

Trends in dForensics, Jun/2013

JK Kim

proneer

proneer@gmail.com

<http://forensic-proof.com>

Security is a people problem...





Digital Forensics Stream

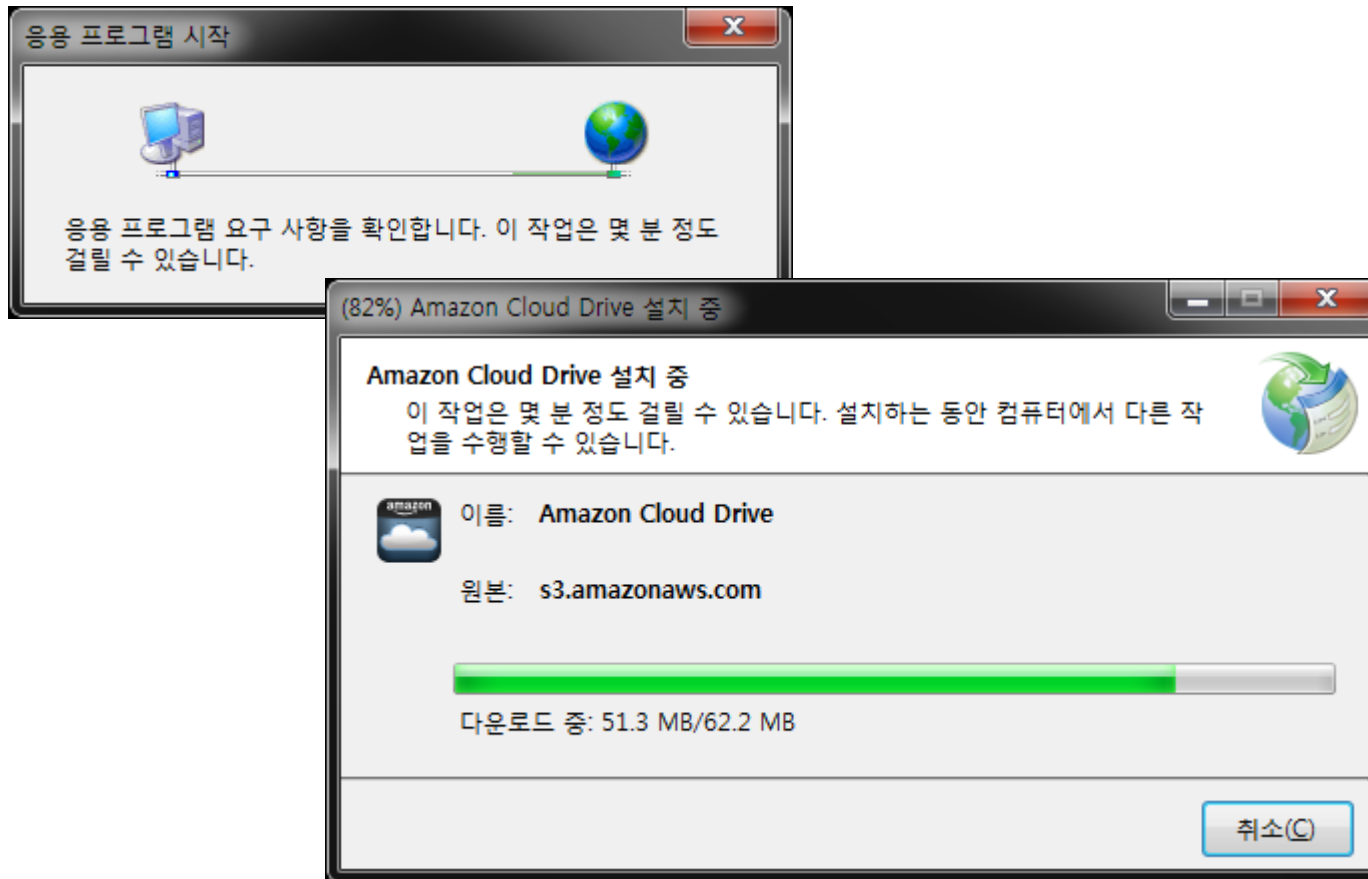
▪ Amazon Cloud Drive Forensics

- 클라우드 이용 방식
 - ✓ 데스크톱 애플리케이션
 - ✓ 온라인 인터페이스 (웹 브라우저)
 - ✓ 모바일 앱 (Amazon Cloud Drive Photos만 존재)



Digital Forensics Stream

Amazon Cloud Drive Forensics – Desktop App





Digital Forensics Stream

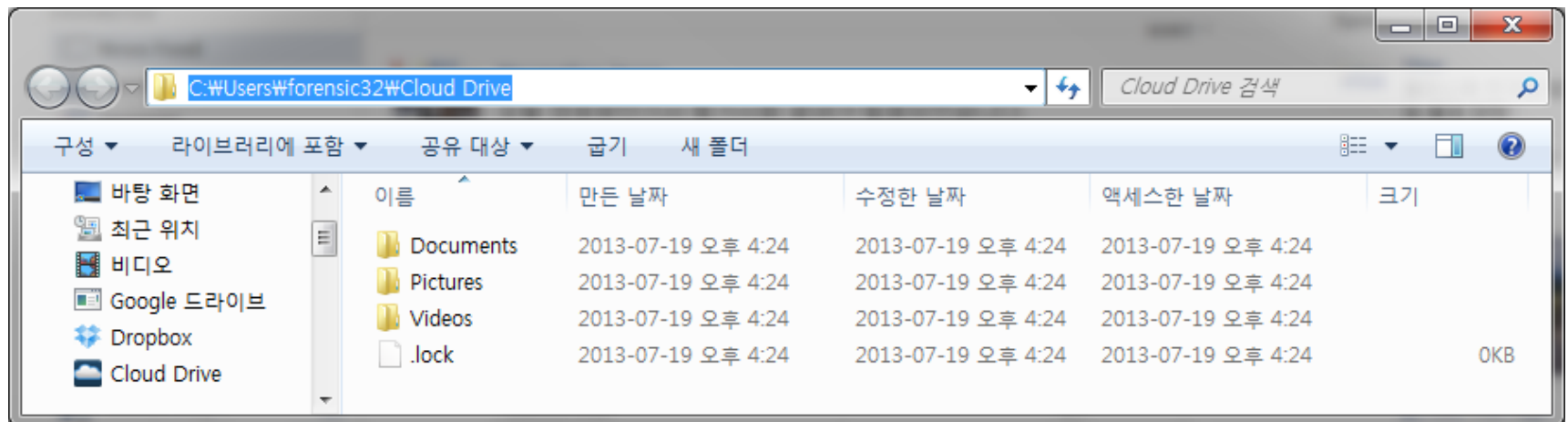
- Amazon Cloud Drive Forensics – Desktop App





Digital Forensics Stream

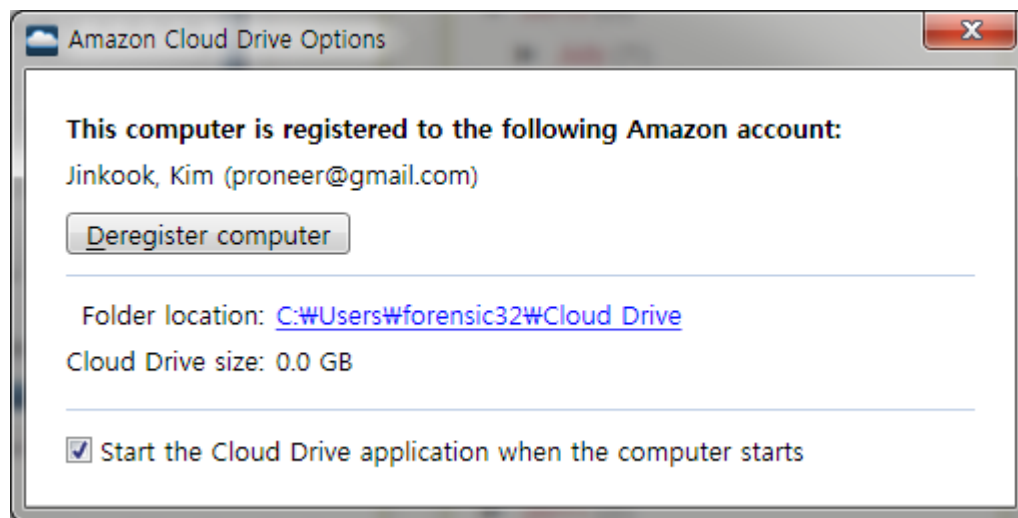
Amazon Cloud Drive Forensics – Desktop App





