



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Digital Forensics Analysis (ACCA7031_LON)

Lecture 5

Cloud Storage Forensics

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

SUMMARY

- Cloud Storage services
- Testing environment and methodology
- Forensics artifacts left by Cloud Storage services on Windows OS
 - Installation
 - Usage by software
 - Usage by browser
 - RAM Analysis
 - Uninstall
- Forensics artifacts left by Cloud Storage software on iOS devices

CLOUD STORAGE

- With Cloud Storage services it is easier for us to access our data and share it with other people
- We can access the files by using a computer, a smartphone or a tablet device
- We can choose between free and commercial solutions
- We obviously have a great problem with the **security of the files stored on Cloud Storage servers**
 - E.g. If we loose the credentials everyone can access our file on the cloud...and on our devices?
- We made different tests to verify the artifacts left by the usage of the most popular Cloud Storage services on personal computers and mobile devices
 - OneDrive (formaly SkyDrive, Dropbox)
 - Google Drive
 - iCloud

TESTING ENVIRONMENT

- Windows 7/10 64 bit Operating System
- Mozilla Firefox and Internet Explorer browsers
- **DiskPulse** tool to track the disk usage (created, modified and deleted files)
- **RegShot** and **RegFromApp** to track the registry changes
- 2 email accounts:
 - cloudstorageforensics2013@gmail.com Google Drive and Dropbox
 - cloudstorageforensics2013@hotmail.com OneDrive
- OneDrive client
- Google Drive client

METHODOLOGY - INSTALLATION

- RegShot execution and state saving
- DiskPulse start
- Client installation
- DiskPulse stop
- RegShot execution and state saving
- RegShot differences
- Registry keys analysis
- File created analysis

GOOGLE DRIVE

- Cloud Storage service available at drive.google.com
- Born in 2012
- Billions of users
- ...also because it is activated for every Gmail email created...



GOOGLE DRIVE

- 15 GB available space for free
- It offers commercial solutions (100/200/500 GB - 1/2/4/8/16TB)
- It works on **desktop** and **mobile OS**
 - Windows Vista/7/8/10/11
 - Mac OS X
 - Android
 - iOS

GOOGLE DRIVE – INSTALLATION FOLDER

- Google Drive client is installed inside the **Program Files** folder

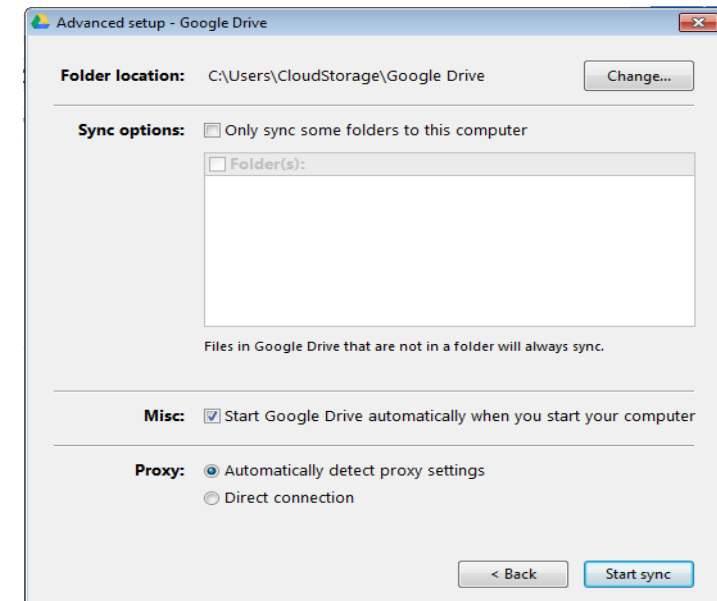
C:\Program Files\Google\Drive

- Client configuration is stored in the **user profile**, so we have different profiles for each user

C:\Users\<username>\AppData\Local\Google\Drive

- The default folder used for syncing files is

C:\Users\<username>\Google Drive



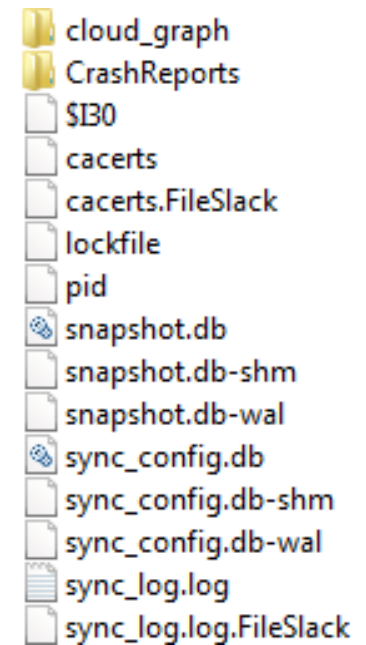
- By default the user folder is **empty**

GOOGLE DRIVE – REGISTRY CHANGES

- During the installation different keys and values are created inside the registry
 - SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\
 - SOFTWARE\Google\Drive
 - NTUSER\Software\Microsoft\Windows\CurrentVersion\Run\GoogleDriveSync
 - NTUSER\Software\Classes
- From the registry we can obtain:
 - Installed version
 - User folder

GOOGLE DRIVE – FILE CREATED

- Configuration files are saved inside the installation folder in the user profile
- Executable and libraries are stored in the **bin** sub-folder
- Other **four files** are created during client installation:
 - C:\Users\<username>\Desktop\Google Drive.Ink
 - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Google Drive\Google Drive.Ink
 - C:\Windows\Prefetch\GOOGLEDRIVESYNC.EXE-NNNNNNNNN.pf
 - C:\Windows\Prefetch\GOOGLEUPDATE.EXE-NNNNNNNNN.pf



GOOGLE DRIVE – SYNC_CONFIG.DB

- The Sync_config.db is a SQLITE3 DB containing profile configuration
 - Client version installed
 - Local Sync Root Path
 - User Email

upgrade_number	value	14
highest_app_version	value	1.11.4865.2530
cloud_docs_feed_mode	value	0
local_sync_root_path	value	\\?\C:\Users\CloudStorage\Google Drive
rlz_brand_code	value	GGLS
selective_sync	value	0
user_email	value	cloudstorageforensics2013@gmail.com

