BHASKARACHARYA NATIONAL INSTITUTE FOR SPACE APPLICATIONS AND GEO-INFORMATICS

WEEKLY PROGRESS REPORT (20/02/2023 – 26/02/2023)

WEEK 5

PROJECT NAME	MALWARE DETECTION USING ML

PROJECT DESCRIPTION :	**DESIGN AND IMPLEMENT ML MODEL TO DETECT MALWARE IN SYSTEM**
GROUP MEMBER :	**PRATHAM PATEL, Shubham Patel, Shashank Sharma, Yash Soni**
GROUP ID :	**I2**
GROUP GUIDE :	**HARSH KIRATSATA**
GROUP COORDINATOR :	**SIDHDHARTH PATEL**
COLLEGE GUIDE NAME :	**MAYANK PATEL, RITIKA LADHA, KINJAL CHAUDHARI**
COLLEGE GUIDE No. :	**+91 9033280445,8866438698, 9723173567**
COLLEGE GUIDE EMAIL. :	**mayank.patel@adaniuni.ac.in, ritika.ladha@adaniuni.ac.in, kinjal.chaudhari@adaniuni.ac.in**
COLLEGE NAME :	**ADANI INSTITUTE OF INFRASTRUCTURE AND ENGINEERING**

20/02/2023 TILL 26/02/2023 (7 DAYS)

Vectorization and data cleaning

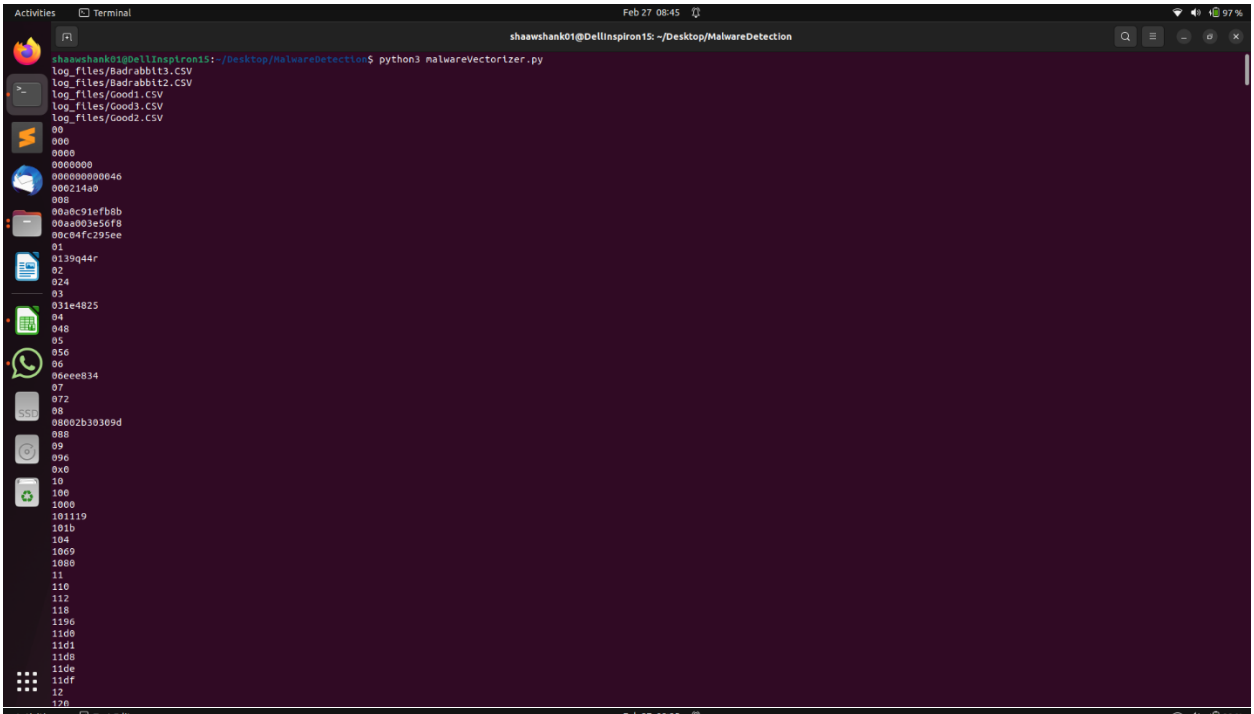
20/02/2023	Explored the malware data set (dummy).
21/02/2023	Explored the non-malware data set.
22/02/2023	Data Preprocessing of the files and log files.
23/02/2023	Learning theory of vectorization and code walkthrough.
24/02/2023	Implementing vectorization code on dataset.
25/02/2023	Noting the insights for feature selection (Holiday)(Saturday).
26/02/2023	Holiday (Sunday).

