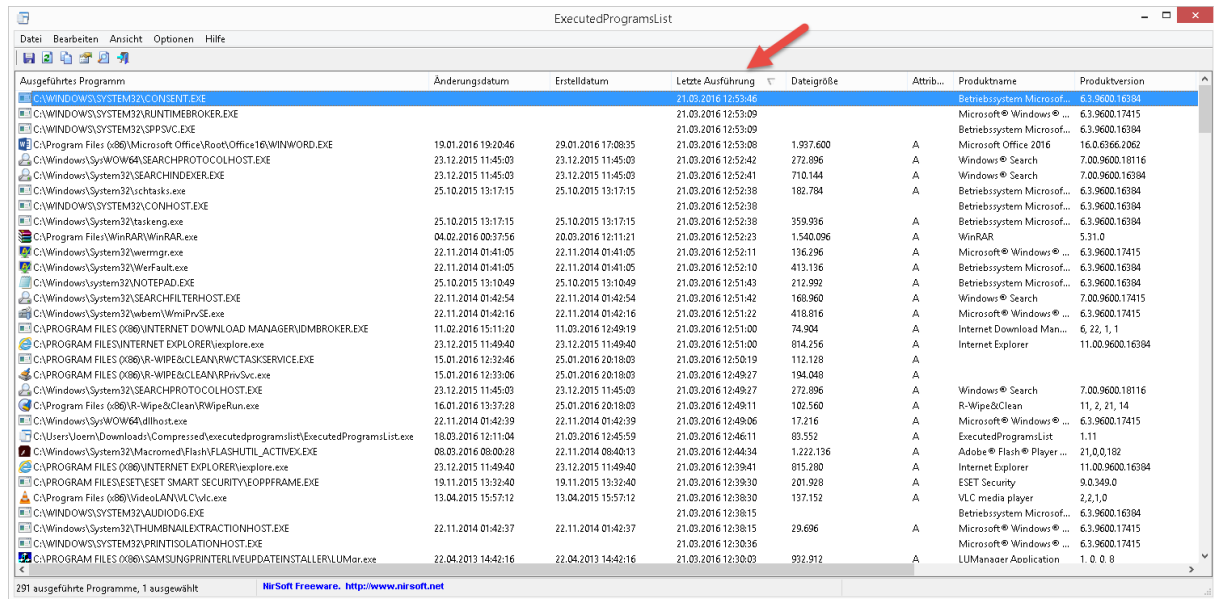


## Windows zuletzt ausgeführten Programme enttarnen

Zur Lösung eines Problems ist es oftmals wichtig zu wissen, welche Programme oder Installationsroutinen zuletzt aufgerufen wurden.

Mit dem Tool **ExecutedProgramsList** von **nirsoft** sind wir nur einen Klick davon entfernt dieses heraus zu finden.

Nach dem Start des Programms werden die zuletzt geöffneten Programme sauber nach Änderungsdatum, Erstelldatum und Letzte Ausführung inkl. dem Pfad und weiteren Details aufgelistet. Hierbei handelt es sich um ausgelesene Einträge verschiedener lokaler Systemquellen.

