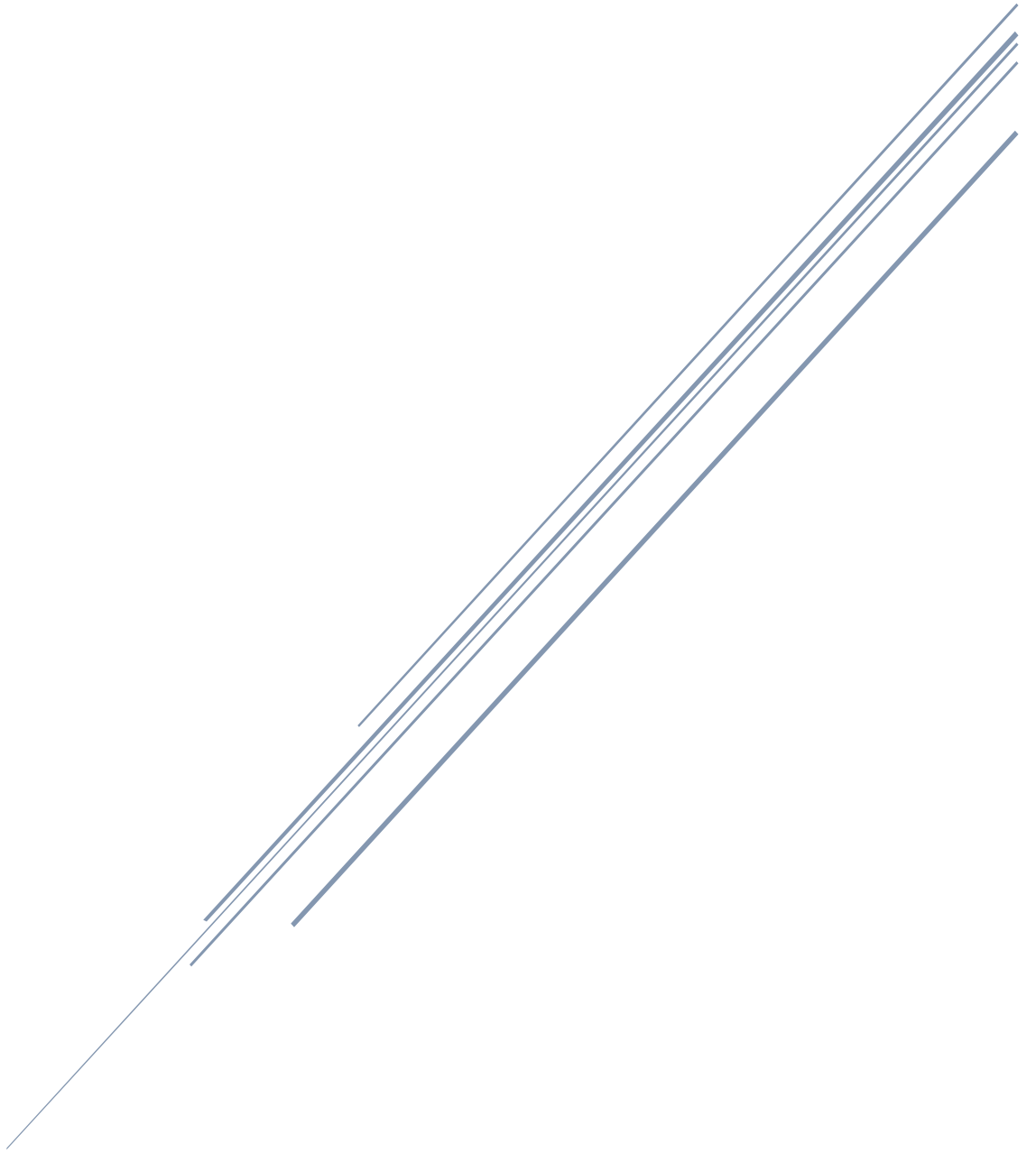


WINDOWS REGISTRY ANALİZİ



Serdal Tarkan ALTUN

İÇİNDEKİLER

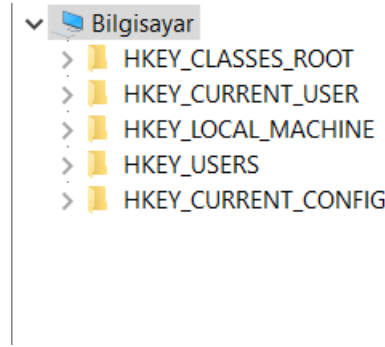
1. REGİSTRY(Kayıt Defteri) Nedir?	3
1.1. Windows Registry Dosyaları Nelerdir ve Manuel Bilgi Nasıl Öğrenilir?	3
1.1.1. SAM Dosyası Nedir?.....	4
1.1.2. SECURITY Dosyası Nedir?.....	4
1.1.3. SOFTWARE Dosyası Nedir?	4
1.1.4. HARDWARE Dosyası Nedir?	4
1.1.5. SYSTEM Dosyası Nedir?.....	4
1.1.6. NTUSER.DAT Dosyası Nedir?.....	4
1.1. Kayıt Defterinden manuel olarak bilgi nasıl çekilir?.....	4
2. İMAJ ALMA	7
2.1. İmaj nedir?.....	7
2.2. İmaj nasıl alınır?	7
2.3. İmajı İçeri Aktarma Nasıl Yapılır?	11
2.4. Dosyaları Export Etme İşlemi Nasıl Yapılır?	12
3. Registry Explorer Yazılımı İle Dosyalar Nasıl İncelenir?.....	13
3.1. Dosyalar İçeri Nasıl Aktarılır?	13
3.2. Veriler Nasıl Analiz Edilir?.....	15
3.2.1. NTUSER.DAT	15
3.2.2. SYSTEM	16
3.2.3. SAM	17
3.2.4. SOFTWARE	18
4. KAYNAKÇA	21

1. REGİSTRY(Kayıt Defteri) Nedir?

Windows'ta çalışan uygulamalar ve hizmetler için kritik olan verileri içeren hiyerarşik bir veri tabanıdır. Bilgisayar sistemi hakkında ki genel bilgileri ile uygulamalara ait geçmiş kayıtların tutulduğu yer olan registry sistemin hızlı, tutarlı ve işlevsel olarak çalışması amacıyla otomatik olarak tutulan kayıtlardan oluşmaktadır.

1.1. Windows Registry Dosyaları Nelerdir ve Manuel Bilgi Nasıl Öğrenilir?

Windows Kayıt defteri olarak da bilinmektedir. Ve registry dosyaları 5 adet KEY(Anahtardan) oluşmaktadır. Dosyalar şunlardır;



- *HKEY_CLASSES_ROOT:*

Dosya uzantı bilgileri, hangi tip dosyanın hangi programla açılması gerektiği ve dosya tipleriyle ilgili tanımlamanın yapıldığı gruptur.

- *HKEY_CURRENT_USER*

O an oturum açmış kullanıcılar alakalı bilgiler içermektedir. Kullanıcılara özgü ayarlar saklanmaktadır. Ortam değişkenleri, masaüstü ayarları, kontrol panel ayarları ve uygulama yapılandırmaları buna örnek verilebilir.

- *HKEY_CURRENT_CONFIG*

Bilgisayardaki donanım profil hakkında saklanan veriler bu grupta bulunmaktadır.

- *HKEY_USERS*

Bilgisayarda hali hazırda açık olan kullanıcıların ayarları ve çalıştırdıkları uygulamalara özgü çeşitli verileri taşımaktadır.

- *HKEY_LOCAL_MACHINE*

Bu grupta bilgisayara özgü yapılandırma bilgileri bulunmaktadır. Donanım, SAM, güvenlik, yazılım ve sistem olmak üzere 5 alt anahtar içermektedir.

1.1.1. SAM Dosyası Nedir?

SAM Güvenlik Hesap Yöneticisi olarak bilinmektedir. Bu dosya içerisinde kullanıcı hesapları, misafir hesaplar ve bunların şifrelerinin tutulduğu veri tabanı dosyasıdır.

1.1.2. SECURITY Dosyası Nedir?

Sistemdeki güvenlik bilgilerini ve ilkelerini içerir. Security içerisinde hangi kullanıcıların sisteme erişmesine izin veriliyor, bu kullanıcılar sisteme hangi kanallardan erişiyor gibi soruların cevabı bu anahtar altında saklanıyor.

1.1.3. SOFTWARE Dosyası Nedir?

Bu dosya da sistemde kurulu olan yazılımlara ve daha önce kurulmuş ve kaldırılmış olan yazılımların bilgilerine ulaşabiliyoruz.

1.1.4. HARDWARE Dosyası Nedir?

Bu dosya içerisinde bağli olan giriş-çıkış(donanım) birimleri hakkında ki bilgilere ulaşabiliyoruz.

1.1.5. SYSTEM Dosyası Nedir?

Bu anahtar normalde yalnızca yerel sistemde yönetici ayrıcalıklarına sahip kullanıcılar tarafında yazılabilir. Windows sistem kurulumu hakkında bilgiler, dosya sistemi içeren şu an takılı aygıtların listesi ve sistem donanım sürücülerini hakkında bilgileri içerisinde tutan anahtardır.

sizlere biraz **NTUSER.DAT** dosyasından bahsetmek istiyorum.

1.1.6. NTUSER.DAT Dosyası Nedir?

Her kullanıcı profil içerisinde gizli olarak bulunmaktadır. Bu dosya içerisinde kullanıcı profil bilgilerin içerir. Aslında Windows kayıt defterinden depolanan kayıtların bir kopyasıdır.

