WebCache01.dat

From examination, it seems the visited pages and other information is written in one or more V01xxxxYY.log files in the

C:\Users\%user%\AppData\Local\Microsoft\Windows\WebCache

folder, and the WebCache01.dat is updated after the PC reboots.

Having typed a few urls in Edge's address bar (pointing to both local and external sites), an examination of the TypedURL's key in 'UsrClass.dat'

Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\TypedURLs

Shows the list of typed urls:

url1 http://192.168.1.2/jsonlz4/scrounger.html
url2 http://192.168.1.2/sv2hui.html
url3 http://10.0.0.2/sv2hui.htm
url4 http://10.0.0.2/sv2hui.html
url5 http://www.google.com/
etc ..

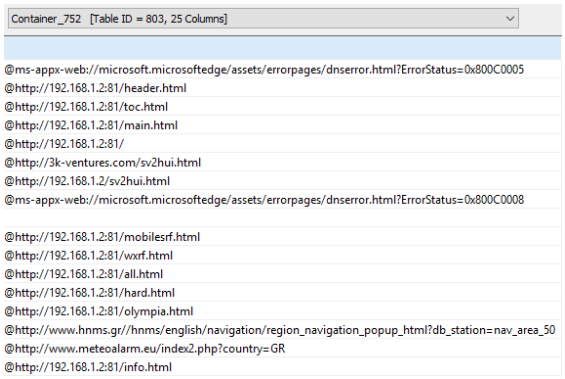
I also copy pasted a website url from Mozilla Firefox for this test.

Examining the containers of WebCache01.dat with ESEDatabaseView, in my test machine I have:

ID 4 for Edge/IE5
ID 727 for Edge/AC
ID 728 for Edge/AC#001
ID 756 for Edge/AC#002
ID 1247 for Edge/AC#005
ID 1524 for Edge/AC#006
ID 752 for Edge/AC#121

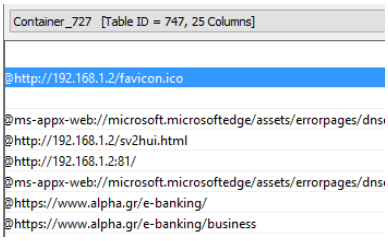
The above typed local urls, as well the url of favicon.ico of the visited local page appear in Container_727 which is the General Edge AC container.

The local urls (192… and 10…) typed, and any subsequent links followed from these local pages, appear in detail in Container_752 which corresponds to local storage AC#!121:

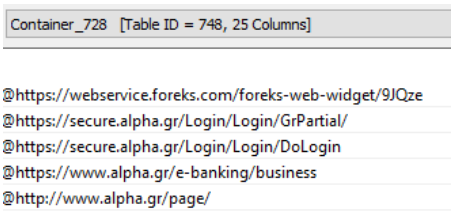


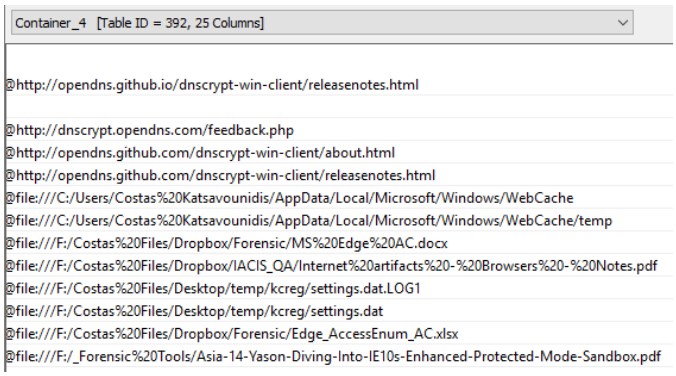
Any internet (web) and intranet (local) sites accessed appeared in Container_727 which corresponds to the General Edge AC container. The internet accessed sites also appear in Container_728, which corresponds to local storage AC#!001.

