WildFire Analysis Report

1 File Information

File Type	PE
File Signer	
SHA-256	5f38708709dd47d0b4a323e3a065e5130464102bfff930275a00ac81db490308
SHA-1	1e66215412704d1ba7373d59c9291b0c67a764af
MD5	e01ede25f5c2be6f5a27953bcb239d5d
File Size	90725bytes
First Seen Timestamp	2021-07-27 03:47:03 UTC
Verdict	**Malware**
Antivirus Coverage	VirusTotal Information

2 Static Analysis

2.1. Suspicious File Properties

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

Contains sections with size discrepancies

Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

Contains sections with high entropy

Entropy is a measurement of the randomness in data. Sections with high entropy may indicate a compressed or encrypted PE file.

Contains sections with zero size

Sections with zero size indicate a packed or obfuscated PE file.

Generated by NSIS as Uninstaller

This PE file was generated by the Nullsoft Scriptable Install System (NSIS), a package for generating software installers in uninstaller mode.

Contains overlay data

Overlay data is extra data appended to the end of a PE image. Many legitimate files, including all files that are digitally signed, contain overlay data. However, malware often uses overlays to embed encoded or encrypted data as well.

Contains overlay data with high entropy

Entropy is a measurement of the randomness in data. Overlays with high entropy indicate encoded or encrypted data.

Contains non-standard section names

Standard section names are defined by the compiler. Non-standard section names may indicate a packed or obfuscated PE file.

3 Dynamic Analysis

3.1. VM1 (Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007)

3.1.1. Behavioral Summary

This sample was found to be **malware** on this virtual machine.

Behavior	Severity
Copied itself Malware often copies itself to new locations both to spread and to establish persistence.	
Sample used SetFileTime to modify file last write time. Sample used SetFileTime to modify file last write time.	
Created or modified a file in the Windows system folder The Windows system folder contains configuration files and executables that control the underlying functions of the system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection.	
Created an executable file in a user folder User folders are storage locations for music, pictures, downloads, and other user-specific files. Legitimate applications rarely place executable content in these folders, while malware often does so to avoid detection.	
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	
Started a process from a user folder User folders are storage locations for music, pictures, downloads, and other user-specific files. Malware often runs executable content out of these folders to avoid detection, while legitimate applications are usually run out of the Windows, Windows system, or Program Files folders.	
Started a process A process running on the system may start additional processes to perform actions in the background. This behavior is common to legitimate software as well as malware.	
Deleted itself Malware often deletes itself after installation to avoid detection. Legitimate applications do not delete themselves directly.	
Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	
Accessed decoy files The WildFire sandbox deploys a number of decoy files crafted to mimic desirable user information like credit card and Social Security numbers. A sample that accesses these files is likely malicious and designed to steal personal information from users.	
Restarted itself in a suspicious manner Malware often exits and restarts itself to avoid detection.	
Deleted cookies Cookies are small pieces of browser data that store information about a user's interaction with a website. Malware often deletes cookies to erase evidence of its own activity or disrupt services provided by other websites.	
Scheduled a file operation for system restart Malware may schedule file rename, move, and delete operations for system restart to avoid detection.	

Sample used SetFileTime to modify file creation time. Sample used SetFileTime to modify file creation time.	

3.1.2. Network Activity

No network data available.

3.1.3. Host Activity

Process Activity

Process Name - Au_.exe

(command: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~nsu.tmp\Au_.exe" _?=C:\Documents and Settings\Administrator\)

File Activity

File	Action	Size(B)	File Type	Hash
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsa8.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsg9.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsg9.tmp\UserInfo.dll	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsg9.tmp\System.dll	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsg9.tmp\modern-header.bmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsa8.tmp	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsg9.tmp	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Documents and Settings\Administrator\3rd\7z.dll	Delete	914432	PE	md5:04AD4B80880B32C94BE8D0886482C774 sha1:344faf61c3eb76f4a2fb6452e83ed16c9cce73e0 sha256:A1E1D1F0FFF4FCCCFBDFA313F3BDFEA4D3DFE2C2D9174A615BBC39A0A6929338
C:\Documents and Settings\Administrator\3rd\7z.exe	Delete	163840	PE	md5:A51D90F2F9394F5EA0A3ACAE3BD2B219 sha1:20fea1314dbed552d5fedee096e2050369172ee1 sha256:AC9674FEB8F2FAD20C1E046DE67F899419276AE79A60E8CC021A4BF472AE044F

C:\Documents and Settings\Administrator\Application Data\desktop.ini	Delete	62	unknown	md5:88CF0FF92A4A9FA7BD9B7513B2E9E22B sha1:38a24edfbc474b55d4cce76e895ff6d81a025dd5 sha256:EC097199B6931EE3FACC515EBA14BE947CB78B98BCCEF84C57CC6C4CC85419DB
C:\Documents and Settings\Administrator\Application Data\Microsoft\Crypto\RSA\S-1-5-21-515967899-776561741-1417001333-500\83aa4cc77f591dfc2374580bbd95f6ba_a3eebfd9-28cb-4cee-b2ac-1c284d06458c	Delete	45	unknown	md5:C8366AE350E7019AEFC9D1E6E6A498C6 sha1:5731d8a3e6568a5f2dfbbc87e3db9637df280b61 sha256:11E6ACA8E682C046C83B721EEB5C72C5EF03CB5936C60DF6F4993511DDC61238
C:\Documents and Settings\Administrator\Application Data\Microsoft\Document Building Blocks\1033\Building Blocks.dotx	Delete	322380	unknown	md5:89E2626A866BC9A18DA185E35228A404 sha1:4bc5718e114fa9cd2d60af37ba3d58d382ed18da sha256:6E9BD1E5638D48C1219C2312B67F2134FF404AB9F9644431DF9B3B33EC33DE66
C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\brndlog.bak	Delete	141	unknown	md5:1F59EB9DB0307A54FE94E7D134AA79FF sha1:7bc2e3848e0c9bc8bfc14c5059cb8f09b7666ca2 sha256:5DA8FE66B1C5CA7E6F2C3AE53554362D4F44B60E2A150CD375423B9D2B812D5E
C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\brndlog.txt	Delete	10389	unknown	md5:2A502A5A3B1A1B9742B4F3F18616EC5E sha1:f81f871688679dbb8ae4dafdceffda0a2cb2e2ee sha256:E3D2868D9922567F5BC3A9DAFE4159F58BD426ED5AD9C2677D33DEB0C6D1E1524
C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\Desktop.htt	Delete	2710	unknown	md5:59A64078A564E5B1B85D0534318CD8CB sha1:deffc666586a314aec0ba5601bb346d7d5ef6467 sha256:2E2520B9BFD60461D7984A5A32AFE0D663536EB170382D3AC6B215349F4D668D
C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\Quick Launch\desktop.ini	Delete	119	unknown	md5:B6F6999BB50AFAB3A0217640527F2AD3 sha1:1796a31cda09160e1775537d12084390fe373a47 sha256:BDCE86274B3BC4A9011298698974E2999704B97516A1865945366233D6BC0A17

C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\Quick Launch\Launch Internet Explorer Browser.lnk	Delete	779	unknown	md5:B06F9AAAAA4AA8F772F534EF6D993D8C sha1:37c8f81d42e9664cae0348218b0bc97d60a80042 sha256:2B241CF87BE49074416A5D46AE4C9E8D815420A8380BDFD8F86141B2B9C82CC1
C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\Quick Launch\Show Desktop.scf	Delete	79	unknown	md5:E48BC01B750611594F9FDAE9A51A38C9 sha1:70e3055fd87c7fb0caee782b26ee5a8795a05fc1 sha256:18B81242E5546D55CF8C3BF787522D3AD43D9BB201B32E39F3004408B1AE8410
C:\Documents and Settings\Administrator\Application Data\Microsoft\Office\MSO1033.acl	Delete	37814	unknown	md5:099EE3BF07EA6B948B5E569E72807192 sha1:a6783fbcf096fb3cc409a4598705578e1e2f6667 sha256:16565E3B09F437274BCABBD54A393A5DE21C57EC946746C616E28EDBC44F466A
C:\Documents and Settings\Administrator\Application Data\Microsoft\Office\Recent\index.dat	Delete	28	unknown	md5:4E30A3397E81DD38A188E78FC94E5A77 sha1:95e2efa493065e02c7370befbe5a4bc1340cf5ef sha256:DDD0B5A9B8BD9275DDD6BD1D9D033C56734A5BB184B4371E50C2200B9033397CB
C:\Documents and Settings\Administrator\Application Data\Microsoft\Office\Recent\Templates.LNK	Delete	794	unknown	md5:8AD0FE6C1377D2264E460A0DE4AB3C4E sha1:60599c4316164bedc5cbff73a65d31384e78e8b1 sha256:7453466876C5805D34BD707858C052C54D84297D258BD22AC2E03BC90041F71B
C:\Documents and Settings\Administrator\Application Data\Microsoft\Office\Word12.pip	Delete	1684	unknown	md5:CDA8D8E26A37CC7BBDB37982CC2A7239 sha1:5a897749f0d0e8f7121457e354bb364e7a372d6a sha256:CD7CAF8BA7FE0C0D3D65C65DEE5B1049EA2AC1C984C68885EDCFDFB9AF865F49
C:\Documents and Settings\Administrator\Application Data\Microsoft\Protect\CREDHIST	Delete	24	unknown	md5:B636D5E8DE89B3BDCC573EBEB7556533 sha1:a880657b2240eb7f671cad49397006de531485 sha256:9B4A1F1BC830E1371FFB390ED95B2CB5EE98DD242F5EF425762F3572B361DFE7

C:\Documents and Settings\Administrator\Application Data\Microsoft\Protect\S-1-5-21-515967899-776561741-1417001333-500\ab794fd6-d34c-4099-af74-1537114d3efb	Delete	388	unknown	md5:4AA757E9F8CCECEAE93E58C894E8A4AB sha1:89eccc7a17506 35cca9ae6ef2f5fd83 81aa3e923 sha256:97C46B32C6 414C9BEF07D2C89F7 83FDB83726424BAF8 A5F296283D251046A A4C
C:\Documents and Settings\Administrator\Application Data\Microsoft\Protect\S-1-5-21-515967899-776561741-1417001333-500\d70dd719-4143-488d-8f0a-c857b04fa79c	Delete	388	unknown	md5:57C7B3461FFA8 D282F1E97649B2D38 53 sha1:974e6895b6cd1 f142b5649db5016d0 673dd9a14f sha256:4DD9254D69 2B44ABCB56A2A00D B0D7A02F8252AA8D E1C36BD6626D0495 6B1477
C:\Documents and Settings\Administrator\Application Data\Microsoft\Protect\S-1-5-21-515967899-776561741-1417001333-500\Preferred	Delete	24	unknown	md5:9C9BE91115EC C17925A237EEFDF65 222 sha1:ed8fd047572f0 136a80ea5af1645e8 974327ed75 sha256:DBAD488C2A E636C4028E87338E0 BE721D7A140B19FA 6F3C61E734A3E16D2 CBA3
C:\Documents and Settings\Administrator\Application Data\Microsoft\Templates\Normal.dotm	Delete	15481	unknown	md5:D247A49C9A15 29EFBEB4E644655E1 206 sha1:4f2e17b119b3d eb8d56dbcb4740326 4b50dc8e6e sha256:28DC4E075D D70C540AE38DE923 5E1BF5A975ACAEB3 B2A380302A76E4B04 472D0
C:\Documents and Settings\Administrator\Application Data\Sun\Java\jdk1.7.0_04\jdk1.7.0_04.msi	Delete	439296	unknown	md5:6C70FF59B48E3 1A6ABF420CC63A1D 6FD sha1:8dcde8046ebbd 388541dff96976daffd 781f7dcd sha256:43A7948821 CB50D3624E67F6274 37DDA2C9F1B9E7F4 545DA2E9DBC05214 E2F2D
C:\Documents and Settings\Administrator\Application Data\Sun\Java\jdk1.7.0_04\sj170040.cab	Delete	17763424	unknown	md5:8B53D80D45C9 BD29B79DEEBA9448 3AE4 sha1:af4c1931f0904f 8659827d1e81ef227f 8760babd sha256:C444DC505B CA8A83EB4831DFE7 ABEEE75615821E9D9 38E9845FDEEF86E6B 9152
C:\Documents and Settings\Administrator\Application Data\Sun\Java\jdk1.7.0_04\ss170040.cab	Delete	18619452	unknown	md5:8D54F9C585E4F 58A7B8391405D55C 18E sha1:7a890f76e9a22 9f1f0ee7e953dde465 c74a5a6b5 sha256:FDD38424C6 2F7C6F32C9E4E38EB 6CF7377E61E9B9C12 F6E2A6A27E147194F 6B2

C:\Documents and Settings\Administrator\Application Data\Sun\Java\jdk1.7.0_04\st170040.cab	Delete	36034650	unknown	md5:41D4824E596A39ABB66BB8A16FAF501E sha1:f6d19918b06b1a968f8eb6f69c989790bf226bfd sha256:C55E71C4A5A0B2C0383FC05BF60544DB7F6058E3BF24CAC3A101A6478C6C50B2
C:\Documents and Settings\Administrator\Application Data\Sun\Java\jdk1.7.0_04\sz170040.cab	Delete	1640	unknown	md5:8280BE327E8A17EDD43C1D8A3A23F024 sha1:f9f63937135cf5d77c71932a108f69c62a7f7d40 sha256:45093EC0BAD6C076B58A461B09A8A7AC4500974CD52ED098DF952CD8E400950E
C:\Documents and Settings\Administrator\Cookies\index.dat	Delete	16384	unknown	md5:D7A950FEFD60DBAA01DF2D85FEFB3862 sha1:15740b197555ba8e162c37a6ba655151e3bebae sha256:75D0B1743F61B76A35B1FEDD32378837805DE58D79FA950CB6E8164BFA72073A
C:\Documents and Settings\Administrator\Desktop\my.txt	Delete	14	unknown	md5:58C14F51D2848978EBC83AA63B960226 sha1:799ba09aca7e24a13a2720ac7ab2796dbe3d3d06 sha256:B3790CCDC8E1761507B0EDA509A0F4192BC1BC54FF0E5B03559ADEF8243CC9E6
C:\Documents and Settings\Administrator\Favorites\Desktop.ini	Delete	122	unknown	md5:FC2BF37169C033A08C1FD7680193CCE2 sha1:b1a6760eef6e3d7173dde13ad1c857a5d6bb8dea sha256:DF6E1089C40792E65F7D7FA7BE72CC259E806E97A4705E3606B44A70D15A1F25
C:\Documents and Settings\Administrator\Favorites\Links\Customize Links.url	Delete	119	unknown	md5:A77F34473C879B9AAE3E740CCE83F22A sha1:582ce2ca4e09e77de7353870271c198f395d8c06 sha256:A461CAF605B6C8663E76F69ECA0575006EBD973D2A3075D055CE2A2CF4EDC745
C:\Documents and Settings\Administrator\Favorites\Links\Free Hotmail.url	Delete	113	unknown	md5:AF6E95C36B3B46EE55069D1DF58E447C sha1:bb92b0c87ee4da1afb344077492d12489e9236f2 sha256:88BB11A76D33E48B48F6595A962197D19F9F789B483CF04B5784650E184B1E9B

C:\Documents and Settings\Administrator\Favorites\Links\Windows Marketplace.url	Delete	169	unknown	md5:C5DDE638802F2C7330E80AF21631BF6F sha1:bb95f564144f7e4bc55b4fe06f1af2d0e2e1eccc sha256:F4682FE575763927903D9C9E5909F6B3C5ECAD2D7E485BF2741AA18B801EA0E4
C:\Documents and Settings\Administrator\Favorites\Links\Windows Media.url	Delete	118	unknown	md5:EA19BA73DA8590BB67D3B74898C39157 sha1:4d5814b3e7acd96e149923f7aefbddb548d6 sha256:E5E9DE295078DC14100BF67DD6CB065AEB6491BEA1DF45998094B52505EC2DFE
C:\Documents and Settings\Administrator\Favorites\Links\Windows.url	Delete	113	unknown	md5:DA9795AA8165E2F6B85D7B264A22DD04 sha1:4dc652064187535c2591ab696e8c971a5682706 sha256:9586141540623E87BCACA6F3572DD8D10AC06F01D03E8C673943F179187BC368
C:\Documents and Settings\Administrator\Favorites\MSN.com.url	Delete	119	unknown	md5:373CFE6A691B83DB74C3305E2F7153B7 sha1:4571eede9bb66aa68fe3bb5efd8570dca5a5659b sha256:82C7F097AF41BFBA80C9C480F14FD5B220F655DB541C14209AFDE66AEBB84EA9
C:\Documents and Settings\Administrator\Favorites\Radio Station Guide.url	Delete	197	unknown	md5:1FA4346AB5041BA3583BD339D515307C sha1:4191103973886785b478db6d9707ce5f519ba91b sha256:DC49EDAD54ED2316823E05A2FE9A3A5A78AAD0ABD1C56434887379A4CB5BBC79
C:\Documents and Settings\Administrator\Kernel\core.inf	Delete	1814	unknown	md5:347D4603EBC6E627B3FDE7EA9BF16DBD sha1:2c34e3c4b129b6599ff540b9c2101edb765b25d5 sha256:AD88245C54097AF87BB23BE237A77C6C09FB172F677403242C69373BBDCAC9CF
C:\Documents and Settings\Administrator\Kernel\core.sys	Delete	29184	PE	md5:C083C737F43A141ACFD8805BCEEE83CC sha1:a8d11918273822245d8249c9c851726e2d8c740b sha256:7A4CF4FCFC048D32F2E58AA8E0D2406B1CDE80DF6B7DD530F408C25514645742

C:\Documents and Settings\Administrator\Kernel\PAN\ApiRules.rule	Delete	1	unknown	md5:01ABFC750A0C942167651C40D088531D sha1:d08f88df745fa795b104e4a707a31cfce7b5841 sha256:334359B90EFED75DA5F0ADA1D5E6B256F4A6BD0AEE7EB39C0F90182A021FFC8B
C:\Documents and Settings\Administrator\Kernel\PAN\FileRules.rule	Delete	5263	unknown	md5:78824A3F3ABAEBFD7E4143279550B963 sha1:90e2f34ed5e568b78f5aeeb4f4e59d716087220b sha256:C38B42DB740277B08342DB7B73D46552B79AC148CD1809218F62E6D533641F0A
C:\Documents and Settings\Administrator\Kernel\PAN\NetworkRules.rule	Delete	194	unknown	md5:EEE0E7366BCEF5BE13F75D186ED9F54F sha1:b929632125525601aaea91677cdc7311f294cb3f sha256:2EAADCD0BB0BA15445D9DE58C1239A3CBD13A358A73BFE42FF4415E301C1FF35
C:\Documents and Settings\Administrator\Kernel\PAN\ProcessRules.rule	Delete	957	unknown	md5:1A72838A00B61C80F3F11C64FD5C348A sha1:cc877610c6ecec162bffcb2d377e0d85f3e701f3 sha256:8D24E271483EFBE4F38A4A860D0F96614B8885B34A4D3381C22FC91BD35CFB10
C:\Documents and Settings\Administrator\Kernel\PAN\RegRules.rule	Delete	14003	unknown	md5:B79A302A973557E5B876DCA592A6C2C5 sha1:4fe77e42e488a8673234d1c18401bc7beaf1e2c1 sha256:A5C1F6323D02B4105F78F1C01AD0D5DF79B1190B49CBCFA236FF8D11D0FBC909
C:\Documents and Settings\Administrator\Kernel\pnfs.inf	Delete	2252	unknown	md5:D4D9E8F263DA9B99B13B75E698CF2D71 sha1:bb3a004b561892cf8cdee361d6f8bec732513009 sha256:9D572F3529D7F799777CAF47655425B7D9623EE0357EF1C687010C4956EB99EC
C:\Documents and Settings\Administrator\Kernel\pnfs.sys	Delete	38400	PE	md5:C974D26F12B5CEC1BC690FD5C789D3E5 sha1:c8bb7c9431234d4c7328ce234a406d933ab2d0ab sha256:528FA517D4AFE0E2D7A42AD81BF2B869C075C7F809C3107BB6AA4015D841DC9A