GOOGLE DRIVE – SNAPSHOT.DB

○ The Snapshot.db is a SQLITE3 DB containing information about local and cloud entry

○ Cloud_entry table

- File name
- Created (UNIXTimestamp)
- Modified (UNIXTimestamp)
- URL
- Checksum (MD5 hash)
- Size
- Shared

resource_id	filename	modified	created	acl_role	doc_type	removed	url	size	checksum	shared
Click here to define a filter										
folder:root	root	<null>	<null>	<null>	<null>	<null>	<null>	<null>	<null>	0
file:0B5YL6DiSvQehQzRIbjBqMm9UT28	secretgooglewordfile.docx	1374835100	1374835100	0	1	0	https://docs.google.com/file/d/0B5YL6DiSvQehQzRIbjBqMm9UT28/edit?usp=doclist_api	11513	042fd83de106745bf827f6a8e5b51645	0
file:0B5YL6DiSvQehc3Jjc2NMMHVASEk	secretgoogleexcelfile.xlsx	1374835084	1374835084	0	1	0	https://docs.google.com/file/d/0B5YL6DiSvQehc3Jjc2NMMHVASEk/edit?usp=doclist_api	8026	f52f4b25094e543e518ac3eefe7918d6	0
file:0B5YL6DiSvQehVE9pRUJPFVZHOXc	secretgoogleimage.jpg	1374835099	1374835099	0	1	0	https://docs.google.com/file/d/0B5YL6DiSvQehVE9pRUJPFVZHOXc/edit?usp=doclist_api	845941	ba45c8f60456a672e003a875e469d0eb	0
file:0B5YL6DiSvQehdGR5NUVPcXFITtg	publicgoogledrivewordfile.rtf	<null>	<null>	0	1	<null>	https://docs.google.com/file/d/0B5YL6DiSvQehdGR5NUVPcXFITtg/edit?usp=doclist_api	<null>	0fb07b669254e49126364f21260394cf	0
file:0B5YL6DiSvQehMHFhMGZ3aV9ETHc	googledrivetodelete.rtf	1374835549	1374835549	0	1	0	https://docs.google.com/file/d/0B5YL6DiSvQehMHFhMGZ3aV9ETHc/edit?usp=doclist_api	225	c1f97bb7a960ac85069aa4e0c6a8da73	0

GOOGLE DRIVE – SNAPSHOT.DB

- The **Snapshot.db** is a **SQLITE3** DB containing information about local and cloud entry
 - **Local_entry**
 - File name
 - Modified (UNIX Timestamp)
 - Checksum (MD5 hash)
 - Size

inode_number	filename	modified	checksum	size
Click here to define a filter				
562949953491029	secretgoogleexclfile.xlsx	1374835084	f52f4b25094e543e518ac3eefe7918d6	8026
844424930231479	\\?\C:\Users\CloudStorage\Google Drive	<null>	<null>	<null>
1125899906938306	googledrivetodelete.rtf	1374835549	c1f97bb7a960ac85069aa4e0c6a8da73	225
3659174697333440	publicgoogledrivewordfile.rtf	1374835374	0fb07b669254e49126364f21260394cf	217
4785074604172744	secretgooglewordfile.docx	1374835100	042fd83de106745bf827f6a8e5b51645	11513
30680772461547148	secretgoogleimage.jpg	1374835099	ba45c8f60456a672e003a875e469d0eb	845941

GOOGLE DRIVE – SNAPSHOT.DB AFTER DELETION

- After file deletion the file information is removed from the cloud_entry and the local_entry table

resource_id	filename	modified	created	acl_role	doc_type	removed	url	size	checksum
Click here to define a filter									
folder:root	root	<null>	<null>	<null>	<null>	<null>	<null>	<null>	<null>
file:0B5YL6DiSvQehQzRIbjBqMm9UT28	secretgooglewordfile.docx	1374835100	1374835100	0	1	0	https://docs.google.com/file/d/0B5YL6DiSvQehQzRIbjBqMm9UT28/edit?usp=docslist_api	11513	042fd83de106745bf827f6a8e5b51645
file:0B5YL6DiSvQehc3Jjc2NMMHVasek	secretgoogleexcelfile.xlsx	1374835084	1374835084	0	1	0	https://docs.google.com/file/d/0B5YL6DiSvQehc3Jjc2NMMHVasek/edit?usp=docslist_api	8026	f52f4b25094e543e518ac3eefe7918d6
file:0B5YL6DiSvQehVE9pRUJPFVZHOxc	secretgoogleimage.jpg	1374835099	1374835099	0	1	0	https://docs.google.com/file/d/0B5YL6DiSvQehVE9pRUJPFVZHOxc/edit?usp=docslist_api	845941	ba45c8f60456a672e003a875e469d0eb
file:0B5YL6DiSvQehdGR5NUVpcXFITTg	publicgoogledrivewordfile.rtf	<null>	<null>	0	1	<null>	https://docs.google.com/file/d/0B5YL6DiSvQehdGR5NUVpcXFITTg/edit?usp=docslist_api	<null>	0fb07b669254e49126364f21260394cf

- But sometimes we can still find the file name with a keyword search on the DB itself

[illegible][illegible][illegible]

GOOGLE DRIVE – SYNC_LOG.LOG

- The **Sync_log.log** is a log file containing information about the client sync session
- Inside the file we can find information about
 - Sync sessions
 - File created
 - File saved
 - File deleted
- We can use a keyword search with the strings:
 - RawEvent(CREATE
 - RawEvent(DELETE
 - RawEvent(MODIFY

```
('Direction.DOWNLOAD', 'Action.CREATE', 'name: secretgoogleexcelfile.xlsx', "route: [CloudEntry(file:0B5YL6DiSvQehc3Jjc2NMMHVASEk,secretgoogleexcelfile.xlsx,1  
( 'Direction.DOWNLOAD', 'Action.CREATE', 'name: secretgoogleimage.jpg', "route: [CloudEntry(file:0B5YL6DiSvQehVE9pRUJPFVZHOXc,secretgoogleimage.jpg,1374835099,  
( 'Direction.DOWNLOAD', 'Action.CREATE', 'name: secretgooglewordfile.docx', "route: [CloudEntry(file:0B5YL6DiSvQehQzRIbjBqMm9UT28,secretgooglewordfile.docx,137
```