Digital Forensics Stream

- Amazon Cloud Drive Forensics – Desktop App



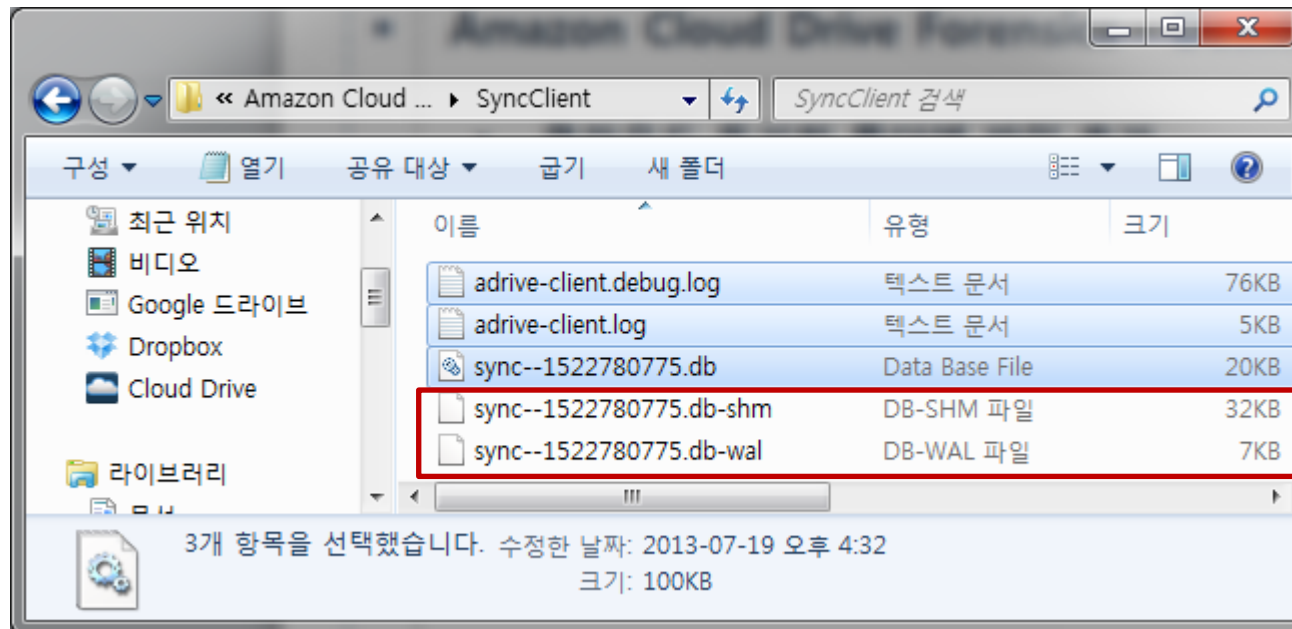


Digital Forensics Stream

Amazon Cloud Drive Forensics – Desktop App Forensic Artifacts

- 클라우드 동기화 폴더에 파일 추가

- ✓ %UserProfile%\AppData\Local\Amazon Cloud Drive\SyncClient



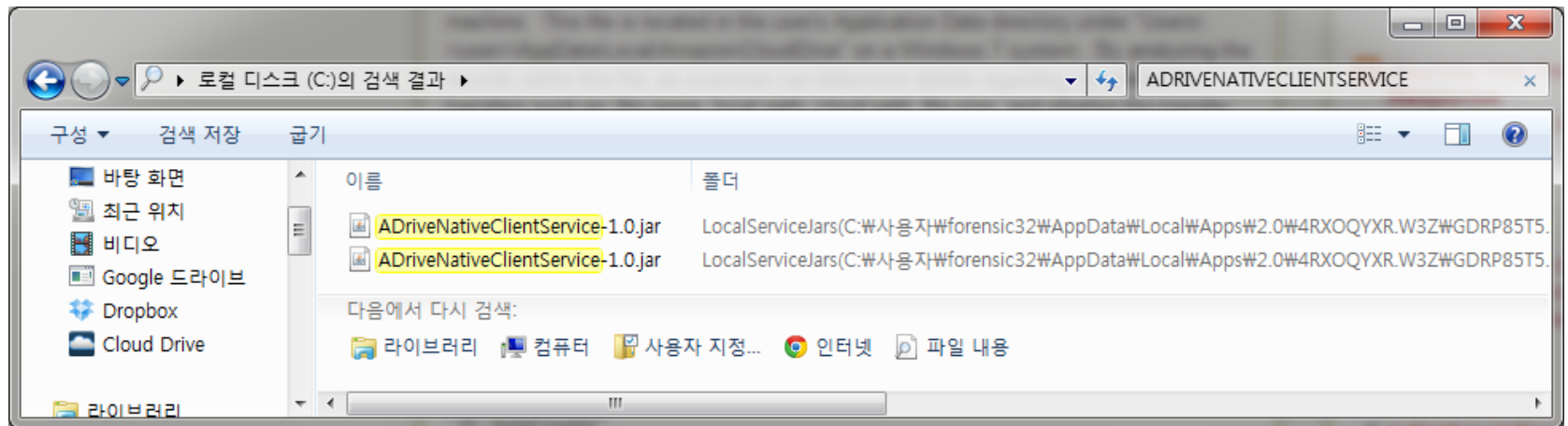
- ✓ Write-Ahead Logging (v3.7.0 부터 rollback journal 대신)



Digital Forensics Stream

Amazon Cloud Drive Forensics – Desktop App Forensic Artifacts

- %UserProfile%\AppData\Local\Amazon Cloud Drive\SyncClient
 - ✓ ADriveNativeClientService.log → **adrive-client.log**
 - ✓ 1319b5c6-2672-49b4-b623-bf5a33fd4c40.db → **sync--1522780775.db**