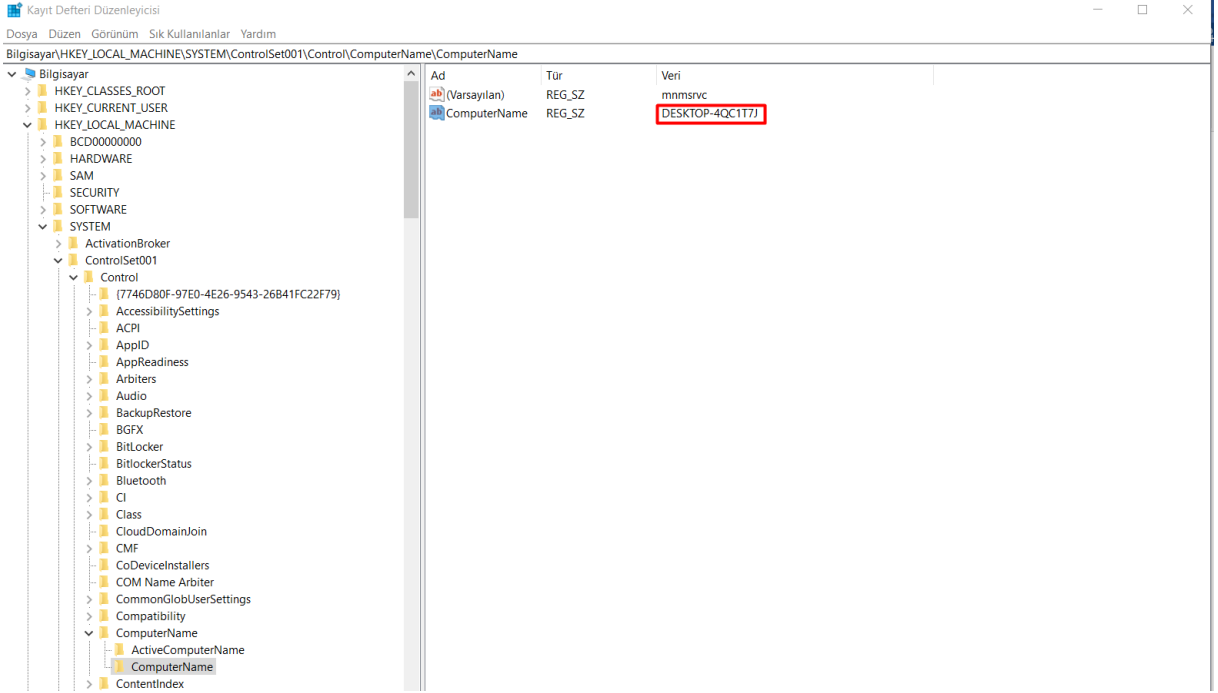
Şimdi ise manuel bir şekilde Windows kayıt defteri dosyalarından bilgiler elde etmeye çalışalım.

1.1. Kayıt Defterinden manuel olarak bilgi nasıl çekilir?

- *Bilgisayar Adı Nasıl Öğrenebiliriz?*

Windows kayıt defterimizde, verdiğim konuma giderek bilgisayar ismini öğrenebiliyoruz.

HKLM \ SYSTEM \ ControlSet### \ Control \ ComputerName \ ComputerName

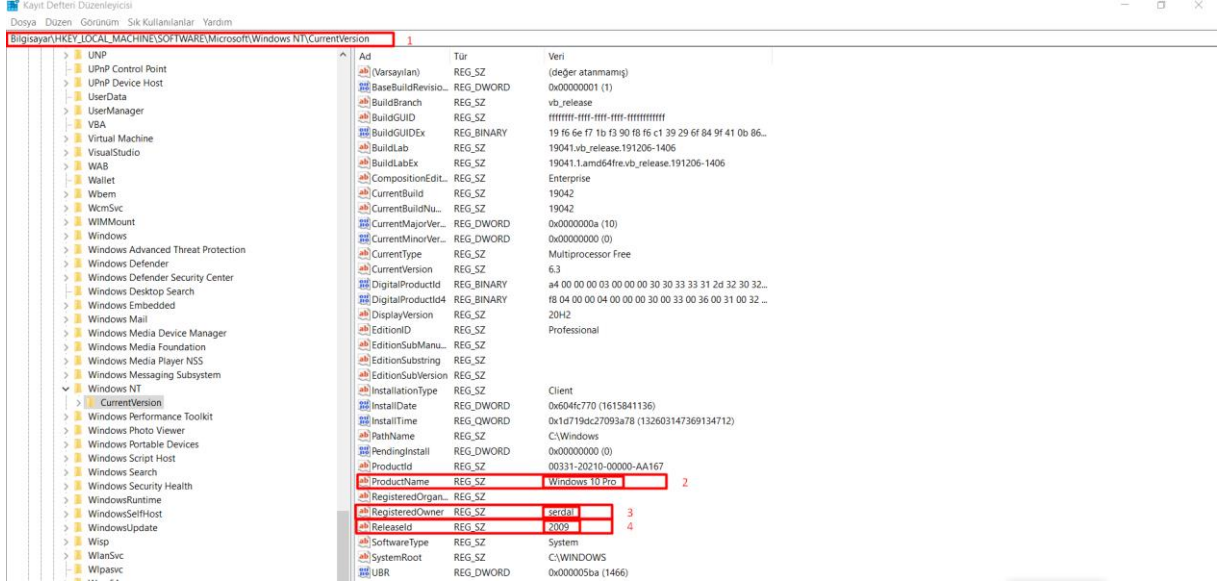


Şekilde ComputerName kısmında bilgisayar ismi gözükmektedir.

- *İşletim Sistemini, Sürümünü ve Kullanıcısını Nasıl Öğreniriz?*

Kayıt defterinden verdiğim konumu takip ederek işletim sistemi, sürümü ve kullanıcısı hakkında bilgi sahibi olabiliriz.

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion



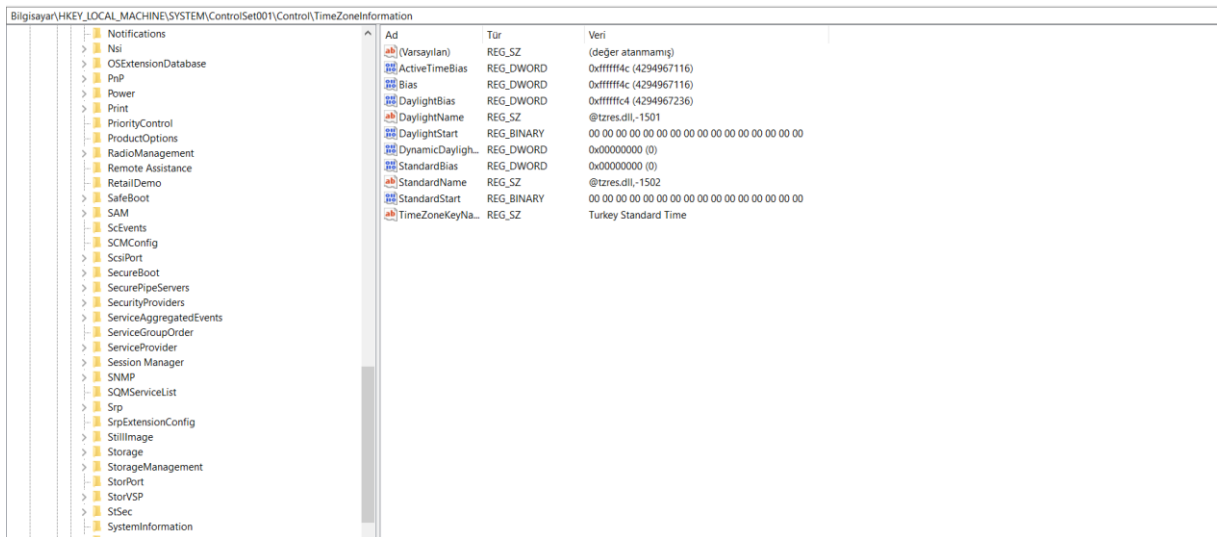
Verdiğim konuma gittiğimizde böyle bir görselle karşılaşıyoruz. Numaralandırma yaptığımız kısımlardan veriler elde edebiliyoruz.

1. Bu kısım bulunduğumuz dosya konumunu göstermektedir.
2. Burada ise bize kullanılan işletim sistemini söylemektedir.
3. Kısımda ise kullanıcı adını görmekteyiz.

• Saat Dilimi Bilgilerine Nasıl Ulaşabiliriz?

Verdiğim konuma giderek Saat Dilimi Bilgilerine ulaşabilirsiniz.

HKEY_LOCAL_MACHINE \ SYSTEM \ ControlSet001 \ Control \ TimeZoneInformation



Buradan gördüğümüz üzere pek sonuç alamadık. Kayıt Defterinde anlamlandıramadığımız dosyaları yazılımlar kullanarak anlaşılabilir hale getirebiliyoruz.

Registry dosyalarından doğrudan bilgiler alabilmemiz mümkün değildir. Bu bilgiler alabilmemiz için bazı yazılımlar kullanmamız gerekmektedir. Sizlere şimdi Eric Zimmerman'ın github hesabından indirmiş olduğum Registry Explorer yazılımı ile Registry dosyalarının içerisinde nasıl bilgiler elde ediyoruz onları anlatacağım.

Registry dosyalarını inceleyebilmemiz için dosyanın orijinali kopyalayarak ya da almış olduğumuz imajlar üzerinden gerçekleştirebiliriz.

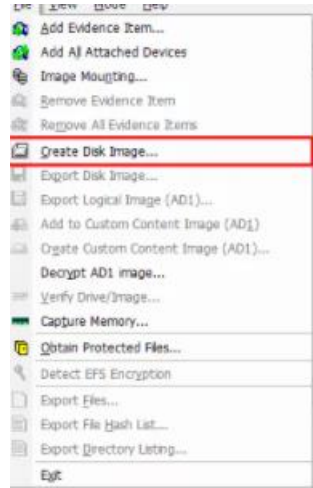
2. İMAJ ALMA

2.1. İmaj nedir?

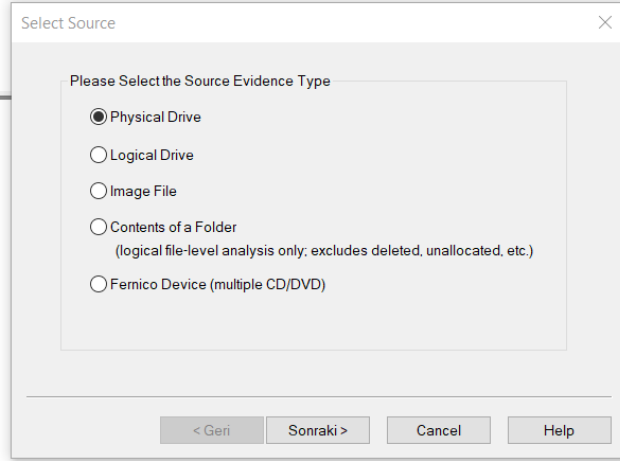
Bir cihazın veya depolama aygıtlarının o andaki verilerinin kopyasının alınmasına denir. Adli bilişim alanında direkt delil üzerinde incelemek yerine imaj yani verinin kopyası üzerinde çalışmamız olası bir veri kaybını ortadan kaldırır. Bir delilin istediğimiz kadar adli kopyasını alabiliriz. Kopya alma işlemi farklı yazılımlarla yapılabilir. Ben sizlere FTK Imager üzerinden kopya alma işlemi göstereceğim.