Container 727



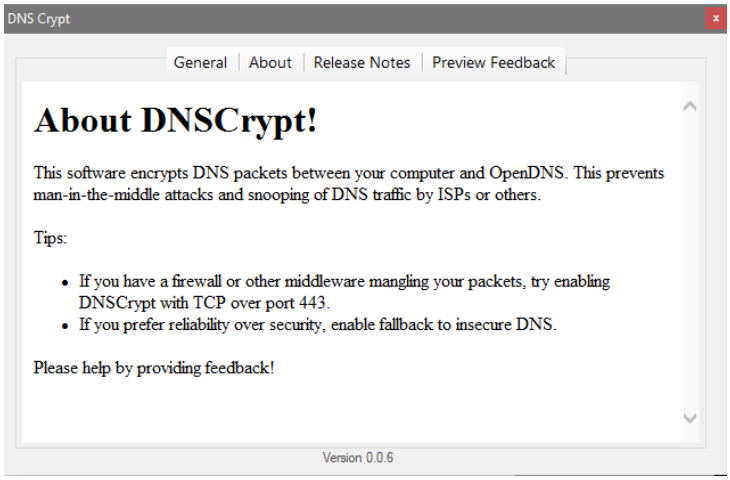
and 728



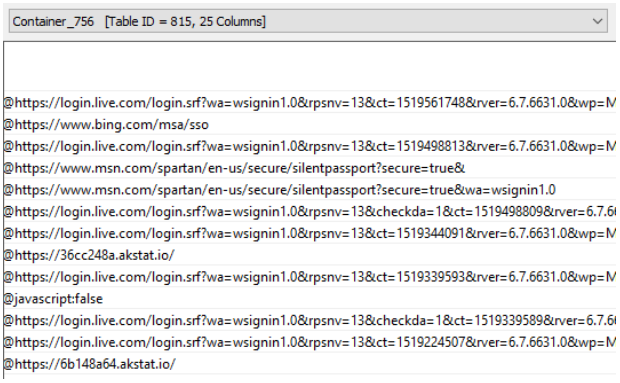


The IE5 (ContainerID_4) seems to list various local files opened with applications (eg pdf-Xchange-Viewer) not related to Internet Explorer or Edge (eg dns-crypt.opendns.com):

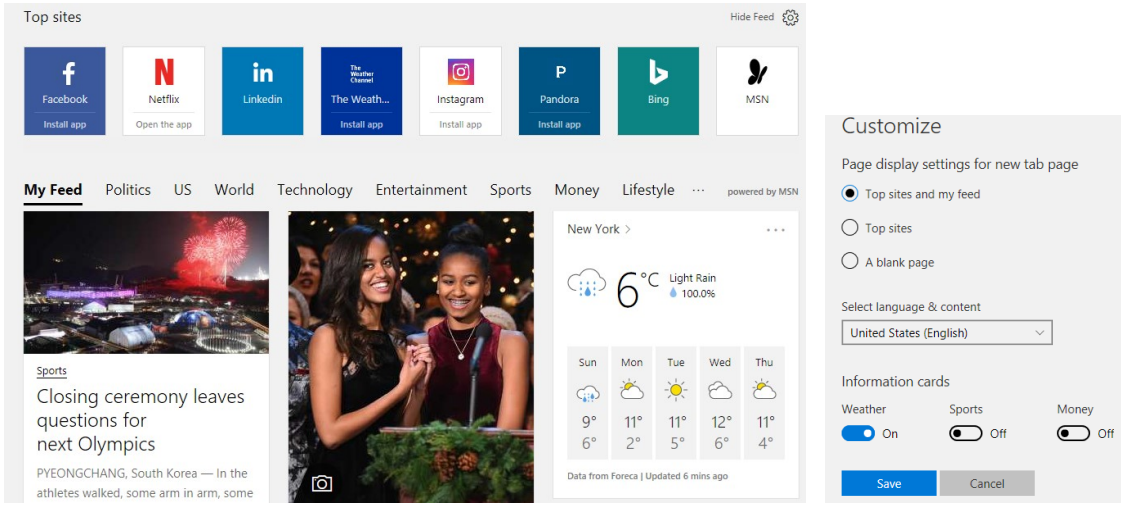
The 3 opendns.com links seen here are from the dnscrypt application's tabs which open when the application first loads in windows.



Container_756 (AC#002 history) contains links to logins, mostly to live.com or msn.com, but I never logged in to either site. They seem to be background processes but that remains to be checked.



They appear to be linked to Edge's start page (Top Sites)



Container_1247 (AC#!005 history) and Container_1524 (AC#!006 history) remain empty.

Registry & Folders SID's and AC permissions

Using the AccessEnum tool from SysInternals we can see the permissions for the Edge AppContainer folders (*screenshot below from Edge_AccessEnum_AC.xlsx*).