C:\Documents and Settings\Administrator\Kernel\pnfsUser.exe	Delete	15872	PE	md5:B877332F23721338D5A0DBF42517CCDE sha1:aefdf01780b6bc2131fa1fd25a79e135c0371a9 sha256:32101682154B9F70DCBB9EFD4D6807A6721B07F0FF8AEF20E22D0C4D0901C08F
C:\Documents and Settings\Administrator\Kernel\x86DriverKickStart.bat	Delete	267	unknown	md5:87F5BD306550F82AA1245419922C4E97 sha1:c16d709117c42cbfb637bcd47651d11cf6085dcb sha256:7902A3215CE7CE5A4DC81E9049D14AC2B41A7E21DE9A72255E2080409DD930A4
C:\Documents and Settings\Administrator\Local Settings\Application Data\Adobe\Acrobat\9.0\Updater\updater.log	Delete	1254	unknown	md5:B9463BA05A6FB933BF315CFE6C9F77CE sha1:bcc67bcb7a672cbb29eabf4c78f47dd5a5745 sha256:F768A669C142A947610212478F3C718F069DE298BFFE47B96060E8FD142072ED
C:\Documents and Settings\Administrator\Local Settings\Application Data\Adobe\Updater6\aumLib.log	Delete	765	unknown	md5:04245DD200CF7052B7793DB73753939D sha1:d03ef82998b1ace9ae94b6dd57d934a394d9c41 sha256:3BDFB919E08483F5025F988B9C9DA415DFC8D759451A25E00D628CA66FF3086C
C:\Documents and Settings\Administrator\Local Settings\Application Data\IconCache.db	Delete	3747524	unknown	md5:A1A0E970FD0FE5DFE12328880FA74716 sha1:d29d1cf5766f742e2fd4f992504665a6d234e53 sha256:AF06AB27EE093F58FB6F17EFB61A700FFC57A294A377CA339EB988BEE4DD9753
C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT	Delete	16384	unknown	md5:B04089E63B11CE4BEA530B6735096270 sha1:7ceb7ea0c9c6a27c96300c189e3cf207d1ebc86 sha256:EFD266CE63DA02267AF2D497AEF2BE6E288D25A92AFEE26F01E775DFF476AFB9
C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Media Player\CurrentDatabase_59R.wmdb	Delete	720896	unknown	md5:921E244B6658EAD12894DBE622314986 sha1:b830f09a667e048da30f05842498ceff7b0d2999 sha256:1C43E769E16213626FCD3E5B80FC04A73E7EB87ABD48358C11FAE687F472E151

C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Wallpaper1.bmp	Delete	1440054	unknown	md5:9537942A400B7E0C9871A15970826D23 sha1:a838ad4f3a10002fbde73fdb6e37ec0ab07e8de sha256:11E7001F541A04928A9239835B577123909044B34FCFD7C215CC80EADE43245A
C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD	Delete	498	unknown	md5:90BE2701C8112BEBC6BD58A7DE19846E sha1:a95be40736982392e2e684fb9ff6602ecad6f1e sha256:644FBCDC20086E16D57F31C5BAD98BE68D02B1C061938D2F5F91CBE88C871FBF
C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows Media\9.0\WMSDKNS.XML	Delete	12787	unknown	md5:9020CF6EEE6267257FCE8145A8DD10DE sha1:9fd99feb4ddb819568eb8294ff4020cb17ccb sha256:F12ACCEFD2303A274B879806A902E51CC7F93F054B6395DA1EC46E5229BAE009
C:\Documents and Settings\Administrator\Local Settings\Application Data\Mozilla\Firefox\Profiles\mp6o6ly1.default\cache2\index	Delete	6	unknown	md5:6C4B27156931889528F5BEC30E25B3F1 sha1:165c0d195e773f66423a873ea964144cc4e92b62 sha256:9A741481EB4561BF9C0F64BD5C88493919962171CF4D6828833660D9D4816F5A
C:\Documents and Settings\Administrator\Local Settings\desktop.ini	Delete	62	unknown	md5:AD99B9121E1C94D9B6FEB18B3573A02E sha1:589c5259ea80dbf52a074645647a883d41482265 sha256:DF2C10A79522275B1D560064FD09EE298AAC8682DF94F6B9947C4407D897B0A6
C:\Documents and Settings\Administrator\Local Settings\History\desktop.ini	Delete	113	unknown	md5:D332CE83B166D5C244D22587AD75AAC4 sha1:d00d4ac1e74d3186bf1aaa01400a02b9df87224f sha256:02FBF2431714ED3902C2284AB91A22ACF4D8B2CFB3FF77B0B55C21A29027F250
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\desktop.ini	Delete	113	unknown	md5:D332CE83B166D5C244D22587AD75AAC4 sha1:d00d4ac1e74d3186bf1aaa01400a02b9df87224f sha256:02FBF2431714ED3902C2284AB91A22ACF4D8B2CFB3FF77B0B55C21A29027F250

C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\index.dat	Delete	32768	unknown	md5:F636580D47036580378977877C9D13E8 sha1:f87377de6f1b52a270984b1dde2bdb8f1fd829b1 sha256:8FCC0F14E4F3EA3208626E49C9A1F3A703CB80B83369139FF70B7F3A454DD9D3
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012017090120170902\index.dat	Delete	32768	unknown	md5:70B3E6DDAAF9BC0871A3F25FBCE0067D sha1:4fe605f64b36dc6858d994adc84ab10029fe05d7 sha256:1B5FBF4386F8F26D14966DA57AEEC0204E9CA8F3B46F54DB15D6A8DCE746BEFC
C:\Documents and Settings\Administrator\Local Settings\Temp\AdobeARM.log	Delete	49274	unknown	md5:CD093302D932D9294229242 29C2C9D81 sha1:5507d2e0c052eec376f58523f4b5e1365f86e4c6 sha256:534762A5BF53FBF68EE464A9BE3AF24C3F55CBBEC035FFF06248B1B0CED2F94B
C:\Documents and Settings\Administrator\Local Settings\Temp\ASPNETSetup.log	Delete	7200	unknown	md5:66C86F4DFEC9CF815AF744B865A9FBDB sha1:485e1027a26e1dfb774442252bebf752e4d12164 sha256:A1C34347A434DD8D8504C8D28F477BCDCCD84A0922A7EE640B6A6090244CDC49
C:\Documents and Settings\Administrator\Local Settings\Temp\ASPNETSetup_00000.log	Delete	5290	unknown	md5:C5B8F0D956B7E65593CA59937D0D964E sha1:db44cb5ac2c69162c836625e46f57c4d50f22bdb sha256:0CCE555BBBD9A055D203C1C3A443076D63CA316E0AC47D6A6C1E9566D9F96D81
C:\Documents and Settings\Administrator\Local Settings\Temp\ASPNETSetup_00001.log	Delete	6792	unknown	md5:6F56B5D4F20C5754ADD1C2BE1217E18A sha1:97445f2c9c7dcf07dbd26fe1102fc15b461787fe sha256:88DC6E70A7FA53DB30C55658D06E10C45F04FFB2EAF29CD33F05B53E7563D817
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_clwireg.txt	Delete	7944	unknown	md5:A409DEA89F59C8911BA67B81F03DE4C2 sha1:890e7c9434a0fd616b75dd48f8a06e4cb367e468 sha256:C937220AEEA7ED75FF1E6287356EE45FC92968110A557E1C18B88CAD9E052F87

C:\Documents and Settings\Administrator\Local Settings\Temp\dd_depcheck_NETFX_EXP_35.txt	Delete	231655	unknown	md5:E0063DCF6E318DEDD6D33AE203B09BA1 sha1:13070f9f977e03acc9323a124ece1ae780da87 sha256:6348B144863864E7F48883745343432FA84C220D43939CE10A711EDF3DF1F899
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_dotnetfx35error.txt	Delete	2	unknown	md5:F3B25701FE362EC84616A93A45CE9998 sha1:d62636d8caec13f04e28442aa6fa1afeb024bbb sha256:B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_dotnetfx35install.txt	Delete	376420	unknown	md5:605EB967C9FB4BD32F5469D22CE9CB29 sha1:9de510ab1b0e82ae3aee52c4564797af38a99a3e sha256:28D1C855BA8DA51A6C3EEC486F0C4B64CEE4C454A6503E0F783C0087A7BD93A8
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_DOTNETFX40_FULL_X86_X64_decompression_log.txt	Delete	1293	unknown	md5:DDE743B6E1BB82246A3762A2FABA3A5A sha1:1aa6be435f7f0023f66902624c8570fae5ce975a sha256:188BB3AF7697CAE2249D3C5BA9CD99E9D719EDEEBC3CAB87B7B1D00BE347B58D
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_NET_Framework20_Setup67E0.txt	Delete	8320784	unknown	md5:A0743A81B5354E9B08D9A707CC2E2BA7 sha1:d755cfe5a6543b69809f8c1254113c8c2d37ca2b sha256:83C9A0A3B0AF0BB97D0E399850F0777A92B861E60350EF5A498D934610BFEB88
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_NET_Framework30_Setup688A.txt	Delete	3200506	unknown	md5:FA3869ECF2796C30F26A663AAB9048FB sha1:3102a7fae855b95b504e4dfa9c25b42f47f950d sha256:51E2006792FB65D81C3C14223DFC1A9A543217CE18C2D45A9326418A94C3AA3F
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_NET_Framework35_MSI68C8.txt	Delete	1446034	unknown	md5:5C25E828E563CB7E597A44B5B9A43C1D sha1:221a35bcd7166216dc6fdbfeb54dd87edcf318f7 sha256:1342FF502BF6BD087238E6BD0F7DE94481AA7F6FFC196818E1F15B8EA15201 8F

C:\Documents and Settings\Administrator\Local Settings\Temp\dd_RGB9RAST_x86.msi67DD.txt	Delete	135722	unknown	md5:8A4225394CBA859DED2B562C6CE37AA2 sha1:ee7f35dfcb8f45b21bc959f449f34c9a533d3340 sha256:1590644EE0F896442D5967E6417B50D39BCBA3984625A044915500719E574352
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredistMSI66E5.txt	Delete	550238	unknown	md5:1CE3BD4F5765ABA47D6EAC869D2249E2 sha1:23cd5c2cd7a2533c329b72c1467d2381a2edec4 sha256:4401ECF7CBB73E41AD91AA1EBDCE7111C94963DB84FB6C0533BE3FD25E878386
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredistUI66E5.txt	Delete	11734	unknown	md5:96E1E858E4046975408398F673E7BF5F sha1:4406c06010f2278f4eb65f3d7a9bbebbfd66a6bd sha256:3CA3BE294081D9CFCDF737D3B184823D3F2DE2A76A640EDF61620ECA57D5206E
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20170901164055.log	Delete	9302	unknown	md5:224970F71B6FC368665F1315AA559C2A sha1:27b31cc5cd8dd1845f067faf412156a059057b50 sha256:B300050C3C6DDF5DAF486C54CA2BFE12093D253A08E0DABE72DD4E31D289D747
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20170901164055_0_vcRuntimeMinimum_x86.log	Delete	169228	unknown	md5:83F396B9DE4DAF99E72125783AD8B993 sha1:8b54407e102dd9cd84d3127193ef980ae3304444 sha256:D9CAC349BD06A287004256F61FD8AD293BB2D12D0199F5547513EE711F6DB5E1
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20170901164055_1_vcRuntimeAdditional_x86.log	Delete	223342	unknown	md5:3615C3B306E287B6193EA7F069E57364 sha1:9810a29578ae64cfbde356fbfec9a2ddb0f085df sha256:0E07872B85457B855E5D4C70CF6E276B02367CAC0BFA6CF0300EE6A7DA2FA9EF
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20170901164059.log	Delete	9039	unknown	md5:FC9F37DCD7109E6144D8FDB911F42584 sha1:efe2d5b83d811e1092ac56296d0b4d1e6942e95b sha256:894BF3B552A8FBBE6DBE413F8FC2867BACD24F777DF3A6230DFCA7D5DF48C349

C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20170901164059_0_vcRuntimeMinimum_x86.log	Delete	165156	unknown	md5:C97559E2164BF758975663FE93DB3EAE sha1:cde53b3c382576f1b66d801f35dc913eab6fb876 sha256:60DEC64C7DF2CC150F5CE3E13644F864507A66C94B8773D397CFE39FBDFC2BA9
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20170901164059_1_vcRuntimeAdditional_x86.log	Delete	215276	unknown	md5:66DD1B67EB811865176CE06873A40427 sha1:1a149843c70cdadd8468026a1a2d36f5bfe07f sha256:14FBD15C8926B4109753AB6595C27D5EDE055402490F5FAB09921511F4456249
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20171017124041.log	Delete	16464	unknown	md5:5577F8B13B5873C665DE3884B95ED520 sha1:6d989caab581005baefe769259f154bbb961c045 sha256:5DD1F7B890B1B8E9AED2AAD51514D5DF2F8722B76557F21B209FD21E34E03904
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20171017124041_000_vcRuntimeMinimum_x86.log	Delete	245916	unknown	md5:D49B432F8772DA9660A8978C7E0AC2C3 sha1:803c25e4b86e633ae4abb061cfa99876801ec3c sha256:58F0EDE587BDF6B21101ADB857946DE1CC659838E7FB4F9F525F8622378B0F15
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20171017124041_001_vcRuntimeAdditional_x86.log	Delete	214624	unknown	md5:67C495BBED508F2012352A3B2D6616D8 sha1:a03d6beca84a036abc41a5e1ce0228f536c86611 sha256:DF50BFACF88721E24E3010995547EA245EB2E28F2BC5A8F56F33C55787B6B32C
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_wcf_CA_smci_20170901_234704_093.txt	Delete	3752	unknown	md5:365AACC701F563BA4776B1D72D842DF6 sha1:92a889e2ef97f5305d3126546a0631d8b7d2d987 sha256:A8B2EEFEC48DF848C7448884E1A9DAD28A89014028147BFEE9CCCA9E2F138050
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_wcf_retCAA48.txt	Delete	4329	unknown	md5:CCB9BE90919AAC0AC10046D13B6F178E sha1:6dd00a28bc0d102a6e5601c715d6219e94ec98a sha256:116539F721D2AA787906E1449CE2E1A88D1DF3D2A4665A02709A0173F33064F0

C:\Documents and Settings\Administrator\Local Settings\Temp\dd_XPS.txt	Delete	12337	unknown	md5:1DDD59787862F4FEE1E90EE9827BA54A sha1:1ec6f7d2ff676180ec4a8672fee96f0ce4344d7 sha256:FF04A71E0B13412D2FCF921B34559F8C5A7D802FAD2433A3C6651223F697B4BA
C:\Documents and Settings\Administrator\Local Settings\Temp\dotNetFx.log	Delete	2430	unknown	md5:31E0F4D658A53AEFB956BAA720259097 sha1:8f1e477cbf1b906c2a67ed5163fd40942a5d1af5 sha256:C981EDF19A9C162DE1B52B87DDD3684BEF1E1A3BCE166C446F5430A3C32EE2B9
C:\Documents and Settings\Administrator\Local Settings\Temp\java_install.log	Delete	70070	unknown	md5:2E182E232C79C47800D0BF4499D0F92E sha1:7db05186a5ef054ab09e069f34474d9de0f9f797 sha256:99FDE9E8B763384A176BBD7D0DEDEBFACEEE5E596112C7B8C8EEC965F85FE901
C:\Documents and Settings\Administrator\Local Settings\Temp\java_install_reg.log	Delete	208	unknown	md5:37D4F8C7B4E7C123675F232737B026E6 sha1:23704b15416dbbcc8c0657cb6da6ea68a3f446a6 sha256:AC7B40B821E2350000D08697CC37F9D8BDA32D53CF949A269F66C59B67D49407
C:\Documents and Settings\Administrator\Local Settings\Temp\jfx_inst.log	Delete	287	unknown	md5:9C15C771FE24D249067560C52D558F77 sha1:978ec6af708a0f3191c420d5c89fac8a5625edd sha256:9C02A19B4F7B0F4FC90CBA77DDF552BB5857A43F742874610F38F4C3C2984288
C:\Documents and Settings\Administrator\Local Settings\Temp\Microsoft .NET Framework 4 Setup_20170901_164343750-MSI_netfx_Core_x86.msi.txt	Delete	5042700	unknown	md5:000314F7AFFA992A16C3C314FA9471FF sha1:5dcc65c396070cfa34c1b32b9d5681d0d8dfb03a sha256:158540D6692F8A93FD723D197767D8053D2B1F73B6470C98C7F0A91048E72F7C
C:\Documents and Settings\Administrator\Local Settings\Temp\Microsoft .NET Framework 4 Setup_20170901_164343750-MSI_netfx_Extended_x86.msi.txt	Delete	2096910	unknown	md5:F902FEF25C28110EB02783A999527005 sha1:9f0357643e7ce7eba9bd45651f4bbf68a176273 sha256:A10C01231144ED3277A6D6EE8555693A618D5C240268BF19CB7301D43586AD8F

C:\Documents and Settings\Administrator\Local Settings\Temp\Microsoft .NET Framework 4 Setup_20170901_164343750.html	Delete	696980	unknown	md5:AA4EBD49689E1418D8B4860D13C34494 sha1:617f0c1b75cf4bef1da4c31abcd4d417c0c4659c sha256:734161F43E13D618D29360BBF3222554B63D4AE89BDA82E0AAFD48448B230CED
C:\Documents and Settings\Administrator\Local Settings\Temp\Microsoft Visual C++ 2010 x86 Redistributable Setup_20170901_164050734-MSI_vc_red.msi.txt	Delete	279314	unknown	md5:63C31FBA577E7CE489C240C6953412C2 sha1:95eb8c66d0186f1f82c62213e9121ba15cb62df sha256:98485BFE60C175E5ED236E75D26D12E1B98E9A0B97DEAD01CD2634EF62FCB220
C:\Documents and Settings\Administrator\Local Settings\Temp\Microsoft Visual C++ 2010 x86 Redistributable Setup_20170901_164050734.html	Delete	76812	unknown	md5:F1EE3A260407429FE4A9F674B086ABA9 sha1:e6bbe9c824621daf9d464047e8473ff7c5a2fb1b sha256:FB0F153055681DE5A75CAEE7E6E2EE6985A8EC01C876C14A73F86475513709 63
C:\Documents and Settings\Administrator\Local Settings\Temp\netfx.log	Delete	2881336	unknown	md5:BE93858C704D27DF98406AAA17D9EEB3 sha1:57babc919613fe9e28922a14e011011755bbf049 sha256:FBE0E0E02155272837E66C05184D9F1C18179218BDD22D99D49BA184246FA2BF
C:\Documents and Settings\Administrator\Local Settings\Temp\nsg9.tmp\modern-header.bmp	Delete	9744	unknown	md5:940C56737BF9BB69CE7A31C623D4E87A sha1:f2f3b4e7b9c28df6687ceeaed300a793e3bac445 sha256:766A893FE962AEFD27C574CB05F25CF895D3FC70A00DB5A6FA73D573F571AEFC
C:\Documents and Settings\Administrator\Local Settings\Temp\nsg9.tmp\UserInfo.dll	Delete	4096	PE	md5:C7CE0E47C835525983FD2C4C9566B4AAD sha1:38b7ad7bb32ffae35540fce373b8a671878dc54e sha256:6293408A5FA6D0F55F0A4D01528EB5B807EE9447A75A28B5986267475EBCD3AE
C:\Documents and Settings\Administrator\Local Settings\Temp\ose00000.exe	Delete	145184	PE	md5:5A432A042DAE460ABE7199B758E8606C sha1:821b965267ee15c6c59178777ae7a8dcfc80f4ba sha256:6E5D1F477D290905BE27CEBF9572BAC6B05FFEF2FAD901D3C8E11F665F8B9A71

C:\Documents and Settings\Administrator\Local Settings\Temp\SetupExe(20170901173709298).log	Delete	104612	unknown	md5:F2101D2C4B9000FCAF11B5D696AEEAE4 sha1:3d84231077ec9f40980fc51ae3f00109c215d3d8 sha256:1959A6804BA6C419637260AD5A1ADA2C7534A0187A8B0E50F4E7CC5BD82975F9
C:\Documents and Settings\Administrator\Local Settings\Temp\uxeventlog.txt	Delete	29700	unknown	md5:9BABEE22FDA8737C9B74F7756E655692 sha1:c731765bc8e17273d88cf671308053542738ead9 sha256:662A5E91317D5FFD4EF1FA69CC66B9EFA73725A369AC16BBE2BB337E866E10BE
C:\Documents and Settings\Administrator\Local Settings\Temp\{0198CDCB-40EF-434E-AEAC-ED6C041CC970}\setup.isn	Delete	84949	unknown	md5:3813B8C0C6D48ADE7685388D64B3BDDB sha1:9fd97c26a12b98f6341dd3ef60378ddc134fb2f5 sha256:7F8575E818BA4037344DB0F891A89104DA41D3E44029EC693167B1318E540DEF
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\0L67SDQ3\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\4T6V8XAN\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\8HYB0T2N\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38