2.2. İmaj nasıl alınır?

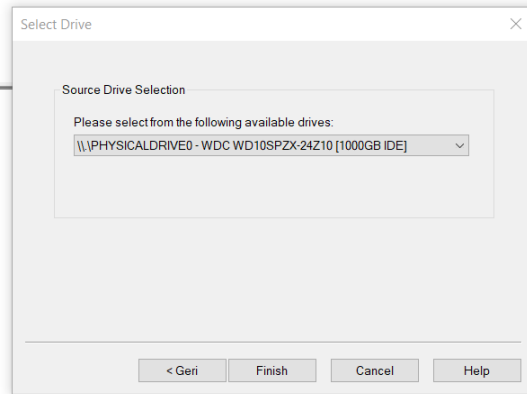
FTK imager yazılımında File sekmesinden Create disk Image seçeneğini seçelim.



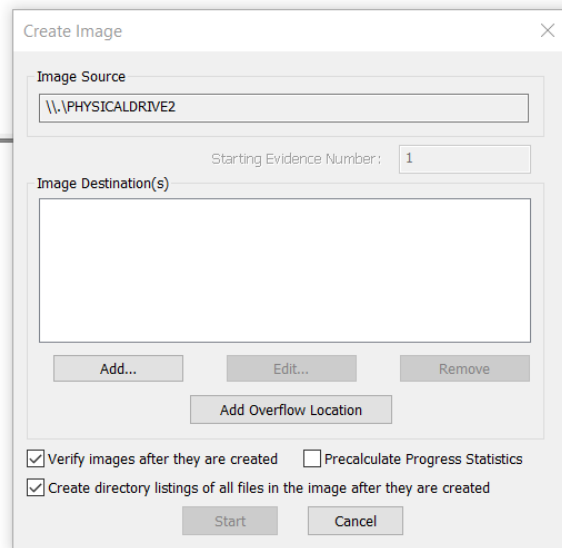
Physical Drive seçeneği ile devam edelim. Ve sonraki seçeneğine tıklayalım.



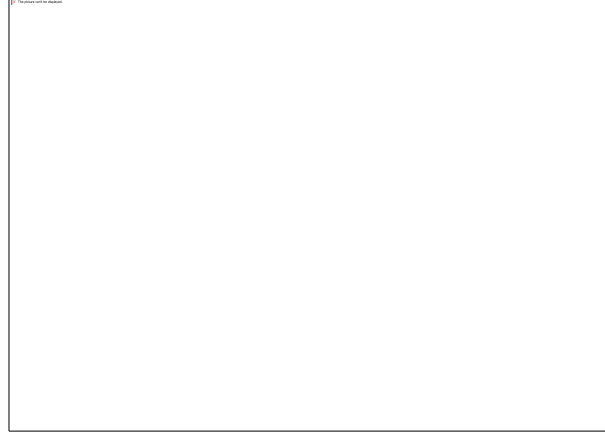
Burada imaj almak istediğimiz diski seçiyoruz. Seçtiğimiz işlemin ardından Finish diyoruz.



Şimdi ise bizi bu şekilde bir sayfa karşılıyor.



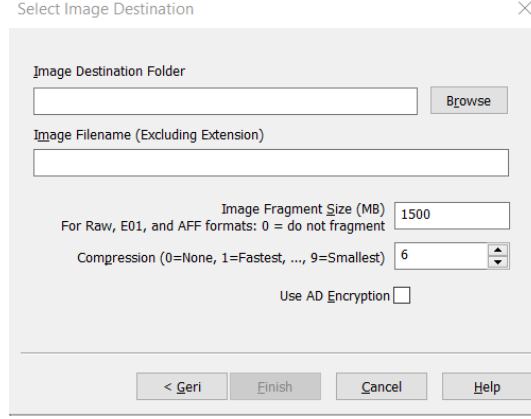
Add seçeneğinden imaj formatını seçiyoruz.



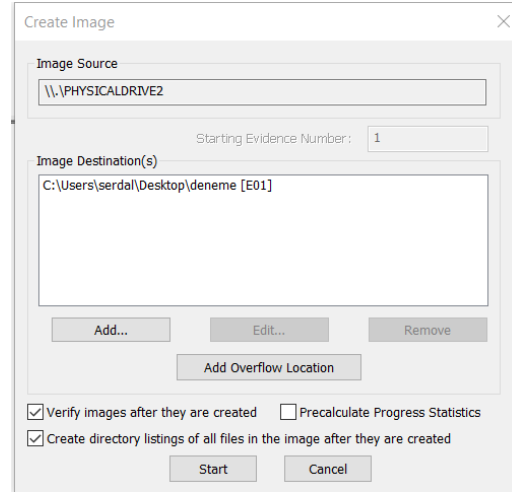
DD formatı: Bu formatta ki imajlar herhangi bir sıkıştırma uygulamadan birebir alınan imajlar olarak bilinirler ve sürücüler ile aynı boyutta olurlar.

Bu açılan sayfada imaj ile alakalı verebileceğimiz bilgileri doldurmamızı istiyor. Bu kısım Adli Bilişim açısından önemlidir. Şimdilik ben hepsine 1 veriyorum ve sonraki seçeneğine tıklayarak devam ediyorum.

Şimdi ki açılan sayfada **Destination Folder** kısmından imajı nereye almak istiyorsak orayı seçiyoruz. **Filename** kısmından imaj dosyasına isim veriyoruz. **Fragment** kısmı imaj dosyasını 1500 mb dan sonra parçalara bölümlendirme işlemi yapmamızı sağlıyor. **Compression** kısmından ise bölümlendirme sayısını seçebiliyoruz. **Use AD Encryption** buradan ise dosyayı şifreleyebiliyoruz.



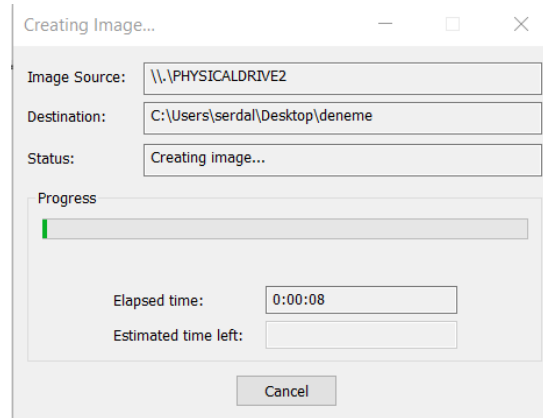
İşlemleri yapmamızın ardından Finish sekmesi açılacak. Tıklayarak devam edelim. Bizi tekrardan bu sayfaya gönderiyor.



Şimdi ise size sayfanın alt kısımda bulunan kutucuklar hakkında bilgi vereceğim.

-Verify Images after they are created kısmından diskin ilk hali ile imaj arasında doğrulama işlemi (hash doğrulaması) yapıyor.

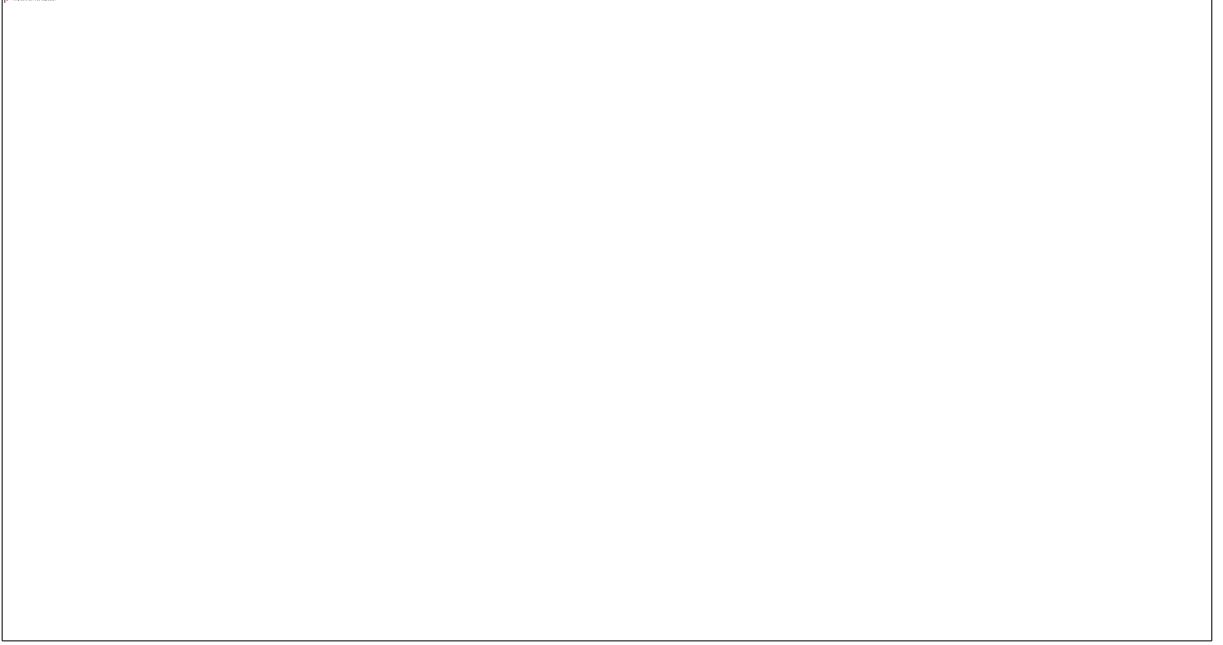
Şimdi ise **Start** diyerek işlemi başlatmış oluyoruz. İşlemin devam ederken şu ekran karşımıza oluyor.



