Windows Execution Artifacts: AmCache Analysis

Windows'un uygulamaların yürütülmesi ve uyumluluk durumunun takip edilmesi için oluşturulan bir veritabanıdır. Önceden yüklenen uygulamaların önbelleğe alınması, uygulama çalışma süresi, uygulama dosyalarının yerleri ve diğer bilgileri içerir. Bu bilgiler ise Windows'un uygulamaların hızlı başlatılmasını sağlamak ve uyumluluk sorunlarını tespit etmek için kullanılır.

Sistem üzerinde silinen programların kayıtları "Amcache.hve" dosyasında silinmemektedir. Bununla birlikte çalıştırılan ya da kullanılan uygulamalara dair kanıtlar sunulabilir.

"C:\Windows\AppCompat\Programs" dizininde bulunur. Amcache.hve dosyasının analizi, kötü amaçlı yazılımların tespiti, sistem aktivitelerinin analizi ve kullanıcı faaliyetlerinin belirlenmesi gibi amaçlarla kullanılabilir. Eric Zimmerman's araçlarından "AmcacheParser" kullanarak amcache.hve dosyası parse edildikten sonra analiz edilecektir.

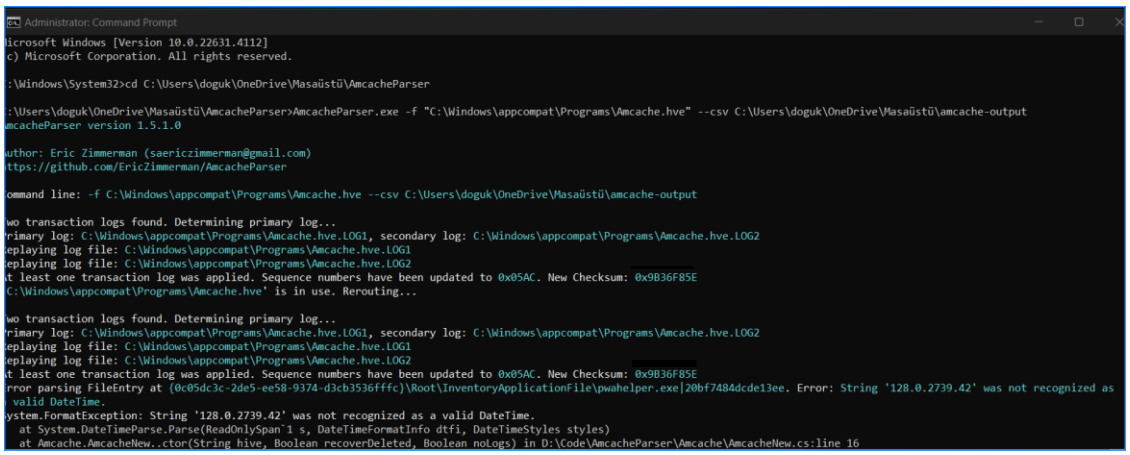


Figure 1 - Amcache Parser

Amcache çıktısının başarılı bir şekilde tamamlandığını ve amcache-output dosyasına kayıt edildiğinin çıktısı verilmiştir.