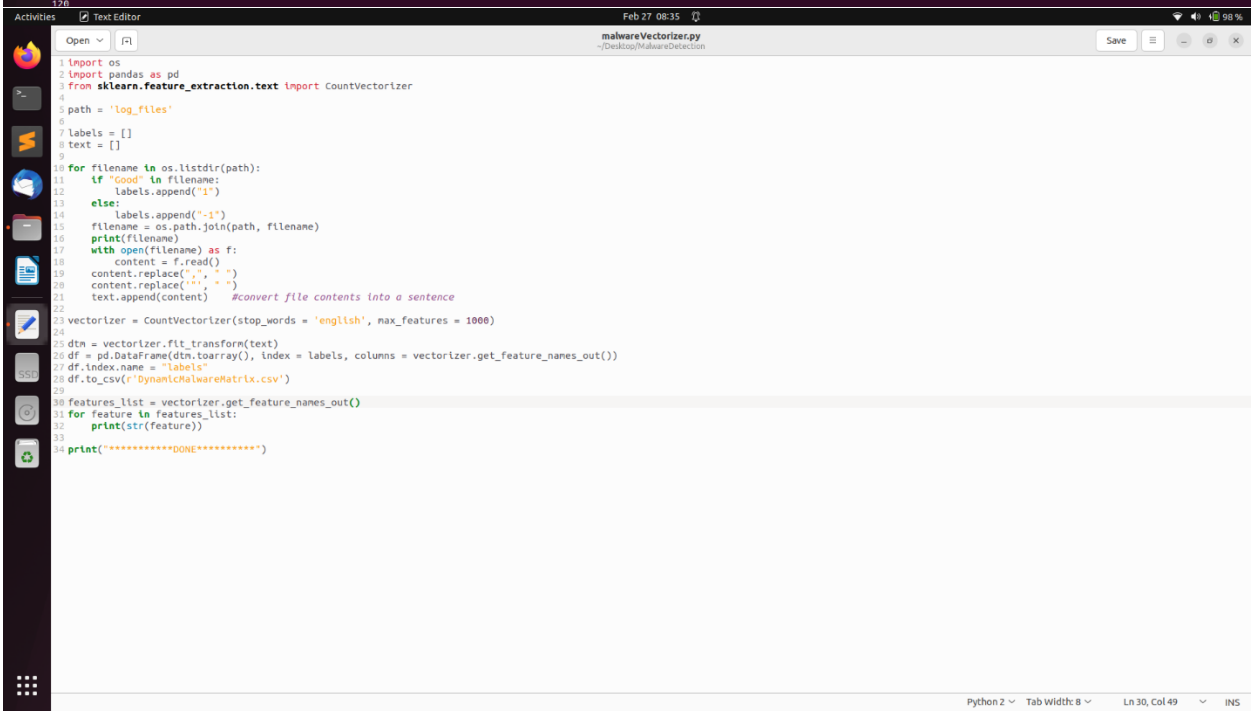
WEEK 6 (PLAN)	In the next week we are planning to clean the real world obtained data and we will try to implement vectorization