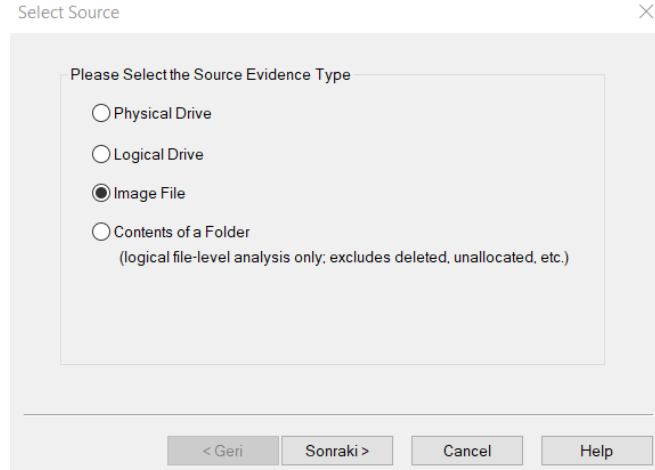
Bu işlem bittikten sonra imaj alma işlemini gerçekleştirmiş oluyoruz.

2.3. İmajı İçeri Aktarma Nasıl Yapılır?

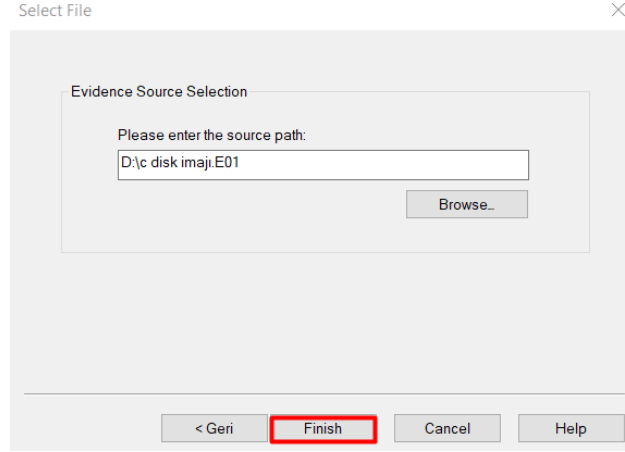
İmaj alma işlemini gerçekleştirdikten sonra FTK Imager yazılımı üzerinden imajı içeri aktarıyoruz. **File > Add Evidence Items** seçeneğine tıklıyoruz.



Ardından açılan sekmede **Image File** butonunu aktif etmemizin ardından sonraki seçeneğine tıklıyoruz.



Burada ise imaj dosyasının konumunu gösterdikten sonra **Finish** seçeneğine tıklayarak imajı içeri aktarmış oluyoruz.



İmaj dosyasını başarılı bir şekilde içeri aktarmamızın ardından verdiğimiz dosya konumuna giderek **NTUSER.DAT** dosyasını export etme işlemini gerçekleştirebiliriz.

2.4. Dosyaları Export Etme İşlemi Nasıl Yapılır?

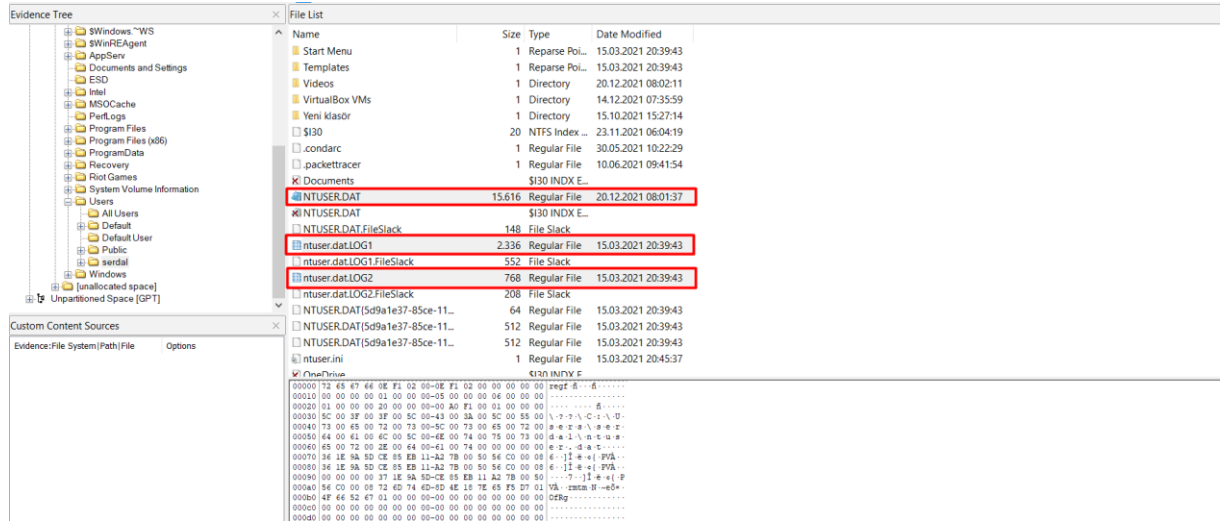
NTUSER.DAT dosyalarının bulunduğu konum;

C:\ users \ kullanıcıadi \ NTUSER.DAT

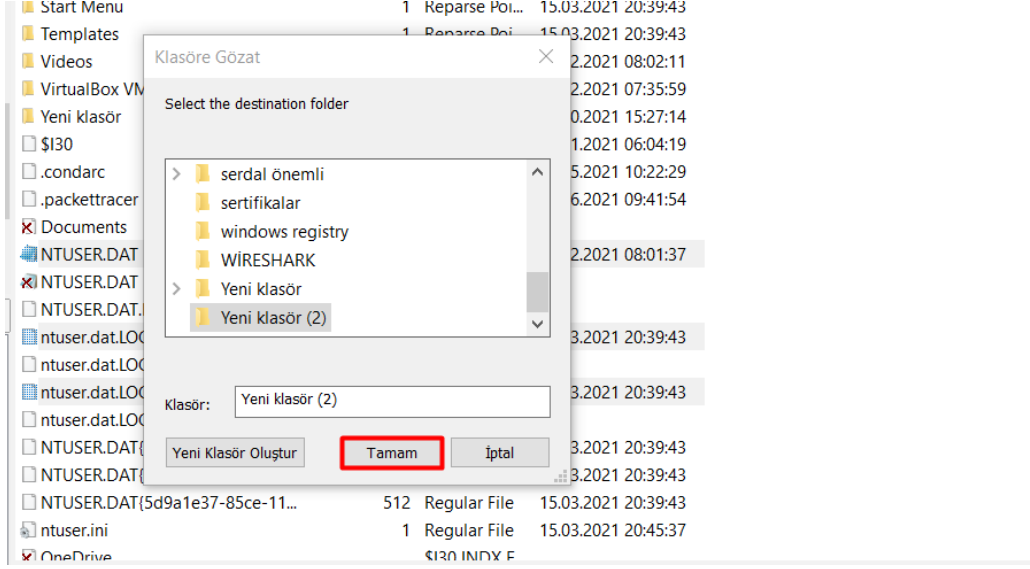
SAM, SECURITY, SOFTWARE ve SYSTEM dosyalarının bulunduğu konum;

C \ Windows \ system32 \ config

Dosyaları bulalım ve export edelim.



Dosyaları seçmemizin ardından sağ tık > Export File diyoruz.



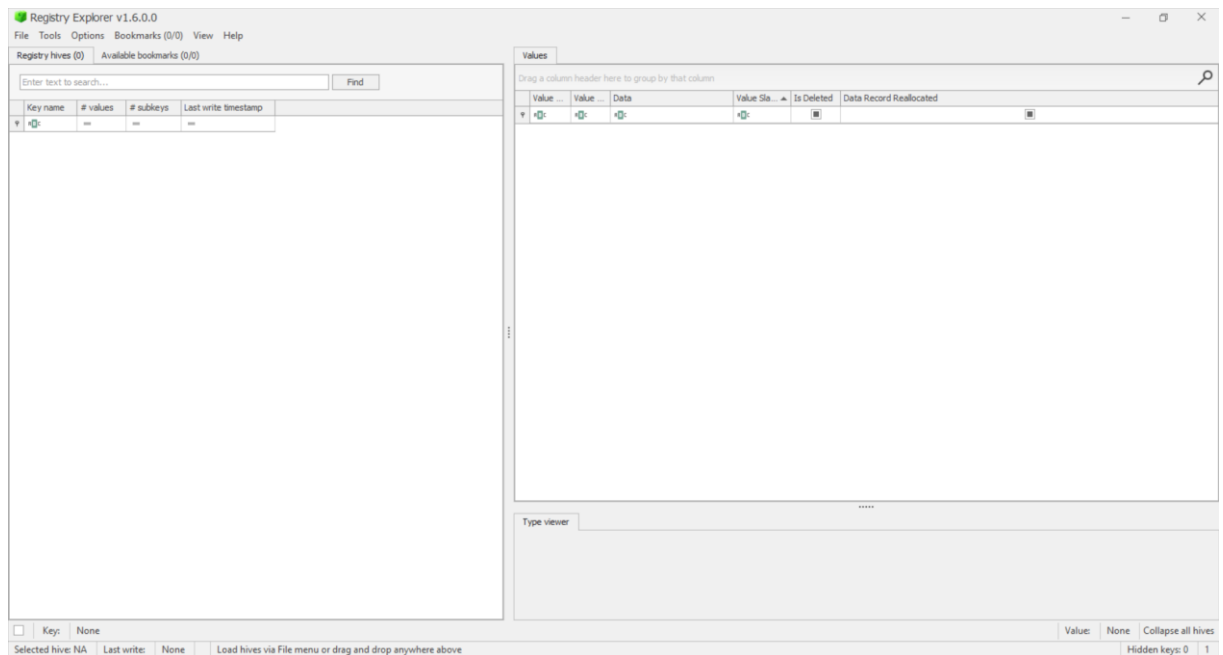
Açılan bu ekranda export edeceğimiz konumu seçtikten sonra tamam seçeneğine tıklayarak export etme işlemini tamamlamış oluyoruz. Bu işlemleri diğer registry dosyalarına da uyguluyoruz.