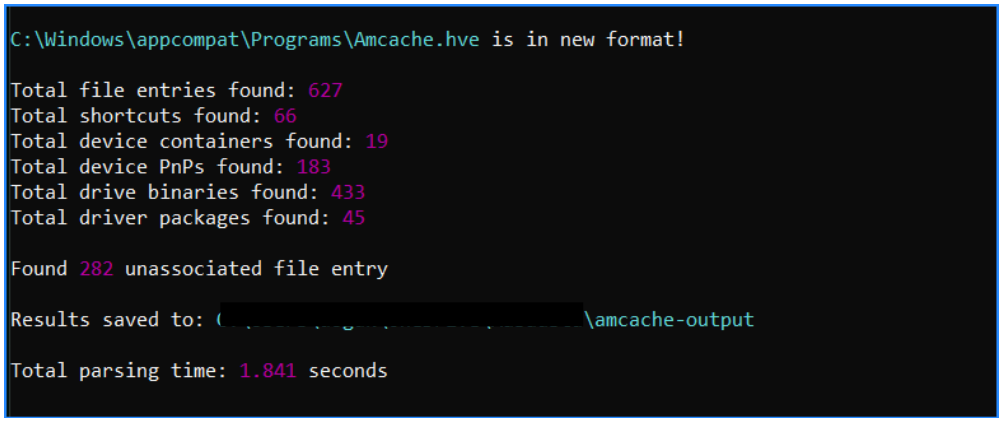
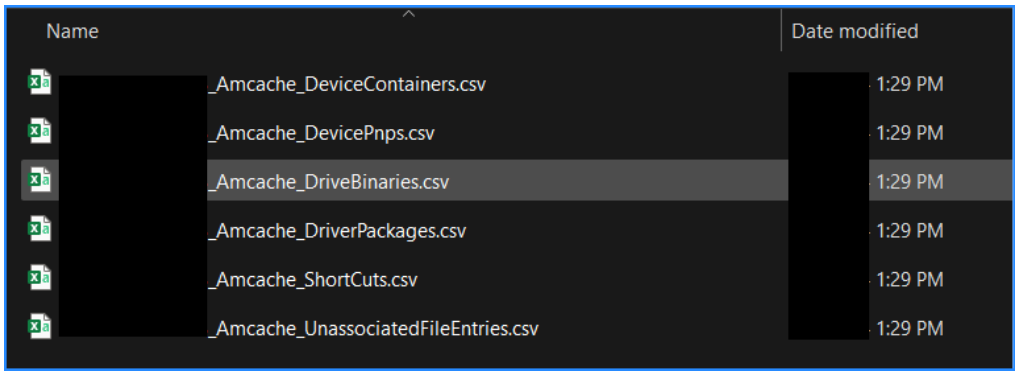


Figure 2 - Amcache Output



Output Files

Parse işlemi gerçekleştirildikten sonra 6 adet .csv dosyası oluşturulmuştur.

Name	Date modified
[redacted]_Amcache_DeviceContainers.csv	[redacted] 1:29 PM
_Amcache_DevicePnps.csv	1:29 PM
_Amcache_DriveBinaries.csv	1:29 PM
_Amcache_DriverPackages.csv	1:29 PM
_Amcache_ShortCuts.csv	1:29 PM
_Amcache_UnassociatedFileEntries.csv	1:29 PM

Figure 3 - .csv Files

1. Amcache_DeviceContainers.csv

Sisteme bağlı cihazlarla ilgili bilgi veren çıktı dosyasıdır.

KeyName	KeyLastWr	Categories	DiscoveryMethod	Fr	Icon	IsActive	IsConnect	IsMachine	IsNetwork	IsPaired	Manufacture	ModelId	Mode	ModelNumber	Prim	State
{[redacted]la-	########	printfax.printer.virtual		Oı	C:\Window	TRUE	TRUE	FALSE	FALSE	FALSE		[redacted]	[redacted]	[redacted]	print	9
{[redacted]06	########	storage			C:\Window	TRUE	FALSE	FALSE	FALSE	FALSE		{[redacted]	[redacted]	[redacted]	stora	8
{[redacted]ed	########	storage			C:\Window	TRUE	FALSE	FALSE	FALSE	FALSE		{[redacted]	[redacted]	[redacted]	stora	8
{[redacted]21	########	computer.notebook		D(	C:\Window	TRUE	TRUE	TRUE	FALSE	FALSE	[redacted]	[redacted]	[redacted]	[redacted]	comp	25
{[redacted]aa	########	storage			C:\Window	TRUE	FALSE	FALSE	FALSE	FALSE		{[redacted]	[redacted]	[redacted]	stora	8
{[redacted]52	########	storage			C:\Window	TRUE	FALSE	FALSE	FALSE	FALSE		{[redacted]	[redacted]	[redacted]	stora	8
{[redacted]7b	########	storage			C:\Window	TRUE	FALSE	FALSE	FALSE	FALSE		{[redacted]	[redacted]	[redacted]	stora	8
{[redacted]5-	########	audio,display.monitor		Ge	C:\Window	TRUE	TRUE	FALSE	FALSE	FALSE		{[redacted]	[redacted]	[redacted]	displ	9
{[redacted]73	########	audio.head	bluetooth	Dc	C:\Window	TRUE	FALSE	FALSE	FALSE	TRUE		{[redacted]	[redacted]	[redacted]a	audi	12
{[redacted]6f-	########	unknown		Ap	C:\Window	TRUE	FALSE	FALSE	FALSE	FALSE		[redacted]	[redacted]	[redacted]	unkn	8