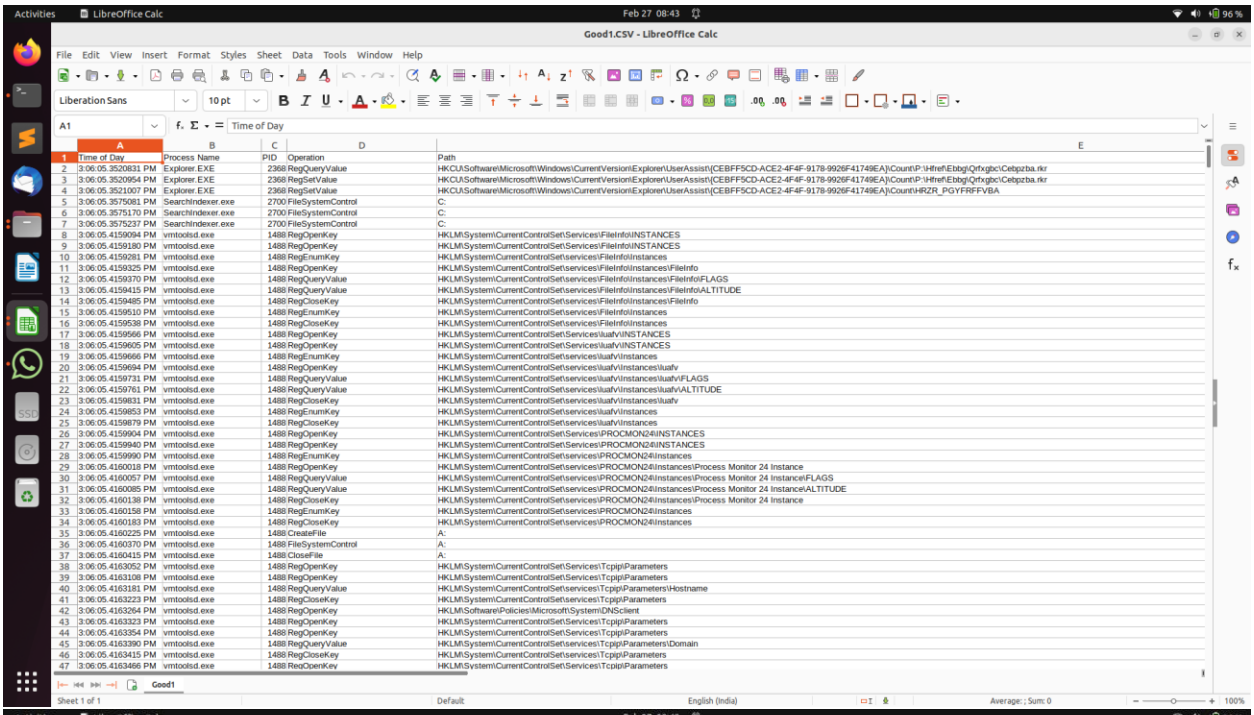
REFERENCE :

- https://towardsdatascience.com/what-is-vectorization-in-machine-learning-6c7be3e4440a
- https://www.geeksforgeeks.org/data-cleansing-introduction/
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7249657/
- https://www.geeksforgeeks.org/bag-of-words-bow-model-in-nlp/
- https://www.youtube.com/watch?v=e3Fqkq5DC_4

Screenshots:

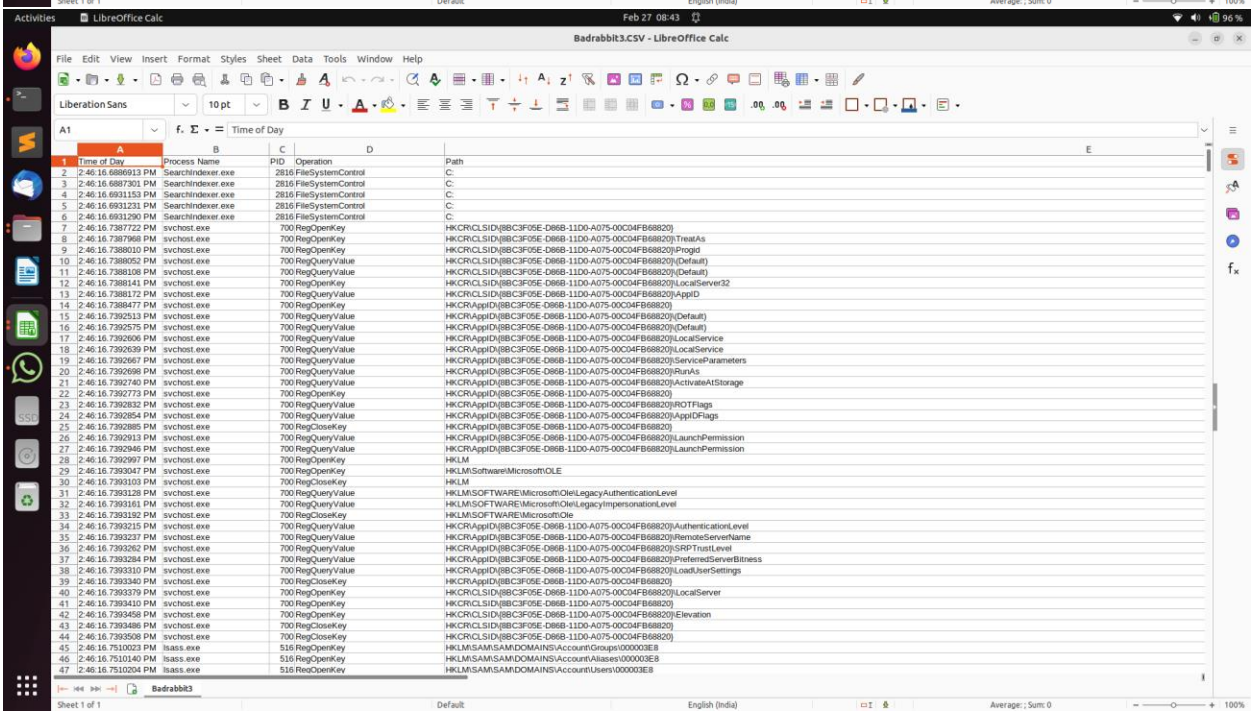






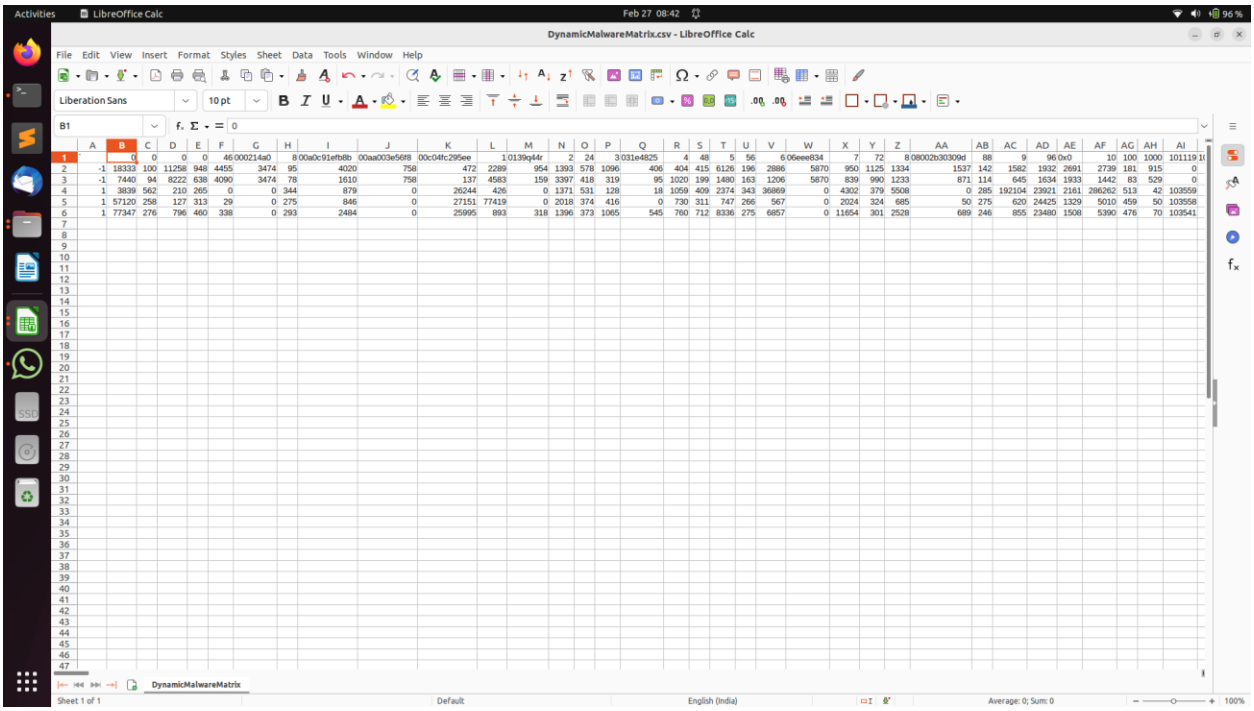
Good1.CSV - LibreOffice Calc

	Time of Day	Process Name	PID	Operation	Path
2	3:06:05.3520831 PM	Explorer.EXE	2368	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\Ebbgl\Qrfxgbc\Cebpzba.rkr
3	3:06:05.3520954 PM	Explorer.EXE	2368	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\Ebbgl\Qrfxgbc\Cebpzba.rkr
4	3:06:05.3521007 PM	Explorer.EXE	2368	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA
5	3:06:05.3575081 PM	SearchIndexer.exe	2700	FileSystemControl	C:
6	3:06:05.3575170 PM	SearchIndexer.exe	2700	FileSystemControl	C:
7	3:06:05.3575237 PM	SearchIndexer.exe	2700	FileSystemControl	C:
8	3:06:05.4159094 PM	vmtoolsd.exe	1488	RegOpenKey	HKLM\System\CurrentControlSet\Services\FileInfo\INSTANCES
9	3:06:05.4159180 PM	vmtoolsd.exe	1488	RegOpenKey	HKLM\System\CurrentControlSet\Services\FileInfo\INSTANCES
10	3:06:05.4159281 PM	vmtoolsd.exe	1488	RegEnumKey	HKLM\System\CurrentControlSet\services\FileInfo\Instances
11	3:06:05.4159325 PM	vmtoolsd.exe	1488	RegOpenKey	HKLM\System\CurrentControlSet\services\FileInfo\Instances\FileInfo
12	3:06:05.4159370 PM	vmtoolsd.exe	1488	RegQueryValue	HKLM\System\CurrentControlSet\services\FileInfo\Instances\FileInfo\FLAGS
13	3:06:05.4159415 PM	vmtoolsd.exe	1488	RegQueryValue	HKLM\System\CurrentControlSet\services\FileInfo\Instances\FileInfo\ALTITUDE
14	3:06:05.4159485 PM	vmtoolsd.exe	1488	RegCloseKey	HKLM\System\CurrentControlSet\services\FileInfo\Instances\FileInfo
15	3:06:05.4159510 PM	vmtoolsd.exe	1488	RegEnumKey	HKLM\System\CurrentControlSet\services\FileInfo\Instances
16	3:06:05.4159538 PM	vmtoolsd.exe	1488	RegCloseKey	HKLM\System\CurrentControlSet\services\FileInfo\Instances