Digital Forensics Stream

Amazon Cloud Drive Forensics – Desktop App Forensic Artifacts

- %UserProfile%\AppData\Local\Amazon Cloud Drive\SyncClient\adrive-client.log

```
1 INFO 2013-07-19 16:19:15,985 [1] Adrive.Desktop.Application.CloudDriveMain - ProcessGlobals(1).Event::
2 cwd=C:\Users\forensic32\AppData\Local\Apps\2.0\4RXOQYXR.W3Z\GDRP85T5.50A\amaz..tion_f2fa081ea2183235_0002.0001_cb34a912a946f839
3 appdata=C:\Users\forensic32\AppData\Local\Amazon Cloud Drive\SyncClient
4 logconfig=C:\Users\forensic32\AppData\Local\Apps\2.0\4RXOQYXR.W3Z\GDRP85T5.50A\amaz..tion_f2fa081ea2183235_0002.0001_cb34a912a946f839\log4Net.config
5 culture=ko-KR
6 INFO 2013-07-19 16:19:16,006 [1] Adrive.Desktop.Application.CloudDriveMain - Trace(1).Event::Begin customizing the uninstaller
7 INFO 2013-07-19 16:19:16,009 [1] Adrive.Desktop.Common.ClickOnce.ClickOnceHelper - Trace(2).Event::The uninstall string is "C:\Users\forensic32\AppData\Local\Apps\2.0\4RXOQYXR.W3Z\GDRP85T5.50A\amaz..tion_f2fa081ea2183235_0002.0001_cb34a912a946f839\log4Net.config"
8 INFO 2013-07-19 16:19:16,009 [1] Adrive.Desktop.Application.CloudDriveMain - Trace(3).Event::End customizing uninstaller
9 INFO 2013-07-19 16:19:16,096 [1] Adrive.Desktop.Network.NetworkInterfaceDetector - Network availability is initialized as: True
10 INFO 2013-07-19 16:19:16,180 [1] Adrive.Desktop.Models.CloudDriveSyncStateModel - New SyncState: Syncing. Old SyncState:Synced. NetworkState:True
11 ERROR 2013-07-19 16:19:16,300 [1] Adrive.Desktop.Utility.Assume - IsTrue:Cloud Drive Exists
12 위키: Adrive.Desktop.Utility.Assume.LogMethodError(Object message)
13 위키: Adrive.Desktop.Utility.Assume.IsTrue(Boolean condition, Object message)
14 위키: Adrive.Desktop.Providers.SyncFolderProvider..ctor(RegistryKey registryKey)
15 위키: Adrive.Desktop.Application.CloudDriveMain.buildApplication(Application wpfApplication)
16 위키: Adrive.Desktop.Application.CloudDriveMain.Main()
17
18 INFO 2013-07-19 16:19:16,568 [1] Adrive.Desktop.Application.CloudDriveApplication - Trace(4).Event::start()
19 INFO 2013-07-19 16:19:16,599 [1] Adrive.Desktop.Services.NamedPipeAWingService - UnpackJRE()
20 INFO 2013-07-19 16:19:16,617 [1] Adrive.Desktop.Services.ClickOnceUpdater - ClickOnceUpdateLocation=http://s3.amazonaws.com/distro-us/Sync/Windows/2_1_2013_1340/AmazonCloudDrive-update.exe
21 INFO 2013-07-19 16:19:16,617 [1] Adrive.Desktop.Services.ClickOnceUpdater - ClickOnceCurrentVersion=2.1.2013.1340
22 INFO 2013-07-19 16:19:19,791 [3] Adrive.Desktop.Services.NamedPipeAWingService - Awaiting started, port=26330
23 INFO 2013-07-19 16:21:57,673 [1] Adrive.Desktop.Application.CloudDriveMain - ProcessGlobals(1).Event::
24 cwd=C:\Users\forensic32\AppData\Local\Apps\2.0\4RXOQYXR.W3Z\GDRP85T5.50A\amaz..tion_f2fa081ea2183235_0002.0001_cb34a912a946f839
25 appdata=C:\Users\forensic32\AppData\Local\Amazon Cloud Drive\SyncClient
26 logconfig=C:\Users\forensic32\AppData\Local\Apps\2.0\4RXOQYXR.W3Z\GDRP85T5.50A\amaz..tion_f2fa081ea2183235_0002.0001_cb34a912a946f839\log4Net.config
27 culture=ko-KR
28 INFO 2013-07-19 16:22:01,014 [1] Adrive.Desktop.Network.NetworkInterfaceDetector - Network availability is initialized as: True
29 INFO 2013-07-19 16:22:02,021 [1] Adrive.Desktop.Models.CloudDriveSyncStateModel - New SyncState: Syncing. Old SyncState:Synced. NetworkState:True
30 ERROR 2013-07-19 16:22:03,122 [1] Adrive.Desktop.Utility.Assume - IsTrue:Cloud Drive Exists
31 위키: Adrive.Desktop.Utility.Assume.LogMethodError(Object message)
32 위키: Adrive.Desktop.Utility.Assume.IsTrue(Boolean condition, Object message)
33 위키: Adrive.Desktop.Providers.SyncFolderProvider..ctor(RegistryKey registryKey)
34 위키: Adrive.Desktop.Application.CloudDriveMain.buildApplication(Application wpfApplication)
35 위키: Adrive.Desktop.Application.CloudDriveMain.Main()
36
37 INFO 2013-07-19 16:22:04,600 [1] Adrive.Desktop.Application.CloudDriveApplication - Trace(1).Event::start()
38 INFO 2013-07-19 16:22:04,607 [1] Adrive.Desktop.Services.NamedPipeAWingService - UnpackJRE()
39 INFO 2013-07-19 16:22:10,228 [3] Adrive.Desktop.Services.NamedPipeAWingService - Awaiting started, port=26330
40 INFO 2013-07-19 16:23:58,565 [1] Adrive.Desktop.Application.CloudDriveApplication - Trace(2).Event::Starting Sync...
41 INFO 2013-07-19 16:24:19,943 [1] Adrive.Desktop.Models.CloudDriveSyncStateModel - New SyncState: Syncing. Old SyncState:Synced. NetworkState:True
42 INFO 2013-07-19 16:29:25,407 [1] Adrive.Desktop.Models.CloudDriveSyncStateModel - New SyncState: Syncing. Old SyncState:Synced. NetworkState:True
43 INFO 2013-07-19 16:29:45,437 [1] Adrive.Desktop.Models.CloudDriveSyncStateModel - New SyncState: Syncing. Old SyncState:Syncing. NetworkState:True
44 INFO 2013-07-19 16:31:35,604 [1] Adrive.Desktop.Models.CloudDriveSyncStateModel - New SyncState: Syncing. Old SyncState:Synced. NetworkState:True
45 INFO 2013-07-19 16:31:55,633 [1] Adrive.Desktop.Models.CloudDriveSyncStateModel - New SyncState: Synced. Old SyncState:Syncing. NetworkState:True
46 INFO 2013-07-19 16:32:10,657 [1] Adrive.Desktop.Models.CloudDriveSyncStateModel - New SyncState: Syncing. Old SyncState:Synced. NetworkState:True
47 INFO 2013-07-19 16:32:30,686 [1] Adrive.Desktop.Models.CloudDriveSyncStateModel - New SyncState: Synced. Old SyncState:Syncing. NetworkState:True
```



Digital Forensics Stream

Amazon Cloud Drive Forensics – Desktop App Forensic Artifacts

- %UserProfile%\AppData\Local\Amazon Cloud Drive\SyncClient\adrive-client.debug.log

```
1 INFO 2013-07-19 16:19:15,985 [1] Adrive.Desktop.Application.CloudDriveMain - ProcessGlobals(1).Event::
2 cwd=C:\Users\forensic32\AppData\Local\Apps\2.0\4RXOQYXR.W3Z\GDRP85T5.50A\amaz..tion_f2fa081ea2183235_0002.0001_cb34a912a946f839
3 appdata=C:\Users\forensic32\AppData\Local\Amazon Cloud Drive\SyncClient
4 logconfig=C:\Users\forensic32\AppData\Local\Apps\2.0\4RXOQYXR.W3Z\GDRP85T5.50A\amaz..tion_f2fa081ea2183235_0002.0001_cb34a912a946f839\log4Net.config
5 culture=ko-KR
6 INFO 2013-07-19 16:19:16,006 [1] Adrive.Desktop.Application.CloudDriveMain - Trace(1).Event::Begin customizing the uninstaller
7 INFO 2013-07-19 16:19:16,009 [1] Adrive.Desktop.Common.ClickOnce.ClickOnceHelper - Trace(2).Event::The uninstall string is "C:\Users\forensic32\AppData\Local\Apps\2.0\4RXOQYXR.W3Z\GDRP85T5.50A\amaz..tion_f2fa081ea2183235_0002.0001_cb34a912a946f839\log4Net.config"
8 INFO 2013-07-19 16:19:16,009 [1] Adrive.Desktop.Application.CloudDriveMain - Trace(3).Event::End customizing uninstaller
9 INFO 2013-07-19 16:19:16,096 [1] Adrive.Desktop.Network.NetworkInterfaceDetector - Network availability is initialized as: True
10 DEBUG 2013-07-19 16:19:16,180 [1] Adrive.Desktop.Models.CloudDriveSyncStateModel - New SyncState: Syncing. Old SyncState: Synced. NetworkState: True
11 INFO 2013-07-19 16:19:16,180 [1] Adrive.Desktop.Models.CloudDriveSyncStateModel - New SyncState: Syncing. Old SyncState: Synced. NetworkState: True
12 ERROR 2013-07-19 16:19:16,300 [1] Adrive.Desktop.Utility.Assume - IsTrue::Cloud Drive Exists
13 위치: Adrive.Desktop.Utility.Assume.LogMethodError(Object message)
14 위치: Adrive.Desktop.Utility.Assume.IsTrue(Boolean condition, Object message)
15 위치: Adrive.Desktop.Providers.SyncFolderProvider..ctor(RegistryKey registryKey)
16 위치: Adrive.Desktop.Application.CloudDriveMain.buildApplication(Application wpfApplication)
17 위치: Adrive.Desktop.Application.CloudDriveMain.Main()
18
19 INFO 2013-07-19 16:19:16,568 [1] Adrive.Desktop.Application.CloudDriveApplication - Trace(4).Event::start()
20 INFO 2013-07-19 16:19:16,599 [1] Adrive.Desktop.Services.NamedPipeAwningService - UnpackJRE()
21 INFO 2013-07-19 16:19:16,617 [1] Adrive.Desktop.Services.ClickOnceUpdater - ClickOnceUpdateLocation=http://s3.amazonaws.com/distro-us/Sync/Windows/2_1_2013_1340/AmazonCloudDrive-update.s
22 INFO 2013-07-19 16:19:16,617 [1] Adrive.Desktop.Services.ClickOnceUpdater - ClickOnceCurrentVersion=2.1.2013.1340
23 DEBUG 2013-07-19 16:19:18,348 [1] Adrive.Desktop.Models.CloudDriveSyncStateModel - Sync state has been changed to Syncing
24 INFO 2013-07-19 16:19:19,791 [3] Adrive.Desktop.Services.NamedPipeAwningService - Awing started, port=26330
25 DEBUG 2013-07-19 16:19:20,094 [1] Adrive.Desktop.Services.LocalServiceRequest - method=getAllLinks, id=1, url=http://127.0.0.1:26330
26 DEBUG 2013-07-19 16:19:20,278 [1] Adrive.Desktop.Services.ADriveLocalService - httpResponse={"id":1,"result":{"links":{"Help":"https://www.amazon.com/clouddrive/help","ThirdPartyLicenses":
27 DEBUG 2013-07-19 16:19:25,330 [1] Adrive.Desktop.Services.LocalServiceRequest - method=getAllLinks, id=2, url=http://127.0.0.1:26330
28 DEBUG 2013-07-19 16:19:25,336 [1] Adrive.Desktop.Services.ADriveLocalService - httpResponse={"id":2,"result":{"links":{"Help":"https://www.amazon.com/clouddrive/help","ThirdPartyLicenses":
29 DEBUG 2013-07-19 16:19:30,354 [1] Adrive.Desktop.Services.LocalServiceRequest - method=getAllLinks, id=3, url=http://127.0.0.1:26330
30 DEBUG 2013-07-19 16:19:30,360 [1] Adrive.Desktop.Services.ADriveLocalService - httpResponse={"id":3,"result":{"links":{"Help":"https://www.amazon.com/clouddrive/help","ThirdPartyLicenses":
31 DEBUG 2013-07-19 16:19:35,409 [1] Adrive.Desktop.Services.LocalServiceRequest - method=getAllLinks, id=4, url=http://127.0.0.1:26330
32 DEBUG 2013-07-19 16:19:35,424 [1] Adrive.Desktop.Services.ADriveLocalService - httpResponse={"id":4,"result":{"links":{"Help":"https://www.amazon.com/clouddrive/help","ThirdPartyLicenses":
33 DEBUG 2013-07-19 16:19:40,415 [1] Adrive.Desktop.Services.LocalServiceRequest - method=getAllLinks, id=5, url=http://127.0.0.1:26330
34 DEBUG 2013-07-19 16:19:40,421 [1] Adrive.Desktop.Services.ADriveLocalService - httpResponse={"id":5,"result":{"links":{"Help":"https://www.amazon.com/clouddrive/help","ThirdPartyLicenses":
35 DEBUG 2013-07-19 16:19:45,427 [1] Adrive.Desktop.Services.LocalServiceRequest - method=getAllLinks, id=6, url=http://127.0.0.1:26330
36 DEBUG 2013-07-19 16:19:45,432 [1] Adrive.Desktop.Services.ADriveLocalService - httpResponse={"id":6,"result":{"links":{"Help":"https://www.amazon.com/clouddrive/help","ThirdPartyLicenses":
37 DEBUG 2013-07-19 16:19:50,431 [1] Adrive.Desktop.Services.LocalServiceRequest - method=getAllLinks, id=7, url=http://127.0.0.1:26330
38 DEBUG 2013-07-19 16:19:50,439 [1] Adrive.Desktop.Services.ADriveLocalService - httpResponse={"id":7,"result":{"links":{"Help":"https://www.amazon.com/clouddrive/help","ThirdPartyLicenses":
39 DEBUG 2013-07-19 16:19:55,438 [1] Adrive.Desktop.Services.LocalServiceRequest - method=getAllLinks, id=8, url=http://127.0.0.1:26330
40 DEBUG 2013-07-19 16:19:55,444 [1] Adrive.Desktop.Services.ADriveLocalService - httpResponse={"id":8,"result":{"links":{"Help":"https://www.amazon.com/clouddrive/help","ThirdPartyLicenses":
41 DEBUG 2013-07-19 16:20:00,446 [1] Adrive.Desktop.Services.LocalServiceRequest - method=getAllLinks, id=9, url=http://127.0.0.1:26330
42 DEBUG 2013-07-19 16:20:00,450 [1] Adrive.Desktop.Services.ADriveLocalService - httpResponse={"id":9,"result":{"links":{"Help":"https://www.amazon.com/clouddrive/help","ThirdPartyLicenses":
43 DEBUG 2013-07-19 16:20:05,474 [1] Adrive.Desktop.Services.LocalServiceRequest - method=getAllLinks, id=10, url=http://127.0.0.1:26330
44 DEBUG 2013-07-19 16:20:05,480 [1] Adrive.Desktop.Services.ADriveLocalService - httpResponse={"id":10,"result":{"links":{"Help":"https://www.amazon.com/clouddrive/help","ThirdPartyLicense":
45 DEBUG 2013-07-19 16:20:10,496 [1] Adrive.Desktop.Services.LocalServiceRequest - method=getAllLinks, id=11, url=http://127.0.0.1:26330
46 DEBUG 2013-07-19 16:20:10,501 [1] Adrive.Desktop.Services.ADriveLocalService - httpResponse={"id":11,"result":{"links":{"Help":"https://www.amazon.com/clouddrive/help","ThirdPartyLicense":
47 DEBUG 2013-07-19 16:20:15,505 [1] Adrive.Desktop.Services.LocalServiceRequest - method=getAllLinks, id=12, url=http://127.0.0.1:26330
```