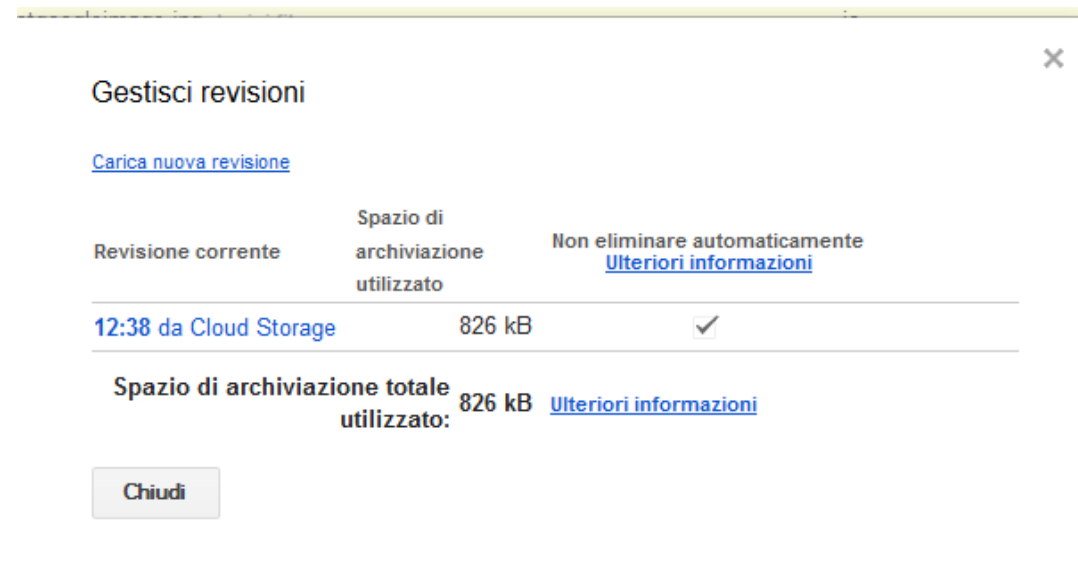
GOOGLE DRIVE ONLINE ACCESS

- By logging in the profile from a browser, the user can access all the information about **deleted files**

CREA 	☐ TITOLO	PROPRIETARIO	MODIFICATI PER ULTIMI
► I miei file Condivisi con me Speciali Recenti Meno ▲ Attività Tutti gli elementi Cestino Proprietario, tipo, altro » Scarica Drive per PC	☐   googledrivetodelete.rtf Cestino	io	12:45 io

GOOGLE DRIVE ONLINE ACCESS

- For every file we can view **version history**
- We can recover previous version of a file



GOOGLE DRIVE ONLINE ACCESS

- We can also recover information about **recent activities**

La tua attività recente ?

14:46	 Accesso da Firefox (Windows)	Italia
12:37	 Accesso da Firefox (Windows)	Italia
25 lug	 Accesso da Internet Explorer (Wind...	Italia
25 lug	 Nome modificato in Cloud Storage	Sconosciuta
25 lug	 Accesso da Firefox (Windows)	Italia
Nessun evento di accesso disponibile prima di questa data		
25 lug	 Indirizzo email di recupero aggiunto	Italia
25 lug	 N. di telefono di recupero aggiunto	Italia

 Connesso
14:46 (0 minuti fa)

Riconosci questa attività?
Se la risposta è no, un'altra persona potrebbe essere in possesso della tua password.

[Cambia password](#)


13 Google - Dati mappa e termini e condizioni d'uso
Posizione approssimativa (basata sull'IP)
Roma, Italia

GOOGLE DRIVE RAM ANALYSIS – CLIENT ACCESS

- If the client is installed on the PC, we can find in RAM information **about the sessions**
- We can use the strings
 - `user_emailvalue`
 - `highest_app_versionvalue`
 - `local_sync_root_pathvalue`
 - `snapshot.db`
 - `sync_config.db`
- We can find
 - User email
 - Version number
 - Sanpshot.db and sync_config.db path
 - Local sync folder path
- Similar values were found during the research inside
 - `Hiberfil.sys`
 - `Pagefile.sys`

```
omain_policydefault_sync_all1.8.!.S.user_emailvaluecloudstoragef
orensics2013@gmail.com...)...selective_syncvalue0...)...rlz_brn
d_codevalueGGLS.E.5.Y.local_sync_root_pathvalue\\?\C:\Users\Clou
dStorage\Google Drive. .5...cloud_docs_feed modevalue0.,.3.)...hig
hest app versionvalue1.11.4865.2530...)...upgrade_numbervalue14.
```

```
C:\Users\CloudStorage\AppData\Local\Google\Drive\snapshot.db.o.
c.a.1.\..8zQ4ø..C:\Users\CloudStorage\AppData\Local\Google\Drive
\sync config.db.c.a.1.\.$8zy4ø..(.....yyyyyyyy.....
```