C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\GL63GHE3\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat	Delete	32768	unknown	md5:ADB3244DBA3219AB6130C1175470E0E9 sha1:7e1f4ed4ae85ebb3e0ec43946c96e5b74c861ba1 sha256:E14F45A2D549FB95D2582FC5B974744408D71074B368759B73B389FC8497EE73
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38
C:\Documents and Settings\Administrator\My Documents\desktop.ini	Delete	84	unknown	md5:2EE411B655413751A5615ABBEF874CD6 sha1:67de4e377d69562f8d57558e6cc5144274d96ad sha256:C5A6EA5297A65F36B8A6C7426359DC8C24D532C2443A412398443345442B6DD9
C:\Documents and Settings\Administrator\My Documents\My Music\Desktop.ini	Delete	189	unknown	md5:D147365112F4E31038E5AABA2D70AB52 sha1:44b36c5debbb8c8cb907f36e70e496067b792a2e sha256:84F7BD965F91BDD1E801A7DD4E56649247952225EF70535E7A68F2FDF4FD9CF3
C:\Documents and Settings\Administrator\My Documents\My Music\Sample Music.lnk	Delete	638	unknown	md5:F2F20F6B4BB0FC4D455282A73028DA63 sha1:9378a20470a891921e31ed0146179b1a615398ae sha256:E815F3CB8EE3DF57C1543BD3017CA65955AEB156B7FA634E9EF0658851D2BBE5
C:\Documents and Settings\Administrator\My Documents\My Pictures\Desktop.ini	Delete	191	unknown	md5:D6254CA9BC0BA25006DABC24972F6D9E sha1:8270cfa9dffa36f94d53bed24945438ef0246d84 sha256:01B5217F714A239251ABD415B45CC11D54B022628DB46BB9FA4D19C2C375B13F

C:\Documents and Settings\Administrator\My Documents\My Pictures\Sample Pictures.lnk	Delete	668	unknown	md5:FAC834FB51D0D90774E6BEBD491BD0AA sha1:276436fcec720d23f4a14420adfa6634ceb69bc sha256:1DEEB23F62F0171BF0E0F76A04884CB64935A2641AF6F6B8E1A04152BCCCCEBD
C:\Documents and Settings\Administrator\My Documents\my_bank_account.rtf	Delete	272	unknown	md5:3315E3B9CBD373AF0BF4850A3B0E8D22 sha1:a0d1803a2de8a55a73cf157d5685b24be8bb230e sha256:F673ACECB7291704B8D8E9E6478E55E8490AEF68021C4F2D94800A796CED0F7B
C:\Documents and Settings\Administrator\My Documents\my_password.txt	Delete	54	unknown	md5:C38365CDA2216812EC2FF3E6B92B0FA7 sha1:3abfc5e0963a8733ddbeaf6fc8ef7bb5545c1ea3 sha256:6AC09900900C75895436DB42194C81B3937879901FAD68667B30F301EAFBDD9F
C:\Documents and Settings\Administrator\ntuser.ini	Delete	178	unknown	md5:CBDA6984D2ECC537AEF07205AE001013 sha1:391c151586cc0a011bb54277a3b79bb7436ce0 sha256:1D5425680452D0BB5E7DF10DE4319F3BE616EBDB5D505911259D5A86DD50C7F3
C:\Documents and Settings\Administrator\Recent\Desktop.ini	Delete	150	unknown	md5:4365E54D9A4F05CC52EDBC7D79D0E13C sha1:8b41436849d4ee5851d1d87bd047dc001840351e sha256:260E4ACD97E1CCDBCCAFF905F12797B75080003702E87529B491523421BD8D54
C:\Documents and Settings\Administrator\SendTo\Bluetooth File Transfer Wizard.LNK	Delete	711	unknown	md5:62C4284E52868891193DFBD377BF379CD sha1:9ca9567f96f6e42aff0a79b56df8df6364baa044 sha256:1B34295DC6479739B583D1259BABA087906D84B4BF0C57CAEC90C4DD18507B13
C:\Documents and Settings\Administrator\SendTo\Compressed (zipped) Folder.ZFSendToTarget	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Documents and Settings\Administrator\SendTo\Desktop (create shortcut).DeskLink	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A

C:\Documents and Settings\Administrator\SendTo\desktop.ini	Delete	257	unknown	md5:EE5282A9CF6C77A3CB57F8DC9D538848 sha1:29115b363f5974387a25f1d69cf1f9c184ebbbf sha256:7C69EC4039F09AB356262EC7F5B27101B9124F05F75ACF45DAFB0F4556321186
C:\Documents and Settings\Administrator\SendTo\Mail Recipient.MAPIMail	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Documents and Settings\Administrator\SendTo\My Documents.mydocs	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Documents and Settings\Administrator\Start Menu\desktop.ini	Delete	62	unknown	md5:87F8888E1D77D9CEF69E901A97D40D73 sha1:72cdb185c7d8d1a7527abc1315be5cc55994a976 sha256:D18EC25D468D4A735EA38C8DFCD694827BB873F00BD67BD92640B850C41C356A
C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Accessibility\desktop.ini	Delete	348	unknown	md5:9F7D56E96FCE7AF0E7599AADD8126239 sha1:cfcbb8e4e0c32500fa5bf9382b103c4199df0276 sha256:B369233C0BE9CE04678FFE71BA9895C3EAF018E4B949A7686647560729B08A45
C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Accessibility\Magnifier.lnk	Delete	1525	unknown	md5:063E1437D5D526E876446B90C184332D8 sha1:6a058523ac6584b68c91ef5a9bbf1877b2f40ab0 sha256:13B6C8D82415298049BA27DE236A3EFE530CCD436282705760AAC113E599191D
C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Accessibility\Narrator.lnk	Delete	1532	unknown	md5:E7C6F8DE71749463AEA8B344DBFC4463 sha1:a08d4964d1705b977f41e3b8e4fff9be16bcbb0 sha256:DE30AD55D7EE6FFC958364C6E686A03904EF1CB1DE7C1957341CCAF99D0CE3CA
C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk	Delete	1501	unknown	md5:FC85984126A533BA25E894C39D9E8C08 sha1:f806328c3c13ee3c644aa71edba9c90a2e0fdc37 sha256:3778704684A74DCB5C277661BD7F84DDFB355D387B2121D18DF117FF6A7CE73A

C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Accessibility\Utility Manager.lnk	Delete	1539	unknown	md5:0D35B2505C94B82979FF69BEB309372B sha1:5018eaa79f237d207aa0c2411237b91880657d27 sha256:04E62772D988EC374E9EF804E6DB0ACF65579BF4C063AE15EA05A44D99B2B4AB
C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Address Book.lnk	Delete	774	unknown	md5:9A5280B5F02FB4D9E19F6A38FA883AC9 sha1:748fa22798ef70a357913e2311ce4b117525da9 sha256:EAA29155168C02876B350E87CA47569CC60BCDDC02DBB8C0216082BBA3577E5C
C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Command Prompt.lnk	Delete	1555	unknown	md5:629890CF6F2DA8E8E092BE9337C11747 sha1:4e814a7ac3253e9e32bb710394fa8a345726f9e8 sha256:868E2E68D20F603207494E215868A7DE09D60CFECFF284BB16F32104DFFF1B69
C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\desktop.ini	Delete	542	unknown	md5:0273C168051E821BE54B2D4FD087C747 sha1:28930402921046a4802b01639e03fe049c913511 sha256:5EF373AA2910DC8FBCBCD09B6C07BF6BD90C037DA14146E2BEA1C64CDB2E60F3
C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Entertainment\desktop.ini	Delete	84	unknown	md5:9406FB6347AE3C0A373ABA7ECE378702 sha1:e904a26d951310d35232af3b378b53b2540de5e8 sha256:EB5F2EB18A9A1073547D2E1C615B167052A732E9306652C500379551C111E8E0
C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk	Delete	804	unknown	md5:5B8DD9657D7844A17B1A42581868A5E7 sha1:90697042ef30d01e24e14c1e8113926d1aa2758f sha256:7F8421EBB723789BA0AEEED521525265A4873A89BC078DE3807809A59E7B03C9
C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Notepad.lnk	Delete	1519	unknown	md5:FF5BF20FF40AB69E36E77664F693C3F1 sha1:7822e9a6d14deca79a11b4a9e73edd9cb35e0218 sha256:F3F1014EDDA2FA8EC90DE464360E2C3EE5381441809A1D678330770D42C3EEAA

C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Program Compatibility Wizard.lnk	Delete	386	unknown	md5:EA85FF47EA2D49C46F10D85AA3594B00 sha1:dfc37f6c15612f7ab155e53a28a69fb5987199a sha256:F94A82D6978F26BF9BBE7196244F458C562220B6F9A6D856102AE9E1CD25D170
C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Synchronize.lnk	Delete	1519	unknown	md5:4D006DAA9800593BE7020531B57B748F sha1:7e06e748c68b074035bc05b2541ae6a730b07680 sha256:9886DB035E292DDF5F72B3A40C52C9E02F788BB51FF2AB5086BD38226D916783
C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Tour Windows XP.lnk	Delete	1527	unknown	md5:2DE8DBD18131E21876EF4779B23AF181 sha1:3b66ba3e79980d82d27271072305a27f3b7e0234 sha256:A8F14DE6A01D6A9E1C881A6E0A1DDBC72DFA740300C1C86365ABE6CBC1CEE4C4
C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Windows Explorer.lnk	Delete	1487	unknown	md5:0ABF7FB5D1E687AD369E5C7794A068CC sha1:c147ff19acd35a4dc773d5f6ee79c4add0a8a844 sha256:A11C18E38280D5CBFA42289840C49F1688D9DB9A225D280D5D977D998E52ECEA
C:\Documents and Settings\Administrator\Start Menu\Programs\desktop.ini	Delete	234	unknown	md5:E694DC03FB0F8B5B3F3A38CCEFEC8B3C sha1:9907a3d31e6722ffc3eae02449b4708c4216c4ec sha256:5541F7889F6741820280552D8FF6C3E0F99ADD8002CE30A83BF078C1840B5D78
C:\Documents and Settings\Administrator\Start Menu\Programs\Internet Explorer.lnk	Delete	767	unknown	md5:B73D3815989361EA0D01507F7465D77B sha1:414a5e7a251ae2a57f91f9fb9a04ac1dfd1f sha256:393CD64FB36CA2CF972F9BF801A3CDBBF0BC705BE5A0A3D7E5EDDE5DB6D85D31
C:\Documents and Settings\Administrator\Start Menu\Programs\Outlook Express.lnk	Delete	738	unknown	md5:6AB761A6E4BF2D0B9628B40CF89F87F2 sha1:e0314039770f3a6c645c9c1fe38220a952f4f771 sha256:E5F61A4E29E60036980261BE910BF1571D2864B99303BAB79210FAF2ED562A8B

C:\Documents and Settings\Administrator\Start Menu\Programs\Remote Assistance.lnk	Delete	1599	unknown	md5:81F8601D596CAC76DA33E3760F95E5E5 sha1:d1181de0f3a0221e21727b3d565c323f9a13b393 sha256:C40126DB105D6337E47BDED604975E531A2B5070DFE22188F58E7916AA3735F3
C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\desktop.ini	Delete	84	unknown	md5:D6A6856702E3F0953E7246A9B4A9FE35 sha1:95e17541fb7200acfea24043ec01778fe9bf2fe sha256:9C5824D33DE6F6476396B89F0FB59453FB16176C2502DD2698AB6E53D89B1ED9
C:\Documents and Settings\Administrator\Start Menu\Programs\Windows Media Player.lnk	Delete	792	unknown	md5:78D5220AA4BC1118D02BDB3E74138777 sha1:2fd04b8c6dfdd5ecc590cd74f1e3f181a268b50f sha256:C1E144C622BA5D3BEA67D76A7F745DF33DA079A545B3F4C15F52F1D09EA5735D
C:\Documents and Settings\Administrator\Templates\amipro.sam	Delete	4570	unknown	md5:1B7D0A7968B776753B588E314AEE322D sha1:3606823e2350a6fcbd838a3e4febbba4eeef2a sha256:C4F73FE84BB916AC77B2CBC70964A26D5547C0A601E5E5C1EDA57AEE43CC759D
C:\Documents and Settings\Administrator\Templates\excel.xls	Delete	5632	unknown	md5:8C488FA7AAE7091B4AC726679BEE3088 sha1:cc153d4632c798709615184c2af898828d211c79b sha256:3EE03BC99613C574CD8561C6F0ED6438D9D65B8AE04739DC45C937740452B7FD
C:\Documents and Settings\Administrator\Templates\excel4.xls	Delete	1518	unknown	md5:79BB371793849C47A92BBD86FBC10FFE sha1:28cd9f322677d00487f2781a5a39cd15e070cddb sha256:DAB571B13CF70520D66907C96C3CED815C50A82A89E3D40DA971AA4DC11EA9AB
C:\Documents and Settings\Administrator\Templates\lotus.wk4	Delete	2448	unknown	md5:6BEC7327818BE648491AD0AED50E002C sha1:9f37b17792136dd869bce14a758f80349fd534e sha256:6FF887D159D9B46B444C2E8C756099785BD8DA04B836915B3F3A2441BA9EE6A0

C:\Documents and Settings\Administrator\Templates\powerpnt.ppt	Delete	12288	unknown	md5:C96C69F52418FC171AD92018E8F42A6B sha1:205486625523978fd102aa8819a305ce1a445d8e sha256:669ED477CA9D1F401421D4A49D3B17FE69F5431905C8846202E76304D9C69BBF
C:\Documents and Settings\Administrator\Templates\presenta.shw	Delete	461	unknown	md5:5F717FD02E77C9624F6EB56839DCA77D sha1:56869a091f60b8d541cc1f7b1ab765889eb4c654d sha256:FBB85DB4A311F567989B072397B7A8DB9EFCC5680AEDB3AF607A820DA8630E91
C:\Documents and Settings\Administrator\Templates\quattro.wb2	Delete	4017	unknown	md5:B66513E596B27802937F726D48A4BD01 sha1:b819e0bde10bb97ff7acb60f854a4b6bb9615de sha256:C37719C45EC901E8483D8B0C6706BDF8B66DAD1F9CEA3C2C7F8BCB7311E8A3E7
C:\Documents and Settings\Administrator\Templates\sndrec.wav	Delete	58	unknown	md5:4CA681147F7D55321B896749196E9909 sha1:720a247ea2ba5e717ba5c7ab6833cb7741af8a74 sha256:C8BD248EC662E5F1C90C54C29B4217AB2C398642F7C5F43CBD9A917881063832
C:\Documents and Settings\Administrator\Templates\winword.doc	Delete	4608	unknown	md5:1A5BFB9857B21B989D67C84E94A49F66 sha1:9a53740f1042ba72d8bad81c1f38aa162a9b6bc sha256:0A711EE12E73F924F397CCB45045B5075FF7B582AA1D0F75EBBCDEEB14DADDC9
C:\Documents and Settings\Administrator\Templates\winword2.doc	Delete	1769	unknown	md5:02C4C0727B30D3011A7B7CBADBA4800D sha1:692d55e27bb1e9dab9afce07b2e5235376e97d9a sha256:30299CD08674E6F5602869A1A7D905E581A51A680156C6A058D11DA074FC49BF
C:\Documents and Settings\Administrator\Templates\wordpfct.wpd	Delete	30	unknown	md5:36B86116E24A6A1D094072CF87872AF3 sha1:df73155da42aa7108726e90ba3b54a52c9913da7 sha256:A8B79AD7A656CD0706BD18DC57995A84E242547497EEB2C5BC408E798F02575F

C:\Documents and Settings\Administrator\Templates\wordpfct.wpg	Delete	57	unknown	md5:D45488DCE67CC6F7EB590B4F3FB45993 sha1:1306da152fc5f66afbf9caa60808d0e439ff7f1 sha256:C2F9F5AC975E2179DE2C02AAA3F1DABB5E474C411ED290FCB4AE09F62606E429
C:\Documents and Settings\Administrator\sample.exe	Delete	90725	PE	md5:E01EDE25F5C2BE6F5A27953BCB239D5D sha1:1e66215412704d1ba7373d59c9291b0c67a764af sha256:5F38708709DD47D0B4A323E3A065E5130464102BFFF930275A00AC81DB490308
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsg9.tmp\System.dll	Delete	11264	PE	md5:BF712F32249029466FA86756F5546950 sha1:75ac4dc4808ac148ddd78f6b89a51afbd4091c2e sha256:7851CB12FA4131F1FEE5DE390D650EF65CAC561279F1CFE70AD16CC9780210AF

Registry Activity

Registry Key	Value	Action
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe44-8f32-11e7-9fce-806d6172696f}\BaseClass	Drive	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe43-8f32-11e7-9fce-806d6172696f}\BaseClass	Drive	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{946eb570-907b-11e7-9580-806d6172696f}\BaseClass	Drive	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\G\BaseClass	Drive	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Start Menu	C:\Documents and Settings\All Users\Start Menu	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Desktop	C:\Documents and Settings\All Users\Desktop	Set
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe44-8f32-11e7-9fce-806d6172696f}\	C:\Documents and Settings\All Users\Desktop	Create
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe43-8f32-11e7-9fce-806d6172696f}\	C:\Documents and Settings\All Users\Desktop	Create
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{946eb570-907b-11e7-9580-806d6172696f}\	C:\Documents and Settings\All Users\Desktop	Create
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\G	C:\Documents and Settings\All Users\Desktop	Create
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	C:\Documents and Settings\All Users\Desktop	Create
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	C:\Documents and Settings\All Users\Desktop	Create

Created Mutexes

Mutex Name
CTF.LBES.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.Compart.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.Asm.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.Layouts.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.TMD.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.TimListCache.FMPDefaultS-1-5-21-515967899-776561741-1417001333-500MUTEX.DefaultS-1-5-21-515967899-776561741-1417001333-500
MSCTF.Shared.MUTEX.EBB

Process Name - sample.exe

(command: C:\Documents and Settings\Administrator\sample.exe)

Process Activity

Child Process	Action
"C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~nsu.tmp\Au_.exe" _?=C:\Documents and Settings\Administrator\	Create

File Activity

File	Action	Size(B)	File Type	Hash
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsa7.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~nsu.tmp\Au_.exe	Create	90725	exe	md5:e01ede25f5c2be6f5a27953bcb239d5d sha1:1e66215412704d1ba7373d59c9291b0c67a764af sha256:5f38708709dd47d0b4a323e3a065e5130464102bfff930275a00ac81db490308
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsa7.tmp	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A

Registry Activity

Registry Key	Value	Action
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe44-8f32-11e7-9fce-806d6172696f}\BaseClass	Drive	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe43-8f32-11e7-9fce-806d6172696f}\BaseClass	Drive	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{946eb570-907b-11e7-9580-806d6172696f}\BaseClass	Drive	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\G\BaseClass	Drive	Set
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe44-8f32-11e7-9fce-806d6172696f}\	Drive	Create
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe43-8f32-11e7-9fce-806d6172696f}\	Drive	Create

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{946eb570-907b-11e7-9580-806d6172696f}\	Drive	Create
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\G	Drive	Create

Created Mutexes

Mutex Name
CTF.LBES.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.Compart.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.Asm.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.Layouts.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.TMD.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.TimListCache.FMPDefaultS-1-5-21-515967899-776561741-1417001333-500MUTEX.DefaultS-1-5-21-515967899-776561741-1417001333-500

Event Timeline

1 Created Process C:\Documents and Settings\Administrator\sample.exe

2 Created mutex CTF.LBES.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500

3 Created mutex CTF.Compart.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500

4 Created mutex CTF.Asm.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500

5 Created mutex CTF.Layouts.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500

6 Created mutex CTF.TMD.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500

7 Created mutex CTF.TimListCache.FMPDefaultS-1-5-21-515967899-776561741-1417001333-500MUTEX.DefaultS-1-5-21-515967899-776561741-1417001333-500

8 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe44-8f32-11e7-9fce-806d6172696f}\BaseClass to value Drive

9 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe43-8f32-11e7-9fce-806d6172696f}\BaseClass to value Drive

10 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{946eb570-907b-11e7-9580-806d6172696f}\BaseClass to value Drive

11 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\G\BaseClass to value Drive

12 Created file C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsa7.tmp

13 Deleted file C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsa7.tmp

14 Created Process "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~nsu.tmp\Au_.exe" _?=C:\Documents and Settings\Administrator\

15 Created mutex CTF.LBES.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500

16 Created mutex CTF.Compart.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500

17 Created mutex CTF.Asm.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500

18 Created mutex CTF.Layouts.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500

19 Created mutex CTF.TMD.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500

20 Created mutex CTF.TimListCache.FMPDefaultS-1-5-21-515967899-776561741-1417001333-500MUTEX.DefaultS-1-5-21-515967899-776561741-1417001333-500