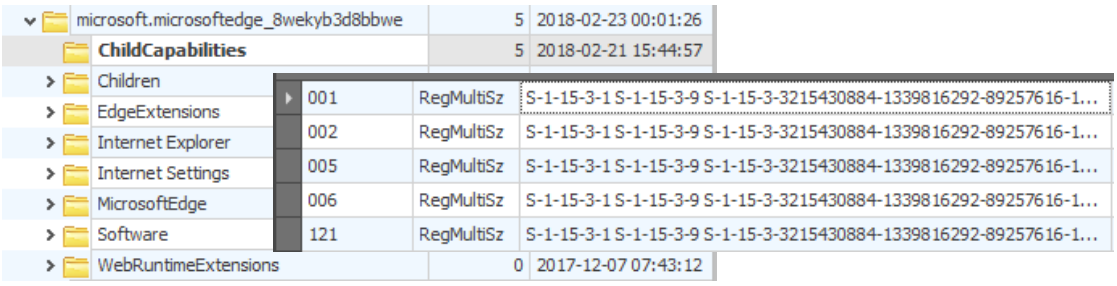
Path	Read	Write
%appdata%\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC	Administrators, HomeUsers, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194	Administrators, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194
%appdata%\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!001	Administrators, HomeUsers, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-4256926629-1688279915-2739229046-3928706915	Administrators, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-4256926629-1688279915-2739229046-3928706915
%appdata%\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!002	Administrators, HomeUsers, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-3513710562-3729412521-1863153555-1462103995	Administrators, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-3513710562-3729412521-1863153555-1462103995
%appdata%\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!005	Administrators, HomeUsers, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-3859068477-1314311106-1651661491-1685393560	Administrators, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-3859068477-1314311106-1651661491-1685393560
%appdata%\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!006	Administrators, HomeUsers, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-1821068571-1793888307-623627345-1529106238	Administrators, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-1821068571-1793888307-623627345-1529106238
%appdata%\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!121	Administrators, HomeUsers, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-2385269614-3243675-834220592-3047885450	Administrators, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194-2385269614-3243675-834220592-3047885450

The same can be seen if we open the "%appdata%\local\Microsoft\Windows\usrclass.dat" (which is a registry file), at the "localsettings\Software\microsoft\windows\currentversion\appcontainer\storage\microsoft.microsoftedge_8wekyb3d8bbwe\childcapabilities"

Or at

"[HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\ childcapabilities \"

in a live system, where we can see the key's values for each container:



Each of these subkeys (001-121) contains the values seen below:

#!001	#!002	#!005	#!006	#!121	Difference	Description
				S-1-15-3-3	Unique	privateNetworkClientServer
				S-1-15-3-8	Unique	enterpriseAuthentication
S-1-15-3-1	S-1-15-3-1	S-1-15-3-1	S-1-15-3-1	S-1-15-3-1	Same in all containers	internetClient
S-1-15-3-9	S-1-15-3-9	S-1-15-3-9	S-1-15-3-9	S-1-15-3-9	Same in all containers	sharedUserCertificates
S-1-15-3-3215430884-1339816292-89257616-1145831019	S-1-15-3-3215430884-1339816292-89257616-1145831019	S-1-15-3-3215430884-1339816292-89257616-1145831019	S-1-15-3-3215430884-1339816292-89257616-1145831019	S-1-15-3-3215430884-1339816292-89257616-1145831019	Same in all containers	location
S-1-15-3-787448254-1207972858-3558633622-1059886964	S-1-15-3-787448254-1207972858-3558633622-1059886964	S-1-15-3-787448254-1207972858-3558633622-1059886964	S-1-15-3-787448254-1207972858-3558633622-1059886964	S-1-15-3-787448254-1207972858-3558633622-1059886964	Same in all containers	microphone
S-1-15-3-3845273463-1331427702-1186551195-1148109977	S-1-15-3-3845273463-1331427702-1186551195-1148109977	S-1-15-3-3845273463-1331427702-1186551195-1148109977	S-1-15-3-3845273463-1331427702-1186551195-1148109977	S-1-15-3-3845273463-1331427702-1186551195-1148109977	Same in all containers	webcam
S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681	S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681		S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681	S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681	Same in all, **except #!005**	
S-1-15-3-1024-3623855041-1826999956-3747069818-3525260223-3747374510-1746272624-950601168-56556331	S-1-15-3-1024-3623855041-1826999956-3747069818-3525260223-3747374510-1746272624-950601168-56556331		S-1-15-3-1024-3623855041-1826999956-3747069818-3525260223-3747374510-1746272624-950601168-56556331	S-1-15-3-1024-3623855041-1826999956-3747069818-3525260223-3747374510-1746272624-950601168-56556331	Same in all, **except #!005**	
S-1-15-3-1024-2405443489-874036122-4286035555-1823921565-1746547431-2453885448-3625952902-991631256	S-1-15-3-1024-2405443489-874036122-4286035555-1823921565-1746547431-2453885448-3625952902-991631256		S-1-15-3-1024-2405443489-874036122-4286035555-1823921565-1746547431-2453885448-3625952902-991631256	S-1-15-3-1024-2405443489-874036122-4286035555-1823921565-1746547431-2453885448-3625952902-991631256	Same in all, **except #!005**	
S-1-15-3-1024-1502825166-1963708345-2616377461-2562897074-4192028372-3968301570-1997628692-1435953622	S-1-15-3-1024-1502825166-1963708345-2616377461-2562897074-4192028372-3968301570-1997628692-1435953622		S-1-15-3-1024-1502825166-1963708345-2616377461-2562897074-4192028372-3968301570-1997628692-1435953622	S-1-15-3-1024-1502825166-1963708345-2616377461-2562897074-4192028372-3968301570-1997628692-1435953622	Same in all, **except #!005**	
S-1-15-3-1024-3203351429-2120443784-2872670797-1918958302-2829055647-4275794519-765664414-2751773334	S-1-15-3-1024-3203351429-2120443784-2872670797-1918958302-2829055647-4275794519-765664414-2751773334		S-1-15-3-1024-3203351429-2120443784-2872670797-1918958302-2829055647-4275794519-765664414-2751773334	S-1-15-3-1024-3203351429-2120443784-2872670797-1918958302-2829055647-4275794519-765664414-2751773334	Same in all, **except #!005**	
S-1-15-3-1024-1788129303-2183208577-3999474272-3147359985-1757322193-3815756386-151582180-1888101193	S-1-15-3-1024-1788129303-2183208577-3999474272-3147359985-1757322193-3815756386-151582180-1888101193		S-1-15-3-1024-1788129303-2183208577-3999474272-3147359985-1757322193-3815756386-151582180-1888101193	S-1-15-3-1024-1788129303-2183208577-3999474272-3147359985-1757322193-3815756386-151582180-1888101193	Same in all, **except #!005**	
S-1-15-3-1024-3153509613-960666767-3724611135-2725662640-12138253-543910227-1950414635-4190290187	S-1-15-3-1024-3153509613-960666767-3724611135-2725662640-12138253-543910227-1950414635-4190290187		S-1-15-3-1024-3153509613-960666767-3724611135-2725662640-12138253-543910227-1950414635-4190290187	S-1-15-3-1024-3153509613-960666767-3724611135-2725662640-12138253-543910227-1950414635-4190290187	Same in all, **except #!005**	
S-1-15-3-1024-126078593-3658686728-1984883306-821399696-3684079960-564038680-3414880098-3435825201	S-1-15-3-1024-126078593-3658686728-1984883306-821399696-3684079960-564038680-3414880098-3435825201		S-1-15-3-1024-126078593-3658686728-1984883306-821399696-3684079960-564038680-3414880098-3435825201	S-1-15-3-1024-126078593-3658686728-1984883306-821399696-3684079960-564038680-3414880098-3435825201	Same in all, **except #!005**	
S-1-15-3-1024-1692970155-4054893335-185714091-3362601943-3526593181-1159816984-2199008581-497492991	S-1-15-3-1024-1692970155-4054893335-185714091-3362601943-3526593181-1159816984-2199008581-497492991		S-1-15-3-1024-1692970155-4054893335-185714091-3362601943-3526593181-1159816984-2199008581-497492991	S-1-15-3-1024-1692970155-4054893335-185714091-3362601943-3526593181-1159816984-2199008581-497492991	Same in all, **except #!005**	
S-1-15-3-1024-220022770-701261984-3991292956-4208751020-2918293058-3396419331-1700932348-2078364891	S-1-15-3-1024-220022770-701261984-3991292956-4208751020-2918293058-3396419331-1700932348-2078364891		S-1-15-3-1024-220022770-701261984-3991292956-4208751020-2918293058-3396419331-1700932348-2078364891	S-1-15-3-1024-220022770-701261984-3991292956-4208751020-2918293058-3396419331-1700932348-2078364891	Same in all, **except #!005**	
S-1-15-3-1024-528118966-3876874398-709513571-1907873084-3598227634-3698730060-278077788-3990600205	S-1-15-3-1024-528118966-3876874398-709513571-1907873084-3598227634-3698730060-278077788-3990600205		S-1-15-3-1024-528118966-3876874398-709513571-1907873084-3598227634-3698730060-278077788-3990600205	S-1-15-3-1024-528118966-3876874398-709513571-1907873084-3598227634-3698730060-278077788-3990600205	Same in all, **except #!005**	
S-1-15-3-1024-1864111754-776273317-3666925027-2523908081-3792458206-3582472437-4114419977-1582884857	S-1-15-3-1024-1864111754-776273317-3666925027-2523908081-3792458206-3582472437-4114419977-1582884857		S-1-15-3-1024-1864111754-776273317-3666925027-2523908081-3792458206-3582472437-4114419977-1582884857	S-1-15-3-1024-1864111754-776273317-3666925027-2523908081-3792458206-3582472437-4114419977-1582884857	Same in all, **except #!005**	
S-1-15-3-1024-4044835139-2658482041-3127973164-329287231-3865880861-1938685643-461067658-1087000422	S-1-15-3-1024-4044835139-2658482041-3127973164-329287231-3865880861-1938685643-461067658-1087000422		S-1-15-3-1024-4044835139-2658482041-3127973164-329287231-3865880861-1938685643-461067658-1087000422	S-1-15-3-1024-4044835139-2658482041-3127973164-329287231-3865880861-1938685643-461067658-1087000422	Same in all, **except #!005**	
S-1-15-3-1024-2922296261-1647482768-2017091146-3858667068-4135663662-2931985894-1627820925-818366431	S-1-15-3-1024-2922296261-1647482768-2017091146-3858667068-4135663662-2931985894-1627820925-818366431		S-1-15-3-1024-2922296261-1647482768-2017091146-3858667068-4135663662-2931985894-1627820925-818366431	S-1-15-3-1024-2922296261-1647482768-2017091146-3858667068-4135663662-2931985894-1627820925-818366431	Same in all, **except #!005**	
S-1-15-3-1024-4092130000-472000003-1670882671-259370826-3862510858-3415016346-1868891083-3396446831	S-1-15-3-1024-4092130000-472000003-1670882671-259370826-3862510858-3415016346-1868891083-3396446831		S-1-15-3-1024-4092130000-472000003-1670882671-259370826-3862510858-3415016346-1868891083-3396446831	S-1-15-3-1024-4092130000-472000003-1670882671-259370826-3862510858-3415016346-1868891083-3396446831	Same in all, **except #!005**	
S-1-15-3-1024-2440306377-3304611049-1494399071-1161926223-163912384-1437065773-1456820560-2390158196	S-1-15-3-1024-2440306377-3304611049-1494399071-1161926223-163912384-1437065773-1456820560-2390158196		S-1-15-3-1024-2440306377-3304611049-1494399071-1161926223-163912384-1437065773-1456820560-2390158196	S-1-15-3-1024-2440306377-3304611049-1494399071-1161926223-163912384-1437065773-1456820560-2390158196	Same in all, **except #!005**	