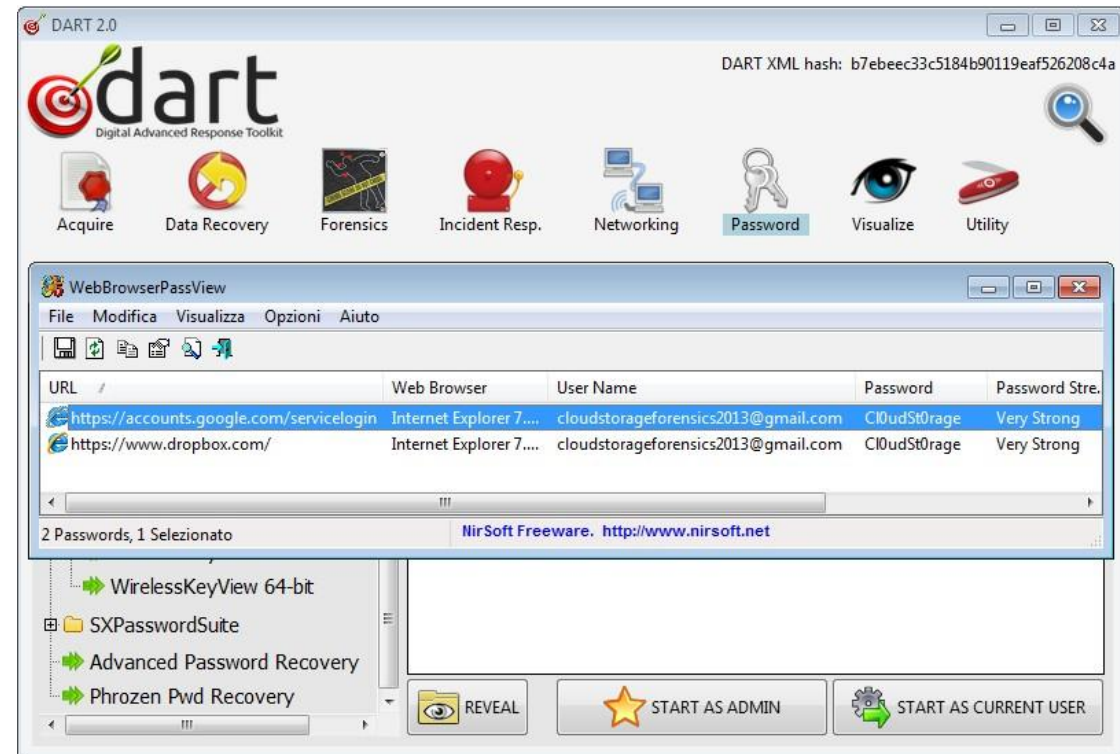
GOOGLE DRIVE RAM ANALYSIS – BROWSER ACCESS

- If the user was logged with a browser session we found in RAM the username and password in clear
- We can use the strings
 - Email=
 - Passwd=

```
3KWZd11XP1rTkhwwJDHnJIulE8Y6sRHy0WZEHiVdUfwIuvW-q5cfIwsfXzqsf289
LdzVi0bT5kUN6vMrG-6g1Gke_O1SruW_kJrw3tLuNnZwI3N9I0qJ9&Email=clou
dstorageforensics2013@gmail.com&Passwd=Cl0udSt0rage&signIn=Acced
i&PersistentCookie=yes&rmShown=1.....hí.....€.....
```

GOOGLE DRIVE ACCESS AND PASSWORD RECOVERY

- We can access the profile in 2 way:
 - Find the password stored somewhere in the PC (ex. Browser, Mail client, etc.) and access through the website
 - Virtualize the forensic image and connect it to Internet

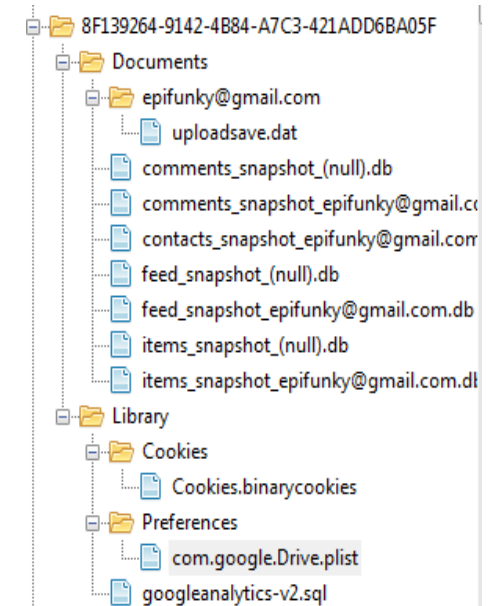


GOOGLE DRIVE UNINSTALL

- During the uninstall process the client config folder is removed
 - We found Sync_log.log entries from unallocated space
- The prefetch file are not deleted
- Local file are not deleted
- If the user deleted the local file we can try to carve it
- We can also recover information from:
 - Registry keys about recent files
 - LNK files
 - Browser history and cache
 - Thumbnails
 - Restore points/ Volume Shadow Copies
 - Pagefile.sys
 - Hiberfil.sys

GOOGLE DRIVE IOS APP

- The Google Drive iOS App is stored in
`\var\mobile\Applications\8F139264-9142-4B84-A7C3-421ADD6BA05F`
- It contains 2 sub folders
 - Documents
 - Library
 - Cookies
 - Preferences
 - Caches
- The Preferences folder contains a file named `com.google.Drive.plist` with
 - User information (Name and Surname)
 - User id
 - User email
- The cache folder contains the cached copy of the opened files, but it can be extracted only if we can perform a physical dump



```
~/drive
<key>signed_in_user_email</key>
<string>epifunky@gmail.com</string>
<key>user_data_map</key>
<dict>
  <key>epifunky@gmail.com</key>
  <dict>
    <key>user_id</key>
    <string>106279378770606320231</string>
    <key>user_name</key>
    <string>Mattia Epifani</string>
  </dict>
</dict>
```

GOOGLE DRIVE IOS APP

- The Documents folder contains 3 interesting SQLite databases:
 - Contacts_snapshot_useremail.db
 - Feed_snapshot_useremail.db
 - Items_snapshot_useremail.db
- The Contacts db contains the user email and name of the contacts with shared files with the user
- The Items db contains all the information about file stored in the user Drive
 - Identifier
 - Title
 - Kind
 - MD5 hash
 - Last Modified By (username)
 - Last Modified Date
 - Last Viewed Date
 - Shared With Me Date
 - Last Modified by Me Date

GOOGLE DRIVE IOS APP – ITEMS_SNAPSHOT_USEREMAIL.DB

title	kind	owner	md5Checksum	last_modified_by	last_modified_date	last_viewed_date	shared_with_me_date	last_modified_by_me_date
Click here to define a filter								
Electronic Evidence Guide	spreadsheet	epifunky@gmail.com	<null>	paolo	1374941933	1372929036	<null>	1372929293
I miei file	folder	<null>	<null>	<null>	<null>	<null>	<null>	<null>
Electronic Evidence Guide.xlsx	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	epifunky@gmail.com	fbcf7c391bc5832de7bc9408afaa27f0	epifunky	1371543822	<null>	<null>	1371543821
Data dell'evento di DFA	spreadsheet	epifunky@gmail.com	<null>	epifunky	1290425344	1347934116	<null>	1290425344