21	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe44-8f32-11e7-9fce-806d6172696f}\BaseClass to value Drive
22	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe43-8f32-11e7-9fce-806d6172696f}\BaseClass to value Drive
23	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{946eb570-907b-11e7-9580-806d6172696f}\BaseClass to value Drive
24	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\G\BaseClass to value Drive
25	Created file C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsa8.tmp
26	Deleted file C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsa8.tmp
27	Created file C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsg9.tmp
28	Deleted file C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsg9.tmp
29	Created file C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsg9.tmp\UserInfo.dll
30	Created file C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsg9.tmp\System.dll
31	Created file C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsg9.tmp\modern-header.bmp
32	Created mutex MSCTF.Shared.MUTEX.EBB
33	Deleted file C:\Documents and Settings\Administrator\3rd\7z.dll
34	Deleted file C:\Documents and Settings\Administrator\3rd\7z.exe
35	Deleted file C:\Documents and Settings\Administrator\Application Data\desktop.ini
36	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Crypto\RSA\S-1-5-21-515967899-776561741-1417001333-500\83aa4cc77f591dfc2374580bbd95f6ba_a3eebfd9-28cb-4cee-b2ac-1c284d06458c
37	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Document Building Blocks\1033\Building Blocks.dotx
38	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\brndlog.bak
39	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\brndlog.txt
40	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\Desktop.htt
41	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\Quick Launch\desktop.ini
42	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\Quick Launch\Launch Internet Explorer Browser.lnk
43	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\Quick Launch\Show Desktop.scf
44	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Office\MSO1033.acl
45	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Office\Recent\index.dat
46	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Office\Recent\Templates.LNK
47	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Office\Word12.pip
48	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Protect\CREDHIST
49	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Protect\S-1-5-21-515967899-776561741-1417001333-500\ab794fd6-d34c-4099-af74-1537114d3efb
50	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Protect\S-1-5-21-515967899-776561741-1417001333-500\d70dd719-4143-488d-8f0a-c857b04fa79c
51	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Protect\S-1-5-21-515967899-776561741-1417001333-500\Preferred
52	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Templates\Normal.dotm

53 Deleted file C:\Documents and Settings\Administrator\Application Data\Sun\Java\jdk1.7.0_04\jdk1.7.0_04.msi

54 Deleted file C:\Documents and Settings\Administrator\Application Data\Sun\Java\jdk1.7.0_04\sj170040.cab

55 Deleted file C:\Documents and Settings\Administrator\Application Data\Sun\Java\jdk1.7.0_04\ss170040.cab

56 Deleted file C:\Documents and Settings\Administrator\Application Data\Sun\Java\jdk1.7.0_04\st170040.cab

57 Deleted file C:\Documents and Settings\Administrator\Application Data\Sun\Java\jdk1.7.0_04\sz170040.cab

58 Deleted file C:\Documents and Settings\Administrator\Cookies\index.dat

59 Deleted file C:\Documents and Settings\Administrator\Desktop\my.txt

60 Deleted file C:\Documents and Settings\Administrator\Favorites\Desktop.ini

61 Deleted file C:\Documents and Settings\Administrator\Favorites\Links\Customize Links.url

62 Deleted file C:\Documents and Settings\Administrator\Favorites\Links\Free Hotmail.url

63 Deleted file C:\Documents and Settings\Administrator\Favorites\Links\Windows Marketplace.url

64 Deleted file C:\Documents and Settings\Administrator\Favorites\Links\Windows Media.url

65 Deleted file C:\Documents and Settings\Administrator\Favorites\Links\Windows.url

66 Deleted file C:\Documents and Settings\Administrator\Favorites\MSN.com.url

67 Deleted file C:\Documents and Settings\Administrator\Favorites\Radio Station Guide.url

68 Deleted file C:\Documents and Settings\Administrator\Kernel\core.inf

69 Deleted file C:\Documents and Settings\Administrator\Kernel\core.sys

70 Deleted file C:\Documents and Settings\Administrator\Kernel\PAN\ApiRules.rule

71 Deleted file C:\Documents and Settings\Administrator\Kernel\PAN\FileRules.rule

72 Deleted file C:\Documents and Settings\Administrator\Kernel\PAN\NetworkRules.rule

73 Deleted file C:\Documents and Settings\Administrator\Kernel\PAN\ProcessRules.rule

74 Deleted file C:\Documents and Settings\Administrator\Kernel\PAN\RegRules.rule

75 Deleted file C:\Documents and Settings\Administrator\Kernel\pnfs.inf

76 Deleted file C:\Documents and Settings\Administrator\Kernel\pnfs.sys

77 Deleted file C:\Documents and Settings\Administrator\Kernel\pnfsUser.exe

78 Deleted file C:\Documents and Settings\Administrator\Kernel\x86DriverKickStart.bat

79 Deleted file C:\Documents and Settings\Administrator\Local Settings\Application Data\Adobe\Acrobat\9.0\Updater\updater.log

80 Deleted file C:\Documents and Settings\Administrator\Local Settings\Application Data\Adobe\Updater6\aumLib.log

81 Deleted file C:\Documents and Settings\Administrator\Local Settings\Application Data\IconCache.db

82 Deleted file C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT

83 Deleted file C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Media Player\CurrentDatabase_59R.wmdb

84 Deleted file C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Wallpaper1.bmp

85 Deleted file C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD

86 Deleted file C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows Media\9.0\WMSDKNS.XML

87 Deleted file C:\Documents and Settings\Administrator\Local Settings\Application Data\Mozilla\Firefox\Profiles\mp6o6ly1.default\cache2\index

88 Deleted file C:\Documents and Settings\Administrator\Local Settings\desktop.ini

89 Deleted file C:\Documents and Settings\Administrator\Local Settings\History\desktop.ini

90 Deleted file C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\desktop.ini

91 Deleted file C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\index.dat

92 Deleted file C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012017090120170902\index.dat

93 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\AdobeARM.log

94 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\ASPNETSetup.log

95 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\ASPNETSetup_00000.log

96 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\ASPNETSetup_00001.log

97 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_clwireg.txt

98 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_depcheck_NETFX_EXP_35.txt

99 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_dotnetfx35error.txt

100 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_dotnetfx35install.txt

101 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_DOTNETFX40_FULL_X86_X64_decompression_log.txt

102 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_NET_Framework20_Setup67E0.txt

103 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_NET_Framework30_Setup688A.txt

104 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_NET_Framework35_MSI68C8.txt

105 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_RGB9RAST_x86.msi67DD.txt

106 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredistMSI66E5.txt

107 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredistUI66E5.txt

108 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20170901164055.log

109 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20170901164055_0_vcRuntimeMinimum_x86.log

110 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20170901164055_1_vcRuntimeAdditional_x86.log

111 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20170901164059.log

112 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20170901164059_0_vcRuntimeMinimum_x86.log

113 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20170901164059_1_vcRuntimeAdditional_x86.log

114 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20171017124041.log

115 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20171017124041_000_vcRuntimeMinimum_x86.log

116 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredist_x86_20171017124041_001_vcRuntimeAdditional_x86.log

117 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_wcf_CA_smci_20170901_234704_093.txt

118 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_wcf_retCAA48.txt

119 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dd_XPS.txt

120 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\dotNetFx.log

121 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\java_install.log

122 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\java_install_reg.log

123 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\jfx_inst.log

124 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\Microsoft .NET Framework 4 Setup_20170901_164343750-MSI_netfx_Core_x86.msi.txt

125 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\Microsoft .NET Framework 4 Setup_20170901_164343750-MSI_netfx_Extended_x86.msi.txt

126 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\Microsoft .NET Framework 4 Setup_20170901_164343750.html

127 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\Microsoft Visual C++ 2010 x86 Redistributable Setup_20170901_164050734-MSI_vc_red.msi.txt

128 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\Microsoft Visual C++ 2010 x86 Redistributable Setup_20170901_164050734.html

129 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\netfx.log

130 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\nsg9.tmp\modern-header.bmp

131 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\nsg9.tmp\UserInfo.dll

132 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\ose00000.exe

133 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\SetupExe(20170901173709298).log

134 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\uxeventlog.txt

135 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\{0198CDCB-40EF-434E-AEAC-ED6C041CC970}\setup.isn

136 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\0L67SDQ3\desktop.ini

137 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\4T6V8XAN\desktop.ini

138 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\8HYB0T2N\desktop.ini

139 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\desktop.ini

140 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\GL63GHE3\desktop.ini

141 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat

142 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\desktop.ini

143 Deleted file C:\Documents and Settings\Administrator\My Documents\desktop.ini

144 Deleted file C:\Documents and Settings\Administrator\My Documents\My Music\Desktop.ini

145 Deleted file C:\Documents and Settings\Administrator\My Documents\My Music\Sample Music.lnk

146 Deleted file C:\Documents and Settings\Administrator\My Documents\My Pictures\Desktop.ini

147 Deleted file C:\Documents and Settings\Administrator\My Documents\My Pictures\Sample Pictures.lnk

148 Deleted file C:\Documents and Settings\Administrator\My Documents\my_bank_account.rtf

149 Deleted file C:\Documents and Settings\Administrator\My Documents\my_password.txt

150 Deleted file C:\Documents and Settings\Administrator\ntuser.ini

151 Deleted file C:\Documents and Settings\Administrator\Recent\Desktop.ini

152 Deleted file C:\Documents and Settings\Administrator\SendTo\Bluetooth File Transfer Wizard.LNK

153 Deleted file C:\Documents and Settings\Administrator\SendTo\Compressed (zipped) Folder.ZFSendToTarget

154 Deleted file C:\Documents and Settings\Administrator\SendTo\Desktop (create shortcut).DeskLink

155 Deleted file C:\Documents and Settings\Administrator\SendTo\desktop.ini

156 Deleted file C:\Documents and Settings\Administrator\SendTo\Mail Recipient.MAPIMail

157 Deleted file C:\Documents and Settings\Administrator\SendTo\My Documents.mydocs

158 Deleted file C:\Documents and Settings\Administrator\Start Menu\desktop.ini

159 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Accessibility\desktop.ini

160 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Accessibility\Magnifier.lnk

161 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Accessibility\Narrator.lnk

162 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk

163 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Accessibility\Utility Manager.lnk

164 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Address Book.lnk

165 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Command Prompt.lnk

166 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\desktop.ini

167 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Entertainment\desktop.ini

168 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk

169 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Notepad.lnk

170 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Program Compatibility Wizard.lnk

171 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Synchronize.lnk

172 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Tour Windows XP.lnk

173 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Windows Explorer.lnk

174 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\desktop.ini

175 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Internet Explorer.lnk

176 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Outlook Express.lnk

177 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Remote Assistance.lnk

178 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\desktop.ini

179 Deleted file C:\Documents and Settings\Administrator\Start Menu\Programs\Windows Media Player.lnk

180 Deleted file C:\Documents and Settings\Administrator\Templates\amipro.sam

181 Deleted file C:\Documents and Settings\Administrator\Templates\excel.xls

182 Deleted file C:\Documents and Settings\Administrator\Templates\excel4.xls

183 Deleted file C:\Documents and Settings\Administrator\Templates\lotus.wk4

184 Deleted file C:\Documents and Settings\Administrator\Templates\powerpnt.ppt

185 Deleted file C:\Documents and Settings\Administrator\Templates\presenta.shw

186 Deleted file C:\Documents and Settings\Administrator\Templates\quattro.wb2

187 Deleted file C:\Documents and Settings\Administrator\Templates\sndrec.wav

188 Deleted file C:\Documents and Settings\Administrator\Templates\winword.doc

189 Deleted file C:\Documents and Settings\Administrator\Templates\winword2.doc

190 Deleted file C:\Documents and Settings\Administrator\Templates\wordpfct.wpd

191 Deleted file C:\Documents and Settings\Administrator\Templates\wordpfct.wpg

192 Deleted file C:\Documents and Settings\Administrator\sample.exe

193 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Start Menu to value C:\Documents and Settings\All Users\Start Menu

194 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Desktop to value C:\Documents and Settings\All Users\Desktop

195 Deleted file C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsg9.tmp\System.dll

3.2. VM2 (Windows 7 x64 SP1, Adobe Reader 11, Flash 11, Office 2010)

3.2.1. Behavioral Summary

This sample was found to be **benign** on this virtual machine.

Behavior	Severity
Copied itself Malware often copies itself to new locations both to spread and to establish persistence.	
Sample used SetFileTime to modify file last write time. Sample used SetFileTime to modify file last write time.	
Created an executable file in a user folder User folders are storage locations for music, pictures, downloads, and other user-specific files. Legitimate applications rarely place executable content in these folders, while malware often does so to avoid detection.	
Started a process from a user folder User folders are storage locations for music, pictures, downloads, and other user-specific files. Malware often runs executable content out of these folders to avoid detection, while legitimate applications are usually run out of the Windows, Windows system, or Program Files folders.	
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	
Started a process A process running on the system may start additional processes to perform actions in the background. This behavior is common to legitimate software as well as malware.	
Deleted itself Malware often deletes itself after installation to avoid detection. Legitimate applications do not delete themselves directly.	
Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	
Accessed decoy files The WildFire sandbox deploys a number of decoy files crafted to mimic desirable user information like credit card and Social Security numbers. A sample that accesses these files is likely malicious and designed to steal personal information from users.	
Deleted cookies Cookies are small pieces of browser data that store information about a user's interaction with a website. Malware often deletes cookies to erase evidence of its own activity or disrupt services provided by other websites.	
Scheduled a file operation for system restart Malware may schedule file rename, move, and delete operations for system restart to avoid detection.	
Sample used SetFileTime to modify file creation time. Sample used SetFileTime to modify file creation time.	

3.2.2. Network Activity

No network data available.

3.2.3. Host Activity

Process Activity

Process Name - Au_.exe

(command: "C:\Users\ADMINI~1\AppData\Local\Temp\~nsu.tmp\Au_.exe" _?=C:\Users\Administrator\)

File Activity

File	Action	Size(B)	File Type	Hash

C:\Users\ADMINI~1\AppData\Local\Temp\nswD050.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsrD080.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsrD080.tmp\UserInfo.dll	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsrD080.tmp\System.dll	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsrD080.tmp\modern-header.bmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nswD050.tmp	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsrD080.tmp	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Administrator\3rd\7z.dll	Delete	914432	PE	md5:04AD4B80880B32C94BE8D0886482C774 sha1:344faf61c3eb76f4a2fb6452e83ed16c9cce73e0 sha256:A1E1D1F0FFF4FCCCFBDFA313F3BDFEA4D3DFE2C2D9174A615BBC39A0A6929338
C:\Users\Administrator\3rd\7z.exe	Delete	163840	PE	md5:A51D90F2F9394F5EA0A3ACAE3BD2B219 sha1:20fea1314dbed552d5fedee096e2050369172ee1 sha256:AC9674FEB8F2FAD20C1E046DE67F899419276AE79A60E8CC021A4BF472AE044F
C:\Users\Administrator\AppData\Local\bluesoleil\bsps.ini	Delete	2174	unknown	md5:C5C4E58613E937256DA03ABD6CBE95B8 sha1:1922df018fb63558210fc1a718f9bbc7507437b2 sha256:3CBF8A7BC4CA04E8D6CD4F8D71275CEBC33A5F0B414207E84396535227407D47
C:\Users\Administrator\AppData\Local\IconCache.db	Delete	901520	unknown	md5:E37C02E0BA7AF054B3F2E33546ACF4DC sha1:798b449281e311757b5ad954e209fca7a34cd53d sha256:8E45D0973E20CA82B2A3370AB178E1329FB84FFD9DCED815DFDD606CA82CD230

C:\Users\Administrator\AppData\Local\Microsoft\Feeds\Feeds for United States~\Popular Government Questions from USA~dgov~.feed-ms	Delete	28672	unknown	md5:D5AEAF1CF2DD0E110DC1A098D47B8368 sha1:b98d0211bd6ecfada654dbb65f19e05a344722d0 sha256:ACB96561781443FF6C1860774D2BED47C0B5CDEBA5520B228CEBA299E4BD0D12
C:\Users\Administrator\AppData\Local\Microsoft\Feeds\Feeds for United States~\USA~dgov Updates~c News and Features~.feed-ms	Delete	28672	unknown	md5:D90C2DE827003FC8DA409C9E6FC85B37 sha1:59590786b2cc74a7bfeb3a52309f0e804998b675 sha256:C9F5201C7699910C958942033E038F10E02A6102549977E4D76698E9E099BCB8
C:\Users\Administrator\AppData\Local\Microsoft\Feeds\FeedsStore.feedsdb-ms	Delete	7168	unknown	md5:522CD7174FF5941A464D861E22685A8D sha1:754554d6ba8e6be25009d2743cf994d181a71614 sha256:47F3D449D1FF953095974135B0D91E4BAF2B1A71511E2EB62425200D70555921
C:\Users\Administrator\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Home~.feed-ms	Delete	28672	unknown	md5:2DE6CEE70436231BBB5B0A6AB59AF958 sha1:13f0ee9aabb7d31a25f298c4a8cdf9a134265e2 sha256:0F9205E5C8FFAA1EE637D6447EEB04C0679B37F8C6F0A597B7D7B97D18EA29D8
C:\Users\Administrator\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Work~.feed-ms	Delete	28672	unknown	md5:73E026CA53F4CBECA186D754113ED17F sha1:9a5a9d94ef810c1fbad5f3b75ecf4ba3495f90e6 sha256:B53ADBC6D74AF4291A283B279347418 42A4690474A6CF05270D03B960369BFB0
C:\Users\Administrator\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\MSNBC News~.feed-ms	Delete	28672	unknown	md5:0879C9BD26D9871C6D46E934D248B91F sha1:7693551b1242e8ba4e5685852d87c22725bf52 sha256:A998D0EC2DFFA976386F74BC18F5BDC84A43DF4377598430B982EE5739AC54D7
C:\Users\Administrator\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Web Slice Gallery~.feed-ms	Delete	28672	unknown	md5:E795BAAB517B7EBB3994973535F70322 sha1:2c53c7eb7e75258d8b79b4111fbe99a2c45b4a01 sha256:14512EF29143F5008244A5128E0B80C5B97B6A13698E946B0ED255ABADC9DFBD

C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\D96JQY3U\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38
C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\D96JQY3U\fwlink[1]	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\D96JQY3U\fwlink[2]	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38
C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\FUTLFAHL\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38
C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\FUTLFAHL\fwlink[1]	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\index.dat	Delete	32768	unknown	md5:6D1AB89D0E081239E865DF666E6EEC10 sha1:be8c0e35c4600b56c0e10fa7955f841c53046b37 sha256:E37440B53B005999DE328C1619240618F22F8C8FC941FA5F8BCF247D4A1DD6DE
C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\O9YY42MG\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38
C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\O9YY42MG\fwlink[1]	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\O9YY42MG\fwlink[2]	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A

C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\Q3FSQLXM\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38
C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\Q3FSQLXM\fwlink[1]	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Administrator\AppData\Local\Microsoft\Internet Explorer\brndlog.bak	Delete	12201	unknown	md5:388E741AF6B9530B165320DBE9E72131 sha1:3accc4fbae758e7a16369c5afb1576926f8a7048 sha256:8DC32CB8EC54A53137FF77559771F2195EC18E98CD9528A2C4CFD553847C9FF7
C:\Users\Administrator\AppData\Local\Microsoft\Internet Explorer\brndlog.txt	Delete	12201	unknown	md5:660DC2C285568B955CE0A17938E66C27 sha1:c45ec66b63865b4ebbc5afe4ca0160e222d5e68b sha256:3EFEEFB6D1696F964ABD94C00F87FA1755FCC603A5E7CC0716F94F1E6793FDB6
C:\Users\Administrator\AppData\Local\Microsoft\Media Player\CurrentDatabase_372.wmdb	Delete	1069056	unknown	md5:99028C1E5054EF62DC741A3EB739D275 sha1:bb2924537d4a7c36dd9be17bc326cd0c603f8159 sha256:FE4E5D53BDB19FDFB67A4D1D3318BFBD1F893D43FA763909B0CEBF371823792D
C:\Users\Administrator\AppData\Local\Microsoft\Media Player\LocalMLS_3.wmdb	Delete	69740	unknown	md5:BF108032FEDC0AEC3F3B665551101926 sha1:2c1a2964f59e944d531e2946a5a06b2a33c3c15 sha256:66910AFCDBEC5BEFC82B0EA794733861345D6DA524CD06ABA61DDC9BF0E81A53
C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\01_Music_auto_rated_at_5_stars.wpl	Delete	1044	unknown	md5:3094088E14AFDC15D7427B093B8B7B17 sha1:ed10bf7cf3df61ba95f45dca39042473efe07197 sha256:B2B5080D83A1853FBEC424E6B179B784C57716600E1B58DD8B2C5FEE0E098FE5