And each of those corresponds (exists) also in the Access Permissions list obtained with AccessEnum tool, except container 121 which has two unique ones:

#!121	Difference	Description
S-1-15-3-3	Unique	privateNetworkClientServer
S-1-15-3-8	Unique	enterpriseAuthentication
S-1-15-3-1	Same in all containers	internetClient
S-1-15-3-9	Same in all containers	sharedUserCertificates
S-1-15-3-3215430884-1339816292-89257616-1145831019	Same in all containers	location
S-1-15-3-787448254-1207972858-3558633622-1059886964	Same in all containers	microphone
S-1-15-3-3845273463-1331427702-1186551195-1148109977	Same in all containers	webcam
S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681	Same in all, **except #!005**	
S-1-15-3-1024-3623855041-1826999956-3747069818-3525260223-3747374510-1746272624-950601168-56556331	Same in all, **except #!005**	

And container 005 which has only 5 SIDs

#!005
S-1-15-3-1
S-1-15-3-9
S-1-15-3-3215430884-1339816292-89257616-1145831019
S-1-15-3-787448254-1207972858-3558633622-1059886964
S-1-15-3-3845273463-1331427702-1186551195-1148109977

and

SIDs obtained from SYSTEM key value:	Check if exists in ChildCapabilities tab
S-1-15-3-1	Exists
S-1-15-3-9	Exists
S-1-15-3-3215430884-1339816292-89257616-1145831019	Exists
S-1-15-3-787448254-1207972858-3558633622-1059886964	Exists
S-1-15-3-3845273463-1331427702-1186551195-1148109977	Exists