Figure 4 - DeviceContainers

2. Amcache_DevicePnps.csv

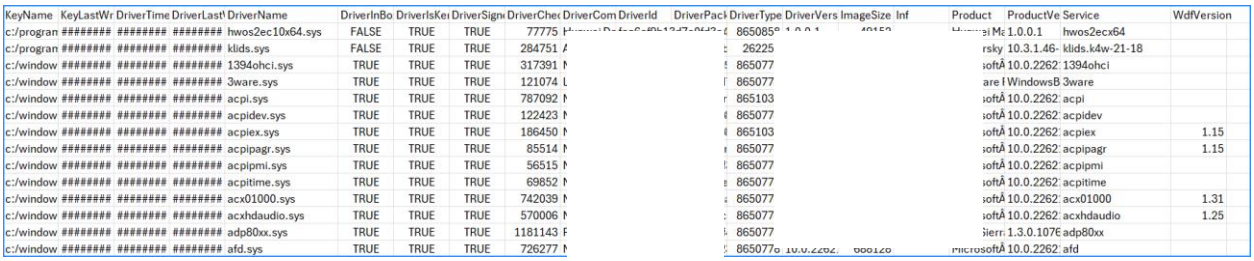
PnP, tak ve çalıştır anlamına gelir. Bir PnP donanımı taktığınızda, herhangi bir sürücü yüklemeye gerek kalmadan çalışmaya başlar. Bu dosya da tak çalıştır cihazları hakkında bilgileri içermektedir.

KeyName	KeyLastWr	BusReport	Class	ClassGuid	Compid	ContainerI	Descriptio	DriverId	DriverPack	DriverNam	DriverVerD	DriverVerV	Enumerato	HWID	Inf	InstallState	Manufactu	MatchingId	Model	ParentId	ProblemCo	Provider
acpi/acpi0	########		battery	{[redacted]	[redacted]11d(	{27db0821	Microsoft /	00007fc73	cmbatt.inf	cmbatt.sys	########	[redacted]	acpi	acpi\ven_a	cmbatt.inf	0	Microsoft	[redacted]	[redacted]	[redacted]i_hal\p	0	Microsof
acpi/acpi0	########		system	{[redacted]	[redacted]11ce	{27db0821	ACPI Proce	0000a927	acpipagr.ir	acpipagr.s	########	10[redacted]	acpi	acpi\ven_a	acpipagr.ir	0	(Standard s	[redacted]	[redacted]	[redacted]i_hal\p	0	Microsof
acpi/essx8	########		media	{[redacted]	[redacted]en_e	{27db0821	Audio Devi	0000ad97	esaudriver	esaudriver	########	20[redacted]	acpi	acpi\ven_e	oem18.inf	0	Audio Devi	a[redacted]	[redacted]	[redacted]\ven_80	0	Everest S
acpi/fixedb	########		system	{[redacted]	[redacted]11ce	{27db0821	ACPI Fixed Feature Bu		machine.inf_amd64_7		########	10[redacted]	acpi	acpi\fixedb	machine.ir	0	(Standard s	a[redacted]	[redacted]	[redacted]i_hal\p	0	Microsof
acpi/genui	########		processor	{[redacted]	[redacted]roce	{27db0821	11th Gen Ir	0000e5e13	cpu.inf_an	intelppm.s	########	10[redacted]	acpi	acpi\genui	cpu.inf	0	Intel	a[redacted]	[redacted]	[redacted]i_hal\p	0	Microsof
acpi/genui	########		processor	{[redacted]	[redacted]roce	{27db0821	11th Gen Ir	0000e5e13	cpu.inf_an	intelppm.s	########	10[redacted]	acpi	acpi\genui	cpu.inf	0	Intel	a[redacted]	[redacted]	[redacted]i_hal\p	0	Microsof
acpi/genui	########		processor	{[redacted]	[redacted]roce	{27db0821	11th Gen Ir	0000e5e13	cpu.inf_an	intelppm.s	########	10[redacted]	acpi	acpi\genui	cpu.inf	0	Intel	a[redacted]	[redacted]	[redacted]i_hal\p	0	Microsof
acpi/genui	########		processor	{[redacted]	[redacted]roce	{27db0821	11th Gen Ir	0000e5e13	cpu.inf_an	intelppm.s	########	10[redacted]	acpi	acpi\genui	cpu.inf	0	Intel	a[redacted]	[redacted]	[redacted]i_hal\p	0	Microsof
acpi/genui	########		processor	{[redacted]	[redacted]roce	{27db0821	11th Gen Ir	0000e5e13	cpu.inf_an	intelppm.s	########	10[redacted]	acpi	acpi\genui	cpu.inf	0	Intel	a[redacted]	[redacted]	[redacted]i_hal\p	0	Microsof
acpi/genui	########		processor	{[redacted]	[redacted]roce	{27db0821	11th Gen Ir	0000e5e13	cpu.inf_an	intelppm.s	########	10[redacted]	acpi	acpi\genui	cpu.inf	0	Intel	a[redacted]	[redacted]	[redacted]i_hal\p	0	Microsof
acpi/genui	########		processor	{[redacted]	[redacted]roce	{27db0821	11th Gen Ir	0000e5e13	cpu.inf_an	intelppm.s	########	10[redacted]	acpi	acpi\genui	cpu.inf	0	Intel	a[redacted]	[redacted]	[redacted]i_hal\p	0	Microsof
acpi/genui	########		processor	{[redacted]	[redacted]roce	{27db0821	11th Gen Ir	0000e5e13	cpu.inf_an	intelppm.s	########	10[redacted]	acpi	acpi\genui	cpu.inf	0	Intel	a[redacted]	[redacted]	[redacted]i_hal\p	0	Microsof
acpi/gxtp7	########		hidclass	{[redacted]	[redacted]np0	{27db0821	I2C HID De	000078da	hidi2c.inf_	hidi2c.sys	########	10[redacted]	acpi	acpi\ven_g	hidi2c.inf	0	Microsoft	a[redacted]	[redacted]	[redacted]\ven_80	0	Microsof
acpi/hwsp	########		system	[redacted]	[redacted]	{27db0821	Huawei Mı	00005326	multipadri	multipadri	########	2.2.2.22	acpi	acpi\ven_h	oem8.inf	0	Huawei Te	[redacted]	[redacted]	pci\ven_80	0	Huawei T