C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\02_Music_added_in_the_last_month.wpl	Delete	1279	unknown	md5:907BFC98CE854AE312127C952D8BE0F2 sha1:2defe8c5f9cc85742e45ba55e4fcfe326fd960c sha256:C475DC7423C2AD60F25ADAAC754CD8B68B57FF04F26ECEF78F3E5961B986A324
C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\03_Music_rated_at_4_or_5_stars.wpl	Delete	1267	unknown	md5:6D791B697AF46D6777182AF7F18C2955 sha1:d73e8b5f4ee646c1c4ab6d23f3cb3394cb833ca8 sha256:4825EB90140F6B2F4F7ED0DF66B24E10FF5D0DA70AF53EA495FD30B3AA791870
C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\04_Music_played_in_the_last_month.wpl	Delete	1284	unknown	md5:F8D3A4CACF055F5EC5C62218EA50D290 sha1:974474ce3fe345d815863bd6ea7242ba118532b sha256:201F2170812CF8041964C4D3C5EF539D96ADEBA6A68B69ECAED0AFFE3AE8E25F
C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\05_Pictures_taken_in_the_last_month.wpl	Delete	797	unknown	md5:821D2BE672F05514127C117CEF460C6E sha1:1c75f314e7658a3dcdcad315e301f2bae6d47b31 sha256:3ABDB6CBD88AD1557054ECE3F10DD1A8494ED32F423B3CF8321B18DECC489474
C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\06_Pictures_rated_4_or_5_stars.wpl	Delete	785	unknown	md5:0A8A40CA87323DC16893194B00C7FE77 sha1:b88a42a85053e0a7483e331b66ba5a40a6290e10 sha256:9AA433BED2E090CC6904F1C24D5A7B5A1ED6D8F71A997E661B886C69383FD53E
C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\07_TV_recorded_in_the_last_week.wpl	Delete	1040	unknown	md5:B9987B1F9DF6D0AFC01558B907E62A16 sha1:ef202d5d6f90b37c71cb757f3babb0857ce54d86 sha256:0892EFDB8459D81D4C5E1085239734D9910B9C6A1DEBD7189CF385141F0B19D1
C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\08_Video_rated_at_4_or_5_stars.wpl	Delete	1020	unknown	md5:A3787A42B81FCE0E448976AD158EDD93 sha1:45ff275cc32eab1f0b56e8b61e8ead18cfd1675 sha256:94BC17AC59BDE92FBCA00FCC69AED68FCBFE2C1754DD45F4810765F5FDF774FF

C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\09_Music_played_the_most.wpl	Delete	1025	unknown	md5:467E71AA2FD951EB0A1AF3D6BB8378E8 sha1:fb654c0b2663d4fa5fd0f1658097d936dd0429ed sha256:A54BC2CAD63CED4FD9FF2A3A094A26E264E8A5CE8139193896D13236F494E2EE
C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\10_All_Music.wpl	Delete	1063	unknown	md5:51AEED11707741118E0706C1259DF22E sha1:6434e915b018c6d15898fe0a4d006bbe3e1edb60 sha256:EC286113E5AD77AC34063589A137A6DC4B4CAB8845CD9C5386519983FA3B48F0
C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\11_All_Pictures.wpl	Delete	585	unknown	md5:74294EF495559ED32731F19096D70312 sha1:fdc6cc849270016d2a382d7ddaabf44a4556cd9 sha256:DB34D82F2CD23E6E55A64E12D2A0A9C27AC2DED156483238F22A336CA6825110
C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\12_All_Video.wpl	Delete	1079	unknown	md5:372D0BEEBEA5460409A6A1C53AC52A18 sha1:1b5a925ef9a4cc3a18feb8f74a2e39ef11eeb6 sha256:5B8B62B35E5DD8A46CCCCAF3FC3743BE9E0965D24CBCD20DA2681065EEB37EF3
C:\Users\Administrator\AppData\Local\Microsoft\Windows\1033\StructuredQuerySchema.bin	Delete	297531	unknown	md5:210B2171F9586FEB0ADEB1889B522B8E sha1:7a9fc1526b3766ec166a1f5a24a7044b66ab656 sha256:A8B67872D14404A33F68E68C4FA260E996223D65A6CCD3F8219E6B9B4C8CD735
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Burn\Burn\desktop.ini	Delete	174	unknown	md5:E0FD7E6B48535592AC9AC73DF9D83783F sha1:2834e77dfa1269ddad948b87d88887e84179594a sha256:FEEA416E5E5C8AA81416B81FB25132D1C18B010B02663A253338DBDFB066E122
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog.etl	Delete	8192	unknown	md5:D247270E6F6BB3B8268D22362F48DDE9 sha1:ad293f041b5f9ed5bc76b5fe11eecc16ed9f216e sha256:7E40FF3EB8C618E8298C48ADB29BBFC5BB7401868B2317D4707265491E67AC4F

C:\Users\Administrator\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog_RunOnce.etl	Delete	16384	unknown	md5:D5CC04C17CA67D0F578C42AA712ABBFE sha1:fd5d576639a8f07aa5c947ec370acadc42b6304b sha256:9121FB36A5D96E282C15E8D881292894536E977C1BF6A49E2DFC5D3C7924A821
C:\Users\Administrator\AppData\Local\Microsoft\Windows\History\desktop.ini	Delete	145	unknown	md5:BA96961F5E22882527919E19DAEA510F sha1:e10e8bebbd0573e3a1494ea3f21682f7490c427b sha256:DACE5AD59099429D8AED4EE279F1263EFB65D64456931398465A396CF0E79BD7
C:\Users\Administrator\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini	Delete	145	unknown	md5:BA96961F5E22882527919E19DAEA510F sha1:e10e8bebbd0573e3a1494ea3f21682f7490c427b sha256:DACE5AD59099429D8AED4EE279F1263EFB65D64456931398465A396CF0E79BD7
C:\Users\Administrator\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	Delete	16384	unknown	md5:D7A950FEFD60DBAA01DF2D85FEFB3862 sha1:15740b197555ba8e162c37a6ba655151e3bebae sha256:75D0B1743F61B76A35B1FEDD32378837805DE58D79FA950CB6E8164BFA72073A
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D76OFA0\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\31L572O7\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38

C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat	Delete	32768	unknown	md5:6A95882C852D6DE4EDE3B10775DCC55E sha1:ff9184356112ab7ad8132c577326ce6c447e04c1 sha256:0C8B970B01E8BA225DB4553B0BF4C143C9436AEE5CC97147A18A16565FA1499D
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TXJ3UQ95\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YUM4IDPG\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\desktop.ini	Delete	67	unknown	md5:4A3DEB274BB5F0212C2419D3D8D08612 sha1:fa52f823b821155cf0ec527d52ce9b1390ec615e sha256:2842973D15A14323E08598BE1DFB87E54BF88A76BE8C7BC94C56B079446EDF38
C:\Users\Administrator\AppData\Local\Microsoft\Windows Media\12.0\WMSDKNS.DTD	Delete	498	unknown	md5:90BE2701C8112BEBC6BD58A7DE19846E sha1:a95be40736982392e2e684fb9ff6602ecad6f1e sha256:644FBCDC20086E16D57F31C5BAD98BE68D02B1C061938D2F5F91CBE88C871FBF
C:\Users\Administrator\AppData\Local\Microsoft\Windows Media\12.0\WMSDKNS.XML	Delete	10191	unknown	md5:7050D5AE8ACFBE560FA11073FEF8185D sha1:5bc38e77ff067785fe0aec5a345c4ccd15752560e sha256:CB87767C4A384C24E4A0F88455F59101B1AE7B4FB8DE8A5ADB4136C5F7EE545B
C:\Users\Administrator\AppData\Local\Microsoft\Windows Sidebar\Settings.ini	Delete	84	unknown	md5:2D969131BCCEC01149620521AAB5D9D2 sha1:ef8864ea141862fbae6eb25cc62b34f5398c304 sha256:63B9A95398FA607BDBD5187B15FFD20AA6FB3055CF6EB524CDBC9450EF5675CB

C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\1zzfgr18.default\cache2\index	Delete	6	unknown	md5:6C4B271569318 89528F5BEC30E25B3 F1 sha1:165c0d195e773 f66423a873ea96414 4cc4e92b62 sha256:9A741481EB 4561BF9C0F64BD5C8 8493919962171CF4D 6828833660D9D4816 F5A
C:\Users\Administrator\AppData\Local\Temp\ASPNETSetup.log	Delete	6515	unknown	md5:CEFC09624BFCB 57E1E9087EC44EEC1 07 sha1:14bed5f98c59d 3bb60c199292026fc5 fe0e003 sha256:48901715CD 39B76EA96B22B566 B918C0480FAE37618 FAD66D7DE7702FE5 74859
C:\Users\Administrator\AppData\Local\Temp\ASPNETSetup_00000.log	Delete	4710	unknown	md5:45796BC126C08 A700AAA3A09D4836C 391 sha1:43ed8d0497a36 c49395e58f4a0bb01e ccd89159 sha256:11E936D725 D390346190C531357 D47E2A60B04A4B03 B10ED58A84A868EC 89E39
C:\Users\Administrator\AppData\Local\Temp\ASPNETSetup_00001.log	Delete	2966	unknown	md5:906D8251C9141 B1EEE8B61CFEBF47F F6 sha1:1405f55a13f6af d88fa8fad1cb8690bc db6331c6 sha256:4D4743FEDC 7A7FD948D36EDB31 126FF98009E3D5461 8214AC41A2B564C8 0A24B
C:\Users\Administrator\AppData\Local\Temp\dd_NDP461-KB3102436-x86-x64-AllOS-ENU_decompression_log.txt	Delete	1277	unknown	md5:E87122F9BEAF3 F0E04BEA22B5F0820 A0 sha1:a636a02293f01 a2dec77b65a9716c7 8aaa7e835 sha256:962D0C77B7 302756A5FB58B1A3 D55B6EA9E34666089 A7E3FB88EB9433E37 D778
C:\Users\Administrator\AppData\Local\Temp\dd_SetupUtility.txt	Delete	1711	unknown	md5:0ED21D0D0969 E80A6C653B085CD1 3D52 sha1:d34b253c3739f b2b47217f2d3a78f62 7b447392 sha256:FDC3FE43807 064D6829697C71966 E8BCA7436991ACE3 9C5521988FBA8BD2 0A28
C:\Users\Administrator\AppData\Local\Temp\dd_vcredistMSI72EC.txt	Delete	432690	unknown	md5:6456651E8A387 52AF5B4882647730D 8B sha1:ebb5ea7e4c8a4 350f904abe2705e12c d3446ae2f sha256:3414D0297C E545DA507E6B4EF80 A71B20E953B33676 D067525AE235F1F6C D7CB

C:\Users\Administrator\AppData\Local\Temp\dd_vcredistMSI79FD.txt	Delete	431510	unknown	md5:696082B58E15D60378B2F844A9DF4E82 sha1:ffe1f717bb7993039e56db3b1c7a669130fdaf65 sha256:2114AE589D990F5EB0FFB7C1CD68D7C2A100C94247D7152528C838E3258C05C9
C:\Users\Administrator\AppData\Local\Temp\dd_vcredistMSI7A07.txt	Delete	421412	unknown	md5:258C0915B4D9028B19A8BD5C075D4E95 sha1:bb771e692cf8b4f9f5bffe78179d5a28e858b1 sha256:F2B46A3F9847716117F58C3C673887A8BCA00225253B828665E529CE83D922B8
C:\Users\Administrator\AppData\Local\Temp\dd_vcredistUI72EC.txt	Delete	11630	unknown	md5:E83E6A3B8764025698C3F050E4ECB386 sha1:b465f06f4ae93d20d1eab029d83c0836f691cb2e sha256:73E0E0F2B4225344FED07814E055362C1E4C37B0D868E9118CFEFF177AE73183
C:\Users\Administrator\AppData\Local\Temp\dd_vcredistUI79FD.txt	Delete	11476	unknown	md5:9C542F9761BB01CE2603E8A8DC01B3EE sha1:88cdb9132562bb337240dc69c12f328bf2fabe7e sha256:4F9085AE8D2A21B5E98C440DA10EB5FC9B352E806F611E7B047A1A9444E6EB3E
C:\Users\Administrator\AppData\Local\Temp\dd_vcredistUI7A07.txt	Delete	11396	unknown	md5:5E5B1230C505451B2A9D089039D52A2FA sha1:ef980f7c228e9ad06f792ccd90a3178bed9598b6 sha256:BAB938D636E6D72CBD1CDEF2F5FC5D6CE2DD258D9BC4F0B210B152C8CA04F198
C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_amd64_20180907154104.log	Delete	17317	unknown	md5:69BE9856C7E3C4E60516C5C54646EE63 sha1:c8dad4a924d7d5d22f5af2838ffac04f90f43de8 sha256:EB53EE055A65D466BF46971B547BDBD12BB4BF3E19AAC6011195978237EFB702
C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_amd64_20180907154104_000_vcRuntimeMinimum_x64.log	Delete	177720	unknown	md5:B7794BFD0E3C939D5EFCE150F917D7BE sha1:388bedd9c10da92a9d61ab4bb0c910bc07fcc0e sha256:0D91EBF7A1211A26F29387ED60D956EA65AA277E7B5B20989A50D7423F7A3AA1

C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_amd64_20180907154104_001_vcRuntimeAdditional_x64.log	Delete	195562	unknown	md5:C9B556425DB5B195A8998F806F709FD1 sha1:57050e39e1a6c0e611dc2d22d07e74615d2b363 sha256:1AE48C270878454C4845A64B6C3C7E11A1AA8954B13B38F516BB4275DE039B2A
C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907153904.log	Delete	9015	unknown	md5:0FC84A036B16D4313D439A31B3438F14 sha1:ba7eb94be9e5b2feb494d938fff87112a33e87b sha256:6375025453E829F25DCEB86EA4992E5D20498418D195C1DFE1067E659245CC4F
C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907153904_0_vcRuntimeMinimum_x86.log	Delete	173476	unknown	md5:980A7F8E1F69696A530D419A4CEB1808 sha1:b74813f1e9333ccec8bb859a7bdffb3629393c2b sha256:64D0D173D92DFD9F0B203CA26E318718FD5A75EC1DBA84207A2E335F6DF2552E
C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907153904_1_vcRuntimeAdditional_x86.log	Delete	211940	unknown	md5:BDFBEB4DEFC878AD34636331A76C7193 sha1:30109c45bf15c169e1439ed3780606fd3ade8ffb sha256:36519244E0EBF2DB0E391019DB36FCD0909742239BB8B698EC6CC56229FF38C4
C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907153943.log	Delete	8752	unknown	md5:04532FA7110C3B17E5D1107F160C5766 sha1:cad48ce9a5e48656e1599cb2c5f2d0deecb8f7de sha256:CD644B52D0535B76246FAB0E089F68D471ACCB26BB01ED975126712E6ABF8F57
C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907153943_0_vcRuntimeMinimum_x86.log	Delete	172994	unknown	md5:38AB1CB18E516A4CEC936E330C6CF3D4 sha1:2f551e8a306f80ff8e30ca8b0bd401b86334e49 sha256:29D51ADB3B4F6D9FFDE0A905B1D37743DF27A437C179FA099737E90D220BE7BB
C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907153943_1_vcRuntimeAdditional_x86.log	Delete	201970	unknown	md5:8F59553AC90535E661DFDDD462667565 sha1:3b6ace131b6e61f9e5f0b4ccabe151e2b3b132b sha256:60428FE4663C8F244F71086029C0FFF1B43E4DE885B7D177ED65A4B856236034

C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907154003.log	Delete	17086	unknown	md5:180907F536CEBB87283F7BAFF0059ACE sha1:5351c769d67a160fe54013f077d5294d30d9e397 sha256:5D996EA0D66FE1975ED69B55A91221FEEADF86255589789990EB188336CB8ADB
C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907154003_000_vcRuntimeMinimum_x86.log	Delete	176758	unknown	md5:2AE57914AF544FAC23074D49FDE4FA11 sha1:6312c2e0db8ade711526152e7768e09ebf78daeb sha256:DE24028C892575171B845C9289775F69FDBD08A69316A406C91915ADF00D8917
C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907154003_001_vcRuntimeAdditional_x86.log	Delete	201514	unknown	md5:752A81F8682C3254AFC0DAD049367581 sha1:c4fb881f23a163d21d7ad1309fea1f52a85b805e sha256:3BE5AE6F64789DC31E6684FDE186BCB8D2B8EA0078C90D3313F52C510A1451D2
C:\Users\Administrator\AppData\Local\Temp\dd_wcf_CA_smci_20180907_224518_374.txt	Delete	7166	unknown	md5:3576E6F26C465DA110987AD04B4CD2BB sha1:706b73fc89642d1b9641f731a8a6e7317a85ab62 sha256:0561288FD5C22B1DBC1079A353F9990A7B5D2726C02CAAFFD7CA63907DEA2FE0
C:\Users\Administrator\AppData\Local\Temp\dd_wcf_CA_smci_20180907_224520_280.txt	Delete	2694	unknown	md5:E6674F5F125DBA8363290C3D4C4CB09C sha1:5e01bfb5787e777d46022e1dfb19a8d19b7483b3 sha256:5D54E0204AE5CE7BCF97FF3080085FF120DED8652BC55B62AE8E762CA6C3D546
C:\Users\Administrator\AppData\Local\Temp\dotNetFx.log	Delete	2445	unknown	md5:445E7B20D8931E919DE32991E589ED2C sha1:877e6d9fa489306af47a12a02ffe9fc66734ab3a sha256:502EF2CF46C9ED5C94D9815A9FCE5097752C9D659CF60747ABDD058A6036189C
C:\Users\Administrator\AppData\Local\Temp\F642.tmp	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A

C:\Users\Administrator\AppData\Local\Temp\InstallPlugin64.exe	Delete	8107168	PE	md5:D2E2E5CD7E70DB1894FD4F65AA6538A6 sha1:ede197032f3194fec74cafed6c775d4ca100b44 sha256:40ED3CBBDA0E68DC0F71927B02DEFCF7781B60C6271FB5222D580165DE87E940
C:\Users\Administrator\AppData\Local\Temp\jusched.log	Delete	56509	unknown	md5:6598A629F713461 10C56D849C74F4881 sha1:8ccfaab73cadefa3eabc0fa55e8dc6214d41dc81 sha256:D96B9ADB3F3488F55F53E97A4691A62476447F5CE54BDE499C4AB0BAF252689A
C:\Users\Administrator\AppData\Local\Temp\KB2600211_20180907_154410655.html	Delete	36600	unknown	md5:2215D9E8B41B50C709030C30D832F830 sha1:2abd29dc7a338ffb498da0b6688db429c9f5f0c6 sha256:408E8D13EF8FA209D3DE866D27602125C38C7513330241FE42B00AD4C373B863
C:\Users\Administrator\AppData\Local\Temp\Microsoft .NET Framework 4.6.1 Setup_20180907_154442905-MSI_netfx_Full_x64.msi.txt	Delete	10728970	unknown	md5:2F590842A29417992BE2E240981C77AE sha1:b5b74b47ef39786a5729549c4804a31985763f74 sha256:B2410A3CCE12A472CA66016B68B4FCEB484D4CE95774E2ECEB174E81984AE821
C:\Users\Administrator\AppData\Local\Temp\Microsoft .NET Framework 4.6.1 Setup_20180907_154442905.html	Delete	879350	unknown	md5:7B3FE87AF1A605CADD2E0AC0C6392CDF sha1:2980bd2680b3a8f96d148bb9adcf1eec9250de8 sha256:88764FFC02A08AA6001C9E01DB2A51A119F592DA48253A6F0FE3DE065F3098A6
C:\Users\Administrator\AppData\Local\Temp\Microsoft Visual C++ 2010 x86 Redistributable Setup_20180907_153900952-MSI_vc_red.msi.txt	Delete	266380	unknown	md5:13027AB8427DFFBE142C47231696D848 sha1:17479f156ca288c096f65b31baa7af5aa82f66af sha256:3B0A3134BCADEFD7F3EF92ED9F8CE9F64345F297524B85CA22CC0838FEF740A6
C:\Users\Administrator\AppData\Local\Temp\Microsoft Visual C++ 2010 x86 Redistributable Setup_20180907_153900952.html	Delete	76100	unknown	md5:3CFEC7B26CCD61B93E5C88D59B865DBD sha1:7d0df0a04397ed82bb208b9e5be2fb78a11a0ab sha256:C6C691D21071060FD7DCCC3FDF0338E61B5FB0B4E2159B3AE218888976CD5DE0