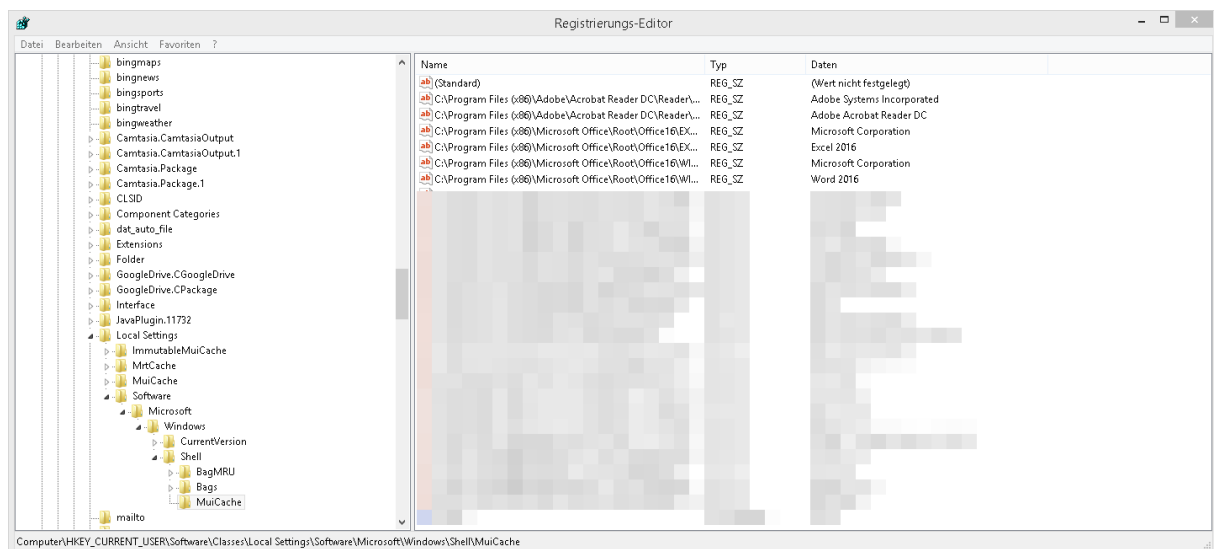


Ausgeführtes Programm	Änderungsdatum	Erstelldatum	Letzte Ausführung	Dateigröße	Attrib...	Produktname	Produktversion
C:\WINDOWS\SYSTEM32\CONSENT.EXE			21.03.2016 12:53:46			Betriebssystem Microsoft...	6.3.9600.16394
C:\WINDOWS\SYSTEM32\RUNTIMEBROKER.EXE			21.03.2016 12:53:09			Microsoft® Windows® ...	6.3.9600.17415
C:\WINDOWS\SYSTEM32\SPPSVC.EXE			21.03.2016 12:53:09			Betriebssystem Microsoft...	6.3.9600.16394
C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE	19.01.2016 19:20:46	29.01.2016 17:08:35	21.03.2016 12:53:08	1.937.600	A	Microsoft Office 2016	16.0.6366.2062
C:\Windows\System32\SEARCHPROTOCOLHOST.EXE	23.12.2015 11:45:03	23.12.2015 11:45:03	21.03.2016 12:52:42	272.896	A	Windows® Search	7.00.9600.18116
C:\Windows\System32\SEARCHINDEXER.EXE	23.12.2015 11:45:03	23.12.2015 11:45:03	21.03.2016 12:52:41	710.144	A	Windows® Search	7.00.9600.16394
C:\Windows\System32\SearchTasks.exe	25.10.2015 13:17:15	25.10.2015 13:17:15	21.03.2016 12:52:38	182.784	A	Betriebssystem Microsoft...	6.3.9600.16394
C:\WINDOWS\SYSTEM32\CONHOST.EXE			21.03.2016 12:52:38			Betriebssystem Microsoft...	6.3.9600.16394
C:\Windows\System32\Taskeng.exe	25.10.2015 13:17:15	25.10.2015 13:17:15	21.03.2016 12:52:38	359.936	A	Betriebssystem Microsoft...	6.3.9600.16394
C:\Program Files\WinRAR\WinRAR.exe	04.02.2016 00:37:56	20.03.2016 12:11:21	21.03.2016 12:52:23	1.540.096	A	WinRAR	5.31.0
C:\Windows\System32\vermgr.exe	22.11.2014 01:41:05	22.11.2014 01:41:05	21.03.2016 12:52:11	136.296	A	Microsoft® Windows® ...	6.3.9600.17415
C:\Windows\System32\WerFault.exe	22.11.2014 01:41:05	22.11.2014 01:41:05	21.03.2016 12:52:10	413.136	A	Betriebssystem Microsoft...	6.3.9600.16394
C:\Windows\System32\notepad.exe	25.10.2015 13:10:49	25.10.2015 13:10:49	21.03.2016 12:51:43	212.992	A	Betriebssystem Microsoft...	6.3.9600.16394
C:\Windows\System32\SearchFilterHost.exe	22.11.2014 01:42:54	22.11.2014 01:42:54	21.03.2016 12:51:42	160.960	A	Windows® Search	7.00.9600.17415
C:\Windows\System32\WmiPrivSE.exe	22.11.2014 01:42:16	22.11.2014 01:42:16	21.03.2016 12:51:22	418.816	A	Microsoft® Windows® ...	6.3.9600.17415
C:\PROGRAM FILES (X86)\INTERNET DOWNLOAD MANAGER\IDMBROKER.EXE	11.02.2016 15:11:20	11.03.2016 12:49:19	21.03.2016 12:51:00	74.904	A	Internet Download Man...	6.22.1.1