3. Registry Explorer Yazılımı İle Dosyalar Nasıl İncelenir?

3.1. Dosyalar İçeri Nasıl Aktarılır?

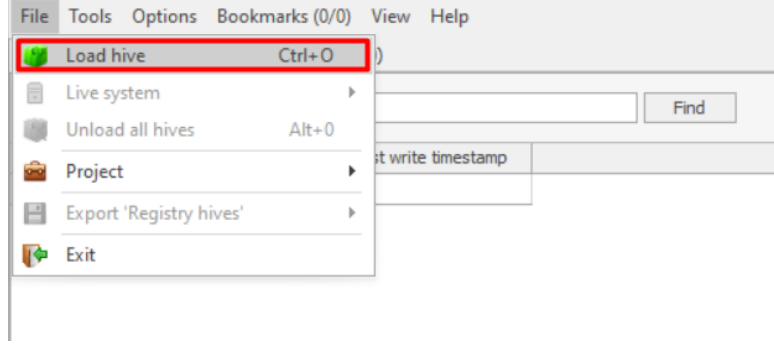
Bu işlemin ardından Eric Zimmerman Github hesabından indirmiş olduğum Registry Explorer yazılımını açıyoruz.

Eric Zimmerman Github hesabı: <http://ericzimmerman.github.io/#!index.md>

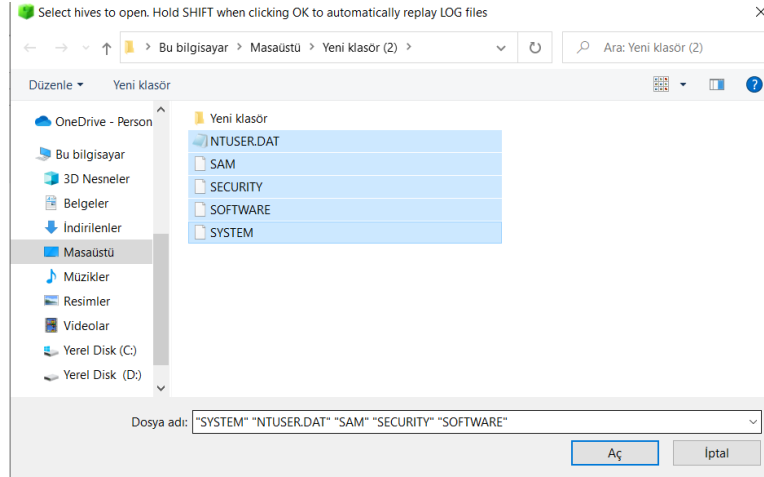


Yazılımı açtıktan sonra bu ekran bizi karşılıyor. Şimdi ise export etmiş olduğumuz NTUSER.DAT dosyasını burada açıp inceleyeceğiz.

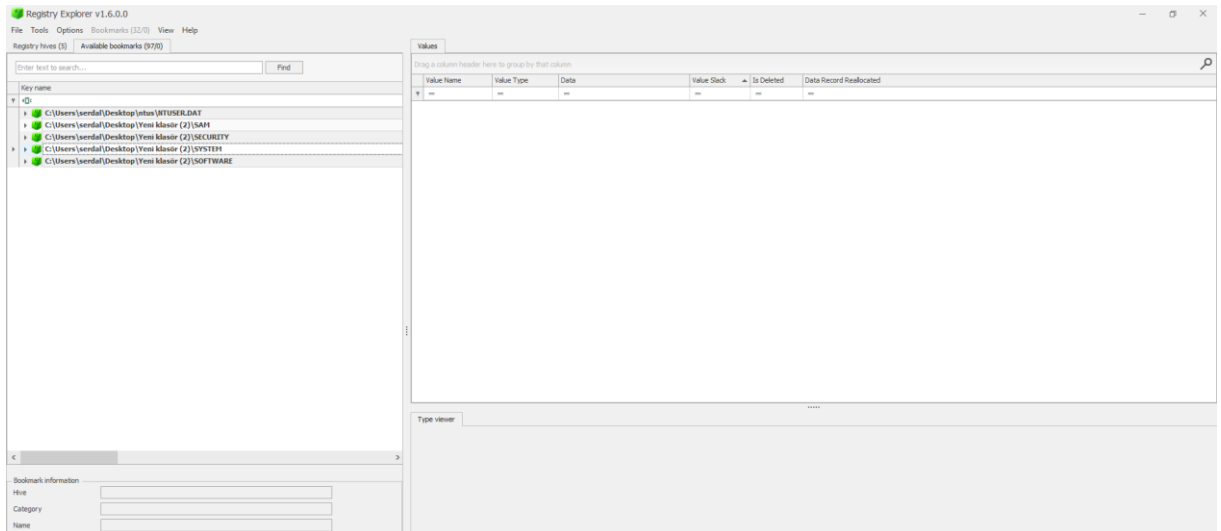
Burada **File > Load Hive** seçeneği ile devam ediyoruz.



Bu seçenekten sonra açılan sayfadan dosyaları seçiyoruz ve Aç seçeneğine tıklıyoruz.



Dosyayı açma işlemini gerçekleştirmiş oluyoruz.



3.2. Veriler Nasıl Analiz Edilir?

3.2.1. NTUSER.DAT

NTUSER.DAT altındaki **RecentDocx** dosyasına giderek son açılan dosyaları görebiliriz.

Registry Hives (5) Available bookmarks (9/70)		Values	Recent documents			
Enter text to search...			Drag a column header here to group by that column			
Key name	Value Name	Target Name	Link Name	File Position	Opened On	Extension Last Opened
<ul style="list-style-type: none"> Users\sendall\Desktop\intel-RTXDESKTOP Accounts Applets ComDlg32 CurrentVersion CurrentVersion CurrentVersion Environment Fontlogage Fliesets FileHistory FileFolder FTP History Internet Settings LYNC Mail Map Network Drive HBU MountPoints2 App Paths Unreal PrinterPorts RecentDocs Run StartMenu RunOnce Shut Folders Taskband Taskbar Taskbar 						
RecentDocs	138	Server	Server	2018-12-20-16-23-57-49.png	0	2021-12-20 07:57:36
RecentDocs	1	Internet	Internet.Lnk		1	
RecentDocs	135	windowsupdate	ms-settings-windowsupdate (2).lnk		2	2021-12-20 07:55:47
RecentDocs	80	Type Generator	Type Generator (2).lnk		3	
RecentDocs	57	(9)SAFE01F854-4418-4358-6E53-22D0A0E5	Windows desktops aç veya kapat.lnk		4	
RecentDocs	145	7. kab 2018-4 - Wireless Attacks - Kabuless Saldirılar	7. kab 2018-4 - Wireless Attacks - Kabuless Saldirılar.lnk		5	
RecentDocs	35	1. WinCrack-ng.mpg4	1. WinCrack-ng.mpg4.lnk		6	2021-12-17 12:04:07
RecentDocs	62	Wireless'nin Şifre Saldirı Analizi	Wireless'nin Şifre Saldirı Analizi.lnk		7	
RecentDocs	139	1. WinCrack-ng.mpg4 - Hemen - Kapatıl	1. WinCrack-ng.mpg4 - Hemen - Kapatıl.lnk		8	
RecentDocs	130	indrieler	indrieler (3).lnk		9	
RecentDocs	136	security-g57b1202_1920.jpg	security-g57b1202_1920.jpg.lnk		10	2021-12-17 11:29:17
RecentDocs	117	internet-g56415506e_1920.jpg	internet-g56415506e_1920.jpg.lnk		11	
RecentDocs	0	windowsupdate	ms-settings-windowsupdate (2).lnk		12	
RecentDocs	42	SEM.docx	SEM.docx.lnk		13	2021-12-16 21:23:06
RecentDocs	21	redirect	http--www.msoftconnect.com-r edirect (6).lnk		14	
RecentDocs	124	senal machine isolat	senal machine isolat (2).lnk		15	
RecentDocs	5	ubuntu-20.04.2.0-desktop-amd64.iso	ubuntu-20.04.2.0-desktop-amd64.iso.lnk		16	2021-12-16 10:42:20
RecentDocs	38	ZENMAP.docx	ZENMAP.docx		17	
RecentDocs	27	windows server	windows server.lnk		18	
RecentDocs	121	Windows_Server_2016_Datacenter - ZENMAP - ZENMAP - ZENMAP - ZENMAP	Windows_Server_2016_Datacenter - ZENMAP - ZENMAP - ZENMAP - ZENMAP.lnk		19	
RecentDocs	33	ms-gamingoverlay-[]	ms-gamingoverlay-[] (6).lnk		20	
RecentDocs	26	lgchex/	ms-gamingoverlay-lgchex-3.k		21	
RecentDocs	148	veri rdbf.d	veri rdbf.d.lnk		22	
Total rows: 515						

RunMRU dosyasından çalıştır uygulaması(Windows tuşu + R) ile aranan ve çalıştırılan uygulamaları göstermektedir.

Registry Items (3)
Available bookmarks (9792)

Enter text to search...

Key name

- [-] HKEY_CURRENT_USER
 - [-] Environment
 - FtpHistory
 - PrintFolder
 - FTP
 - History
 - Internet Settings
 - Lync
 - Main
 - Map Network Drive MRU
 - MagnetRsync2
 - App Paths
 - Uninstall
 - PrinterPorts
 - RecentDocs
 - Run
 - RunMRU
 - RunOnce
 - Shell Folders
 - Tastband
 - TypePaths
 - TypeURLs
 - USBR
 - User Assist
 - WinSxS
 - WindowsCommon-Log
 - [+] C:\Users\jensdal\Desktop\Yeni klasör (2)\SAF
 - [+] C:\Users\jensdal\Desktop\Yeni klasör (2)\SECURITY
 - [+] C:\Users\jensdal\Desktop\Yeni klasör (2)\SYSTEM
 - [+] C:\Users\jensdal\Desktop\Yeni klasör (2)\SOFTWARE

Values RunMRU

Group a column header here to group by that column

Value Name	MrU Position	Executable	Opened On
f	0	cmd	2021-10-18 18:40:57
g	1	dvdag	
e	2	services.msc	
d	3	msconfig	
c	4	temp	
b	5	appwiz.cpl	
a	6	taskmgr.exe	

TypedPaths dosyasından Windows gezginde hızlı erişim kısmında dosya konumunu vererek yaptığımız aramaları bizler göstermektedir.