There are no descriptions for these SIDs in the registry (or anywhere else that I found) except in https://www.blackhat.com/docs/asia-14/materials/Yason/WP-Asia-14-Yason-Diving-Into-IE10s-Enhanced-Protected-Mode-Sandbox.pdf where this can be seen in page 5:

"If private network access (2.2.5) is turned on, IE uses a separate AppContainer with the following additional capabilities assigned in order to allow access to private network resources:

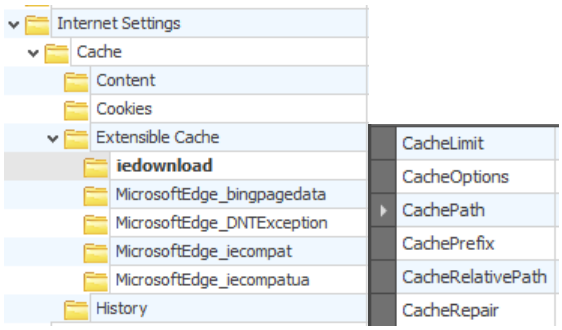
- privateNetworkClientServer (S-1-15-3-3)
- enterpriseAuthentication (S-1-15-3-8)"

From this we can deduce that container **#!121** is used for private network resources.

If we look at "*%appdata%\local\Microsoft\Windows\usrclass.dat*" 's key:

"localsettings\Software\microsoft\windows\currentversion\appcontainer\storage\microsoft.microsoftedge_8wekyb3d8bbwe\Internet Settings\Cache\Extensible Cache\"

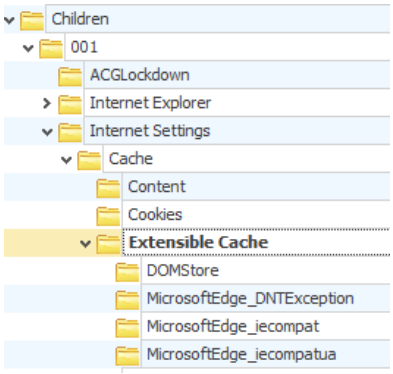
we see a list of 5 keys which contain relevant cache paths.



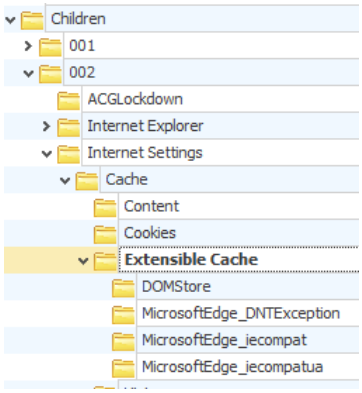
For example at the "CachePath" subkey we see the value:
"%AppData%\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\DownloadHistory"

Similarly,

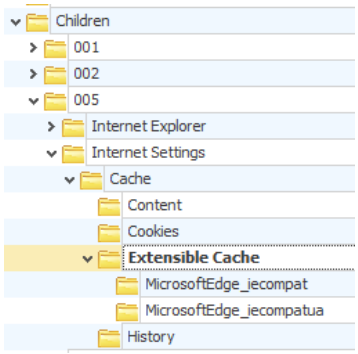
Child 001 has 4 subkeys:



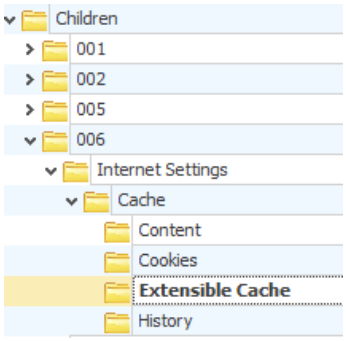
Child 002 has 4 subkeys:



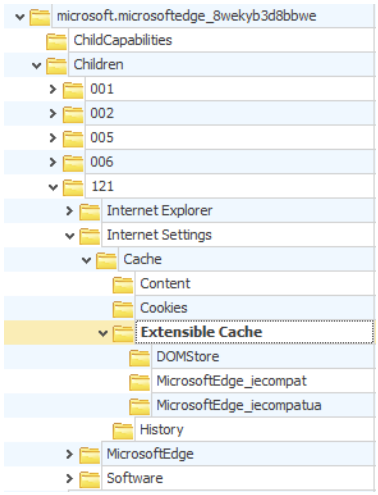
Child 005 has 2 subkeys:



Child 006 has no subkeys:



And Child 121 has 3 subkeys:



From the above we can deduce that all Children Containers (except 006) have the "MicrosoftEdge_iecompatua", "MicrosoftEdge_iecompat" and "DOMStore" keys with values similar to the ones below:

"Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\Children\121\Internet Settings\Cache\Extensible Cache\MicrosoftEdge_iecompatua"

Value:

%AppData%\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#!121\MicrosoftEdge\IECompatUaCache

“Local *Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\Children\121\Internet Settings\Cache\Extensible Cache\MicrosoftEdge_iecompat”*

Value

“%AppData%\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#!121\MicrosoftEdge\IECompatCache”

Local

“*Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\Children\121\Internet Settings\Cache\Extensible Cache\DOMStore”*

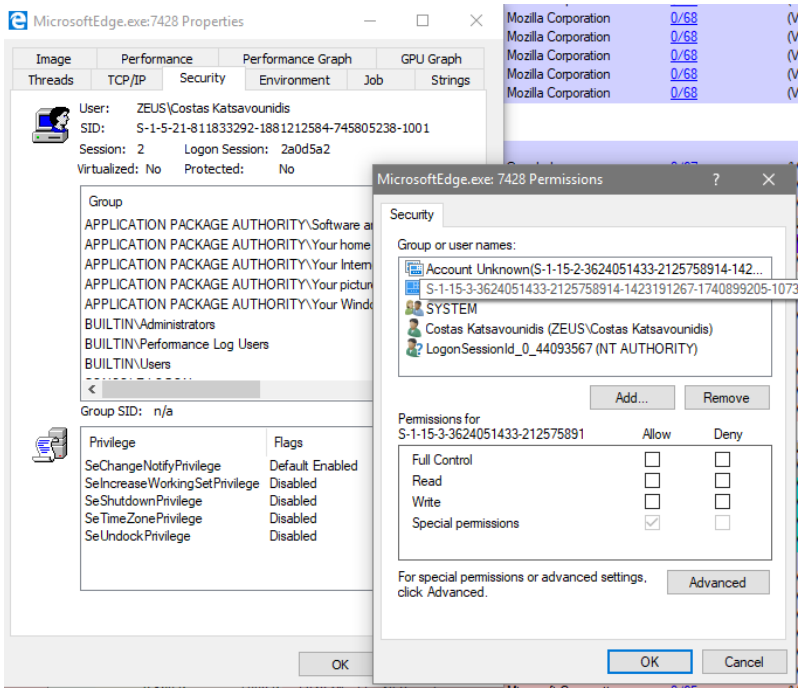
Value

“%AppData%\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#!121\MicrosoftEdge\User\Default\DOMStore”

Opening Process Explorer and then opening MS Edge we see 5 entries

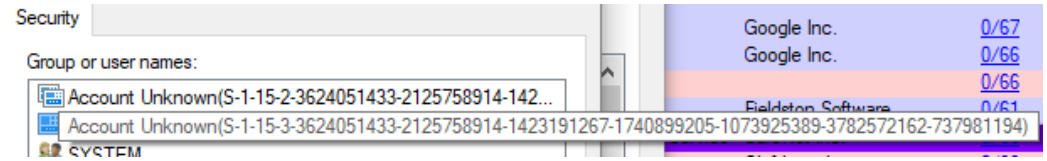
MicrosoftEdge.exe	< 0.01	37.760 K	82.972 K	7428 Microsoft Edge	Microsoft Corporation	0/68	(Verified) Microsoft Corporation
MicrosoftEdgeCP.exe	< 0.01	5.808 K	24.020 K	12036 Microsoft Edge Content Proc...	Microsoft Corporation	0/68	(Verified) Microsoft Corporation
MicrosoftEdgeCP.exe	0.25	90.980 K	122.956 K	13560 Microsoft Edge Content Proc...	Microsoft Corporation	0/68	(Verified) Microsoft Corporation
MicrosoftEdgeCP.exe		5.856 K	25.740 K	7908 Microsoft Edge Content Proc...	Microsoft Corporation	0/68	(Verified) Microsoft Corporation
MicrosoftEdgeCP.exe		5.924 K	25.908 K	5512 Microsoft Edge Content Proc...	Microsoft Corporation	0/68	(Verified) Microsoft Corporation

If we open the properties and then the Security tab, we can see the permissions:



The first 2 permissions of MicrosoftEdgeCP.exe which are identical

Path	Read	Write
%appdata%\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC	Administrators, HomeUsers, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194	Administrators, S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194