Digital Forensics Stream

▪ Amazon Cloud Drive Forensics – Desktop App Forensic Artifacts

- %UserProfile%\AppData\Local\Amazon Cloud Drive\SyncClient\adrive-client.debug.log

```
INFO 2013-07-19 16:23:58,565 [1] Adrive.Desktop.Application.CloudDriveApplication - Trace(2).Event::Starting Sync...
DEBUG 2013-07-19 16:23:58,566 [1] Adrive.Desktop.Services.LocalServiceRequest - method=startSync, id=20,
url=http://127.0.0.1:26330
DEBUG 2013-07-19 16:24:00,716 [1] Adrive.Desktop.Services.LocalServiceRequest - method=getAllLinks, id=21,
url=http://127.0.0.1:26330
DEBUG 2013-07-19 16:24:02,133 [1] Adrive.Desktop.Services.ADriveLocalService -
httpResponse={"id":21,"result":{"links":{"Help":"https://www.amazon.com/cloudrive/help","ThirdPartyLicenses":"https://www.amazon.com/gp/drive/attribution","Manage":"https://www.amazon.com/cloudrive/manage","CloudDriveWebPage":"https://www.amazon.com/cloudrive","Feedback":"https://www.amazon.com/cloudrive/feedback","Faq":"https://www.amazon.com/help/cloudrive/errors","DeletedItems":"https://www.amazon.com/cloudrive?sf=1&cdpath=DeletedItems","TermsOfUse":"https://www.amazon.com/gp/drive/tou"},"default":false},"jsonrpc":"2.0"}
DEBUG 2013-07-19 16:24:03,909 [1] Adrive.Desktop.Services.ADriveLocalService -
httpResponse={"id":20,"result":{"name":"SYNCING","state":1},"jsonrpc":"2.0"}
```



Digital Forensics Stream

▪ Amazon Cloud Drive Forensics – Desktop App Forensic Artifacts

- %UserProfile%\AppData\Local\Amazon Cloud Drive\SyncClient\sync--1522780775.db

✓ Table

- filter__resolve
- local_scan
- remote_scan
- synced



Digital Forensics Stream

Amazon Cloud Drive Forensics – Desktop App Forensic Artifacts

- %UserProfile%\AppData\Local\Amazon Cloud Drive\SyncClient\sync--1522780775.db

✓ **Table:** local_scan

RecNo	inode_id	path	data
Click here to define a filter			
1	1688849860308639	#Pictures	...
2	1688849860308640	#Documents	
3	1688849860308641	#Pictures#proneer.JPG	
4	1688849860308642	#Documents#Dropbox analysis, Data remnants on user machines.pdf	
5	2814749767151262	#Videos	
6	365073044793741747	#Documents#[F-INSIGHT] Trends in dForensics (Jun, 2013).pptx	



Digital Forensics Stream

Amazon Cloud Drive Forensics – Desktop App Forensic Artifacts

- %UserProfile%\AppData\Local\Amazon Cloud Drive\SyncClient\sync--1522780775.db

✓ **Table:** remote_scan

RecNo	object_id	parent_id	data	md5	filter_status
Click here to define a filter					
1	f437c55a-d65d-4660-9e2c-cee1a10712b0	5d556e2c-eb31-435e-b8f5-20174a0398fe	...	<null>	1
2	496b622a-34f8-4ac3-b837-e5b62603e8d3	5d556e2c-eb31-435e-b8f5-20174a0398fe		<null>	1
3	a13e50d1-19a6-401b-95dd-54b6aa8fdd71	496b622a-34f8-4ac3-b837-e5b62603e8d3		5fdfc01d91b0c8a99d5d97c4c575492c	1
4	a5b2cd11-8f55-49b3-984b-62843483234c	7395c903-c5e8-4fa6-8aa5-d4cd59174c64		a61468b7e982b699482c4d824b752d86	1
5	56b701c6-2eaf-47cb-8fdd-5a76003393a9	c183a7d0-3fb3-429c-b244-3edf781b4a35		3ef0f13fd5f90ef169a6bc20335425c7	4
6	8a3aca80-6ffb-4a1b-9bca-0d14586eefa4	c183a7d0-3fb3-429c-b244-3edf781b4a35		3ef0f13fd5f90ef169a6bc20335425c7	4
7	a2b4fff8-0419-4694-a304-6b03e06a32c6	7395c903-c5e8-4fa6-8aa5-d4cd59174c64		3ef0f13fd5f90ef169a6bc20335425c7	1
8	7395c903-c5e8-4fa6-8aa5-d4cd59174c64	5d556e2c-eb31-435e-b8f5-20174a0398fe		<null>	1