Registry Hives

Displays all loaded Registry Hives

Drag and drop hives or use the File menu to load hives

- FileHistory
- FileVault
- FSP
- History
- Internet Settings
- Local
- Main
- Map Network Drive (NLU)
- MountPoints2
- App Paths
- Uninstall
- PrinterPorts
- RecentDocs
- Sam
- RunHKL
- RunOnce
- Shell Folders
- Taskbar
- TypedPaths
- TypedURLs
- USER
- User-Assist
- WinRAR
- WordWheelQuery
- C:\Users\jensaltdesktop\Yemi Maslar (2)\SAH
- C:\Users\jensaltdesktop\Yemi Maslar (2)\SECURITY
- C:\Users\jensaltdesktop\Yemi Maslar (2)\SYSTEM
- C:\Users\jensaltdesktop\Yemi Maslar (2)\SOFTWARE

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Stack	Is Deleted	Data Record Reallocated
u11	RegSz	C:\Users\jensaltdesktop\AppData\Roaming\Microsoft\Windows			
u11	RegSz	C:\Users\jensaltdesktop\hualles 106	SC-00-4D-00-69-00-63-00-7...		
u12	RegSz	Serdar Tarkan Altun	61-00-74-00-61-00-SC-00-5...		

UserAssist dosyasından ise hangi uygulamanın ne zaman, kaç kez yürütüldüğünü göstermektedir.

Registry Hives (1) Available bookmarks (7/70)		Values	User Asset			
Enter text to search...		Group a column header here to group by that column				
Key name		Program Name	Run Counter	Focus Count	Focus Time	Last Executed
+	+	UEMF_CTLCLICountCtrl	0	0	06, 0h, 00m, 00s	—
	+	UEMF_CTLSESSION	176	1547	15, 0h, 24m, 46s	—
+	+	Microsoft.WindowsFeedbackHub_Bitelby3d8bweApp	0	0	06, 0h, 00m, 00s	2020-12-11 16:21:13
+	+	System32 SnippingTool.exe	0	0	06, 0h, 00m, 00s	2021-11-16 10:42:06
+	+	Microsoft.WindowsCalculator_Bitelby3d8bweApp	0	0	06, 0h, 00m, 00s	2021-07-23 12:33:55
+	+	System32 ipconfig4.exe	4	4	04, 0h, 03m, 49s	2021-12-14 09:12:32
+	+	System32 notepad.exe	1	1	03, 0h, 00m, 20s	2021-12-02 17:50:51
+	+	System.Windows.ShellExperienceHost_cx5n3h2zyenwApp	0	19	05, 0h, 11m, 38s	2021-11-14 17:04:04
+	+	Microsoft.Windows Explorer	13	124	05, 0h, 43m, 41s	2021-12-10 06:21:58
+	+	Microsoft.MicrosoftEdge_Bitelby3d8bweMicrosoftEdge	0	0	2020-06-04 11:33:31	2020-06-04 11:33:31
+	+	Microsoft.Windows.ControlPanel	5	9	0h, 04m, 31s	2021-12-10 06:21:58
+	+	windows.immersivecontrolpanel_cx5n3h2zyenw/microsoft.windows.immersivecontrolpanel	6	15	06, 0h, 00m, 00s	2021-12-10 07:55:46
+	+	Microsoft.Windows.Cortana_cx5n3h2zyenw/Cortana.exe	0	0	06, 0h, 00m, 00s	—
+	+	OperaSoftware.OperaBrowser_1576321079	0	0	06, 0h, 00m, 00s	2020-03-04 13:43:14
+	+	System32 cmd.exe	6	11	06, 0h, 05m, 12s	2021-12-17 10:14:02
+	+	System32 vmact.exe	0	0	2021-11-11 05:53:32	2021-11-11 05:53:32
+	+	Chrome_372A61F932D6ACBEB93F78A>UserData.Default	0	0	2020-11-13 12:41:04	2020-11-13 12:41:04
+	+	Chrome_372A61F932D6ACBEB93F78A	33	598	06, 19m, 21m, 56s	2021-12-10 05:56:23
+	+	Microsoft.WindowsStore_Bitelby3d8bweApp	0	0	2021-09-06 12:37:36	2021-09-06 12:37:36
+	+	Microsoft.WindowsCommunicationsApps_Bitelby3d8bwe/microsoft.windowscommunication	5	20	05, 0h, 11m, 30s	2021-12-10 05:52:01
+	+	Program Files (x86)\Steam\Steam.exe	0	0	06, 0h, 00m, 00s	2021-11-16 07:57:30
+	+	Microsoft.Windows.SecurityHealth_cx5n3h2zyenw/SecurityHealth	0	2	05, 0h, 00m, 29s	2021-04-14 09:25:07
+	+	Microsoft.Windows.CloudExperienceHost_cx5n3h2zyenw/CloudExperienceHost	0	1	06, 0h, 00m, 06s	2019-12-16 08:47:05
		Total rows: 336				

3.2.2. SYSTEM

USBTOR dosyası altına giderek takılan usb aygıtların üreticilerini, seri numaralarını ve zamanlarını detaylı bir şekilde görebilmekteyiz.

Open key: C:\Users\seanli\Desktop\Yeni Masin (2)\SYSTEM

Enter text to search...

Find

Key name

C:\Users\seanli\Desktop\Yeni Masin (2)\SYSTEM

- (04975b-b6d1-41e1-8318-4d5c875666c5)
- (4d36972-125-11e4-bfc1-08002030181e)
- (1239307-b6bf-11e5-84f2-08002030181e)
- (80d116c-82cf-11b7-bec7-000020302030)
- AppCompatCache
- ban
- Devices
- ComputerName
- CrashControl
- DeviceClasses
- Environment
- EventLog
- FileHistorySnapshot
- FileSystem
- HardwareId
- Memory Management
- MountedDevices
- PartitionParameters
- Win7
- SafeBoot
- Services
- Shares
- Terminal Server
- TimeZoneInformation
- USB
- USB\VID
- USB\VEN_General\Prod_U Disk\Rev_5.00
- USB\VEN_General\Prod_Flash Disk\Rev_8.07

Values

USBSTOR

Drop a column header here to group by that column

Timestamp	Manufacturer	Title	Version	Disk ID	Serial Number	Device Name	Installed	First Installed	Last Connected	Last Removed
2021-11-07 19:04:26	Veri_General	Prod_U Disk	Rev_5.00	{ec862117-8055-11e4-c2aa-000c302030a0}	68352e167580A_50	General USB Device	2021-11-07 19:04:26	2021-11-07 19:04:26	2021-12-03 16:36:39	2021-02-16 16:36:15
2021-11-19 13:22:19	Veri_Generic	Prod_Flash_Disk	Rev_8.07	{49500095-4786-11e4-c2af-000c302030a0}	122A518F80	Generic Flash Disk USB Device	2021-11-19 13:22:19	2021-11-19 13:22:19	2021-11-19 18:01:06	2021-11-19 18:01:22
2021-11-05 14:01:03	Veri_Kingston	Prod_DataTransfer_3_0	Rev_2000	{c01958f8-3055-11e4-c2aa-000c302030a0}	00358586470135C51414427180	Kingston DataTransfer 3.0 USB Device	2021-11-05 14:01:03	2021-11-05 14:01:03	2021-11-05 14:32:01	2021-11-05 14:32:10
2021-12-01 12:30:52	Veri_SanDisk	Prod_Ultra_USB_3.0	Rev_1.00	{55343836-9008-11e4-c2af-000c302030a0}	03114594c6afe14ef088D50954499488baf613536-165091127535-B948db	SanDisk Ultra USB 3.0 Device	2021-12-01 12:30:52	2021-12-01 12:30:52	2021-12-01 14:54:22	2021-12-01 15:02:19
2021-05-09 07:04:14	Veri_SMD	Prod_USB_DSKK	Rev_1.00	{469ca36-4308-11e4-b266-000c6206efac7}	833A34403B80	SMD USB DSKK USB Device	2021-05-09 07:04:14	2021-05-09 07:04:14	2021-12-14 14:35:43	2021-12-14 14:36:38
2021-11-12 09:53:18	Veri_TOSHIBA	Prod_TransMemory	Rev_1.00	{ec0c7963-3055-11e4-c2aa-000c302030a0}	0022C7F68B9BC340570F0ED3360	TOSHIBA TransMemory USB Device	2021-11-12 09:53:18	2021-11-12 09:53:18	2021-11-12 09:53:18	2021-11-12 09:55:04
2021-11-19 10:21:24	Veri_TOSHIBA	Prod_TransMemory	Rev_9HAP	{47479aa-4786-11e4-c2af-000c302030a0}	0838F993323E3230140E142180	TOSHIBA TransMemory USB Device	2021-11-19 10:21:24	2021-11-19 10:21:24	2021-11-19 10:21:24	2021-11-19 10:36:12

MountedDevices mount edilmiş cihazları göstermektedir.

[illegible]

İnterface bilgileri:

ControlSet001\Services\Tcpip\Parameters\Interfaces\{e6161b02-8f42-4410-9024-f273b87f3f70}

Konumuna giderek interfacelerimiz hakkında önemli bilgileri detaylı bir şekilde vermektedir.

Registry Hives (5)Available bookmarks (970)

Enter text to search...