C:\Users\Administrator\AppData\Local\Temp\MSI8f258.LOG	Delete	176350	unknown	md5:ECE9E0D2BCDCE6AFDCBACFDAD4485F28 sha1:963fdcc2497d09c26f7da8fb72565b5c42995ca sha256:8E6A3CBD276ACC403E1F913056F75BB5C8D3468E777226D05F7781B18C8AD076
C:\Users\Administrator\AppData\Local\Temp\netfx.log	Delete	4096618	unknown	md5:D8009A773C51DBCC26D511982372639A sha1:becc3ed0fddb79ba393859fb2060d29d20e98737 sha256:0704791B911A6EBD80E52B306599FEFEEBDBE2BED6E49CFC0D8CD13452D7BB53
C:\Users\Administrator\AppData\Local\Temp\nsrD080.tmp\modern-header.bmp	Delete	9744	unknown	md5:940C56737BF9BB69CE7A31C623D4E87A sha1:f2f3b4e7b9c28df6687ceeaed300a793e3bac445 sha256:766A893FE962AEFD27C574CB05F25CF895D3FC70A00DB5A6FA73D573F571AEFC
C:\Users\Administrator\AppData\Local\Temp\nsrD080.tmp\UserInfo.dll	Delete	4096	PE	md5:C7CE0E47C835255983FD2C4C9566B4AAD sha1:38b7ad7bb32ffae35540fce373b8a671878dc54e sha256:6293408A5FA6D0F55F0A4D01528EB5B807EE9447A75A28B5986267475EBCD3AE
C:\Users\Administrator\AppData\Local\Temp\ose00000.exe	Delete	149352	PE	md5:9D10F99A6712E28F8ACD5641E3A7EA6B sha1:835e982347db919a681ba12f3891f62152e50f0d sha256:70964A0ED9011EA94044E15FA77EDD9CF535CC79ED8E03A3721FF007E69595CC
C:\Users\Administrator\AppData\Local\Temp\RGIBB84.tmp	Delete	10434	unknown	md5:DBEF78447120E830587017C581F994F1 sha1:ea5214b9503e9a3b5335053b9f2e85c1bd26f3ce sha256:A380116D80066949811B29C5B53C20488C1CA6B05A955C1698AFF58FC18EBF94
C:\Users\Administrator\AppData\Local\Temp\RGIBB84.tmp-tmp	Delete	9000	unknown	md5:4AAE089D3731C3F9DCA27587E61CC4A2 sha1:97b570c8cce9d68fbdd728f8524d92bce4a5c35 sha256:ED8F2F1786D5C57AEE9C8228286F41B1665F46B88B882557675350D5108B438C

C:\Users\Administrator\AppData\Local\Temp\SetupExe(20180907160837944).log	Delete	211614	unknown	md5:4465F7A90CA13B16FFBE79A535E89337 sha1:129e578b8a4f2a0cc5d4bc20fc9534f4724e1cb3 sha256:8EB3349EE5ED79C1BCD0806AA029D71CE930F6AC32788071A48B268B99A3CA93
C:\Users\Administrator\AppData\Local\Temp\wmsetup.log	Delete	1621	unknown	md5:4F07F569030D8F809A10FB3BFC4528D9 sha1:300173f0f0d975dc150f573bcac091e0daaf4b6d sha256:7AC4E5E7010250B391FFB782CA6C54C41AF02D4F6536718B3E54962672061F37
C:\Users\Administrator\AppData\Local\Temp\{1D5DBEAA-1A43-4BD8-BB91-48E4EF702C34}\setup.isn	Delete	84949	unknown	md5:3813B8C0C6D48ADE7685388D64B3BDDB sha1:9fd97c26a12b98f6341dd3ef60378ddc134fb2f5 sha256:7F8575E818BA4037344DB0F891A89104DA41D3E44029EC693167B1318E540DEF
C:\Users\Administrator\AppData\Local\Temp\{825EED85-C929-42FA-B378-811E0CED8CA7}\ISBEW64.exe	Delete	107392	PE	md5:B83D2774CDAF5016CD8765A630FA1150 sha1:50b7f86488926c6b6322af6a5176e4c7786058d sha256:4935372DAA99F6C10033ACCF0CD6403B6F7061477500C1EB65D7CA2DEDBCBFD8
C:\Users\Administrator\AppData\LocalLow\Oracle\Java\jdk1.8.0_92_x64\jdk1.8.0_92.msi	Delete	1228800	unknown	md5:15BEBD13AF5D6E80167E4742FE874034 sha1:869a9bae2899c2348939e9cb3f5c98af33306c0 sha256:658B4087E107AD3A3E013DDDA6B935E31AC18E2C7FF50608E98F0E91C9ED3C37
C:\Users\Administrator\AppData\LocalLow\Oracle\Java\jdk1.8.0_92_x64\sj180920.cab	Delete	59364858	unknown	md5:6FB806279924DCD104529B206DF8399D sha1:729a64dee1a03e63263c18a52a9ce5439d81a5a sha256:BE38E678D224384B5002C8BA03914D204D8CFE5720B8DC5866F50E9F0C18ACE8
C:\Users\Administrator\AppData\LocalLow\Oracle\Java\jdk1.8.0_92_x64\ss180920.cab	Delete	19760786	unknown	md5:E4FC63583EC72615E9D341CD20B99DFB sha1:ea5b6e2ac782bdadd1a59d85bf7f23eb9e98d16d sha256:7250EA1ED41A5A971776E82EC2FD2D97982633274E7F300B5C49C5AF88B0F0B1

C:\Users\Administrator\AppData\LocalLow\Oracle\Java\jdk1.8.0_92_x64\st180920.cab	Delete	120288648	unknown	md5:8A1900F172B4B3F0B62B615C5676EE92 sha1:58e7f1d57cf9c6d36fabb8e03a4b091403bbbae sha256:EF55EFDFCC33424353B288C8AF9FBF6B89B71BF1B9D5F560A7223D039CEAAAF3
C:\Users\Administrator\AppData\LocalLow\Oracle\Java\jdk1.8.0_92_x64\sz180920.cab	Delete	1504	unknown	md5:405AC58FEAE873D72CDF8FE7E57E9CE1 sha1:4347c40181d8b8606493fcb5b39653bb7ff04d71 sha256:108856C9B49BD09DD0CA3BC9C361210DE5B1413A6BDB3E05E4A901285526228E
C:\Users\Administrator\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sol	Delete	317	unknown	md5:A0AFA4D63C09F85B6924CB0D545CAF4E sha1:3c1b206541a6e9956c722c074eb302c893cb2a0 sha256:4710EE6638F07A99320687EC3C69C7832907E7B57D202765DB6B1503268021D3
C:\Users\Administrator\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-843043956-3771856219-1177494106-500\61ff37d6c196852c3fe91c028c7590e1_c7928fc6-52fd-4727-ae12-abab87adf76c	Delete	1465	unknown	md5:BD9CDD33D231C3C9B6AD3EEDA98B83A1 sha1:36f39e429d07fe8dcaae0a5b4ef7b8ecbc1050ba sha256:A1A60A7E98D81FA10AA9DF6DE1F374F48D03EC6D02552D09D58C371AB779FD11
C:\Users\Administrator\AppData\Roaming\Microsoft\Document Building Blocks\1033\14\Built-In Building Blocks.dotx	Delete	4187307	unknown	md5:D572F3C193CBFC88C4F3779657B8E20D sha1:db07b42317293f2e331c4f34a34fc44abb4c9793 sha256:5E9B4E081ABE7439AF6FE53489108D8DE3D0C9DBC297F080A1CF17E4913FDFD5
C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini	Delete	146	unknown	md5:926B5FFFE90D05BD50F0FF7D523032 18 sha1:f75f2bd24a67a238c03cb2175422a6db535b1192 sha256:806128CD8D7680E86E1E9A09D99152CC73F8C410C1552EB441CDD86055371B04
C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk	Delete	290	unknown	md5:9A79C9E1AD63ED2E7932536570775B9F sha1:db556bc8dc2e60d0a5aef1bfba930a6fdceb7cca sha256:20BADD15197EF7F52351C378A6B9204863CC114DBE1034BF86180E7E74810F86

C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\desktop.ini	Delete	211	unknown	md5:E11E5A356FE79A77992BAF3C6BEDBA79 sha1:9e3eb3b6ddda8664dc17e314223be3aef41fc1 sha256:E9BBC871326524376AFF5AA95076F6562D8416BB94876ED4E6D5668C3C20B1AC
C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Internet Explorer.lnk	Delete	1450	unknown	md5:9CF2D6B5B28AB6ACAD862D63BC722277 sha1:13a4853e1c2e8f3ce3c8af61b3c30467c27f16d3 sha256:B80BB975723038437113210B9A694E15F3D5E49A4ED7AAC63138BFCB5D58A542
C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Explorer.lnk	Delete	1228	unknown	md5:47B2E1C4DDD5FA161F4E7314222D7A29 sha1:f8e0a57ad324aa0ce6eafcbee54361cfc3fac7a4 sha256:20B9BA1869ED5D109962522C7C9A09E2675C457EDD780F3723D33F9B40475772
C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Media Player.lnk	Delete	1547	unknown	md5:CDB087898E7B6CA198C7B536CE501C7D sha1:5197b3b496842335d8ba86c4a9bb7f995b3facd8 sha256:1D30728A5B94ED7EE3ADFFA1B98D03433BAF139BB5EFC5E402036E28F8E73921
C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk	Delete	272	unknown	md5:E14F6EF5E8DC4C628FE28AC893E9309D sha1:f29803c16d3e11a196d62026279b72854c4d751f sha256:6142A68127514D4919F584A7541C242C9AF5E471FCDB6065D40133439E8421A1
C:\Users\Administrator\AppData\Roaming\Microsoft\Office\MSO1033.acl	Delete	37762	unknown	md5:20FA6BD2549542BC929AE0CCE8C088D9 sha1:81445de34ad930bb78de7b4ea85a745bc9006564 sha256:C0F0188E5B91B9FA2DECD1FBA77AF6BA22EB1F75F13E7A0B3668300BF3F01364
C:\Users\Administrator\AppData\Roaming\Microsoft\Office\Recent\index.dat	Delete	28	unknown	md5:4E30A3397E81DD38A188E78FC94E5A77 sha1:95e2efa493065e02c7370befbe5a4bc1340cf5ef sha256:DDD0B5A9B8BD9275DDD6BD1D9D033C56734A5BB184B4371E50C2200B903397CB

C:\Users\Administrator\AppData\Roaming\Microsoft\Office\Recent\Templates.LNK	Delete	1114	unknown	md5:AD6A924419F1E8DDAB732FE2A38CAB3C sha1:9c009b032f3f28a23ed67d1467c4043bab896c54 sha256:A85AB1578C24ADABF9638A82787910BC5825CCBB57C4F50124D290D3BFE8D942
C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\CREDHIST	Delete	24	unknown	md5:D0D520FEADE1D2D35693A81854203C7B sha1:885043653125b3b530997257b211487e428f8b sha256:D6A9F19B7BBAB8EDB715634C9874058F9BA1822BEF592839C0AE62552315EC01
C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\S-1-5-21-843043956-3771856219-1177494106-500\5f574c9f-aed5-44f0-8289-329ca0fc690e	Delete	468	unknown	md5:B4E77DC761B2E17B747EA2557CC1DAA7 sha1:3d556bdb77d08046c8dc35a15793e97d69445fec sha256:270E44F47558E601316EEBB391133FAE3B62041A8068881A1B05DB29A140B3E8
C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\S-1-5-21-843043956-3771856219-1177494106-500\Preferred	Delete	24	unknown	md5:523ACBA248A5E9EA774184CFA3B50562 sha1:a06d41821ddfe9da63bc5cbe8ec3e24abd4f63c sha256:201DE973BDC31B25FCE8D17C11BFC08BA5387791EC802E02D722B32A27065224
C:\Users\Administrator\AppData\Roaming\Microsoft\Templates\Normal.dotm	Delete	20526	unknown	md5:C1178AE12FD88E1DB4722F23FDC82583 sha1:a3b0146115df57863a37e12d17e16713e51a37d3 sha256:0BE1B9355E24A8EFB2F46053EAC66552A584BBC1D9E3A826248329FB2D2500C4
C:\Users\Administrator\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	Delete	2	unknown	md5:F3B25701FE362EC84616A93A45CE9998 sha1:d62636d8caec13f04e28442aa6fa1afeb024bbb sha256:B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Cookies\index.dat	Delete	16384	unknown	md5:D7A950FEFD60DBAA01DF2D85FEFB3862 sha1:15740b197555ba8e162c37a6ba655151e3bebae sha256:75D0B1743F61B76A35B1FEDD32378837805DE58D79FA950CB6E8164BFA72073A

C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat	Delete	262144	unknown	md5:764C7EAC8E1B93D65A10E62F8753A399 sha1:aca8c81a60cf7e636f3211b56ed731273274ac63 sha256:945D43A851689DE1B208555EA6F8BA72FF74020AAD1F2CAB5DC7AB15208FECD2
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Libraries\desktop.ini	Delete	274	unknown	md5:453249F95D75EB5E450EB91FA755E1C8 sha1:3e200e187e8cd21d3d1976eaf7356626254de18 sha256:01BEF150C18E377A57843965D55F18F0B5CB3FA867C5AB30F1E67EACD6ECE48A
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms	Delete	3589	unknown	md5:B0EE96F3CA797C1E5074E74F6F7F4C2F sha1:c62c1ce94bfb87819a094c2a2b96539b6d50a0 sha256:9EAC43B23B9772565AE6148D7E2255126D56C64AB8DBEAB0CFAF606542AC6D94
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms	Delete	3546	unknown	md5:4C403BDA2BDE035C6A233E75ECC21CF7 sha1:4533387358656 61021a13866909ec319dd2770f sha256:FF66944935D966CFB0EE32060EF3240BAC13131A788ADD615E4C6B67E7291D37
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms	Delete	3581	unknown	md5:183DF7D961AFEBFBCCE59FFCF0A289CD sha1:80200b9ffae8df8ab93e1fd72181c0576ae1b6 sha256:1592581E89C154A39C4ECFC1964A90AB76F3057848B872F3445282D28901B191
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms	Delete	3560	unknown	md5:FEE3295CAD3EC91D09759F13805B9C1F sha1:e8467161f6a95dadbe35d0a3dd5f9af05696f33a sha256:C41908687A47CE4D2DB6810CE1AB858CAB6CADEEDD153B031375E878DC4BCB5D
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms	Delete	5632	unknown	md5:1B93EE6E009A86CF3BD0BCEE18E0FA94 sha1:e1a2df5e4c1b7933d560419cc60df46e94c6d87 sha256:27DD7A809B251A9C3C07657442227348DFB83FCE8374A8142CC20E02C6CE55AF

C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\7e4dca80246863e3.automaticDestinations-ms	Delete	5120	unknown	md5:0DAB8ADC14BC8DD5ADF7248E410B7962 sha1:784175e915155245db010f4235ea51a0bbabe3e4 sha256:0B10C34A7E713BBD03EFCDE33B7492B7D3F34713E5A75B705D98162DF38F5AD8
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1b4dd67f29cb1962.customDestinations-ms	Delete	24	unknown	md5:B9BD716DE6739E51C620F2086F9C31E4 sha1:9733d9467a3cba277e567af584510edd9febf62 sha256:7116FF028244A01F3D17F1D3BC2E1506BC9999C2E40E388458F0CCCC4E117312
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms	Delete	8044	unknown	md5:4233B4AAE97F761A62F88B11D3AD8299 sha1:e624ae8f2a880ce48fbf710d80ec6767fea1b889 sha256:7D7F84E74D9F64BB20B828B43D9CE26779CF3F90AEDF7049768F04039D21D102
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\5afe4de1b92fc382.customDestinations-ms	Delete	17324	unknown	md5:7ED393F74719F4D84DF54F897BDA15FB sha1:30db9242ff5ed06c48798dc85811fa8dff38a7ef sha256:BBFC95EE7EC82906D0D2DADE0121A445B2DD7E5416F9A3D8397AF09E42EBE66D
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\7e4dca80246863e3.customDestinations-ms	Delete	24	unknown	md5:6852E3A0BF1C01BB4DBFCB51C1A7C087 sha1:707c3647eec303e0801efdf2d4636b3d409f42b9 sha256:74D6D8C58D0BEB0716EEECDC55366E193186924A616E057CD210F4104E5D85E9
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\desktop.ini	Delete	432	unknown	md5:F107D0270E21A2FE91099FDC15918D44 sha1:dabc2f24f4a4e900053743166e5c4175dcf2b2d2d sha256:EB315C9D165B4916E3B00E4D148B53A6C03A2F0694A6A8821D98E76F935CA6A8
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo\Compressed (zipped) Folder.ZFSendToTarget	Delete	3	unknown	md5:963AB0BBEA32F1F9D19AFB00D08BE14D sha1:aec742c8cd57ac5fee0ad76b17e91c6d76608cb3 sha256:7BC88EBB6D01D4DD3EF364010B10F0BBA125BCD23F901F0137CD55D7F3FD4563

C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink	Delete	7	unknown	md5:B2C79AD7DCF03BA266DC0885E1266675 sha1:3b5a9f7948a58d58bd432360863a719c95485504 sha256:68693D02AB4FBB2331B8CC39915322E48E61F06D4D1B31E7D19913202857BC8A
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo\Desktop.ini	Delete	558	unknown	md5:10702225FD4F79C780CF4CDC815EE757 sha1:6677d41e231034e78d2a0403b6b6912869074cae sha256:4388DF4A35071B0A4DD8AD274310F3A4F272E6008AD4DBECECCAC12F0E96086A
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo\Documents.mydocs	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo\Fax Recipient.lnk	Delete	1238	unknown	md5:B8729D4521304A80C9F51E498C6F859A sha1:e44edba07a94a4c0f040fbdfcce2317b8ae2d66c sha256:5D78EB581E6C890D0172A2805A4C6FC0677AA76CBE889CC53A4DFADAFCAA892D
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo\Mail Recipient.MAPIMail	Delete	4	unknown	md5:4DFBB099EAFD3C82E033BF92946D3CE6 sha1:92379cbb8ecf696194b47b619a87e9e4f9a75db2 sha256:07ED6CCF6BF6393D18684D1D4F774639D44C7D2D2895FD30491CCC50614ED4EA
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini	Delete	174	unknown	md5:A2D31A04BC38EEAC22FCA3E30508BA47 sha1:9b7c7a42c831fcd77e77ade6d3d6f033f76893d2 sha256:8E00A24AE458EFFE00A55344F7F34189B4594613284745FF7D406856A196C531
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Desktop.ini	Delete	704	unknown	md5:6F254C82A0513B4D7E19DC34E282820DA sha1:a8b18e5987d5768f369f388051061ec92bfa42ac sha256:D2BB224A86BE552471BB359E9E8AAF3FDE6859F6EBD84F48B121AA0F8961358B

C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Ease of Access.lnk	Delete	1358	unknown	md5:34A52DDC76A09D003765D09276B7720F sha1:3765465fad7cde7b48697ba33c414f109c1b6a6a sha256:439942456CADD72C8A50DB1AD4258DA91AD1235E55CCB9250A8DB5692254717C
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Magnify.lnk	Delete	1258	unknown	md5:AF87D986EF018B88AADE4A257B01865E sha1:fbe6ed4c60950b49991bc8ecffd869557cebbd2d1 sha256:ADC6A967238100D3630FB8040AEC1481E29EFECB0D947695C2606830B9DC09E4
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Narrator.lnk	Delete	1262	unknown	md5:AD86A82AE065094400492FE6354A303A sha1:c415d4f4ed271a596d2888e3e53ea36b6ed5d4a sha256:CA803351EA5E37DA8096E63FE30CA42406351DC803A5F85E3C5D72B022A52A87
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk	Delete	1250	unknown	md5:CD6A30ED8419B84DD18437FD29B9D07F sha1:c40b1eeb78999f32f8f9ec867b116496bf227a8a sha256:AE24A0EBEE300F003B92411633FE126F5AFEAC34303C215BA7FE5F04301C67A7
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Command Prompt.lnk	Delete	1280	unknown	md5:11A856C7323FF0BAF1669FB2346395B7 sha1:a209391b9b2c9435c4a431b6be6eaddacf49f9a sha256:3EC21C18156557770A014933CE14F2D282B37D4C04109262FE81F7CEA2064423
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Desktop.ini	Delete	678	unknown	md5:94F4F5600EC0596ECD43291B8A34AA45 sha1:6e2f8c587750074142f6c5b6e532a312a5517e7a sha256:B6D940DAFFAEEC2225743A4D2851A4CA287B5D847028B46FE3AE8FCE1A3B8EA0
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Notepad.lnk	Delete	1304	unknown	md5:B314F70E2471B24836DC682425597F40 sha1:a64b74e91ba9eae8e0d871c39da516e7d0b2a57f sha256:EACBFB78275CBEA92A3FCB52E9EC2A60F22FD5BBD885899BA255DC1FE0EF6346