Digital Forensics Stream

Amazon Cloud Drive Forensics – Desktop App Forensic Artifacts

- %UserProfile%\AppData\Local\Amazon Cloud Drive\SyncClient\sync--1522780775.db

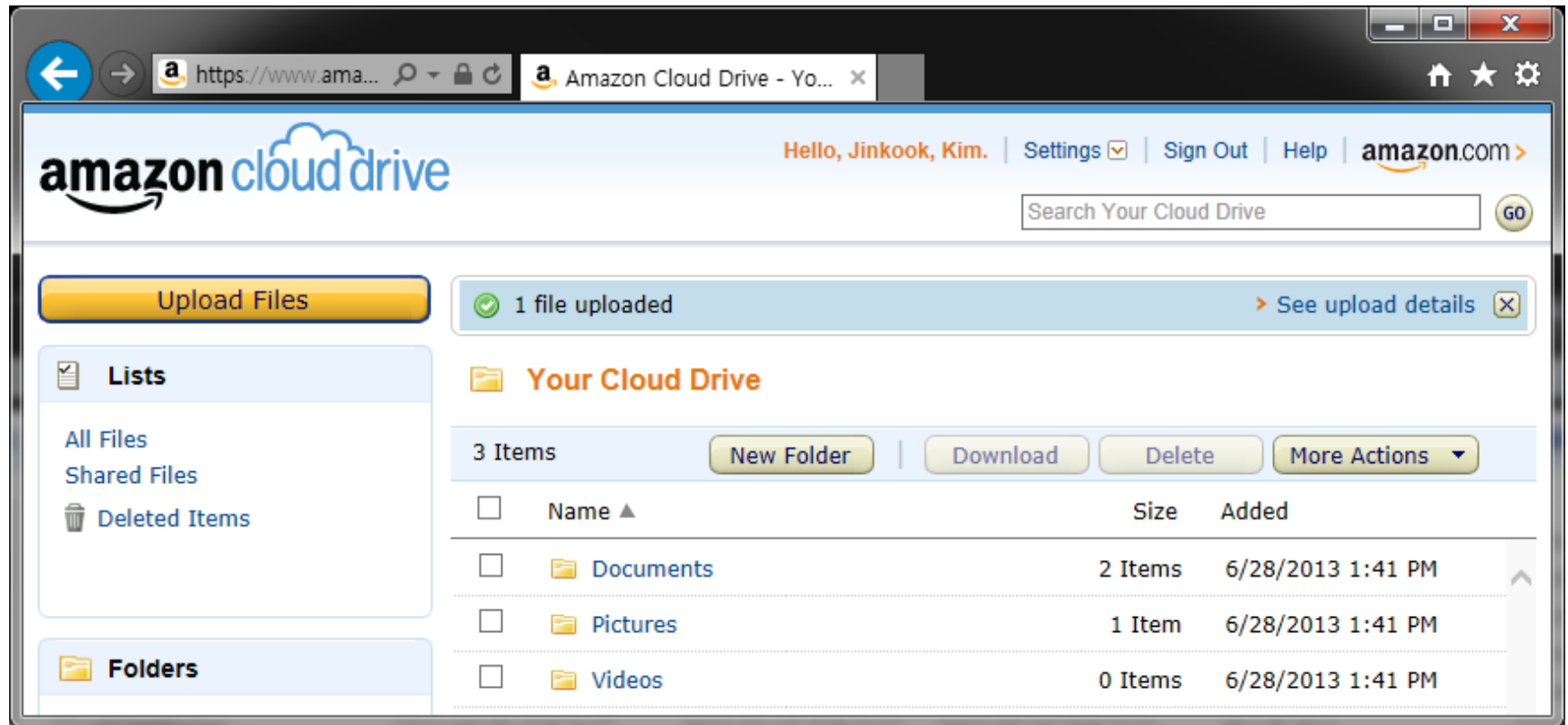
✓ **Table:** synced

RecNo	local_id	remote_id	local_path	local_data	remote_parent_id	remote_data	synced_md5
Click here to define a filter							
1	1688849860308639	496b622a-34f8-4ac3-b837-e5b62603e8d3	#Pictures	...	5d556e2c-eb31-435e-b8f5-20174a0398fe	...	<null>
2	1688849860308640	7395c903-c5e8-4fa6-8aa5-d4cd59174c64	#Documents		5d556e2c-eb31-435e-b8f5-20174a0398fe		<null>
3	1688849860308641	a13e50d1-19a6-401b-95dd-54b6aa8fdd71	#Pictures#proneer.JPG		496b622a-34f8-4ac3-b837-e5b62603e8d3		5fdcf01d91b0c8a99d5d97c4c575492c
4	1688849860308642	a5b2cd11-8f55-49b3-984b-62843483234c	#Documents#Dropbox analysis, Data remnants on user machines.pdf		7395c903-c5e8-4fa6-8aa5-d4cd59174c64		a61468b7e982b699482c4d824b752d86
5	2814749767151262	f437c55a-d65d-4660-9e2c-cee1a10712b0	#Videos		5d556e2c-eb31-435e-b8f5-20174a0398fe		<null>
6	365073044793741747	a2b4fff8-0419-4694-a304-6b03e06a32c6	#Documents#[F-INSIGHT] Trends in dForensics (Jun, 2013).pptx		7395c903-c5e8-4fa6-8aa5-d4cd59174c64		3ef0f13fd5f90ef169a6bc20335425c7



Digital Forensics Stream

- Amazon Cloud Drive Forensics – Web Browser App





Digital Forensics Stream

- Amazon Cloud Drive Forensics – Web Browser App

The screenshot shows the Amazon Cloud Drive web interface. The browser address bar displays <https://www.amazon.com/cloudrive>. The page header includes the Amazon Cloud Drive logo, a greeting "Hello, Jinkook, Kim.", and links for "Settings", "Sign Out", "Help", and "amazon.com". A search bar labeled "Search Your Cloud Drive" is also present.

On the left sidebar, under the "Lists" section, "Deleted Items" is selected. The main content area shows a notification "1 file uploaded" and a section titled "Deleted Items" with a trash can icon. Below this, it says "3 Items" and provides buttons for "Permanently Delete All" (highlighted with a red box) and "Restore To Folder".

A table of deleted items is displayed, with the entire table area highlighted by a red box. The table has columns for "Name", "Folder", "Size", and "Deleted".

<input type="checkbox"/>	Name	Folder	Size	Deleted
<input type="checkbox"/>	[F-INSIGHT] Trends in dForensics (Jun, 2013) (3).pptx	Documents	775.6 KB	7/19/2013 5:11 PM
<input type="checkbox"/>	[F-INSIGHT] Trends in dForensics (Jun, 2013) (2).pptx	Documents	775.6 KB	7/19/2013 4:31 PM
<input type="checkbox"/>	[F-INSIGHT] Trends in dForensics (Jun, 2013).pptx	Documents	775.6 KB	7/19/2013 4:31 PM



Digital Forensics Stream

- **Amazon Cloud Drive Forensics – Web Browser App Forensic Artifacts**
 - %UserProfile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\
 - ✓ **ACD 브라우저 캐시 파일**이 존재하지 않음



Digital Forensics Stream

▪ Amazon Cloud Drive Forensics – Web Browser App Forensic Artifacts

- %UserProfile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\

apiCA20H5UW.json

```
https://www.amazon.com/clouddrive/api/?_=1374221497170&Operation=selectMetadata&customerId=AQKWZ4UCHAU02&ContentType=JSON&query=select+count(*)+from+object+where+hidden+!%3D+true+and+paren  
tObjectId%3D'c183a7d0-3fb3-429c-b244-3edf781b4a35'+and+status+!%3D+'PENDING'+and+type+!%3D+'RECYCLE'
```

_timestamp__2013-07-

19T08_11_13.724Z}_{_metricIdentifier__Delete_,_selectAll__No_,_numberOfFiles__1,_context__List_,_timestamp__2013-07-19T08_11_35[1].gif

```
https://fls-na.amazon.com/1/adrive-  
metrics/1/OP/customerId=AQKWZ4UCHAU02;%7B%22metricIdentifier%22:%22uploadButtonClicked%22,%22co  
ntext%22:%22List%22,%22timestamp%22:%222013-07-  
19T08:11:13.724Z%22%7D;%7B%22metricIdentifier%22:%22Delete%22,%22selectAll%22:%22No%22,%22number  
OfFiles%22:1,%22context%22:%22List%22,%22timestamp%22:%222013-07-19T08:11:35.044Z%22%7D;
```