17	3:06:05.4159566 PM	vmtoolsd.exe	1488	RegOpenKey	HKLM\System\CurrentControlSet\Services\luafv\INSTANCES
18	3:06:05.4159605 PM	vmtoolsd.exe	1488	RegOpenKey	HKLM\System\CurrentControlSet\Services\luafv\INSTANCES
19	3:06:05.4159666 PM	vmtoolsd.exe	1488	RegEnumKey	HKLM\System\CurrentControlSet\services\luafv\Instances
20	3:06:05.4159694 PM	vmtoolsd.exe	1488	RegOpenKey	HKLM\System\CurrentControlSet\services\luafv\Instances\luafv
21	3:06:05.4159731 PM	vmtoolsd.exe	1488	RegQueryValue	HKLM\System\CurrentControlSet\services\luafv\Instances\luafv\FLAGS
22	3:06:05.4159761 PM	vmtoolsd.exe	1488	RegQueryValue	HKLM\System\CurrentControlSet\services\luafv\Instances\luafv\ALTITUDE
23	3:06:05.4159831 PM	vmtoolsd.exe	1488	RegCloseKey	HKLM\System\CurrentControlSet\services\luafv\Instances\luafv
24	3:06:05.4159853 PM	vmtoolsd.exe	1488	RegEnumKey	HKLM\System\CurrentControlSet\services\luafv\Instances
25	3:06:05.4159879 PM	vmtoolsd.exe	1488	RegCloseKey	HKLM\System\CurrentControlSet\services\luafv\Instances
26	3:06:05.4159904 PM	vmtoolsd.exe	1488	RegOpenKey	HKLM\System\CurrentControlSet\Services\PROCMON24\INSTANCES
27	3:06:05.4159940 PM	vmtoolsd.exe	1488	RegOpenKey	HKLM\System\CurrentControlSet\Services\PROCMON24\INSTANCES
28	3:06:05.4159990 PM	vmtoolsd.exe	1488	RegEnumKey	HKLM\System\CurrentControlSet\services\PROCMON24\Instances
29	3:06:05.4160018 PM	vmtoolsd.exe	1488	RegOpenKey	HKLM\System\CurrentControlSet\services\PROCMON24\Instances\Process Monitor 24 Instance
30	3:06:05.4160057 PM	vmtoolsd.exe	1488	RegQueryValue	HKLM\System\CurrentControlSet\services\PROCMON24\Instances\Process Monitor 24 Instance\FLAGS