Figure 5 - DevicePnps

3. Amcache_DriveBinaries.csv

Sistem dosyaları hakkında bilgiler yer almaktadır. İmza tarihlerinin verisini tutmaktadır.

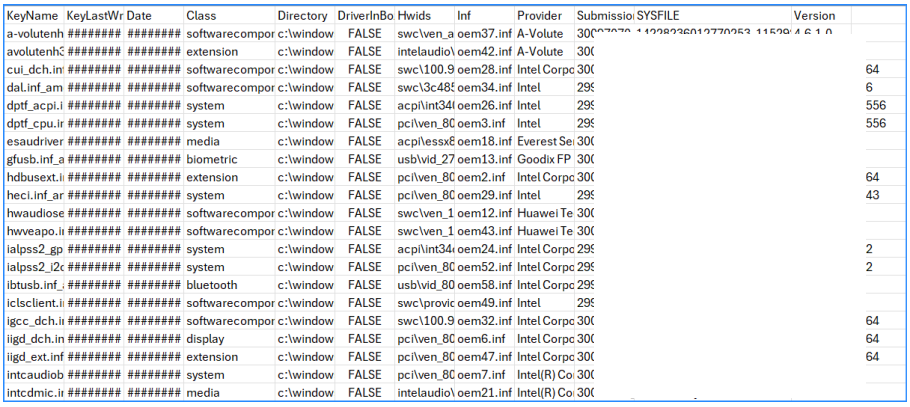


KeyName	KeyLastWr	DriverTime	DriverLast	DriverName	DriverInBo	DriverIsKe	DriverSign	DriverChe	DriverCom	DriverId	DriverPack	DriverType	DriverVers	ImageSize	Inf	Product	ProductVe	Service	WdfVersion
c:/progran	########	########	########	hwos2ec10x64.sys	FALSE	TRUE	TRUE	77775				865085					1.0.0.1	hwos2ecx64	
c:/progran	########	########	########	klids.sys	FALSE	TRUE	TRUE	284751				26225				rsky	10.3.1.46-	klids.k4w-21-18	
c:/window	########	########	########	1394ohci.sys	TRUE	TRUE	TRUE	317391				865077				oftÂ	10.0.2262	1394ohci	
c:/window	########	########	########	3ware.sys	TRUE	TRUE	TRUE	121074				865077				are I	WindowsB	3ware	
c:/window	########	########	########	acpi.sys	TRUE	TRUE	TRUE	787092				865103				oftÂ	10.0.2262	acpi	
c:/window	########	########	########	acpidev.sys	TRUE	TRUE	TRUE	122423				865077				oftÂ	10.0.2262	acpidev	
c:/window	########	########	########	acpiex.sys	TRUE	TRUE	TRUE	186450				865103				oftÂ	10.0.2262	acpiex	1.15
c:/window	########	########	########	acpipagr.sys	TRUE	TRUE	TRUE	85514				865077				oftÂ	10.0.2262	acpipagr	1.15
c:/window	########	########	########	acpipmi.sys	TRUE	TRUE	TRUE	56515				865077				oftÂ	10.0.2262	acpipmi	
c:/window	########	########	########	acpitime.sys	TRUE	TRUE	TRUE	69852				865077				oftÂ	10.0.2262	acpitime	
c:/window	########	########	########	acx01000.sys	TRUE	TRUE	TRUE	742039				865077				oftÂ	10.0.2262	acx01000	1.31
c:/window	########	########	########	acxhdaudio.sys	TRUE	TRUE	TRUE	570006				865077				oftÂ	10.0.2262	acxhdaudio	1.25
c:/window	########	########	########	adp80xx.sys	TRUE	TRUE	TRUE	1181143				865077				ierr	1.3.0.1076	adp80xx	
c:/window	########	########	########	afd.sys	TRUE	TRUE	TRUE	726277				865077				MicrosoftÂ	10.0.2262	afd	

Figure 6 - DriveBinaries

4. Amcache_DriverPackages.csv

Sistemdeki drive paketleri hakkında bilgi vermektedir.