Digital Forensics Stream

▪ Amazon Cloud Drive Forensics – Web Browser App Forensic Artifacts

- %UserProfile%\AppData\Local\Microsoft\Windows\History\History.IE5\

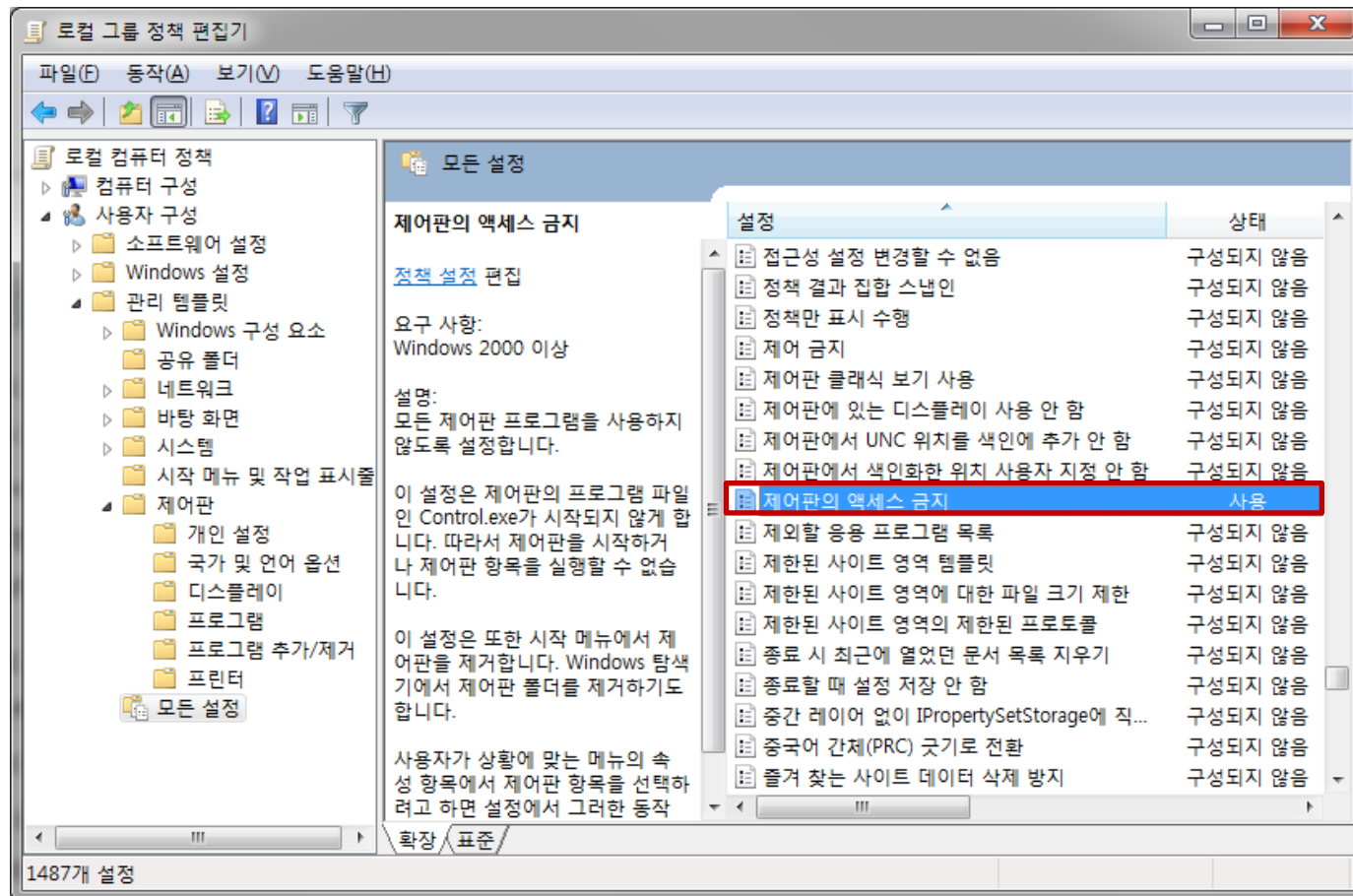
Visited:

forensic32@[forensicsight.org](https://www.amazon.com/clouddrive?_encoding=UTF8&ref_=cd_spl_def_ycd&sf=1&openid.assoc_handle=amzn_clouddrive_us&aToken=5%7CjSAVqSVWYsOS2JvwHHA5SJQmz%2BIs%2Be4wLFNGrb1nd424U7DDaWe%2BxqIK9gZYY3%2FE%2BRDlxx1%2F3aDtvTIV%2BPAIRY8Iz7Ngs7bj5U0QejWtM6TkzK2bIl%2FOdBYe%2F98UTUNrVZMRTnA9nSlpnqxHiEE75aey3CIYUOGTwSKDESIYpk8jl15245REqsdD%2FSo9I9o20nO9BfPSn52CKwNWO75EoYKVQ1KMGwY&openid.claimed_id=https%3A%2F%2Fwww.amazon.com%2Fap%2Fid%2Famzn1.account.AF55WGWLGWZNPTQTZZENLULFQV2A&openid.identity=https%3A%2F%2Fwww.amazon.com%2Fap%2Fid%2Famzn1.account.AFS5WGWLGWZNPTQTZZENLULFQV2A&openid.mode=id_res&openid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0&openid.op_endpoint=https%3A%2F%2Fwww.amazon.com%2Fap%2Fsignin&openid.response_nonce=2013-07-19T10%3A08%3A47Z6526231790617976937&openid.return_to=https%3A%2F%2Fwww.amazon.com%2Fclouddrive%3F_encoding%3DUTF8%26ref_%3Dcd_spl_def_ycd%26sf%3D1&openid.signed=assoc_handle%2CaToken%2Cclaimed_id%2Cidentity%2Cmode%2Cns%2Cop_endpoint%2Cresponse_nonce%2Creturn_to%2Cpape.auth_policies%2Cpape.auth_time%2Cns.pape%2Csigned&openid.ns.pape=http%3A%2F%2Fspecs.openid.net%2Fextensions%2Fpape%2F1.0&openid.pape.auth_policies=http%3A%2F%2Fschemas.openid.net%2Fpape%2Fpolicies%2F2007%2F06%2Fnone&openid.pape.auth_time=2013-07-19T10%3A08%3A47Z&openid.sig=LoWsvL%2FKPm9M%2FVUN8GgOJBjrb%2FLb5Z1UOc71E5hOyspo%3D&</p></div><div data-bbox=)



SANS Computer Forensics Blog

- Control Panel Forensics: Evidence of Time Manipulation and More
 - GUI Control Panel





SANS Computer Forensics Blog

▪ Control Panel Forensics: Evidence of Time Manipulation and More

- 제어판 감사 항목

- ✓ 비인가된 소프트웨어에 의해 방화벽 설정 변경 (firewall.cpl)
- ✓ 사용자 계정 추가 혹은 수정 (nusrmgr.cpl)
- ✓ 시스템 복원 및 볼륨 새도 복사본 끄기 (sysdm.cpl)
- ✓ 시스템 시간 변경 (timedate.cpl)
- ✓ 타사 보안 소프트웨어 애플릿과의 통신



SANS Computer Forensics Blog

▪ Control Panel Forensics: Evidence of Time Manipulation and More

• 제어판 구성

- ✓ 제어판은 다수의 애플릿(.cpl)으로 구성 (%SystemRoot%\System32 폴더에 존재)
- ✓ 애플릿 접근 방법
 - GUI 제어판 이용
 - 시작 ➔ 실행
 - 작업바 (시스템 시간 변경)
 - 명령 프롬프트 (control.exe timedate.cpl)
 -
- ✓ 접근 방법에 따라 상이한 아티팩트



SANS Computer Forensics Blog

Control Panel Forensics: Evidence of Time Manipulation and More

- 제어판 애플릿 실행 흔적

1. 윈도우 프리패치 (Prefetch)

The screenshot shows the PrefetchForensics application window. The main table lists prefetch files with columns for File Name, Created Date/Time, Modified Date/Time, Date Last Run, and Num Times Below the table, there are tabs for 'Files Accessed' and 'Volume Information'. The 'Files Accessed' tab is active, showing a list of files accessed, including system files like CRYPTBASE.DLL, TIMEDATE.CPL, and ATL.DLL.