31	3:06:05.4160085 PM	vmtoolsd.exe	1488	RegQueryValue	HKLM\System\CurrentControlSet\services\PROCMON24\Instances\Process Monitor 24 Instance\ALTITUDE
32	3:06:05.4160138 PM	vmtoolsd.exe	1488	RegCloseKey	HKLM\System\CurrentControlSet\services\PROCMON24\Instances\Process Monitor 24 Instance
33	3:06:05.4160158 PM	vmtoolsd.exe	1488	RegEnumKey	HKLM\System\CurrentControlSet\services\PROCMON24\Instances
34	3:06:05.4160183 PM	vmtoolsd.exe	1488	RegCloseKey	HKLM\System\CurrentControlSet\services\PROCMON24\Instances
35	3:06:05.4160225 PM	vmtoolsd.exe	1488	CreateFile	A:
36	3:06:05.4160370 PM	vmtoolsd.exe	1488	FileSystemControl	A:
37	3:06:05.4160415 PM	vmtoolsd.exe	1488	CloseFile	A:
38	3:06:05.4163052 PM	vmtoolsd.exe	1488	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters
39	3:06:05.4163108 PM	vmtoolsd.exe	1488	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters
40	3:06:05.4163181 PM	vmtoolsd.exe	1488	RegQueryValue	HKLM\System\CurrentControlSet\services\Tcpip\Parameters\Hostname
41	3:06:05.4163223 PM	vmtoolsd.exe	1488	RegCloseKey	HKLM\System\CurrentControlSet\services\Tcpip\Parameters
42	3:06:05.4163264 PM	vmtoolsd.exe	1488	RegOpenKey	HKLM\SoftwarePolicies\Microsoft\System\DNSclient
43	3:06:05.4163323 PM	vmtoolsd.exe	1488	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters
44	3:06:05.4163354 PM	vmtoolsd.exe	1488	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters
45	3:06:05.4163390 PM	vmtoolsd.exe	1488	RegQueryValue	HKLM\System\CurrentControlSet\services\Tcpip\Parameters\Domain
46	3:06:05.4163415 PM	vmtoolsd.exe	1488	RegCloseKey	HKLM\System\CurrentControlSet\services\Tcpip\Parameters
47	3:06:05.4163466 PM	vmtoolsd.exe	1488	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters