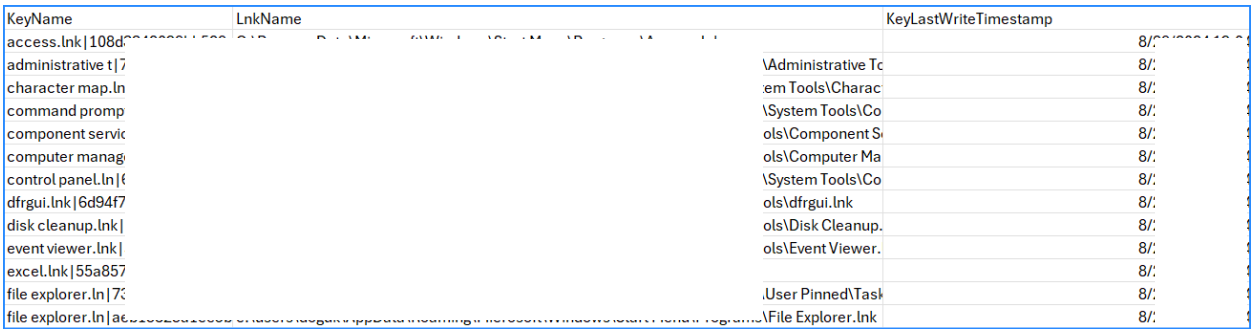


KeyName	KeyLastWr	Date	Class	Directory	DriverInBo	Hwids	Inf	Provider	Submissio	SYSFILE	Version	
a-volutenh	########	########	softwarecompor	c:\window	FALSE	swc\ven_a	oem37.inf	A-Volute	30			
avolutenh	########	########	extension	c:\window	FALSE	intelaudio\	oem42.inf	A-Volute	30			
cui_dch.in	########	########	softwarecompor	c:\window	FALSE	swc\100.9	oem28.inf	Intel Corpc	30			64
dal.inf_am	########	########	softwarecompor	c:\window	FALSE	swc\3c485	oem34.inf	Intel	29			6
dptf_acpi.i	########	########	system	c:\window	FALSE	acpi\int340	oem26.inf	Intel	29			556
dptf_cpu.ir	########	########	system	c:\window	FALSE	pci\ven_80	oem3.inf	Intel	29			556
esaudriver	########	########	media	c:\window	FALSE	acpi\essx8	oem18.inf	Everest Se	30			
gfusb.inf_a	########	########	biometric	c:\window	FALSE	usb\vid_27	oem13.inf	Goodix FP	30			
hdbusext.i	########	########	extension	c:\window	FALSE	pci\ven_80	oem2.inf	Intel Corpc	30			64
heci.inf_ar	########	########	system	c:\window	FALSE	pci\ven_80	oem29.inf	Intel	29			43
hwaudiose	########	########	softwarecompor	c:\window	FALSE	swc\ven_1	oem12.inf	Huawei Te	30			
hwveapo.i	########	########	softwarecompor	c:\window	FALSE	swc\ven_1	oem43.inf	Huawei Te	30			
ialpss2_gp	########	########	system	c:\window	FALSE	acpi\int34	oem24.inf	Intel Corpc	29			2
ialpss2_i2	########	########	system	c:\window	FALSE	pci\ven_80	oem52.inf	Intel Corpc	29			2
ibtusb.inf_	########	########	bluetooth	c:\window	FALSE	usb\vid_80	oem58.inf	Intel Corpc	29			