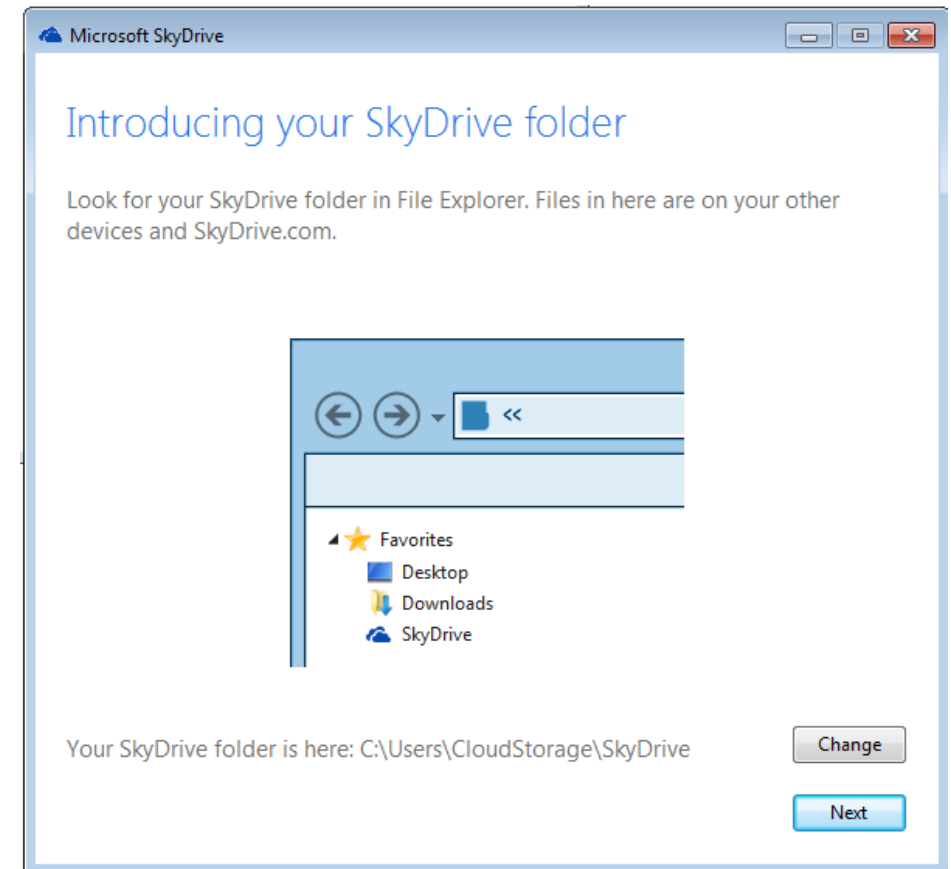
OneDRIVE – INSTALLATION FOLDER

- SkyDrive client is installed inside the **user profile**, so we have different profiles for each user

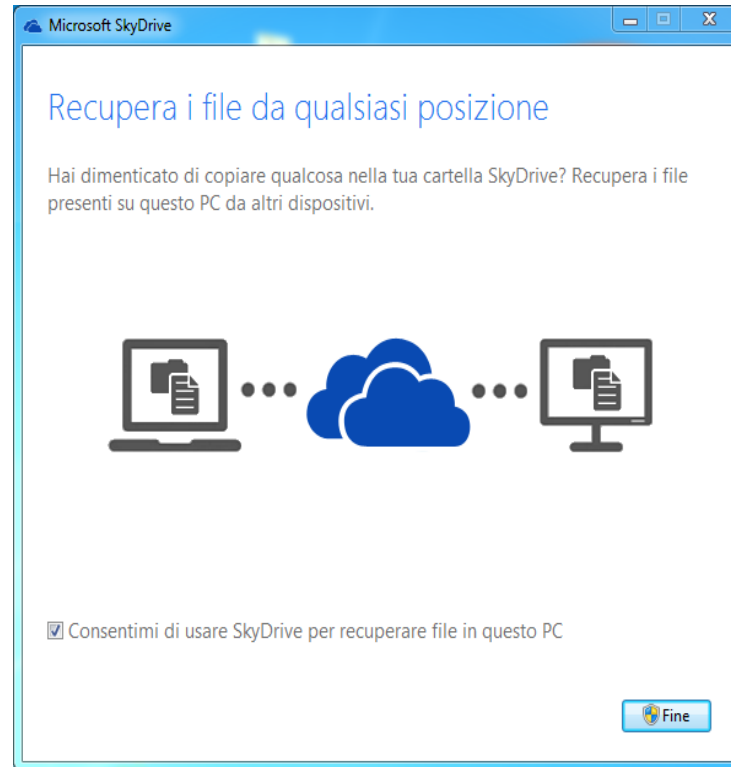
C:\Users\\AppData\Local\Microsoft\SkyDrive

- The default folder used for syncing files is
C:\Users\\SkyDrive

- By default the user folder contains **3 empty folders**
 - Documents
 - Images
 - Public



OneDrive – LOCAL FILE SHARING!

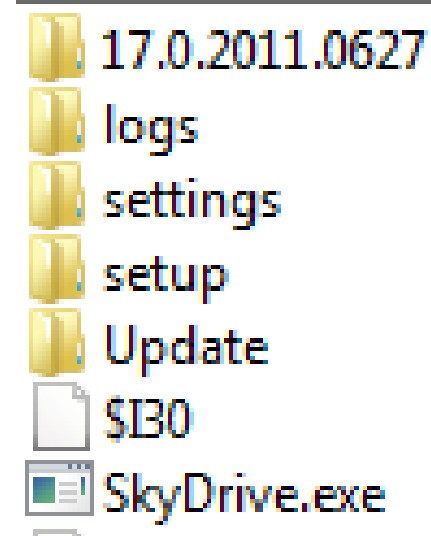


OneDrive – REGISTRY CHANGES

- During the installation different keys and values are created inside the registry
 - SYSTEM\ControlSet001\Services\Parameters\FirewallPolicy\FirewallRules
 - SOFTWARE\Microsoft\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\SkyDrive1
 - SOFTWARE\Microsoft\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\SkyDrive2
 - SOFTWARE\Microsoft\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\SkyDrive3
 - NTUSER\Software\Microsoft\Windows\CurrentVersion\Uninstall
 - NTUSER\Software\Microsoft\Windows\CurrentVersion\Run
 - NTUSER\Software\Microsoft\Windows\CurrentVersion\UFH\SHC
 - NTUSER\Software\Microsoft\SkyDrive
 - NTUSER\Software\Classes\SkyDrive.SyncFileInformationProvider
 - NTUSER\Software\Classes\SkyDriveClient.SkyDriveClient
- From the registry we can obtain:
 - **Current Version Path**
 - **User folder**