C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Run.lnk	Delete	262	unknown	md5:84FA65EB2B09C2B09CD0050731F37CF8 sha1:51ffc6ad339b31707741dc94dc236bb7c75ef504 sha256:284EC026FCA0E384E68BD9B882B6FB06F3E2168E4D635C7EAFC3C35C7854AABB
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\computer.lnk	Delete	262	unknown	md5:658D7ADBDDEB614463CA71663A644C25 sha1:433037dd6227b27eb614d4fa41bb214e8b62a17 sha256:E064C3187AC30780FD7792753C3F28C85A3B49B5C90F0FC55A00C9AF926AE518
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Control Panel.lnk	Delete	262	unknown	md5:46078BD3CB2044421452D214D7473D50 sha1:99fc97a44abb143a78468cfbfd4159cf3dc56ffa sha256:637B252CB21DF410DCC729A3CBD57664D1D1065A65603B9F9C5A9C469ADEF1BD
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Desktop.ini	Delete	738	unknown	md5:3A33FAAC6513738FD86F43DFF8989882 sha1:afd4390e6b63c40e55ca08d27661a23d657b01a2 sha256:21A4315CBAE2B0E8DB633E86C344171DA86F115BCBBB745680FF6F577668C910
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Internet Explorer (No Add-ons).lnk	Delete	1500	unknown	md5:3D63B35AB177BA3ADD8609EFBED13DB9 sha1:a6abbd7b8f0e50a2bcb9b30184e3c82645ee90f6 sha256:EDD0E71993376E3900E9C8CC9394D7878C7A9C4B00E65AAA200F65800E845118
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Private Character Editor.lnk	Delete	1306	unknown	md5:D4EB12E61067C1236E5962399190EE6B sha1:7b3357f2343b9eb0f802ffaa53e2dc58944dc648 sha256:1F2D5547F03B7E98AD48C39A68DFE0A289541DAB3E2FD879F7FF9F48DD664080
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Explorer.lnk	Delete	1228	unknown	md5:47B2E1C4DDD5FA161F4E7314222D7A29 sha1:f8e0a57ad324aa0ce6eafcbee54361cfc3fac7a4 sha256:20B9BA1869ED5D109962522C7C9A09E2675C457EDD780F3723D33F9B40475772

C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools\desktop.ini	Delete	174	unknown	md5:548B310FBC7A26D0B9DA3A9F2D604A0C sha1:1e20c38b721dff06faa8aa69a69e616c228736c1 sha256:BE49AFF1E82FDDFC2AB9DFFFCB7E7BE100800E3653FD1D12B6F8FA6A0957FCAC
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini	Delete	476	unknown	md5:3FBED1EB54DBA794CCA4829601DE00B7 sha1:49893bd0d24a3ad2ad2b697a7bcd677c6f43a1d sha256:E894BC132CF4DA402EDAEB5E9B85ABB5FC8E12551405E06F7A24591FA6755A41
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer (64-bit).lnk	Delete	1416	unknown	md5:A5C694FB4290BE85AFAFC7FA1841A52A sha1:fee464e267b8b3d0d2d044a6b51fdded4c0e2a3e sha256:6C7E66395B85ABF3E65334B04A5C0428C1986D2E9C63B7AE37FDCB1D26024C96
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer.lnk	Delete	1450	unknown	md5:9CF2D6B5B28AB6ACAD862D63BC722277 sha1:13a4853e1c2e8f3ce3c8af61b3c30467c27f16d3 sha256:B80BB975723038437113210B9A694E15F3D5E49A4ED7AAC63138BFCB5D58A542
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\Desktop.ini	Delete	318	unknown	md5:75AFACA653816A09D9DBFBF27722A4F1 sha1:540718309bf55cd5c15eca0244843de15738ac77 sha256:F8C213671E8396EF081532D00929A3D85C7561AFBDD1C4BF4EEEA45244F529FC
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\Help.lnk	Delete	262	unknown	md5:6F824D308D1EA6179653F60CE0329293 sha1:126f4865adad10a7dc1667c3bb43d16d024f8c2 sha256:F2ABAD2FA9D21FFA1625FB923EBE4620F6690AD608A64F37AE9BE99275A6FB99
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini	Delete	174	unknown	md5:7F1698BAB066B764A314A589D338DAAE sha1:524abe4db03afef220a2cc96bf0428fd1b704342 sha256:CDB11958506A5BA5478E22ED472FA3AE422FE9916D674F290207E1FC29AE5A76

C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper.jpg	Delete	642987	unknown	md5:DA288DCEAAFD7C97F1B09C594EAC7868 sha1:b433a6157cc21fc3258495928cd0ef4b487f99d3 sha256:6EA9F8468C76AA511A5B3CFC36FB212B86E7ABD377F147042D2F25572BF206A2
C:\Users\Administrator\Contacts\desktop.ini	Delete	412	unknown	md5:449F2E76E519890A212814D96CE67D64 sha1:a316a38e1a8325bef6f68f18bc967b9aaa8b6ebd sha256:48A6703A09F1197EE85208D5821032B77D20B3368C6B4DE890C44FB482149CF7
C:\Users\Administrator\Desktop\desktop.ini	Delete	282	unknown	md5:9E36CC3537EE9EE1E3B10FA4E761045B sha1:7726f55012e1e26cc762c9982e7c6c54ca7bb303 sha256:4B9D687AC625690FD026ED4B236DAD1CAC90EF69E7AD256CC42766A065B50026
C:\Users\Administrator\Desktop\my.txt	Delete	14	unknown	md5:58C14F51D2848978EBC83AA63B960226 sha1:799ba09aca7e24a13a2720ac7ab2796dbe3d3d06 sha256:B3790CCDC8E1761507B0EDA509A0F4192BC1BC54FF0E5B03559ADEF8243CC9E6
C:\Users\Administrator\Documents\desktop.ini	Delete	402	unknown	md5:ECF88F261853FE08D58E2E903220DA14 sha1:f72807a9e081906654ae19665e681d5938a2e6c sha256:CAFEC240D998E4B6E92AD1329CD417E8E9CBD73157488889FD93A542DE4A4844
C:\Users\Administrator\Documents\my_bank_account.rtf	Delete	272	unknown	md5:3315E3B9CBD373AF0BF4850A3B0E8D22 sha1:a0d1803a2de8a55a73cf157d5685b24be8bb230e sha256:F673ACECB7291704B8D8E9E6478E55E8490AEF68021C4F2D94800A796CED0F7B
C:\Users\Administrator\Documents\my_password.txt	Delete	54	unknown	md5:C38365CDA2216812EC2FF3E6B92B0FA7 sha1:3abfc5e0963a8733ddbeaf6fc8ef7bb5545c1ea3 sha256:6AC09900900C75895436DB42194C81B3937879901FAD68667B30F301EAFBDD9F

C:\Users\Administrator\Downloads\desktop.ini	Delete	282	unknown	md5:3A37312509712D4E12D27240137FF377 sha1:30ced927e23b584725cf16351394175a6d2a9577 sha256:B029393EA7B7CF644FB1C9F984F57C1980077562EE2E15D0FFD049C4C48098D3
C:\Users\Administrator\Favorites\desktop.ini	Delete	402	unknown	md5:881DFAC93652EDB0A8228029BA92D0F5 sha1:5b317253a63fecb167bf07befa05c5ed9c4ccea sha256:A45E345556901CD98B9BF8700B2A263F1DA2B2E53DBDF69B9E6CFAB6E0BD3464
C:\Users\Administrator\Favorites\Links\desktop.ini	Delete	80	unknown	md5:3C106F431417240DA12FD827323B7724 sha1:2345cc77576f666b812b55ea7420b8d2c4d2a0b5 sha256:E469ED17B4B54595B335DC51817A52B81FCF13AAD7B7B994626F84EC097C5D57
C:\Users\Administrator\Favorites\Links\Web Slice Gallery.url	Delete	226	unknown	md5:AD93EAAC4AC4A095F8828F14790C1F8C sha1:f84f24c4ca9d04485a000577e3ef1ca30eede55 sha256:729111C923821A7AD0BB23D1A1DEA03EDBF503CD8B732E2D7EB36CF88EAA0CAC
C:\Users\Administrator\Favorites\Links for United States\desktop.ini	Delete	224	unknown	md5:87A61A68C2DB9B094112D4F4290FB795 sha1:1b5e6ec32415d010e5311caea31df96b294fb65 sha256:E25A84C6E593A5BD6592ECA920FBC126D3E96C8D80F2BB0B17A36E40ED42C1DB
C:\Users\Administrator\Favorites\Links for United States\GobiernoUSA.gov.url	Delete	134	unknown	md5:8D9042FBCBD10F1F3A4E6DB58AC7A496 sha1:22e6e0b361ddb8319cfc375c2226853b41421012 sha256:0E050C4BDB60ED5AE279170B28A45DAE60B7CFFF68EFD603C9CD44200B47980A
C:\Users\Administrator\Favorites\Links for United States\USA.gov.url	Delete	134	unknown	md5:9AD9B8D8511456791E5620A75310E275 sha1:d3e71f08d1c297382326560d9d699bddd482b3f0 sha256:40B010E21BDD1ABBF6D264DD7C58160E7B8D694112E61C6A497B3CB7C0D4C418

C:\Users\Administrator\Favorites\Microsoft Websites\IE Add-on site.url	Delete	133	unknown	md5:2A58591017EA14E620EEB8601BAF646F sha1:162a2c131265ce2b7014492af63dfa3bbb687723 sha256:4277685F26A736EEA792C0FCFD6786B7A49254CC87A989D986D73D058BE184A1
C:\Users\Administrator\Favorites\Microsoft Websites\IE site on Microsoft.com.url	Delete	133	unknown	md5:6B7A44974780C6C44EF6BF44BB0EBA98 sha1:7995d38eadb1f73f3a6dee5367248e6691216c6b sha256:4FA923786C4848E4CA88FD8F230CC1C61BC358B912CD4DD094B6B062352606E9
C:\Users\Administrator\Favorites\Microsoft Websites\Microsoft At Home.url	Delete	133	unknown	md5:673BF2F00CFA19A48514647DFF6071BD sha1:1b08ba362e115fbf57a6ee713d708ca3a45f8fa1 sha256:6DC92AA1565EE1D65F151E002C4C52DB11B6C46BD54ABF1E626538BF02CF078C
C:\Users\Administrator\Favorites\Microsoft Websites\Microsoft At Work.url	Delete	133	unknown	md5:420C53B55FA342510D1DFD7E5688CCF0 sha1:63bb3d32579ee9f0df14a39b73ba1d92bbcf4289 sha256:54C317098A616B8D4C4D4B8FB40CF3EE07D1727605D84999329A3711B850DAD0
C:\Users\Administrator\Favorites\Microsoft Websites\Microsoft Store.url	Delete	134	unknown	md5:F2423E1BC5EA0A0E6E015BAD7F8BF01D sha1:1ab5152ea11ab531bc1ed8df350621f05f4f5455 sha256:C553BB9DC3379F33E130592EE852A6AD8556BC24D89D19143D67BBD1CBC6DAAD
C:\Users\Administrator\Favorites\MSN Websites\MSN Autos.url	Delete	133	unknown	md5:565CD85806D5DEF7E40BEBF0380DB5A6 sha1:9503419e545b85406f957ab470764b0665b04df1 sha256:6EBCE2B3A842F331B1D6FAF48D4FB51C8EF2044EBBB62CB17688CAFFBE9785E8
C:\Users\Administrator\Favorites\MSN Websites\MSN Entertainment.url	Delete	133	unknown	md5:29D291C2200AF2C23EFBC115F2DC5D3A sha1:83aac07b8077870ff013bacfe711afcd12d8d9c2 sha256:4D77C5A2BBB3C5835936BD1D10F544C190446918C38DCC17A883BADCD1DD7A5E

C:\Users\Administrator\Favorites\MSN Websites\MSN Money.url	Delete	133	unknown	md5:0A12FB5CAC3ECA000153F9337EE5DAAC sha1:d0c0e980ad643efb9db6f4c77fbc75e13de4b7dc sha256:7FB0CC9927CEEEDD0CEC19B5D9520561A9825913FAEB81C04D6DA81BA46B0753
C:\Users\Administrator\Favorites\MSN Websites\MSN Sports.url	Delete	133	unknown	md5:8F69786E3EC17011CED26D372EAEB3EE sha1:7371caf81cb1d81bd6ee2830b8e94dcdbd53c35c sha256:BF31E7D0433C5E50C607618481FF09ECC3085AD7C971AAE4BE0EB8A5B41C2CF9
C:\Users\Administrator\Favorites\MSN Websites\MSN.url	Delete	133	unknown	md5:E7B80E9C6721BD7500DB104993F4EC72 sha1:6c59cae06e27926782949f502275075d105bce14 sha256:CBA36D1979C45E4CAC400FB66BF9C6D717BB48BE4658EB01E2CAD96201EA7FD8
C:\Users\Administrator\Favorites\MSN Websites\MSNBC News.url	Delete	133	unknown	md5:0A4FB135AA3002DC7D80B0BEC2AAB5FC sha1:815061cd99ba30fbacf504966ba89949c1d449b sha256:2C494C8B770150F59018BD85FD43C9E107C9574768277BCF02F40081C65A7DB6
C:\Users\Administrator\Favorites\Windows Live\Get Windows Live.url	Delete	133	unknown	md5:C7F2E7D3466314545A62E154E9571FDB sha1:8c9432a693cdfb2edfdd04ad6e5dc7d7465294 sha256:735B6AEAB5624C8F57C1E9152AC07B60E731752B32FF10CE9A580FFD7467C98B
C:\Users\Administrator\Favorites\Windows Live\Windows Live Gallery.url	Delete	133	unknown	md5:70C618F40F686A462C933F3EE7811571 sha1:377c458513f363545e0df395f36ff56af36c61ac sha256:91DD0C1F3267F5C4AAEBD564B515F9ACB9A8EED02D89E12B37449674FFBC5100
C:\Users\Administrator\Favorites\Windows Live\Windows Live Mail.url	Delete	133	unknown	md5:F1D69EC4BC8F3BC62804487B1AFC91FC sha1:dec9eae4a0d8a78d160d6024f72fce9677c800b6 sha256:846EBF1AAFF5D3DBA6707BBC5B013EFA437E1811C87CDE6137D46882E4519313

C:\Users\Administrator\Favorites\Windows Live\Windows Live Spaces.url	Delete	133	unknown	md5:113F4E9D0DB8CDDE7FC2C85B0FDC9FFB sha1:5e0ce3abaffb218f24f346dc395158d282cb706f sha256:B643AED41E6A6B44F6CCDAC91BFB15186C4ED5D1C7A0D2B3451D81BB15885B1F
C:\Users\Administrator\Init\PanConfig.ps1	Delete	503	unknown	md5:19D787441E5ADB19FEFB655961B202DA sha1:ba3e09ec2e9f12de3e4dba282bf7d799f7dc08bf sha256:13F3FF49CFEDB78E6028DB51B213656951C3AEB8E6B8B854E679E4C96254F4EF
C:\Users\Administrator\Kernel\CertMgr.exe	Delete	71168	PE	md5:1B362414EFD15D858DA5039EC83C2B8C sha1:da0374813ec929bac0ebd29988a1f7bfaf1f7f sha256:A76183E748A6ABD3179AFE3DFEF1C1B26629FF4299B58DF68EDDD3FE246942B4
C:\Users\Administrator\Kernel\core.inf	Delete	1814	unknown	md5:347D4603EBC6E627B3FDE7EA9BF16DBD sha1:2c34e3c4b129b6599ff540b9c2101edb765b25d5 sha256:AD88245C54097AF87BB23BE237A77C6C09FB172F677403242C69373BBDCAC9CF
C:\Users\Administrator\Kernel\core.sys	Delete	43416	PE	md5:FB4C34B81BA9BADD8C0439548F818862 sha1:38a31fbbce1f33ca7abe40962a6f78121dcfd2a9 sha256:656A46946FA9C6437B3573BA165D2501B44E7D92ED36E5EFB105703AE1DB7EC1
C:\Users\Administrator\Kernel\PAN\ApiRules.rule	Delete	1	unknown	md5:01ABFC750A0C942167651C40D088531D sha1:d08f88df745fa795b104e4a707a31cfce7b5841 sha256:334359B90EFED75DA5F0ADA1D5E6B256F4A6BD0AEE7EB39C0F90182A021FFC8B
C:\Users\Administrator\Kernel\PAN\FileRules.rule	Delete	5263	unknown	md5:78824A3F3ABAEBFD7E4143279550B963 sha1:90e2f34ed5e568b78f5aeeb4f4e59d716087220b sha256:C38B42DB740277B08342DB7B73D46552B79AC148CD1809218F62E6D533641F0A

C:\Users\Administrator\Kernel\PAN\NetworkRules.rule	Delete	194	unknown	md5:EEE0E7366BCEF5BE13F75D186ED9F54F sha1:b929632125525601aaea91677cdc7311f294cb3f sha256:2EAADCD0BB0BA15445D9DE58C1239A3CBD13A358A73BFE42FF4415E301C1FF35
C:\Users\Administrator\Kernel\PAN\ProcessRules.rule	Delete	957	unknown	md5:1A72838A00B61C80F3F11C64FD5C348A sha1:cc877610c6ecec162bffcb2d377e0d85f3e701f3 sha256:8D24E271483EFBE4F38A4A860D0F96614B8885B34A4D3381C22FC91BD35CFB10
C:\Users\Administrator\Kernel\PAN\RegRules.rule	Delete	14003	unknown	md5:B79A302A973557E5B876DCA592A6C2C5 sha1:4fe77e42e488a8673234d1c18401bc7beaf1e2c1 sha256:A5C1F6323D02B4105F78F1C01AD0D5DF79B1190B49CBCFA236FF8D11D0FBC909
C:\Users\Administrator\Kernel\pnfs64.inf	Delete	2234	unknown	md5:962691F998AB4E8383B1125F23C12DFA sha1:2eb4ea26b1b6f4b54c69b331531dc0f5b6841bd2 sha256:387903DD7DBF99DE0AACB3D3003B545D7CB06B0F649133F3FE84B3FD4027F7A
C:\Users\Administrator\Kernel\pnfs64.sys	Delete	50584	PE	md5:5BB8C38BEB3C729F0D1FBFD2E243D8F4 sha1:2c4c02c6b44ad7ce7ab37bed5f00ede2f5f79f sha256:42EFAD10F9EF990EEF85239EA72C5289F6465BCD401AD82E8FAD1461CF4333A9
C:\Users\Administrator\Kernel\pnfsUser.exe	Delete	15872	PE	md5:B877332F23721338D5A0DBF42517CCDE sha1:aefdf01780b6bc2131fa1fd25a79e135c0371a9 sha256:32101682154B9F70DCBB9EFD4D6807A6721B07F0FF8AEF20E22D0C4D0901C08F
C:\Users\Administrator\Kernel\testcert.cer	Delete	495	unknown	md5:BFDF188015A07943C3ECA0291F6EC99B sha1:71ff2d5754b1f106cc604a58b9c5bf9e644d2f1d sha256:8569F2E0C1C4F7F3993F26DB0B36F17084953BD80775B3A3A2A5F8AF0493FFB8