C:\PROGRAM FILES\INTERNET EXPLORER\explore.exe	23.12.2015 11:49:40	23.12.2015 11:49:40	21.03.2016 12:51:00	814.256	A	Internet Explorer	11.00.9600.16394
C:\PROGRAM FILES (X86)\R-WIPE&CLEAN\RWCTASKSERVICE.EXE	15.01.2016 12:32:46	25.01.2016 20:18:03	21.03.2016 12:50:19	112.128	A		
C:\PROGRAM FILES (X86)\R-WIPE&CLEAN\RWPrivSvc.exe	15.01.2016 12:32:06	25.01.2016 20:18:03	21.03.2016 12:49:27	194.048	A		
C:\Windows\System32\SEARCHPROTOCOLHOST.EXE	23.12.2015 11:45:03	23.12.2015 11:45:03	21.03.2016 12:49:27	272.896	A	Windows® Search	7.00.9600.18116
C:\Program Files (x86)\R-Wipe&Clean\RWipeRun.exe	16.01.2016 13:37:28	25.01.2016 20:18:03	21.03.2016 12:49:11	102.560	A	R-Wipe&Clean	11.2.21.14
C:\Windows\System32\WOW64\DllHost.exe	22.11.2014 01:42:39	22.11.2014 01:42:39	21.03.2016 12:49:06	17.216	A	Microsoft® Windows® ...	6.3.9600.17415
C:\Users\loerni\Downloads\Compressed\executedprogramslist\ExecutedProgramsList.exe	18.03.2016 13:11:04	21.03.2016 13:45:59	21.03.2016 12:46:11	83.352	A	ExecutedProgramsList	1.11
C:\Windows\System32\Flash\FLASHUTIL_ACTIVEVEX.EXE	08.03.2016 08:00:28	22.11.2014 08:40:13	21.03.2016 12:44:34	1.222.136	A	Adobe® Flash® Player ...	21.0.0.182
C:\PROGRAM FILES (X86)\INTERNET EXPLORER\iepl.exe	23.12.2015 11:49:40	23.12.2015 11:49:40	21.03.2016 12:39:41	815.280	A	Internet Explorer	11.00.9600.16394
C:\PROGRAM FILES\ESSET\SET SMART SECURITY\EOPFRAME.EXE	19.11.2015 13:32:40	19.11.2015 13:32:40	21.03.2016 12:39:30	201.928	A	ESET Security	9.0.349.0
C:\Program Files (x86)\VideoLAN\VLNCVidC.exe	13.04.2015 15:57:12	13.04.2015 15:57:12	21.03.2016 12:38:30	137.152	A	VLC media player	2.2.1.0
C:\WINDOWS\SYSTEM32\AUDIOODG.EXE			21.03.2016 12:38:15			Betriebssystem Microsoft...	6.3.9600.16394
C:\Windows\System32\HUMBNAL\EXTRACTIONHOST.EXE	22.11.2014 01:42:37	22.11.2014 01:42:37	21.03.2016 12:38:15	29.696	A	Microsoft® Windows® ...	6.3.9600.17415
C:\WINDOWS\SYSTEM32\PRINTINSTALLATIONHOST.EXE			21.03.2016 12:30:36			Microsoft® Windows® ...	6.3.9600.17415
C:\PROGRAM FILES (X86)\SAM\SUNJUNTPRINTERLIVEUPDATE\INSTALLER\LUMar.exe	22.04.2013 14:42:16	22.04.2013 14:42:16	21.03.2016 12:30:03	932.912	A	LUManager Application	1.0.0.8