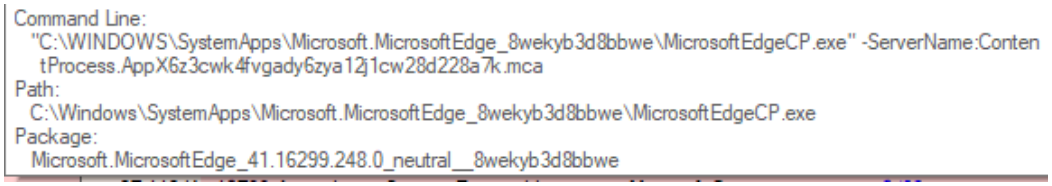


And correspond to "*Microsoft.MicrosoftEdge_41.16299.248.0_neutral__8wekyb3d8bbwe*"

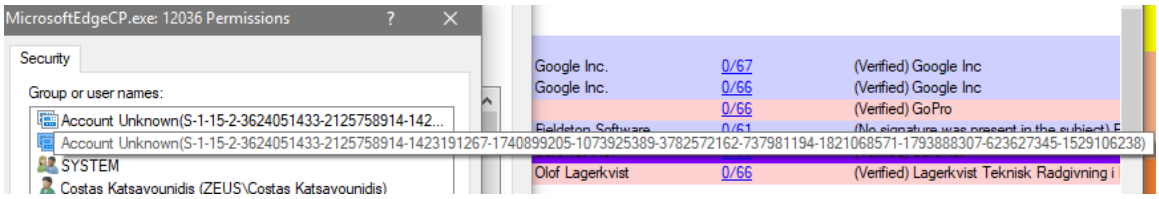
With a LocalAppData folder:

\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC

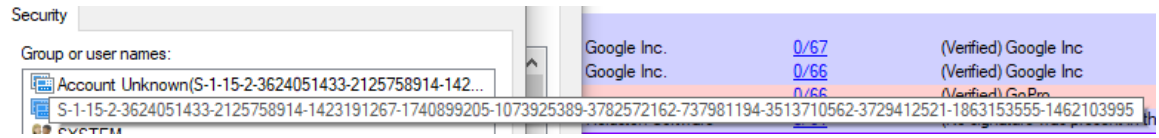
The rest of the entries provide this info:



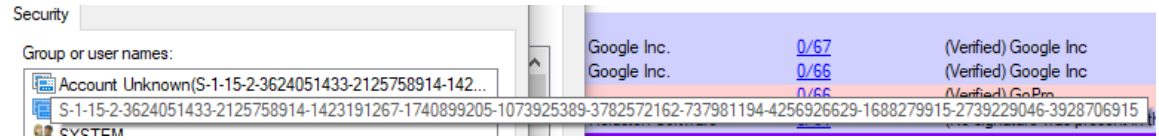
Each of which corresponding (respectively to the list above) to:



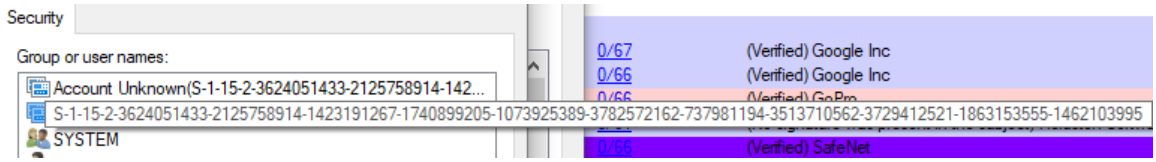
"microsoft.microsoftedge_8wekyb3d8bbwe/006"
with a LocalAppData folder pointing to \AC\#!006



"microsoft.microsoftedge_8wekyb3d8bbwe/002"
with a LocalAppData folder pointing to \AC\#!002



"microsoft.microsoftedge_8wekyb3d8bbwe/001"
with a LocalAppData folder pointing to \AC\#!001



And again, *microsoft.microsoftedge_8wekyb3d8bbwe/002*.

In all the entries the first permissions is for

"*Microsoft.MicrosoftEdge_41.16299.248.0_neutral__8wekyb3d8bbwe*"

Which is logical as they are all Children Containers of the general Edge Application Container: *%appdata%\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC*

Registry Files Examined:

- ✓ AmCache.hve
- ✓ UsrClass.dat
- ✓ Ntuser.dat
- ✓ Components
- ✓ Security
- ✓ Sam
- ✓ Software
- ✓ System

MS Windows version: 1709 (Build: 16299.248)

MS Edge version: 41.16299.248.0
MS EdgeHTML: 16.16299