File Name	Created Date/Time	Modified Date/Time	Date Last Run	Num Times ...
DLLHOST.EXE-5E46FA0D.pf	2013년 7월 19일 금요일...	2013년 7월 19일 금요일...	2013년 7월 19일 금요일 (금) 오전 11:51:46	3364
CONTROL.EXE-817F8F1D.pf	2013년 7월 19일 금요일...	2013년 7월 19일 금요일...	2013년 7월 19일 금요일 (금) 오전 11:52:10	11
RUNDLL32.EXE-89545801.pf	2013년 7월 19일 금요일...	2013년 7월 19일 금요일...	2013년 7월 19일 금요일 (금) 오전 11:52:10	1
IGFXSRVC.EXE-96A493A4.pf	2013년 7월 19일 금요일...	2013년 7월 19일 금요일...	2013년 7월 19일 금요일 (금) 오전 11:52:15	1424
RUNDLL32.EXE-A9C6AC7F.pf	2013년 7월 19일 금요일...	2013년 7월 19일 금요일...	2013년 7월 19일 금요일 (금) 오전 11:52:18	1
RUNDLL32.EXE-FB318F38.pf	2013년 7월 19일 금요일...	2013년 7월 19일 금요일...	2013년 7월 19일 금요일 (금) 오전 11:52:39	1
CMD.EXE-4A81B364.pf	2013년 7월 19일 금요일...	2013년 7월 19일 금요일...	2013년 7월 19일 금요일 (금) 오전 11:52:50	34
CONHOST.EXE-1F3E9D7E.pf	2013년 7월 19일 금요일...	2013년 7월 19일 금요일...	2013년 7월 19일 금요일 (금) 오전 11:52:50	2612
FORECOPY_HANDY.EXE-45358...	2013년 7월 19일 금요일...	2013년 7월 19일 금요일...	2013년 7월 19일 금요일 (금) 오전 11:52:58	3

File Name
\\DEVICE\\HARDDISKVOLUME2\\WINDOWS\\SYSTEM32\\CRYPTBASE.DLL
\\DEVICE\\HARDDISKVOLUME2\\WINDOWS\\SYSTEM32\\TIMEDATE.CPL
\\DEVICE\\HARDDISKVOLUME2\\WINDOWS\\SYSTEM32\\ATL.DLL
\\DEVICE\\HARDDISKVOLUME2\\WINDOWS\\WINSXS\\X86_MICROSOFT, WINDOWS, COMMON-CONTROLS_6595B64144CCF1DF_6,0,7601,17514_NON...
\\DEVICE\\HARDDISKVOLUME2\\WINDOWS\\WINSXS\\X86_MICROSOFT, WINDOWS, GDIPLUS_6595B64144CCF1DF_1,1,7601,18120_NONE_72D2E82386...
\\DEVICE\\HARDDISKVOLUME2\\WINDOWS\\WINDOWSSHELL.MANIFEST
\\DEVICE\\HARDDISKVOLUME2\\WINDOWS\\SYSTEM32\\WKO-KRW\\TIMEDATE.CPL.MUI
\\DEVICE\\HARDDISKVOLUME2\\WINDOWS\\SYSTEM32\\CLBCATQ.DLL
\\DEVICE\\HARDDISKVOLUME2\\WINDOWS\\SYSTEM32\\TZRES.DLL



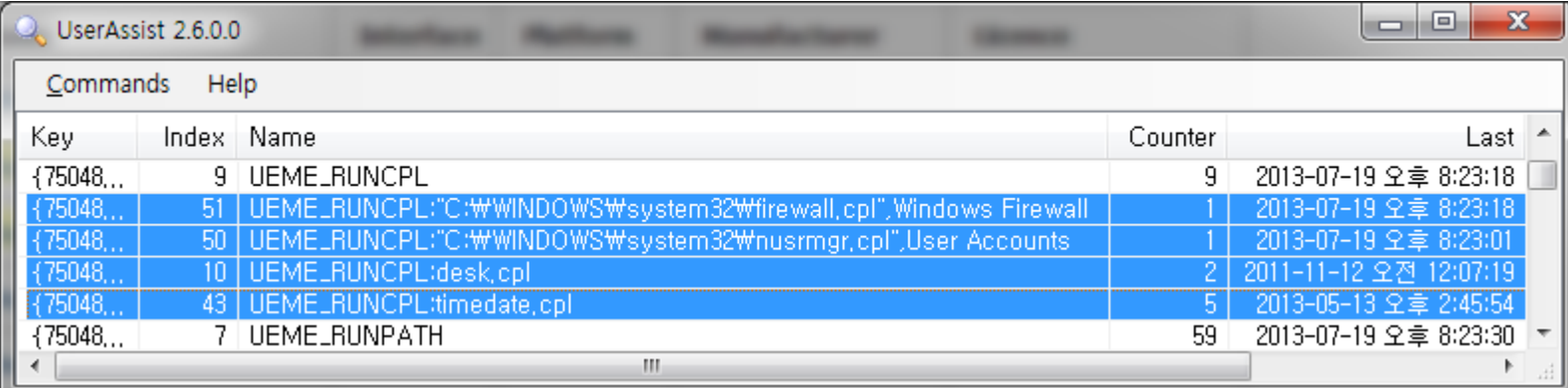
SANS Computer Forensics Blog

Control Panel Forensics: Evidence of Time Manipulation and More

- 제어판 애플릿 실행 흔적

2. 레지스트리 응용프로그램 사용로그(UserAssist) 키 (XP/Vista)

- NTUSER.DAT\Software\Microsoft\Windows\Current\Version\Explorer\UserAssist



The screenshot shows a window titled "UserAssist 2.6.0.0" with a menu bar containing "Commands" and "Help". Below the menu bar is a table with five columns: "Key", "Index", "Name", "Counter", and "Last". The table contains several entries, with the last five rows highlighted in blue. The "Last" column contains timestamps in Korean, such as "2013-07-19 오후 8:23:18".

Key	Index	Name	Counter	Last
{75048,..}	9	UEME_RUNCPL	9	2013-07-19 오후 8:23:18
{75048,..}	51	UEME_RUNCPL:"C:\WINDOWS\system32\firewall,cpl", Windows Firewall	1	2013-07-19 오후 8:23:18
{75048,..}	50	UEME_RUNCPL:"C:\WINDOWS\system32\nusrmgr,cpl", User Accounts	1	2013-07-19 오후 8:23:01
{75048,..}	10	UEME_RUNCPL:desk,cpl	2	2011-11-12 오전 12:07:19
{75048,..}	43	UEME_RUNCPL:timedate,cpl	5	2013-05-13 오후 2:45:54
{75048,..}	7	UEME_RUNPATH	59	2013-07-19 오후 8:23:30



SANS Computer Forensics Blog

Control Panel Forensics: Evidence of Time Manipulation and More

- 제어판 애플릿 실행 흔적

3. 레지스트리 실행명령 로그(RunMRU) 키

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

실행순서	명령어	최종실행시각 (UTC+09:00)
1	regedit	2013-07-19 19:59:05 Fri
2	control wscui.cpl	
3	control sysdm.cpl	
4	control firewall.cpl	
5	control nusrmgr.cpl	
6	firewall.cpl	
7	control panel	
8	gpedit.msc	
9	sysdm.cpl	



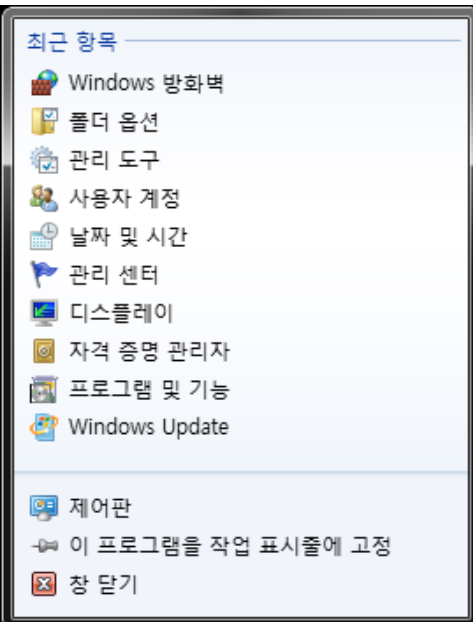
SANS Computer Forensics Blog

▪ Control Panel Forensics: Evidence of Time Manipulation and More

- 제어판 애플릿 실행 흔적

4. 점프 목록 (Win7/Win8)

- %UsrProfile%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\7e4dca80246863e3.automaticDestinations-ms





SANS Computer Forensics Blog

Control Panel Forensics: Evidence of Time Manipulation and More

- 제어판 애플릿 실행 흔적

4. 점프 목록 (Win7/Win8)