iclsclient.i	########	########	softwarecompor	c:\window	FALSE	swc\provic	oem49.inf	Intel	29			
igcc_dch.i	########	########	softwarecompor	c:\window	FALSE	swc\100.9	oem32.inf	Intel Corpc	30			64
iigd_dch.in	########	########	display	c:\window	FALSE	pci\ven_80	oem6.inf	Intel Corpc	30			64
iigd_ext.inf	########	########	extension	c:\window	FALSE	pci\ven_80	oem47.inf	Intel Corpc	30			64
intcaudiob	########	########	system	c:\window	FALSE	pci\ven_80	oem7.inf	Intel(R) Co	30			
intcdmic.i	########	########	media	c:\window	FALSE	intelaudio\	oem21.inf	Intel(R) Co	30			

Figure 7 - DriverPackages

5. Amcache_ShortCuts.csv

Uygulamaların çalıştırma kısayollarını ve bilgilerini göstermektedir.

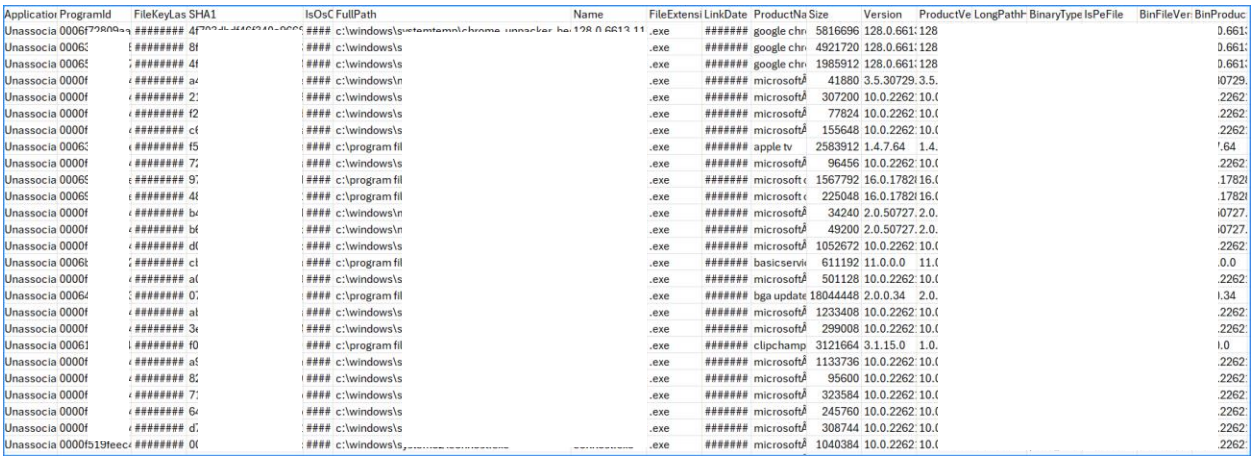


KeyName	LnkName		KeyLastWriteTimestamp
access.lnk|108d			8/
administrative t|7		\Administrative To	8/
character map.ln		em Tools\Charac	8/
command promp		\System Tools\Co	8/
component servic		ols\Component S	8/
computer manag		ols\Computer Ma	8/
control panel.ln|{		\System Tools\Co	8/
dfrgui.lnk|6d94f7		ols\dfrgui.lnk	8/
disk cleanup.lnk|		ols\Disk Cleanup.	8/
event viewer.lnk|		ols\Event Viewer.	8/
excel.lnk|55a857			8/
file explorer.ln|7		.User Pinned\Task	8/
file explorer.ln|ae		\File Explorer.lnk	8/

Figure 8 - Shortcuts

6. Amcache_UnassociatedFileEntries.csv

Bu dosya çalıştırılan uygulamaların bilgilerini tutmaktadır. Bu dosya ile sistemde zararlı bir yazılım çalışması durumunda incelenebilir.