C:\Users\Administrator\Kernel\x64DriverKickStart.bat	Delete	268	unknown	md5:5921AF529807DA13DD42C2333764E460 sha1:a0055809ec5634df639bbd767a44cbfd4ce49ed8 sha256:04C5BC79F7B51BCE36912F8471ECF1F31BAF82DE772D407F08C5E40965E98679
C:\Users\Administrator\Links\desktop.ini	Delete	580	unknown	md5:DE8858093993987D123060097A2BAD66 sha1:a89e87ba46538cb73aff1a47e4dc0bcfb4760d5 sha256:4C0D757717DEC80ECA8C6CBBFDDA4706EB38FBBB7624933D5429DAFC7BB9F0EC
C:\Users\Administrator\Links\Desktop.lnk	Delete	468	unknown	md5:D27AC07B5082EB540E98A1FACDC65FB3 sha1:3da9de7e5251d71d9118299a75194373a0adddef sha256:CAE75EB756771A8BA2A34ACC460ECBF7A28E497AC7080996B4167F671562E413
C:\Users\Administrator\Links\Downloads.lnk	Delete	895	unknown	md5:6876B22FDF203D01B7FBDDBAB1D7AD91 sha1:a5080c7d1bb830b74910e8383ecdd62849cd3933 sha256:26AB3180F6015B6A62B159C463F7AB8EEDB558C46FB02BD63A3E8C7DE0674D8F
C:\Users\Administrator\Links\RecentPlaces.lnk	Delete	363	unknown	md5:0025C3A7D7C4E90E58332958B00D83C4 sha1:1dd4fdb260f66923004acb5a874111a9d14da38 sha256:36DB348143DA1B5C16B9074940E85761950EE30B533B7CA75924F2F4EF6B253B
C:\Users\Administrator\Music\desktop.ini	Delete	504	unknown	md5:06E8F7E6DDD666DBD323F7D9210F91AE sha1:883ae527ee83ed9346cd82c33dfc0eb97298dc14 sha256:8301E344371B0753D547B429C5FE513908B1C9813144F08549563AC7F4D7DA68
C:\Users\Administrator\ntuser.ini	Delete	20	unknown	md5:6FC234AD3752E1267B34FB12BCD6718B sha1:7894ec01651ff3fcdf9d117f416875bbaef03b6d sha256:5AD8F52071D25165E7E68064AB194EC27A074A3846149ED0689AF23E7F7F2D00

C:\Users\Administrator\officeSetReg.reg	Delete	1804	unknown	md5:7685A80303BBCD9288EACD6E91648147 sha1:1d47965abff896fb6698444633f81e0317e222d sha256:EFA412D2FE53A5B8722C66A8BDE7082CAEDC3B4EE326BE9784BC9F2B9C188140
C:\Users\Administrator\Pictures\desktop.ini	Delete	504	unknown	md5:29EAE335B77F438E05594D86A6CA22FF sha1:d62ccc83c249de6b6532381b4c16a5f17f95d89 sha256:88856962CEF670C087EDA4E07D8F78465BEEABB6143B96BD90F884A80AF925B4
C:\Users\Administrator\Saved Games\desktop.ini	Delete	282	unknown	md5:B441CF59B5A64F74AC3BED45BE9FADFC sha1:3da72a52e451a26ca9a35611fa87160044a7c0bbc sha256:E6FDF8ED07B19B2A3B8EFF05DE7BC71152C85B377B9226F126DC54B58B930311
C:\Users\Administrator\Searches\desktop.ini	Delete	524	unknown	md5:089D48A11BFF0DF720F1079F5DC58A83 sha1:88f1c647378b5b22ebadb465dc80fcfd9e7b97c9 sha256:A9E8AD0792B546A4A8CE49EDA82B327AD9581141312EFEC3AC6F2D3AD5A05F17
C:\Users\Administrator\Searches\Everywhere.search-ms	Delete	248	unknown	md5:0FA26B6C98419B5E7C00EFFFB5835612 sha1:d904d6683a548b03950d94da33cdfccbb55a9bc7 sha256:4094D158E3B0581BA433A46D0DCE62F99D8C0FD1B50BB4D0517DDC0A4A1FDE24
C:\Users\Administrator\Searches\Indexed Locations.search-ms	Delete	248	unknown	md5:B6ACBEB59959AA5412A7565423EA7BAB sha1:4905f02dbef69c83b807a32e9a4b6206bd01dc6 sha256:99653A38C445AE1D4C373EE672339FD47FD098E0D0ADA5F0BE70E3B2BF711D38
C:\Users\Administrator\Videos\desktop.ini	Delete	504	unknown	md5:50A956778107A4272AAE83C86ECE77CB sha1:10bce7ea45077c0baab055e0602eef787dba735e sha256:B287B639F6EDD612F414CAF000C12BA0555ADB3A2643230CBDD5AF4053284978

C:\Users\Administrator\sample.exe	Delete	90725	PE	md5:E01EDE25F5C2BE6F5A27953BCB239D5D sha1:1e66215412704d1ba7373d59c9291b0c67a764af sha256:5F38708709DD47D0B4A323E3A065E5130464102BFFF930275A00AC81DB490308
C:\Users\ADMINI~1\AppData\Local\Temp\nsrD080.tmp\System.dll	Delete	11264	PE	md5:BF712F32249029466FA86756F5546950 sha1:75ac4dc4808ac148ddd78f6b89a51afbd4091c2e sha256:7851CB12FA4131F1FEE5DE390D650EF65CAC561279F1CFE70AD16CC9780210AF

Process Name - sample.exe

(command: C:\Users\Administrator\sample.exe)

Process Activity

Child Process	Action
"C:\Users\ADMINI~1\AppData\Local\Temp\~nsu.tmp\Au_.exe" _?=C:\Users\Administrator\	Create

File Activity

File	Action	Size(B)	File Type	Hash
C:\Users\ADMINI~1\AppData\Local\Temp\nstBCF7.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\~nsu.tmp\Au_.exe	Create	90725	exe	md5:e01ede25f5c2be6f5a27953bcb239d5d sha1:1e66215412704d1ba7373d59c9291b0c67a764af sha256:5f38708709dd47d0b4a323e3a065e5130464102bfff930275a00ac81db490308
C:\Users\ADMINI~1\AppData\Local\Temp\nstBCF7.tmp	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A

Event Timeline

1 Created Process C:\Users\Administrator\sample.exe

2 Created file C:\Users\ADMINI~1\AppData\Local\Temp\nstBCF7.tmp

3 Deleted file C:\Users\ADMINI~1\AppData\Local\Temp\nstBCF7.tmp

4 Created Process "C:\Users\ADMINI~1\AppData\Local\Temp\~nsu.tmp\Au_.exe" _?=C:\Users\Administrator\

5 Created file C:\Users\ADMINI~1\AppData\Local\Temp\nswD050.tmp

6 Deleted file C:\Users\ADMINI~1\AppData\Local\Temp\nswD050.tmp

7 Created file C:\Users\ADMINI~1\AppData\Local\Temp\nsrD080.tmp

8 Deleted file C:\Users\ADMINI~1\AppData\Local\Temp\nsrD080.tmp

9 Created file C:\Users\ADMINI~1\AppData\Local\Temp\nsrD080.tmp\UserInfo.dll

10 Created file C:\Users\ADMINI~1\AppData\Local\Temp\nsrD080.tmp\System.dll

11 Created file C:\Users\ADMINI~1\AppData\Local\Temp\nsrD080.tmp\modern-header.bmp

12 Deleted file C:\Users\Administrator\3rd\7z.dll

13 Deleted file C:\Users\Administrator\3rd\7z.exe

14 Deleted file C:\Users\Administrator\AppData\Local\bluesoleil\bsps.ini

15 Deleted file C:\Users\Administrator\AppData\Local\IconCache.db

16 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds\Feeds for United States~\Popular Government Questions from USA~dgov~.feed-ms

17 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds\Feeds for United States~\USA~dgov Updates~c News and Features~.feed-ms

18 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds\FeedsStore.feedsdb-ms

19 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Home~.feed-ms

20 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Work~.feed-ms

21 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\MSNBC News~.feed-ms

22 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\We Slice Gallery~.feed-ms

23 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\D96JQY3U\desktop.ini

24 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\D96JQY3U\fwlink[1]

25 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\D96JQY3U\fwlink[2]

26 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\desktop.ini

27 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\FUTLFAHL\desktop.ini

28 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\FUTLFAHL\fwlink[1]

29 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\index.dat

30 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\O9YY42MG\desktop.ini

31 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\O9YY42MG\fwlink[1]

32 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\O9YY42MG\fwlink[2]

33 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\Q3FSQLXM\desktop.ini

34 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\Q3FSQLXM\fwlink[1]

35 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Internet Explorer\brndlog.bak

36 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Internet Explorer\brndlog.txt

37 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Media Player\CurrentDatabase_372.wmdb

38 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Media Player\LocalMLS_3.wmdb

39 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\01_Music_auto_rated_at_5_stars.wpl

40 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\02_Music_added_in_the_last_month.wpl

41 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\03_Music_rated_at_4_or_5_stars.wpl

42 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\04_Music_played_in_the_last_month.wpl

43 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\05_Pictures_taken_in_the_last_month.wpl

44 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\06_Pictures_rated_4_or_5_stars.wpl

45 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\07_TV_recorded_in_the_last_week.wpl

46 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\08_Video_rated_at_4_or_5_stars.wpl

47 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\09_Music_played_the_most.wpl

48 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\10_All_Music.wpl

49 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\11_All_Pictures.wpl

50 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004DB2\12_All_Video.wpl

51 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows\1033\StructuredQuerySchema.bin

52 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows\Burn\Burn\desktop.ini

53 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog.etl

54 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog_RunOnce.etl

55 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows\History\desktop.ini

56 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini

57 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat

58 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D76OFA0\desktop.ini

59 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\31L572O7\desktop.ini

60 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\desktop.ini

61 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat

62 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TXJ3UQ95\desktop.ini

63 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YUM4IDPG\desktop.ini

64 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\desktop.ini

65 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows Media\12.0\WMSDKNS.DTD

66 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows Media\12.0\WMSDKNS.XML

67 Deleted file C:\Users\Administrator\AppData\Local\Microsoft\Windows Sidebar\Settings.ini

68 Deleted file C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\1zzfgr18.default\cache2\index

69 Deleted file C:\Users\Administrator\AppData\Local\Temp\ASPNETSetup.log

70 Deleted file C:\Users\Administrator\AppData\Local\Temp\ASPNETSetup_00000.log

71 Deleted file C:\Users\Administrator\AppData\Local\Temp\ASPNETSetup_00001.log

72 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_NDP461-KB3102436-x86-x64-AllOS-ENU_decompression_log.txt

73 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_SetupUtility.txt

74 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredistMSI72EC.txt

75 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredistMSI79FD.txt

76 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredistMSI7A07.txt

77 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredistUI72EC.txt

78 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredistUI79FD.txt

79 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredistUI7A07.txt

80 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_amd64_20180907154104.log

81 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_amd64_20180907154104_000_vcRuntimeMinimum_x64.log

82 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_amd64_20180907154104_001_vcRuntimeAdditional_x64.log

83 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907153904.log

84 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907153904_0_vcRuntimeMinimum_x86.log

85 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907153904_1_vcRuntimeAdditional_x86.log

86 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907153943.log

87 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907153943_0_vcRuntimeMinimum_x86.log

88 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907153943_1_vcRuntimeAdditional_x86.log

89 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907154003.log

90 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907154003_000_vcRuntimeMinimum_x86.log

91 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_vcredist_x86_20180907154003_001_vcRuntimeAdditional_x86.log

92 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_wcf_CA_smci_20180907_224518_374.txt

93 Deleted file C:\Users\Administrator\AppData\Local\Temp\dd_wcf_CA_smci_20180907_224520_280.txt

94 Deleted file C:\Users\Administrator\AppData\Local\Temp\dotNetFx.log

95 Deleted file C:\Users\Administrator\AppData\Local\Temp\F642.tmp

96 Deleted file C:\Users\Administrator\AppData\Local\Temp\InstallPlugin64.exe

97 Deleted file C:\Users\Administrator\AppData\Local\Temp\jusched.log

98 Deleted file C:\Users\Administrator\AppData\Local\Temp\KB2600211_20180907_154410655.html

99 Deleted file C:\Users\Administrator\AppData\Local\Temp\Microsoft .NET Framework 4.6.1 Setup_20180907_154442905-MSI_netfx_Full_x64.msi.txt

100 Deleted file C:\Users\Administrator\AppData\Local\Temp\Microsoft .NET Framework 4.6.1 Setup_20180907_154442905.html

101 Deleted file C:\Users\Administrator\AppData\Local\Temp\Microsoft Visual C++ 2010 x86 Redistributable Setup_20180907_153900955 MSI_vc_red.msi.txt

102 Deleted file C:\Users\Administrator\AppData\Local\Temp\Microsoft Visual C++ 2010 x86 Redistributable Setup_20180907_153900952.html

103 Deleted file C:\Users\Administrator\AppData\Local\Temp\MSI8f258.LOG

104 Deleted file C:\Users\Administrator\AppData\Local\Temp\netfx.log

105 Deleted file C:\Users\Administrator\AppData\Local\Temp\nsrD080.tmp\modern-header.bmp

106 Deleted file C:\Users\Administrator\AppData\Local\Temp\nsrD080.tmp\UserInfo.dll

107 Deleted file C:\Users\Administrator\AppData\Local\Temp\ose00000.exe

108 Deleted file C:\Users\Administrator\AppData\Local\Temp\RGIBB84.tmp

109 Deleted file C:\Users\Administrator\AppData\Local\Temp\RGIBB84.tmp-tmp

110 Deleted file C:\Users\Administrator\AppData\Local\Temp\SetupExe(20180907160837944).log

111 Deleted file C:\Users\Administrator\AppData\Local\Temp\wmsetup.log

112 Deleted file C:\Users\Administrator\AppData\Local\Temp\{1D5DBEAA-1A43-4BD8-BB91-48E4EF702C34}\setup.isn

113 Deleted file C:\Users\Administrator\AppData\Local\Temp\{825EED85-C929-42FA-B378-811E0CED8CA7}\ISBEW64.exe

114 Deleted file C:\Users\Administrator\AppData\LocalLow\Oracle\Java\jdk1.8.0_92_x64\jdk1.8.0_92.msi

115 Deleted file C:\Users\Administrator\AppData\LocalLow\Oracle\Java\jdk1.8.0_92_x64\sj180920.cab

116 Deleted file C:\Users\Administrator\AppData\LocalLow\Oracle\Java\jdk1.8.0_92_x64\ss180920.cab

117 Deleted file C:\Users\Administrator\AppData\LocalLow\Oracle\Java\jdk1.8.0_92_x64\st180920.cab

118 Deleted file C:\Users\Administrator\AppData\LocalLow\Oracle\Java\jdk1.8.0_92_x64\sz180920.cab

119 Deleted file C:\Users\Administrator\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.s

120 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-843043956-3771856219-1177494106-500\61ff37d6c196852c3fe91c028c7590e1_c7928fc6-52fd-4727-ae12-abab87adf76c

121 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Document Building Blocks\1033\14\Built-In Building Blocks.dotx

122 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini

123 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk

124 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\desktop.ini

125 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Internet Explorer.lnk

126 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Explorer.lnk

127 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Media Player.lnk

128 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk

129 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Office\MSO1033.acl

130 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Office\Recent\index.dat

131 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Office\Recent\Templates.LNK

132 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\CREDHIST

133 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\S-1-5-21-843043956-3771856219-1177494106-500\5f574c9 aed5-44f0-8289-329ca0fc690e

134 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\S-1-5-21-843043956-3771856219-1177494106-500\Preferre

135 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Templates\Normal.dotm

136 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC

137 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Cookies\index.dat

138 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat

139 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Libraries\desktop.ini

140 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms

141 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms

142 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms

143 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms

144 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinati ms

145 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\7e4dca80246863e3.automaticDestinati ms

146 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1b4dd67f29cb1962.customDestinations-m

147 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-r

148 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\5afe4de1b92fc382.customDestinations-m

149 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\7e4dca80246863e3.customDestinations-n

150 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\desktop.ini

151 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo\Compressed (zipped) Folder.ZFSendToTarget

152 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink

153 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo\Desktop.ini

154 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo\Documents.mydocs

155 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo\Fax Recipient.lnk

156 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo\Mail Recipient.MAPIMail

157 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini

158 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Desktop.ini

159 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Ease of Access.lnk

160 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Magnify.lnk

161 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Narrator.lnk

162 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk

163 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Command Prompt.lnk

164 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Desktop.ini

165 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Notepad.lnk

166 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Run.lnk

167 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\computer.

168 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Control Panel.lnk

169 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Desktop.ir

170 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Internet Explorer (No Add-ons).lnk

171 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Private Character Editor.lnk

172 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Explorer.lnk

173 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools\desktop.ini

174 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini

175 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer (64-bit).lnk

176 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer.lnk

177 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\Desktop.ini

178 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\Help.lnk

179 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini

180 Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper.jpg

181 Deleted file C:\Users\Administrator\Contacts\desktop.ini

182 Deleted file C:\Users\Administrator\Desktop\desktop.ini

183 Deleted file C:\Users\Administrator\Desktop\my.txt

Deleted file C:\Users\Administrator\Documents\desktop.ini

Deleted file C:\Users\Administrator\Documents\my_bank_account.rtf

Deleted file C:\Users\Administrator\Documents\my_password.txt

Deleted file C:\Users\Administrator\Downloads\desktop.ini

Deleted file C:\Users\Administrator\Favorites\desktop.ini

Deleted file C:\Users\Administrator\Favorites\Links\desktop.ini

Deleted file C:\Users\Administrator\Favorites\Links\Web Slice Gallery.url

Deleted file C:\Users\Administrator\Favorites\Links for United States\desktop.ini

Deleted file C:\Users\Administrator\Favorites\Links for United States\GobiernoUSA.gov.url

Deleted file C:\Users\Administrator\Favorites\Links for United States\USA.gov.url

Deleted file C:\Users\Administrator\Favorites\Microsoft Websites\IE Add-on site.url

Deleted file C:\Users\Administrator\Favorites\Microsoft Websites\IE site on Microsoft.com.url

Deleted file C:\Users\Administrator\Favorites\Microsoft Websites\Microsoft At Home.url

Deleted file C:\Users\Administrator\Favorites\Microsoft Websites\Microsoft At Work.url

Deleted file C:\Users\Administrator\Favorites\Microsoft Websites\Microsoft Store.url

Deleted file C:\Users\Administrator\Favorites\MSN Websites\MSN Autos.url

Deleted file C:\Users\Administrator\Favorites\MSN Websites\MSN Entertainment.url

Deleted file C:\Users\Administrator\Favorites\MSN Websites\MSN Money.url

Deleted file C:\Users\Administrator\Favorites\MSN Websites\MSN Sports.url

Deleted file C:\Users\Administrator\Favorites\MSN Websites\MSN.url

Deleted file C:\Users\Administrator\Favorites\MSN Websites\MSNBC News.url

Deleted file C:\Users\Administrator\Favorites\Windows Live\Get Windows Live.url

Deleted file C:\Users\Administrator\Favorites\Windows Live\Windows Live Gallery.url

Deleted file C:\Users\Administrator\Favorites\Windows Live\Windows Live Mail.url

Deleted file C:\Users\Administrator\Favorites\Windows Live\Windows Live Spaces.url

Deleted file C:\Users\Administrator\Init\PanConfig.ps1

Deleted file C:\Users\Administrator\Kernel\CertMgr.exe

Deleted file C:\Users\Administrator\Kernel\core.inf

Deleted file C:\Users\Administrator\Kernel\core.sys

Deleted file C:\Users\Administrator\Kernel\PAN\ApiRules.rule

Deleted file C:\Users\Administrator\Kernel\PAN\FileRules.rule

Deleted file C:\Users\Administrator\Kernel\PAN\NetworkRules.rule

Deleted file C:\Users\Administrator\Kernel\PAN\ProcessRules.rule

Deleted file C:\Users\Administrator\Kernel\PAN\RegRules.rule

Deleted file C:\Users\Administrator\Kernel\pnfs64.inf

Deleted file C:\Users\Administrator\Kernel\pnfs64.sys

Deleted file C:\Users\Administrator\Kernel\pnfsUser.exe

Deleted file C:\Users\Administrator\Kernel\testcert.cer

Deleted file C:\Users\Administrator\Kernel\x64DriverKickStart.bat

Deleted file C:\Users\Administrator\Links\desktop.ini

Deleted file C:\Users\Administrator\Links\Desktop.lnk

Deleted file C:\Users\Administrator\Links\Downloads.lnk

Deleted file C:\Users\Administrator\Links\RecentPlaces.lnk

Deleted file C:\Users\Administrator\Music\desktop.ini

Deleted file C:\Users\Administrator\ntuser.ini

Deleted file C:\Users\Administrator\officeSetReg.reg

Deleted file C:\Users\Administrator\Pictures\desktop.ini

Deleted file C:\Users\Administrator\Saved Games\desktop.ini

Deleted file C:\Users\Administrator\Searches\desktop.ini

Deleted file C:\Users\Administrator\Searches\Everywhere.search-ms

Deleted file C:\Users\Administrator\Searches\Indexed Locations.search-ms

Deleted file C:\Users\Administrator\Videos\desktop.ini

Deleted file C:\Users\Administrator\sample.exe

Deleted file C:\Users\ADMINI~1\AppData\Local\Temp\nsrD080.tmp\System.dll