OneDrive– FILE CREATED

- Configuration files are saved inside the installation folder in the user profile
- There are 4 sub folders:
 - **Settings:** client settings
 - **Log:** activities log
 - **Setup:** client update log
 - **Update:** last client update
- Other 7 files are created during client installation:
 - C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\SkyDrive.Ink
 - C:\Users\Default\Links\SkyDrive.Ink
 - C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\SkyDrive.Ink
 - C:\Users\<username>\Links\SkyDrive.Ink
 - C:\Windows\Prefetch\SKYDRIVE.EXE-NNNNNNNN.pf
 - C:\Windows\Prefetch\SKYDRIVECONFIG.EXE-NNNNNNNN.pf
 - C:\Windows\Prefetch\SKYDRIVESETUP.EXE-NNNNNNNN.pf



OneDrive – SETTINGS FOLDER

- Settings folder contains
 - **ClientPolicy.ini**: client configuration parameters
 - Max File Size Bytes
 - Max Client MB Transferred Per Day
 - Max Client Requests Per Day
 - Max Items In One Folder
 - Number Of Concurrent Uploads
 - **ApplicationSettings.xml**: it contains the **UserCid**
 - **<UserCid>.ini**: user configuration parameters
 - **installName**: personal computername
 - **lastRefreshTime**: date and time of the last online sync
 - **library**: user folder path
 - **<UserCid>.dat**: file and folder name

```
[PolicySettings]
PolicyDocumentPollIntervalSeconds = 24066
BackoffOnErrorsIntervalSeconds = 246
PolicyDocumentPrefetchIntervalSeconds = 6066
BackgroundPollShortIntervalSeconds = 306
BackgroundPollLongIntervalSeconds = 88866
UploadBatchMaxFolderCount = 50
UploadBatchMaxDocumentCount = 50
UploadBlockSizeKB = 4096
DownloadBlockSizeKB = 4096
MaxFileSizeBytes = 2147483647
Tier1MaxFileSizeBytes = 2147483647
Tier1FileInclusionList = |doc|docm|docx|dot|dotm|dotx|odc|odp|ods|odt|pot|potm|potx|pps|ppsm|ppsx|ppt|pptm|pptx|rtf|vdw|vdx|vsd|vsdm|vsdx|vssm|vssx|vs:
MaxItemsInOneFolder = 150000
LowVisibilityFileExclusionList = ~$*.*|*.laccdb|Desktop.ini|Thumbs.db|EhThumbs.db|.ds_store|Icon\r|.lock
HighVisibilityFileExclusionList =
DavUrlMatch = ^(?:http|https):\/\/([a-zA-Z0-9])+\.([a-zA-Z0-9\~]+)\.)*docs(-df|-bvt|-s3|-gd|-current|-dev)*\.live(-tst)*\.net(?:\:|[0-9]*)?\/(?:'cid'(?:[A-F]
DocumentBackgroundPollIntervalSeconds = 3600
DavUrlTemplate = https://d.docs.live.net/{hexcid}/{path}
ShareUrlTemplate = https://skydrive.live.com/?cid={hexcid}&id={resourceid}&action=Share
PathEncoding = CaretEncode
OfficeProgID = Office.LocalSyncClient
OfficeRegKey = HKEY_CURRENT_USER\Software\Microsoft\Office\15.0
OfficeExcludeList = |
WacUrlTemplate = https://skydrive.live.com/redir.aspx?cid={hexcid}&resid={ResourceID}&type=3&page=view
MaxClientMBTransferredPerDay = 131072
MaxClientRequestsPerDay = 500000
NumberOfConcurrentUploads = 3
AllowUserOverrideOfConcurrentUploads = true
SkyApiURL = https://skyapi.live.net
```

OneDrive – APPLICATIONSETTINGS.XML

```
- <setting name="UserCid">  
    <value>a12fcc3b7af059c0</value>  
  </setting>  
- <setting name="ProviderOptInEnabled">  
    <value>1</value>  
  </setting>  
</Global>  
</userSettings>  
</configuration>
```

OneDrive – USERCID.INI

```
nickname =  
installID = 1  
installName = WIN-OQR27BIU3K9  
maxNumRequests = 10  
originatorID = 55c5aa7f-4661-45d0-81f7-4bd85d3d3d82  
lastRefreshTime = 1374768391  
requestsSent = 7  
bytesTransferred = 14630  
  
library = 1 4 A12FCC3B7AF059C0 103 1374768202 "SkyDrive" Me personal "C:\Users\CloudStorage\SkyDrive"
```

→ Fri, 26 Jul 2013 16:38:49 GMT

OneDrive – USERCID.DAT – BEFORE DELETION

[illegible]

OneDrive– USERCID.DAT – AFTER DELETION

[illegible]

OneDrive – USERCID.DAT – IEF – BEFORE DELETION

IEF Report Viewer v6.1.0.0380 - Case: Not Entered - Evidence Number: Not Entered

File Edit **Tools** Go To Help

Go To #: Default Encoding Search:

Recovered Artifacts	Items	★ #	File Name	Last Modified Date/Time - (UTC) (dd/MM/yy...)	Located At
Cloud		1	««««««««Immagini		File offset 2068
		2	««««««««Pubblica		File offset 2812
		3	««««««««Documenti		File offset 3556
		4	secretskydrivefile.jpg	26/07/2013 16:38:02	File offset 4300
		5	secretskydrivewordfile.docx	26/07/2013 16:38:03	File offset 5044
		6	secretskydriveexcelfile.xlsx	26/07/2013 16:38:02	File offset 5788
		7	publicskydrivewordfile.rtf	26/07/2013 16:39:45	File offset 6532
		8	skydrivetodelete.rtf	26/07/2013 16:44:17	File offset 7276