Applicatior	ProgramId	FileKeyLas	SHA1	IsOsC	FullPath	Name	FileExtensi	LinkDate	ProductNa	Size	Version	ProductVe	LongPathF	BinaryType	IsPeFile	BinFileVer	BinProduc
Unassocia	0006f72809aa	########	4f7	####	c:\windows\systemtemp\chrome_unpacker_be	128.0.6613.11	.exe	#######	google chr	5816696	128.0.661	128					0.661
Unassocia	0006	########	8f	####	c:\windows\s		.exe	#######	google chr	4921720	128.0.661	128					0.661
Unassocia	0006	########	4f	####	c:\windows\s		.exe	#######	google chr	1985912	128.0.661	128					0.661
Unassocia	0000f	########	ac	####	c:\windows\n		.exe	#######	microsoftÂ	41880	3.5.30729.	3.5.					10729.
Unassocia	0000f	########	2	####	c:\windows\s		.exe	#######	microsoftÂ	307200	10.0.2262	10.(					.2262
Unassocia	0000f	########	f2	####	c:\windows\s		.exe	#######	microsoftÂ	77824	10.0.2262	10.(					.2262
Unassocia	0000f	########	c6	####	c:\windows\s		.exe	#######	microsoftÂ	155648	10.0.2262	10.(					.2262
Unassocia	00063	########	f5	####	c:\program fil		.exe	#######	apple tv	2583912	1.4.7.64	1.4.					'.64
Unassocia	0000f	########	7	####	c:\windows\s		.exe	#######	microsoftÂ	96456	10.0.2262	10.(					.2262
Unassocia	00069	########	97	####	c:\program fil		.exe	#######	microsoft (	1567792	16.0.1782	16.(					.1782
Unassocia	00069	########	48	####	c:\program fil		.exe	#######	microsoft (	225048	16.0.1782	16.(					.1782
Unassocia	0000f	########	b4	####	c:\windows\n		.exe	#######	microsoftÂ	34240	2.0.50727.	2.0.					i0727.
Unassocia	0000f	########	b6	####	c:\windows\n		.exe	#######	microsoftÂ	49200	2.0.50727.	2.0.					i0727.
Unassocia	0000f	########	d0	####	c:\windows\s		.exe	#######	microsoftÂ	1052672	10.0.2262	10.(					.2262
Unassocia	0006t	########	c1	####	c:\program fil		.exe	#######	basicservi	611192	11.0.0.0	11.(					.0.0
Unassocia	0000f	########	a0	####	c:\windows\s		.exe	#######	microsoftÂ	501128	10.0.2262	10.(					.2262
Unassocia	00064	########	07	####	c:\program fil		.exe	#######	bga update	18044448	2.0.0.34	2.0.					l.34
Unassocia	0000f	########	ab	####	c:\windows\s		.exe	#######	microsoftÂ	1233408	10.0.2262	10.(					.2262
Unassocia	0000f	########	3e	####	c:\windows\s		.exe	#######	microsoftÂ	299008	10.0.2262	10.(					.2262
Unassocia	00061	########	f0	####	c:\program fil		.exe	#######	clipchamp	3121664	3.1.15.0	1.0.					l.0
Unassocia	0000f	########	a5	####	c:\windows\s		.exe	#######	microsoftÂ	1133736	10.0.2262	10.(					.2262
Unassocia	0000f	########	82	####	c:\windows\s		.exe	#######	microsoftÂ	95600	10.0.2262	10.(					.2262
Unassocia	0000f	########	7	####	c:\windows\s		.exe	#######	microsoftÂ	323584	10.0.2262	10.(					.2262
Unassocia	0000f	########	64	####	c:\windows\s		.exe	#######	microsoftÂ	245760	10.0.2262	10.(					.2262
Unassocia	0000f	########	d7	####	c:\windows\s		.exe	#######	microsoftÂ	308744	10.0.2262	10.(					.2262
Unassocia	0000f519feec	########	0(	####	c:\windows\s		.exe	#######	microsoftÂ	1040384	10.0.2262	10.(					.2262

Figure 9 – UnassociatedFileEntries