numaralar en çok kullanılan 10 veriyi gösteriyor. Bunları tek tek incelediğimizde steam ugyulaması içinde en çok kullandığımız kısımları görebiliriz. Örneğin 1 numaralı seçenek herhangi bir oyun olabilir ancak 9 numaralı seçenek steam arkadaşlarını gösteriyor. Bu şekilde jumplist verilerini inceleyebiliriz. 

Şekil 9.Steam uygulaması jumplister aracı ile analizi



Şekil 9.1. Steam uygulaması jumplister aracı ile analizi

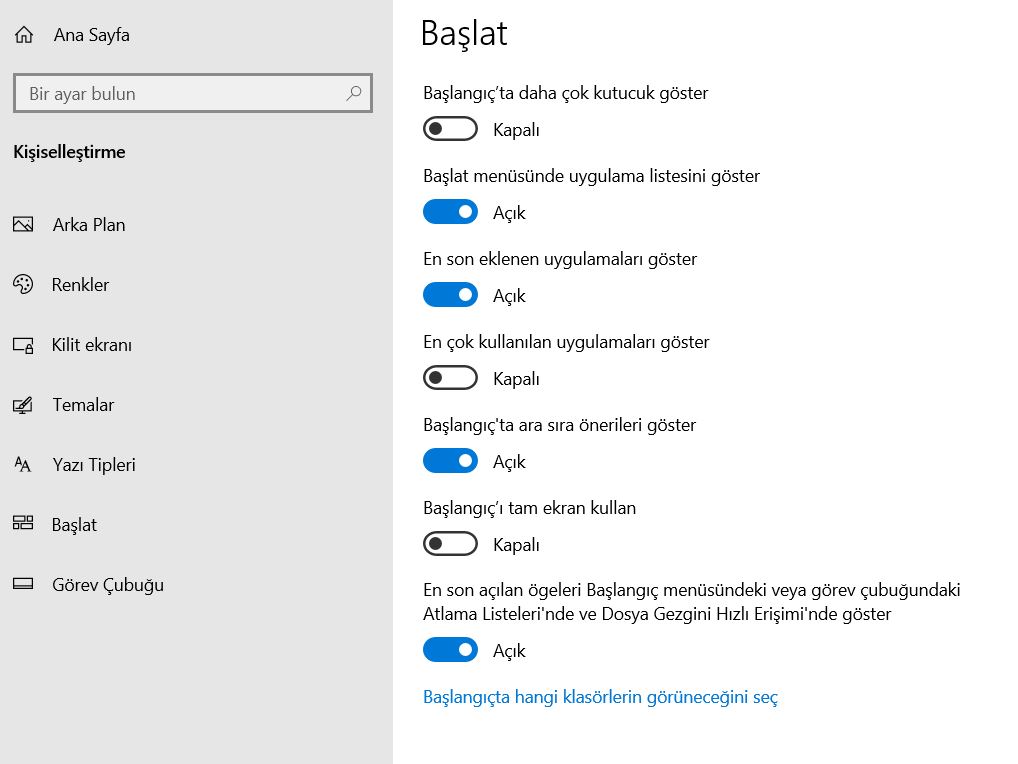
Ayrıca yukarıda ki resimde gösterilen dosyaların local base path kısmında yazan dizine giderek dosyayı inceleyebiliriz. Eğer dosya yoksa kurtarmayı deneriz. Örneğin steam jumplistini açtığımız için onun dizinine gidip inceleyelim;



Şekil 10. Jumplister uygulamasının dizin yolu ile stream uygulamasına erişim

# WİNDOWS JUMPLİST DEVRE DIŞI BIRAKMA

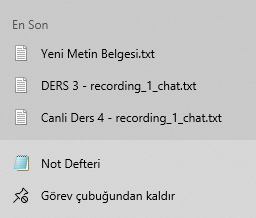
Windows jumplist dosyalarını varsayılan olarak kullanıcılara sağlıyor. Eğer kullanıcı tarafından istenirse bu özellik kapatılabilir. Öncelikle masaüstü ekranında kişiselleştir menüsü seçilir. Seçilen menü ekranından başlat kısmı seçilir. Başlat kısmı içindeki en son açılan ögeleri Başlangıç menüsündeki veya görev çubuğundaki atlama listelerinde ve dosya gezgini hızlı erişiminde göster seçeneği kapatılır.



Şekil 11. Windows üzerinden jumplist devre dışı bırakma

**WİNDOWS GÖRÜNEN** JUMPLİST SAYISINI DÜZENLEME

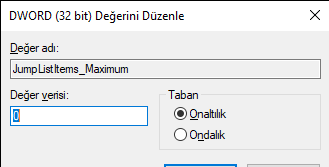
Jumplist verilerini en basit hali ile görev çubuğunda ki uygulamaya sağ tıklayarak görebiliriz.