Previous Showing results 1 - 8 of 8 Next

OneDrive – USERCID.DAT – IEF – AFTER DELETION

IEF Report Viewer v6.1.0.0380 - Case: Not Entered - Evidence Number: Not Entered

File Edit Tools Go To Help Go To #: Default Encoding Search:

Recovered Artifacts	Items	★ #	File Name	Last Modified Date/Time - (UTC) (dd/MM/yyyy)	Located At
Cloud		1	««««««Immagini		File offset 2068
		2	««««««Pubblica		File offset 2812
		3	««««««Documenti		File offset 3556
SkyDrive	7	4	secretskydrivefile.jpg	26/07/2013 16:38:02	File offset 4300
		5	secretskydrivewordfile.docx	26/07/2013 16:38:03	File offset 5044
		6	secretskydriveexcelfile.xlsx	26/07/2013 16:38:02	File offset 5788
		7	publicskydrivewordfile.rtf	26/07/2013 16:39:45	File offset 6532

Previous Showing results 1 - 7 of 7 Next

OneDrive– LOGS FOLDER

- It contains a log file about **client software activities**
 - **SyncDiagnostics.log**: contains information about last sync
 - **<PCNAME>.dev=0.YYYY-MM-DD.HHMM,SSSS-1.log**: contains detailed sync logs for a particular day

```
Sync Progress Diagnostics v1  
UtcNow: 2013-07-26T16:39:32.0000000Z
```

```
-----  
cid = a12fcc3b7af059c0  
clientType = win32  
clientVersion = 17.0.2011.0627  
cloudFolders = 3  
device = WIN-OQR27BIU3K9  
deviceID = 097f0de2-15b7-7d01-92e5-0ca4ec013d4f  
timeUtc = 2013-07-26T14:55:01.0000000Z  
username = WIN-OQR27BIU3K9\CloudStorage
```

OneDrive – LOG FILE

- We can find information about all the files, including the **deleted ones**
- We can use a string search
 - **CreateNewFileRealizerWorkItem**: function invoked every time a file is created in the local folder
 - **FILE_ACTION_ADDED**: invoked every time a file is added locally
 - **FILE_ACTION_REMOVED**: invoked every time a file is removed locally
 - **FILE_ACTION_RENAMED**: invoked every time a file is renamed locally

```
SyncServiceProxy::CreateNewFileRealizerWorkItem (NORMAL): told to add file=A12FCC3B7AF059C0  
SyncServiceProxy::CreateNewFileRealizerWorkItem (NORMAL): told to add file=A12FCC3B7AF059C0  
SyncServiceProxy::CreateNewFileRealizerWorkItem (NORMAL): told to add file=A12FCC3B7AF059C0
```

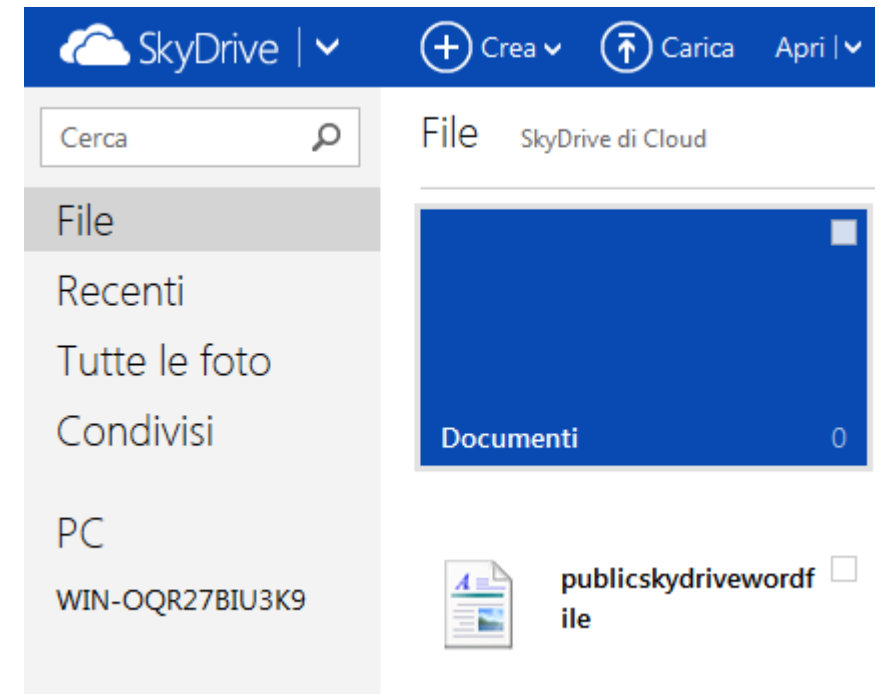
```
SCANNER: FILE_ACTION_ADDED for 'C:\Users\CloudStorage\SkyDrive\New Text Document.txt'  
: SCANNER: FILE_ACTION_ADDED for 'C:\Users\CloudStorage\SkyDrive\genoa secret-logo.png'  
: SCANNER: FILE_ACTION_ADDED for 'C:\Users\CloudStorage\SkyDrive\genoa secret-logo.png'  
: SCANNER: FILE_ACTION_ADDED for 'C:\Users\CloudStorage\SkyDrive\250px-Mickey_Mouse.png'  
: SCANNER: FILE_ACTION_ADDED for 'C:\Users\CloudStorage\SkyDrive\250px-Mickey_Mouse.png'
```

```
SCANNER: FILE_ACTION_REMOVED for 'C:\Users\CloudStorage\SkyDrive\250px-Mickey_Mouse.png'
```

```
SCANNER: FILE_ACTION_RENAMED_OLD_NAME for 'C:\Users\CloudStorage\SkyDrive\New Text Document.txt'  
SCANNER: FILE_ACTION_RENAMED_NEW_NAME for 'C:\Users\CloudStorage\SkyDrive\secret text document.txt'
```