Find

Key name	# values	# subkeys	Last write timestamp
SetpSvc	10	2	2021-05-12 20
StateRepository	11	2	2021-05-12 20
Steam Client Service	8	1	2021-05-12 20
stecor	7	2	2021-05-12 20
stetvc	10	2	2021-05-14 19
stetvc	8	1	2021-12-20 07
stetvc	9	2	2021-05-15 14
stetvc	8	1	2021-12-20 07
stetvc	9	1	2021-05-12 20
stetvc	11	2	2021-05-12 20
stetvc	8	2	2021-11-13 08
stetvc	7	2	2021-05-12 20
stetvc	13	2	2021-05-12 20
stetvc	8	2	2021-12-20 07
stetvc	10	1	2021-05-12 20
SynthSvc	7	0	2021-05-12 20
SysMain	15	1	2021-05-12 20
SystemEventBroker	12	3	2021-05-12 20
SystemUpdateService	12	3	2021-05-12 20
TagSvc	11	3	2021-05-12 20
Topic	13	5	2021-05-15 20
Unlauge	3	0	2021-11-15 15
Parameters	14	6	2021-12-20 07
Adapters	0	9	2021-11-15 15
ChkRegistedAdapters	0	0	2021-05-12 20
Interfaces	0	10	2021-12-20 07
{00617339-b0-43-49e1-b0-19-bc355e96cafd}	5	0	2021-12-17 10
{00-16a3-0003-4862-6f1a-b6-7759a112d}	27	0	2021-12-20 07
{20ac3771-3a3d-11e0-a211-0006395646c0}	0	0	2021-12-20 07
{3b58087f-d6d4-4c40-9e37-dad9649629c4}	5	0	2021-12-17 10
{81441c46-020f-4005-8f11-b61608baac93}	18	0	2021-12-20 07
{80-16a8-b0a7-4316-8974-30b8-1a567a2}	5	0	2021-12-17 10
{a0803232-327c-4209-998c-7017a5a8b04c}	0	0	2021-12-17 10
{a27837bc-c94c-4135-9d66-43b3c2f44b65}	0	0	2021-12-20 07
{94880547-6373-44d1-8799-b717c11a6b4c}	16	0	2021-12-17 10
{e6163302-8642-4410-9024-92738b...}	24	2	2021-12-17 10
NacOpsSecurity	0	0	2019-12-07 09
NetworkRoutes	0	0	2019-12-07 09
Winsock	3	0	2019-12-07 09
Performance	5	0	2019-12-07 09

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Stack	Is Deleted	Data Record Reallocated
EnableDHCP	RegDword	1			
Domain	RegSz				
NameServer	RegSz				
Lease	RegDword	691200			
LeaseObtainedTime	RegDword	1639732185			
T1	RegDword	1640077785			
T2	RegDword	1640369685			
LeaseTerminatedTime	RegDword	1640423385			
AddressType	RegDword	0			
IsServerNameAware	RegDword	0			
DhcpConnForBroadcastFlag	RegDword	1			
DhcpNameServer	RegSz	10.1.1.224 10.1.1.223			
DhcpGatewayHardwareCount	RegDword	1			
RegistrationEnabled	RegDword	1			
RegistrationAdapterName	RegDword	0			
DhcpDomain	RegSz	first.local	00-00-79-7E-4E		
DhcpInterfaceOptions	RegBinary	FC-00-			

3.2.3. SAM

SAM dosyası altında sadece kullanıcıların son giriş tarihi, parola ipucu ve parola değiştirme tarihlerine ulaşabiliyoruz.

Registry Hives (5)

Available bookmarks (970)

Enter text to search...

Find

Key name

C:\Users\serdal\Desktop\Yeni klasör (2)\USER.DAT

C:\Users\serdal\Desktop\Yeni klasör (2)\SAM

Users

000001F4

000001F6

000001F7

000001F8

000001E9

Names

C:\Users\serdal\Desktop\Yeni klasör (2)\SECURITY

C:\Users\serdal\Desktop\Yeni klasör (2)\SYSTEM

C:\Users\serdal\Desktop\Yeni klasör (2)\SOFTWARE

Bookmark information

C:\Users\serdal\Desktop\Yeni klasör (2)\SAM

Operating system

Users

SAM\Domains\Account\Users

User accounts

User accounts in SAM file

Drop a column header here to group by that column

User ID	Initial	Total	Created	Last L	Last P	Expire	User	Full N.	Passw.	Groups	Comm.	User	Home	Intern.	Accou.	Home	Passw.	Temp	Norm	Phn L	Intend	Workst	Service	Passw	Auto L
500	0	0	2021-...				Adminis	trator		Adminis	trator	Bilgiyay	aracılığı	alınan	çalışma	edici	kullanıla	n	örnekle	n tanımla					
501	0	0	2021-...				Guest			Guests		Bilgiyay	aracılığı	alınan	çalışma	edici	kullanıla	n	örnekle	n tanımla					
503	0	0	2021-...				Yeni kullanıcı			Sistem	Tarayıcı	Sistem	Tarayıcı	dan	çalışma	edici	kullanıla	n	örnekle	n tanımla					
504	0	0	2021-...		2019-...		Windows	Defend		Windows	Defend	er	Defend	er	Defend	er	Defend	er	Defend	er					

Total rows: 5

Export

Type viewer

Value name

Default

Value type

RegDword

Value

0

Raw value

Key: SAM\Domains\Account\Users

Value: (default)

Collapse all

3.2.4. SOFTWARE

CurrentVersion işletim sistemi hakkında bilgi vermektedir.

Value Name	Value Type	Data	Value Stack	Is Deleted	Data Record Reallocated
CommonFileDir	RegDz	C:\Program Files\Common Files			
CommonW432Dir	RegDz	C:\Program Files\Common Files			
SH_SameName	RegDz	Games			
ProgramFileDir	RegDz	C:\Program Files	00-00		
DevicePath	RegExpandSz	%SystemRoot%\inf	00-00		
ProgramW432Dir	RegDz	C:\Program Files	00-00		
CommonFileDir (x86)	RegDz	C:\Program Files (x86)\Common Files	00-00-00-00		
SH_ConfigureProgramName	RegDz	Set Program Access and Defaults	00-00-00-00		
ProgramFileDir (x86)	RegDz	C:\Program Files (x86)	00-00-00-00-00-00		
MediaPathUnexpanded	RegExpandSz	%SystemRoot%\Media	00-00-00-00-00-00		
ProgramFileDir	RegExpandSz	%ProgramFiles%	00-00-00-00-00-00		

NetworkList kısmından bağlanılan kablosuz ağlarla ilgili ağ ismi, bağlanma tarihi, ayrılma tarihi vb. bilgilere ulaşabiliyoruz.

First Network	Network Name	Name Type	First Connect LOCAL	Last Connected LOCAL	Managed	DNS Suffix	Gateway Mac Address	Profile GUID
GSBWIFI 2	GSBWIFI 2	Wireless	2021-10-24 23:18:20	2021-10-24 23:18:20		kywell.com	70-69-5A-E2-0D-01	{187F4D60-130C-44C3-A1-2B-86A0C3389F65}
Cruise	Cruise	Wireless	2021-11-07 22:09:29	2021-11-28 17:52:08		cyko>	7E-79-A2-70-A7-8B	{28D1950-5481-48F0-A23-2-68D30230A202}
SERIAL TARKAN 3	SERIAL TARKAN 3	Wireless	2021-11-15 16:24:34	2021-11-19 18:10:20		cyko>	08B8CE5-258F-4FC3-835-E-238E7258A425	{08B8CE5-258F-4FC3-835-E-238E7258A425}
FiberGW_7P4730_2_4GHz	FiberGW_7P4730_2_4GHz	Wireless	2021-10-15 18:21:03	2021-10-15 19:09:06		cyko>	E8-4B-8B-05-47-3E	{C2763523-6334-4D8A-899-2-803C71A3D79F}
FU_WIFI	FU_WIFI	Wireless	2021-11-09 11:06:40	2021-12-17 12:09:47		first.local	90-00-5E-00-01-78	{3486E24C-039A-4B80-9A-CC-76A3D8F45A35}
Yuga Kaban	Yuga Kaban	Wireless	2021-11-27 20:14:30	2021-11-27 20:14:30		cyko>	3E-0C-6C-68-08-0E	{DC348D02-6275-4D06-A3-75-458C73D6A455}
SERIAL TARKAN 2_4G	SERIAL TARKAN 2_4G	Wireless	2021-05-15 00:14:26	2021-09-23 21:02:04		cyko>	E4-C3-2A-9A-11-F4	{DFAC457B-A3B8-4480-8E5-F-7F6A8625C625}
SERIAL TARKAN 2	SERIAL TARKAN 2	Wireless	2021-09-10 13:51:30	2021-12-14 17:34:48		cyko>	F2-12-8D-7F-EB-69	{A8A38CF-8913-43D0-820-F-4F35634701C2}
M SIT	M SIT	Wireless	2021-10-24 22:44:49	2021-10-24 22:44:49		cyko>	35-A5-9C-F6-15-05	{C78D7441-E531-4F6A-8EA-9-C2B3D3D9F159}
Mem u mem	Mem u mem	Wireless	2021-11-02 23:08:44	2021-11-02 23:08:44		cyko>	00-81-2B-A6-62-4F	{08A233F-3888-43D8-8B7-E-4F5F72F688F0}
SERIAL TARKAN	SERIAL TARKAN	Wireless	2021-08-24 10:35:48	2021-08-24 10:35:48		cyko>	0A-87-08-FD-7C-C3	{5A8C4F90-0122-4F68-95-A5-6358C3F9F7A4}
DESKTOP-4QC-IT71 0663	DESKTOP-4QC-IT71 0663	Wireless	2021-11-15 15:53:28	2021-11-15 16:24:22		cyko>	8138D97E-299C-44CC-615-F-7B5003A1A8F7	{8138D97E-299C-44CC-615-F-7B5003A1A8F7}
GSBWIFI	GSBWIFI	Wireless	2021-10-16 08:31:58	2021-12-17 00:24:03		kywell.com	90-00-5C-4F-F1-76	{824C3991-68E2-4D39-A3E-4A13E0D3B269F0}
Superbox_WIFI_BH49	Superbox_WIFI_BH49	Wireless	2021-09-13 10:43:22	2021-09-06 20:39:07		cyko>	3C-13-86-6A-2B-48	{82C4384F-4882-4D4D-A4-11-8087C1C468F1}
FRONALIN	FRONALIN	Wireless	2021-11-27 20:08:57	2021-11-29 21:46:47		cyko>	46-EB-08-3D-4D-05	{DC3DCE36-C4E9-448B-93-8F-4F5F72F688F0}
VodafoneNet-HBWGN	VodafoneNet-HBWGN	Wireless	2021-05-19 10:04:01	2021-07-27 15:37:45		cyko>	E4FB-5D-46-03-34	{F1C2D3C7-0511-4B39-4F-01-E2145338F9F7F0}
TEKNO PC	TEKNO PC	Wireless	2021-05-19 17:10:02	2021-05-19 17:10:02		cyko>	90-8F-68-6A-F3-5A	{6A828B05-0CA2-49B8-B9-E7-08B8582CF0AF}
AndroidAP 3D9C	AndroidAP 3D9C	Wireless	2021-12-07 18:04:24	2021-12-07 19:19:12		cyko>	4E-29-55-63-EB-67	{80C85525-43E3-4970-91B-2-074735846038}
SERIAL TARKAN 4	SERIAL TARKAN 4	Wireless	2021-11-22 08:40:27	2021-11-23 10:30:10		cyko>		{812E0662-01C2-4637-AE-...