Şekil 12. Windows jumplist dosyaları

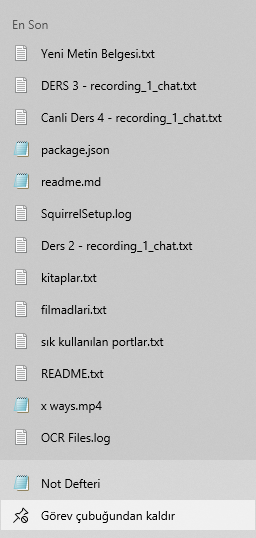
Bu gördüğümüz en son kısmında bulunan 3 tane veriyi çoğaltabilir veya azaltabiliriz. Bunu da şu şekilde yapıyoruz;

İlk önce başlat menüsünden kayıt defterini açıyoruz(regedit) Bilgisayar\HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced seçeneğine geldikten sonra advanced üzerinde sağ tıklayarak yeni ardından DWOR(32 bit) seçeneğine tıklıyoruz. İsmine JumpListItems\_Maximum dedikten sonra çift tıklayarak açıyoruz.



Şekil 13. Jumplist dosya görüntüleme

Bu ekranda değer verisine hangi değeri girersek Şekil 14 numaralı resimde görünen 3 veriyi çoğaltabiliriz. Örneğin 10 yapalım ve bakalım.

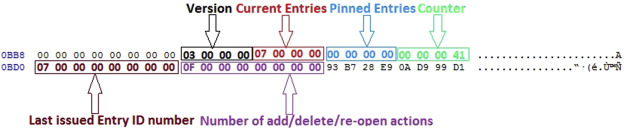


Şekil 13.1. Jumplist dosya görüntüleme

Gördüğünüz gibi not defterinde görüntülenen son açılanlar listesi 13’e çıktı. Bunun sebebi de zaten 3 vardı biz üzerine 10 adet eklemiş olduk. Gizliliğiniz için bu değeri sıfıra(0) da çekebilirsiniz

# JUMPLİST’İN HEX OLARAK İNCELENMESİ

Aşağıda verilen tabloda bir jumplist dosyasının hex olarak ne ifade ettiğini açıklayan bir görsel bulunmaktadır.



Şekil 14. Jumplist dosyalarının hex analizi

# SIK KULLANILAN BAZI APPID’LER

|  |  |
| --- | --- |
| 65009083bfa6a094 | (uygulama XPMode aracılığıyla başlatıldı) |
| b0459de4674aab56 | (.vmcx) |
| 89b0d939f117f75c | Adobe Acrobat 9 Pro Genişletilmiş (32 bit) |
| 26717493b25aa6e1 | Adobe Dreamweaver CS5 (32 bit) |
| e2a593822e01aed3 | Adobe Flash CS5 (32 bit) |
| c765823d986857ba | Adobe Illustrator CS5 (32 bit) |
| 84f066768a22cc4f | Adobe Photoshop CS5 (64 bit) |
| 44a398496acc926d | Adobe Premiere Pro CS5 (64 bit) |
| 23646679aaccfae0 | Adobe Okuyucu 9. |
| 23646679aaccfae0 | Adobe Okuyucu 9x64 |
| d5c3931caad5f793 | Adobe Soundbooth CS5 (32 bit) |
| 7e4dca80246863e3 | Kontrol Paneli (?) |
| 5c450709f7ae4396 | Firefox 3.6.13 (32 bit) |
| bc03160ee1a59fc1 | Foxit PDF Okuyucu 5.4.5 |
| 28c8b86deab549a1 | Internet Explorer 8/9/10 (32-bit) |
| 5da8f997fd5f9428 | Internet Explorer x64 |
| 83b03b46dcd30a0e | iTunes 10 |
| 271e609288e1210a | Microsoft Office Erişimi 2010 x86 |
| cdf30b95c55fd785 | Microsoft Office Excel 2007 |
| 9839aec31243a928 | Microsoft Office Excel 2010 x86 |

Her uygulamanın kendine özgü bir AppID değeri vardır.

# KAYNAKÇA

[1]Öztürkci Halil, ‘Windows Jumplist Forensics’ <http://halilozturkci.com/windows-jump-list-forensics/> (15.03.2014)

[2] ‘What is a Jump list in Windows’,<https://superuser.com/questions/496059/what-is-a-jump-list-in-windows> (30.12.2012)

# [3] Jones Larry,’ Windows 10 Jump List and Link File Artifacts - Saved, Copied and Moved’, <https://dfir.pubpub.org/pub/wfuxlu9v/release/1> , (25.09.2020)

# [4]Weng.Shiuh-Ku,’ A Visualization Jump Lists tool for Digital Forensics of Windows’ <https://www.koreascience.or.kr/article/JAKO202011161036565.page> (31.01.2020)

[5] Jhala Kritarth , “Forensic Analysis of Jump Lists in Windows Operating System”, *International Journal of Engineering Research & Techonology, 04(03),1-7,2015*