Badrabbit3.CSV - LibreOffice Calc

	Time of Day	Process Name	PID	Operation	Path
2	2:46:16.6886913 PM	SearchIndexer.exe	2816	FileSystemControl	C:
3	2:46:16.6887301 PM	SearchIndexer.exe	2816	FileSystemControl	C:
4	2:46:16.6931153 PM	SearchIndexer.exe	2816	FileSystemControl	C:
5	2:46:16.6931231 PM	SearchIndexer.exe	2816	FileSystemControl	C:
6	2:46:16.6931290 PM	SearchIndexer.exe	2816	FileSystemControl	C:
7	2:46:16.7387722 PM	svchost.exe	700	RegOpenKey	HKCR\CLSID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}
8	2:46:16.7387968 PM	svchost.exe	700	RegOpenKey	HKCR\CLSID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\TreatAs
9	2:46:16.7388010 PM	svchost.exe	700	RegOpenKey	HKCR\CLSID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\ProgId
10	2:46:16.7388052 PM	svchost.exe	700	RegQueryValue	HKCR\CLSID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\(Default)
11	2:46:16.7388108 PM	svchost.exe	700	RegQueryValue	HKCR\CLSID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\(Default)
12	2:46:16.7388141 PM	svchost.exe	700	RegOpenKey	HKCR\CLSID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer32
13	2:46:16.7388172 PM	svchost.exe	700	RegQueryValue	HKCR\CLSID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\AppID
14	2:46:16.7388477 PM	svchost.exe	700	RegOpenKey	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}
15	2:46:16.7392513 PM	svchost.exe	700	RegQueryValue	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\(Default)
16	2:46:16.7392575 PM	svchost.exe	700	RegQueryValue	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\(Default)
17	2:46:16.7392606 PM	svchost.exe	700	RegQueryValue	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\LocalService
18	2:46:16.7392639 PM	svchost.exe	700	RegQueryValue	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\LocalService
19	2:46:16.7392667 PM	svchost.exe	700	RegQueryValue	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\ServiceParameters
20	2:46:16.7392698 PM	svchost.exe	700	RegQueryValue	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\RunAs
21	2:46:16.7392740 PM	svchost.exe	700	RegQueryValue	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\ActivateAtStorage
22	2:46:16.7392773 PM	svchost.exe	700	RegOpenKey	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}
23	2:46:16.7392832 PM	svchost.exe	700	RegQueryValue	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\ROTFlags
24	2:46:16.7392854 PM	svchost.exe	700	RegQueryValue	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\AppIDFlags
25	2:46:16.7392885 PM	svchost.exe	700	RegCloseKey	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}
26	2:46:16.7392913 PM	svchost.exe	700	RegQueryValue	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\LaunchPermission
27	2:46:16.7392946 PM	svchost.exe	700	RegQueryValue	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\LaunchPermission
28	2:46:16.7392997 PM	svchost.exe	700	RegOpenKey	HKLM
29	2:46:16.7393047 PM	svchost.exe	700	RegOpenKey	HKLM\Software\Microsoft\OLE
30	2:46:16.7393103 PM	svchost.exe	700	RegCloseKey	HKLM
31	2:46:16.7393128 PM	svchost.exe	700	RegQueryValue	HKLM\SOFTWARE\Microsoft\Ole\LegacyAuthenticationLevel
32	2:46:16.7393161 PM	svchost.exe	700	RegQueryValue	HKLM\SOFTWARE\Microsoft\Ole\LegacyImpersonationLevel
33	2:46:16.7393192 PM	svchost.exe	700	RegCloseKey	HKLM\SOFTWARE\Microsoft\Ole
34	2:46:16.7393215 PM	svchost.exe	700	RegQueryValue	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\AuthenticationLevel
35	2:46:16.7393237 PM	svchost.exe	700	RegQueryValue	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\RemoteServerName
36	2:46:16.7393262 PM	svchost.exe	700	RegQueryValue	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\SRPTrustLevel
37	2:46:16.7393284 PM	svchost.exe	700	RegQueryValue	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\PreferredServerBitness
38	2:46:16.7393310 PM	svchost.exe	700	RegQueryValue	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\LoadUserSettings
39	2:46:16.7393340 PM	svchost.exe	700	RegCloseKey	HKCR\AppID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}
40	2:46:16.7393379 PM	svchost.exe	700	RegOpenKey	HKCR\CLSID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\LocalServer
41	2:46:16.7393410 PM	svchost.exe	700	RegOpenKey	HKCR\CLSID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}
42	2:46:16.7393458 PM	svchost.exe	700	RegOpenKey	HKCR\CLSID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}\Elevation
43	2:46:16.7393486 PM	svchost.exe	700	RegCloseKey	HKCR\CLSID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}
44	2:46:16.7393508 PM	svchost.exe	700	RegCloseKey	HKCR\CLSID\{BBC3F05E-D86B-11D0-A075-00C04FB68820}
45	2:46:16.7510023 PM	lsass.exe	516	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\Groups\000003E8
46	2:46:16.7510140 PM	lsass.exe	516	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\Aliases\000003E8
47	2:46:16.7510204 PM	lsass.exe	516	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\Users\000003E8



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI
1		0	0	0	0	46	000214a0	8	00a0c91efb8b	00aa003e56f8	00c04fc295ee	1	0139q4r	2	24	3	031e4825	4	48	5	56	6	06eee834	7	72	8	08002b30309d	88	9	96	0x0	10	100	1000	101119 1
2	-1	18333	100	11258	948	4455	3474	95	4020	758	472	2289	954	1393	578	1096	406	404	415	6126	196	2886	5870	950	1125	1334	1537	142	1582	1932	2691	2739	181	915	0
3	-1	7440	94	8222	638	4090	3474	78	1610	758	137	4583	159	3397	418	319	95	1020	199	1480	163	1206	5870	839	990	1233	871	114	645	1634	1933	1442	83	529	0
4	1	3839	562	210	265	0	0	344	879	0	26244	426	0	1371	531	128	18	1059	409	2374	343	36869	0	4302	379	5508	0	285	192104	23921	2161	286262	513	42	103559
5	1	57120	258	127	313	29	0	275	846	0	27151	77419	0	2018	374	416	0	730	311	747	266	567	0	2924	324	685	50	275	620	24425	1329	5010	459	50	103558
6	1	77347	276	796	460	338	0	293	2484	0	25995	893	318	1396	373	1065	545	760	712	8336	275	6857	0	11654	301	2528	689	246	855	23480	1508	5390	476	70	103541