Run dosyası içerisinde ise başlangıç programlarını göstermektedir.

Value Name	Value Type	Data	Value Stack	Is Deleted	Data Record Reallocated
SecurityHealth	RegExpandSz	%windir%\system32\securityhealth\sysray.exe	00-00-00-00		

LogonUI dosyasında ise en son giriş yapan kullanıcı bilgileri bulunmaktadır.

The screenshot shows the Windows Registry Editor. The left pane displays the tree structure with 'LogonUI' selected under 'Microsoft\Windows\CurrentVersion\Authentication'. The right pane shows the 'ShowTabletKeyboard' registry value, which is a 'RegDword' type with a value of '0'. The 'Value' field is highlighted, and the 'Raw value' is '00-00-00-00'.

Value Name	Value Type	Data	Value Stack	Is Deleted	Data Record Reallocated
ShowTabletKeyboard	RegDword	0			
IdleTime	RegDword	0			
EnvironmentCached	RegDword	0			
LastLoggedOnUser	RegSz	.\jerdal	3C-04		
LastLoggedOnProvider	RegSz	{00E78E8B-EAD6-445C-9C7D-0B37F7E45C}	33-36-34-37-2D-34		
LastLoggedOnUser	RegSz	.\jerdal	39-04		
LastLoggedOnDisplay/Name	RegSz	Serdar Tarkan Altun	61-64-33-36		
SelectedUserSID	RegSz	S-1-5-21-2744121022-2643601262-147854	76-33-33-33-77-76		
LastLoggedOnUserSID	RegSz	S-1-5-21-2744121022-2643601262-147854	84-03-60-E8-64-03		

VolumeInfoCache dosyası altında disk bölümlerini görmekteyiz.

The screenshot shows the Windows Registry Editor. The left pane displays the tree structure with 'VolumeInfoCache' selected under 'Microsoft\Windows\Search'. The right pane shows the 'VolumeInfoCache' registry value, which is a 'Binary' type. The 'Value' field is highlighted, and the 'Raw value' is '00-00-00-00'.

Timestamp	Drive Name	Volume Label
2023-05-18 20:46:24	C:	
2023-05-20 12:36:19	D:	
2023-12-14 14:36:44	E:	Yerdal Disk
2023-10-24 20:28:21	F:	SERIAL

Uninstall burada ise kaldırılan uygulamalar hakkında bilgi verilmektedir.

Registry Hives (3)Available bookmarks (970)

Order text to search...

Find

Key name

Control Panel

CurrentVersion

CurrentVersion

Windows Defender

Windows Defender

Devices

Image File Execution Options

Internet Explorer

LogonUI

NetworkCards

NetworkList

Products

UserData

ProfileList

Run

RunOnce

App Paths

Uninstall

StartMenu\Internet

System

System

TaskCache

Tracing

VolumetricCache

Windows Portable Devices

Winlogon

Tracing

Uninstall

ValuesUninstall

Drop a column header here to group by that column

Timestamp	Key Name	Display Name	Display Version	Publisher	Install Date	Install Source	Install Location	Uninstall String
2021-03-15 20:37:38	Dev-C++	Dev-C++	5.11	Bloodshed Software				C:\Program Files (x86)\Dev-Cpp\uninstall.exe
2019-12-07 09:17:27	DirectDrawEx							
2019-12-07 14:45:47	DWM_Runtime							
2019-12-07 09:17:27	FontCore							
2019-12-07 09:17:27	IE40							
2019-12-07 09:17:27	IE4Data							
2019-12-07 09:17:27	IE4Index							
2019-12-07 09:17:27	IE4Data							
2021-03-15 20:37:38	InstallShield Uninstall Information							
2021-03-15 20:37:38	Internet Download Manager	Internet Download Manager	6.38.1	Tonec Inc.				C:\Program Files (x86)\Internet Download Manager\Uninstall.exe
2021-03-15 20:37:38	KLiteCodecPack_9.1	K-Lite Codec Pack 9.2.0 (Full)	9.2.0		20191214		C:\Program Files (x86)\K-Lite Codec Pack\	"C:\Program Files (x86)\K-Lite Codec Pack\uninstall.exe"
2021-12-20 05:51:16	Microsoft Edge	Microsoft Edge	96.0.1094.62	Microsoft Corporation	20211220		C:\Program Files (x86)\Microsoft\Edge\Application	"C:\Program Files (x86)\Microsoft\Edge\Application\atom196.0.1094.62\update\msedge.exe" --channel=stable --system-level --verbose-logging
2021-12-12 14:03:00	Microsoft Edge Update	Microsoft Edge Update	1.3.153.55					
2021-03-15 20:37:38	Microsoft Help Viewer 2.2	Microsoft Help Viewer 2.2	2.2.23.107	Microsoft Corporation			C:\Program Files (x86)\Microsoft Help Viewer\2.2\	msedge.exe /A1372588A-33CA-37AC-9D75-7F605857C62
2019-12-07 09:17:27	MobileOptionPack							
2019-12-07 14:45:47	MPlayer2							
2021-04-28 07:25:53	OBS Studio	OBS Studio	26.1.1	OBS Project				C:\Program Files\obs-studio\uninstall.exe
2018-11-02 06:13:37	Shockwave							
Total items: 41								

WindowsPortableDevice dosya altında ise bağlanmış olan cihazlar hakkında bilgiler bulunmaktadır.

Registry Hives (3) Available bookmarks (970)		Values Windows Portable Devices				
Order text to search... Find		Drop a column header here to group by that column				
Key Name		Timestamp	Device	Serial Number	Guid	Friendly Name
Control Panel		2021-12-03 16:34:09	DISKVEN_GENERALPRD_LJEDISKREY_5.00	68353E367580A_B0	{53F56307-666F-12D0-94F2-0A0C91EFB8B}	GENERAL
CurrentVersion		2021-11-19 13:22:20	DISKVEN_GENERALPRD_FLASH_DISKREY_8.0	123A13F960	{53F56307-666F-12D0-94F2-0A0C91EFB8B}	ARP
CurrentVersion		2021-03-15 20:37:38	DISKVEN_GENERALPRD_FLASH_DISKREY_8.0	CAEA8B8C30	{53F56307-666F-12D0-94F2-0A0C91EFB8B}	SARSILMAZ
Windows Defender		2021-11-05 14:03:03	DISKVEN_KINGSTONPRD_DATA_TRAVELER_3.0	E0D580864701551C914427160	{53F56307-666F-12D0-94F2-0A0C91EFB8B}	KINGSTON
Windows Defender		2021-03-15 20:37:38	DISKVEN_SANDISKPRD_CRUIZER_BLACKREY_1.27	20042032113F8226E380	{53F56307-666F-12D0-94F2-0A0C91EFB8B}	OLG22
Image File Execution Options		2021-12-01 12:30:52	DISKVEN_SANDISKPRD_ULTRA_USB_2.0REY_1.00	0121498C4AFD14088B3F61049A91D8BAE1826E180CE912752C9144B	{53F56307-666F-12D0-94F2-0A0C91EFB8B}	E:\
Internet Explorer		2021-03-15 20:37:38	DISKVEN_S46PRD_USB_DISKREY_1100	5706F8B2Q9H4R9N6	{53F56307-666F-12D0-94F2-0A0C91EFB8B}	D:\
NetworkCards		2021-11-18 14:30:25	DISKVEN_S46PRD_USB_DISKREY_1100	6A8B48F940	{53F56307-666F-12D0-94F2-0A0C91EFB8B}	SERIAL
NetworkList		2021-11-12 09:53:18	DISKVEN_TOSHIBAPRD_TRANSMEMORYREY_1.00	8022CF48B8C34CFD0FED3360	{53F56307-666F-12D0-94F2-0A0C91EFB8B}	MONSTER
Products		2021-11-19 10:21:24	DISKVEN_TOSHIBAPRD_TRANSMEMORYREY_1.00	8838F93632C2810002140460	{53F56307-666F-12D0-94F2-0A0C91EFB8B}	ESD-USB
RunOnce		2021-10-24 09:47:53	DISKVEN_TOSHIBAPRD_TRANSMEMORYREY_1.00	C03FD9F7D8E38A316147960	{53F56307-666F-12D0-94F2-0A0C91EFB8B}	SERIAL
App Paths		2021-03-15 20:37:38	DISKVEN_USBPRD_FLASH_DISKREY_1100	6A1ACE45780	{53F56307-666F-12D0-94F2-0A0C91EFB8B}	D:\
Uninstall		2021-03-15 20:37:38	DISKVEN_USBPRD_FLASH_DISKREY_1100	890168104027C0DE100100F008C32A5802P03C0003F8C3040113A403	{53F56307-666F-12D0-94F2-0A0C91EFB8B}	ORTUĞRUL DOĞUN
StartMenu\Internet		2021-03-15 20:37:38				
System		2021-03-15 20:37:38				
System		2021-03-15 20:37:38				
TaskCache		2021-03-15 20:37:38				
Tracing		2021-03-15 20:37:38				
VolumetricCache		2021-03-15 20:37:38				
Windows Portable Devices						
Winlogon						
Tracing						
Uninstall						

Anlatacaklarım buraya kadardı. Umarım faydalı olabilmişimdir. Hatalarım konusunda benimle iletişime geçebilirsiniz. 😊

4. KAYNAKÇA

<http://www.blockcyforen.com/2021/01/windows-registry-nedir-windows.html>

<https://www.youtube.com/watch?v=xekpJkf2ItE>

<https://www.youtube.com/watch?v=VYROU-ZwZX8>