- %UsreProfile%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\7e4dca80246863e3.automaticDestinations-ms

source type	appid	MRU/MFU	stream#	MRU date	MRU-UTC	target name
JMPLIST (automatic)	7e4dca80246863e3	1	16	07/19/2013	11:52:43.937	{CLSID_ControlPanel}\#{CLSID_WindowsFirewall}
JMPLIST (automatic)	7e4dca80246863e3	2	13	07/19/2013	11:52:39.017	{CLSID_ControlPanel}\#{CLSID_FolderOptions}
JMPLIST (automatic)	7e4dca80246863e3	3	9	07/19/2013	11:52:34.766	{CLSID_ControlPanel}\#{CLSID_AdminTools}
JMPLIST (automatic)	7e4dca80246863e3	4	17	07/19/2013	11:52:29.786	{CLSID_ControlPanel}\#{CLSID_UserAccounts}
JMPLIST (automatic)	7e4dca80246863e3	5	18	07/19/2013	11:52:18.176	{CLSID_ControlPanel}\#{CLSID_DateAndTime}
JMPLIST (automatic)	7e4dca80246863e3	6	15	07/19/2013	10:57:29.258	{CLSID_ControlPanel}\#{CLSID_ActionCenterControlPanel}
JMPLIST (automatic)	7e4dca80246863e3	7	8	07/19/2013	10:48:06.555	{CLSID_ControlPanel}\#{CLSID_Display}
JMPLIST (automatic)	7e4dca80246863e3	8	14	07/19/2013	10:45:20.423	{CLSID_ControlPanel}\#{CLSID_CredentialManager}
JMPLIST (automatic)	7e4dca80246863e3	9	4	07/19/2013	07:15:29.855	{CLSID_ControlPanel}\#{CLSID_ProgramsAndFeatures}
JMPLIST (automatic)	7e4dca80246863e3	10	12	07/19/2013	06:42:04.604	{CLSID_ControlPanel}\#{CLSID_WindowsUpdate}
JMPLIST (automatic)	7e4dca80246863e3	11	2	07/19/2013	06:34:43.139	{CLSID_ControlPanel}\#{CLSID_NetworkSharingCenter}
JMPLIST (automatic)	7e4dca80246863e3	12	1	07/19/2013	05:19:02.011	{CLSID_ControlPanel}\#{CLSID_Display}
JMPLIST (automatic)	7e4dca80246863e3	13	7	07/19/2013	05:06:46.544	{CLSID_ControlPanel}\#{CLSID_PersonalizationControlPanel}
JMPLIST (automatic)	7e4dca80246863e3	14	11	07/08/2013	04:30:36.598	{CLSID_ControlPanel}\#{CLSID_Mouse}
JMPLIST (automatic)	7e4dca80246863e3	15	5	07/04/2013	13:33:41.905	{CLSID_ControlPanel}\#{CLSID_System}
JMPLIST (automatic)	7e4dca80246863e3	16	3	06/21/2013	13:22:24.195	{CLSID_ControlPanel}\#{CLSID_PowerOptions}
JMPLIST (automatic)	7e4dca80246863e3	17	6	06/07/2013	02:20:08.811	{CLSID_ControlPanel}\#{CLSID_TaskbarNotificationIconsControlPanel}
JMPLIST (automatic)	7e4dca80246863e3	18	10	03/28/2013	08:39:29.709	{CLSID_ControlPanel}\#{CLSID_RegionAndLanguage}



Paul Melson's Blog

▪ GrrCON 2012 Forensics Challenge Walkthrough

- 부팅 가능한 라이브 이미지
 - ✓ ID: analyst
 - ✓ PW: grrcon2012
- 바탕화면 – 3개의 파일
 - ✓ memdump.img
 - ✓ out.pcap
 - ✓ compromised.timeline
- 설치된 도구
 - ✓ TSK, Volatility, Yara, Foremost, tcpflow
- 주어진 20개 문제의 답을 찾는 챌린지



Paul Melson's Blog

▪ GrrCON 2012 Forensics Challenge Walkthrough

- 부팅 가능한 라이브 이미지
 - ✓ ID: analyst
 - ✓ PW: grrcon2012
- 바탕화면 – 3개의 파일
 - ✓ memdump.img
 - ✓ out.pcap
 - ✓ compromised.timeline
- 설치된 도구
 - ✓ TSK, Volatility, Yara, Foremost, tcpflow
- 주어진 20개 문제의 답을 찾는 챌린지



FORENSIC FOCUS

- **Catching the ghost: how to discover ephemeral evidence with Live RAM analysis**
 - 휘발성 메모리의 증거 항목
 - ✓ 동작 중인 프로세스와 서비스, 언팩/복호화된 프로그램 데이터
 - ✓ 시스템/사용자 로그인 정보, 레지스트리/웹 브라우징 흔적
 - ✓ 네트워크 연결 정보, SNS, MMORPG의 통신 및 채팅 내역
 - ✓ 웹 메일/클라우드 서비스 흔적, 암호화된 볼륨의 복호화 키
 - ✓ 최근 열람한 문서 및 사진, 동작 중인 악성코드 정보
 - 휘발성 메모리 흔적은 명이 짧음
 - 따라서, 조사관은 남아 있는 흔적을 최대한 가져올 수 있어야 함



FORENSIC FOCUS

- **Catching the ghost: how to discover ephemeral evidence with Live RAM analysis**
 - 휘발성 데이터가 법적으로 인정받을 수 있는가?
 - ✓ 검증된 도구의 사용
 - ✓ 휘발성 메모리 수집은 필연적으로 풋프린트를 남김
 - ✓ 기술적 타당성과 법적 타당성은 별개의 문제 → 수집의 모든 단계를 문서화



FORENSIC FOCUS

- **Catching the ghost: how to discover ephemeral evidence with Live RAM analysis**
 - **ACPO(Association of Chief Police Officers) 메모리 덤프 표준 절차**
 1. **상황에 대한 위험 평가:** 증거로서 필요하고 안전하게 수집이 가능한가?
 2. 그렇다면, **휘발성 데이터 캡처 장비 장착** (USB Flash Drive, USB Hard Drive 등)
 3. **휘발성 데이터 수집 스크립트 실행**
 4. 완료 후 **장치 중지** (반드시, "안전하게 제거")
 5. **장치 제거**
 6. 별도의 조사 컴퓨터에서 **수집 데이터 검증** (절대 용의자 시스템에서 하지 말것)
 7. **표준 전원 종료 절차에 따름**



FORENSIC FOCUS

- **Catching the ghost: how to discover ephemeral evidence with Live RAM analysis**
 - 메모리 덤프 도구 요구 사항
 1. 커널 모드 동작
 2. 풋프린트 최소화
 3. 포터블 방식
 4. 읽기 모드 접근



FORENSIC FOCUS

▪ Catching the ghost: how to discover ephemeral evidence with Live RAM analysis

- FireWire Attack

- ✓ 아무것도 실행하지 않고 DMA를 이용해 메모리 덤프 → 알려진 방법 중 가능

- Freezer Attack

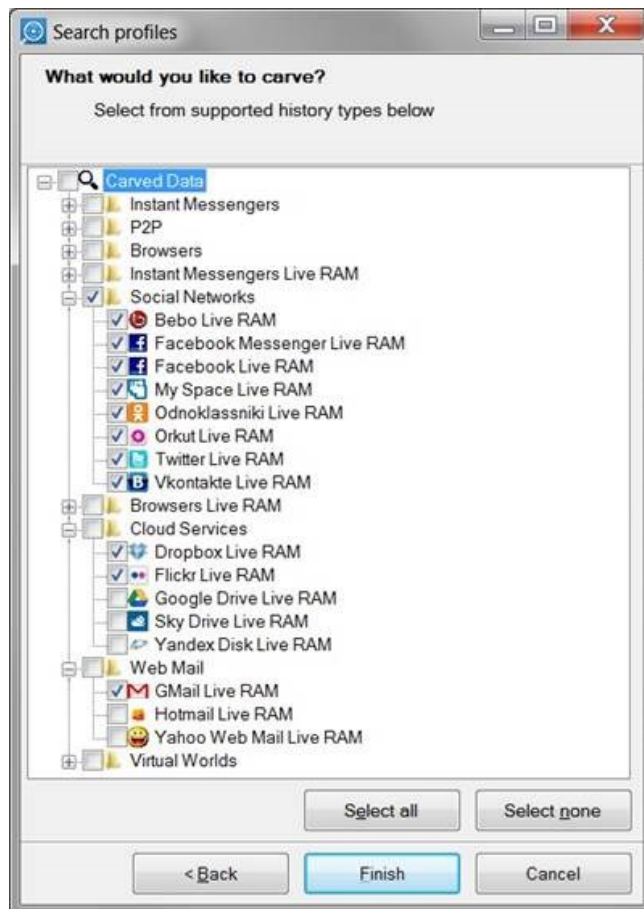
- ✓ 콜드 부트를 이용해 암호화된 스마트폰의 암호화 키를 메모리에서 획득
- ✓ FROST(Forensic Recovery Of Scrambled Telephones)





FORENSIC FOCUS

- Catching the ghost: how to discover ephemeral evidence with Live RAM analysis
 - Belkasoft Evidence Center





Others

▪ **Open Security Research**

- Reversing Basics Part 1: Understanding the C Code
- Reversing Basics Part 2: Understanding the Assembly
- Reversing Basics Part 3: Dynamically Reversing main()

▪ **Microsoft Security Blog**

- Microsoft Releases New Mitigation Guidance for Active Directory

▪ **EnCase® Forensic Blog**

- Safari Form Value Decryptor

▪ **FORENSICMETHODS**

- Memory Forensics Cheat Sheet v1.2



Events

- **WDFS (The Workshop of Digital Forensics)**
 - 2013-08-27, Hana-Square Auditorium in Korea University.
 - **Early Bird** : ₩ 20,000 (Student), ₩ 50,000 (General)
 - **Standard** : ₩ 30,000 (Student), ₩ 70,000 (General)

- **CSS (Cyber Security Summer) 2013**
 - 2013-08-30, COEX
 - **Early Bird** : ₩ 350,000
 - **Standard** : ₩ 450,000