Aber wie wird man diese Liste an Einträgen wieder los bzw. wie leert man diese?

Kein Problem, diese Daten finden wir z.B. in der Registry unter folgenden Pfad:

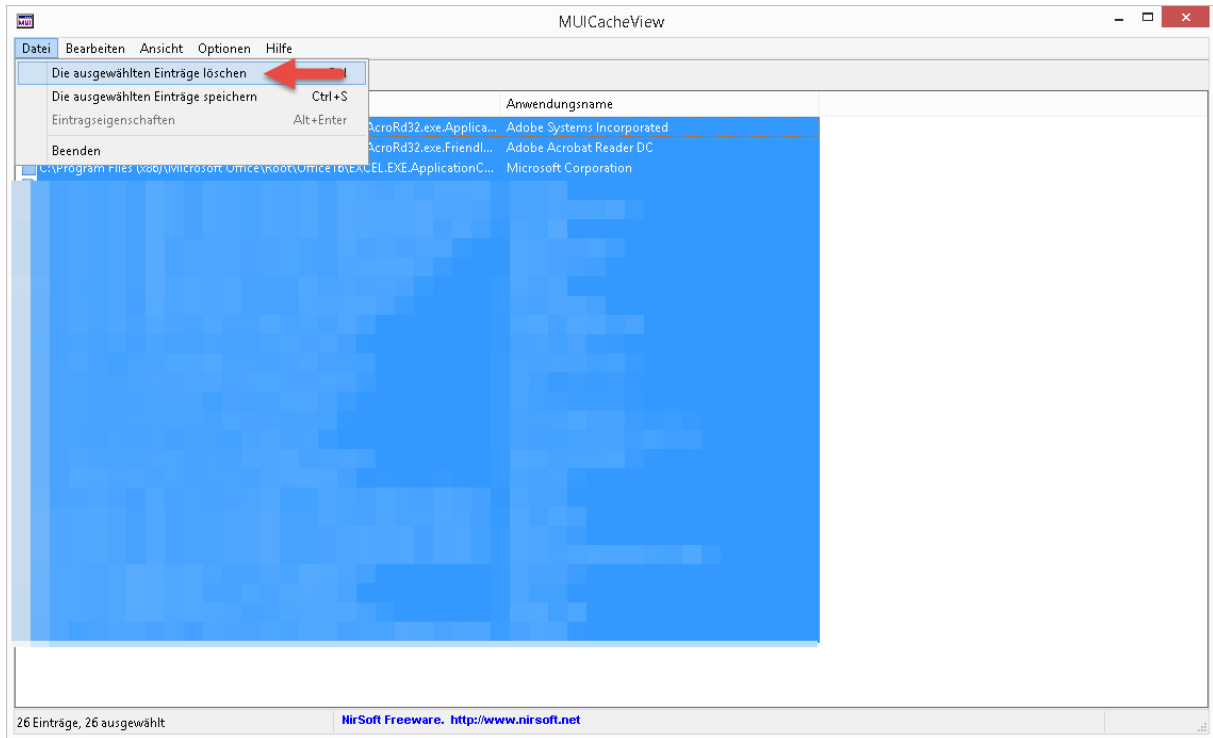
**HKEY\_CURRENT\_USER\Software\Classes\LocalSettings\Software\Microsoft\Windows\Shell\MuiCache**



Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\...	REG_SZ	Adobe Systems Incorporated
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\...	REG_SZ	Adobe Acrobat Reader DC
C:\Program Files (x86)\Microsoft Office\Root\Office16\EX...	REG_SZ	Microsoft Corporation
C:\Program Files (x86)\Microsoft Office\Root\Office16\EX...	REG_SZ	Excel 2016
C:\Program Files (x86)\Microsoft Office\Root\Office16\WIL...	REG_SZ	Microsoft Corporation
C:\Program Files (x86)\Microsoft Office\Root\Office16\WIL...	REG_SZ	Word 2016

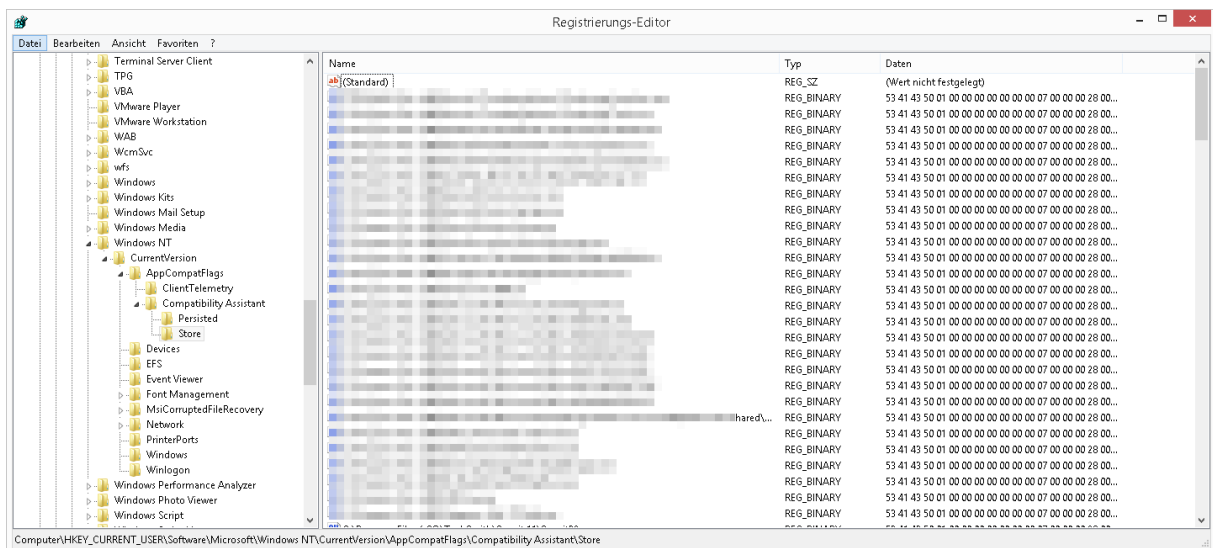
## Windows zuletzt ausgeführten Programme enttarnen

Mit dem Tool **MUICacheView** von **nirsoft** können wir genau diese oben gezeigten Einträge aus der Registry löschen.



Der nächste sehr informative Pfad wäre:

**HKEY\_CURRENT\_USER\Software\Microsoft\Windows  
NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store**

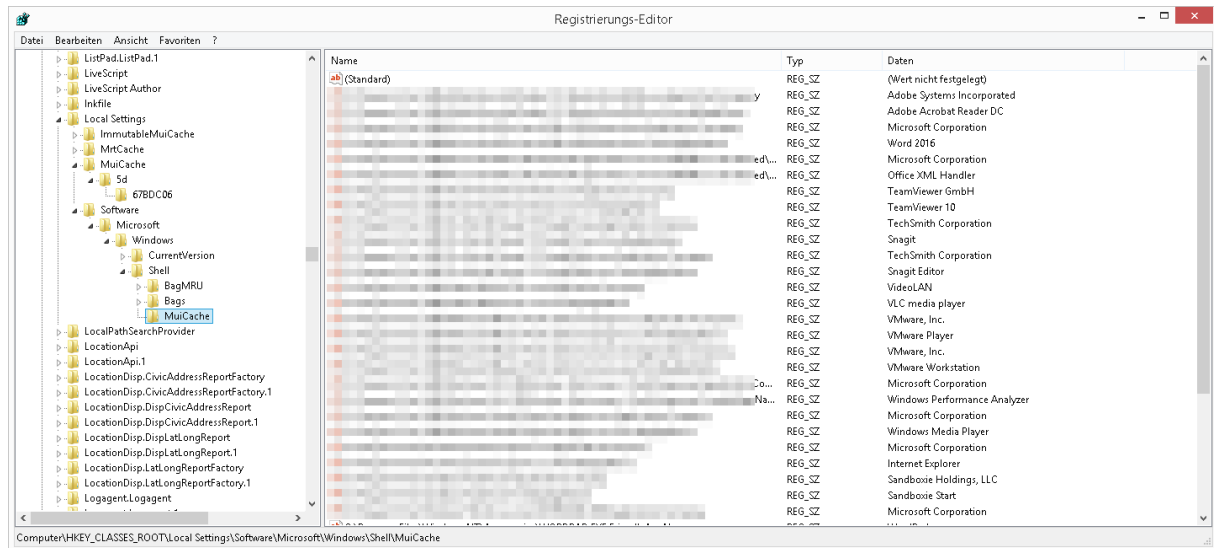


Der REG-Schlüssel **Store** kann ohne Probleme samt Inhalt gelöscht werden.

## Windows zuletzt ausgeführten Programme enttarnen

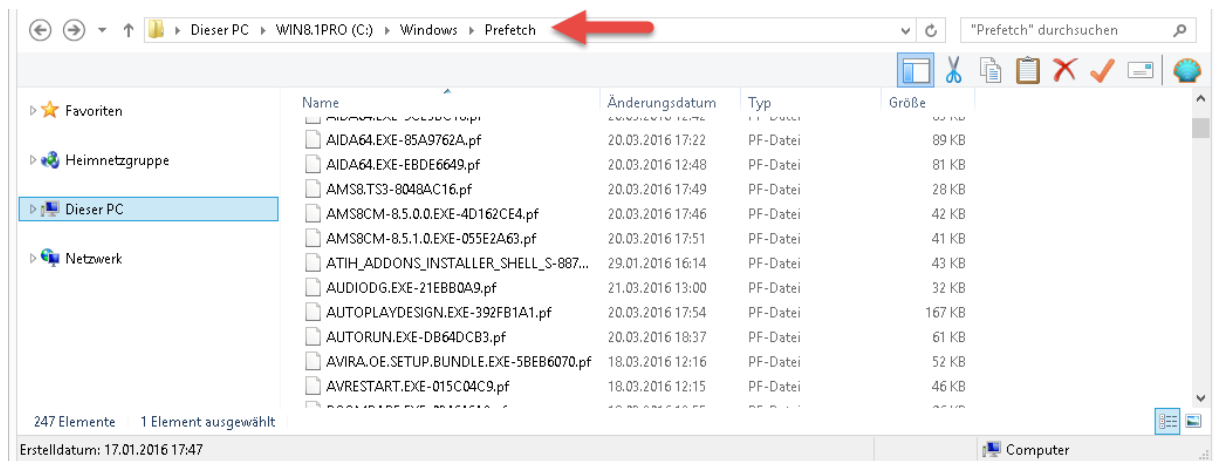
Dann haben wir noch den Pfad:

**HKEY\_CLASSES\_ROOT\Local Settings\Software\Microsoft\Windows\Shell\MuiCache**



Der REG-Schlüssel **MuiCache** kann ohne Probleme geleert werden.

Ein weiterer nennenswerter Ordner wäre **C:\Windows\Prefetch**



Wir sehen, dass alle Aktivitäten geloggt werden und an den verschiedensten Orten gespeichert werden.

**So sieht der Scan nach einer erfolgten Bereinigung aus. Im direkten Vergleich zu oben...**