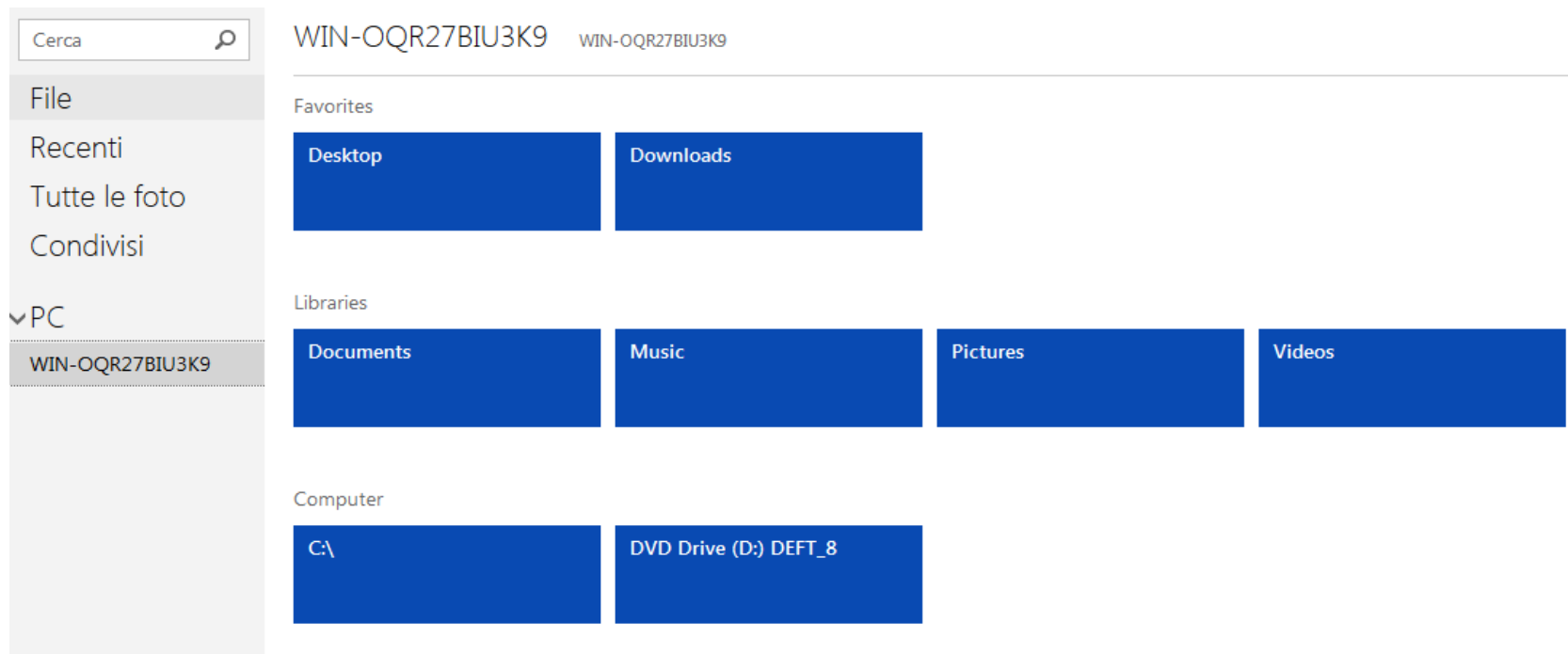
OneDrive ONLINE ACCESS

- By logging in the profile from a browser, the user can access all the information about **deleted file**
- We can also view all the **device used to sync** the account through a client



OneDrive DRIVE ONLINE ACCESS

- We can access to the file stored inside a synced PC ...



OneDrive ONLINE ACCESS

- If a user has deleted a file we can still access to a copy inside a **Recycle Bin** for a **30 days period**
- We can also access to different revisions of a file

 secretsk
ile

Apri in Excel Web App

Apri in Excel

Scarica

Condivisione

Incorpora

Rinomina

Elimina

Sposta in

Copia in

Cronologia versioni

Proprietà

Cancella la selezione

 SkyDrive |  [Ripristina tutti gli elementi](#) [Svuota Cestino](#)

Cerca 

File

Recenti

Tutte le foto

Condivisi

PC

WIN-OQR27BIU3K9

Cestino

☐ Nome ↑	Percorso originale	Data di elimin...	Dimensione
☐  250px-Mickey_Mouse	SkyDrive di Cloud Storage	16:59	24,4 KB
☐  secret text document	SkyDrive di Cloud Storage	16:41	52 byte
☐  skydrivetodelete	SkyDrive di Cloud Storage	26/07/2013	40,4 KB

OneDrive RAM ANALYSIS – CLIENT ACCESS

- If the client is installed on the PC, we can find in RAM information about the sessions
- We can use the strings
 - login.live.com
 - skydrive
- We can find
 - User email
 - Version number
 - Config Path
 - Local sync folder path
 - File names
- Similar values were found during the research inside
 - Hiberfil.sys
 - Pagefile.sys

```
50E1DA80 37 39 38 36 0A 32 34 35 31 35 31 38 38 36 33 0A 7986.2451518863.
50E1DA90 33 30 33 31 32 37 38 34 0A 2A 0A 4D 53 50 50 72 30312784.*.MSPPPr
50E1DAA0 65 0A 63 6C 6F 75 64 73 74 6F 72 61 67 65 66 6F e.cloudstoragefo
50E1DAB0 72 65 6E 73 69 63 73 32 30 31 33 40 68 6F 74 6D rensics2013@hotm
50E1DAC0 61 69 6C 2E 63 6F 6E 7C 61 31 32 66 63 63 33 62 ail.com|a12fcc3b
50E1DAD0 37 61 66 30 35 39 63 30 7C 7C 0A 6C 6F 67 69 6E 7af059c0||.login
50E1DAE0 2E 6C 69 76 65 2E 63 6F 6D 2F 0A 31 30 32 34 0A .live.com/.1024.

064E7130 5D 0D 0A 49 63 6F 6E 52 65 13 6F 13 12 63 65 3D j..iconksource=
064E7140 43 3A 5C 55 73 65 72 73 5C 43 6C 6F 75 64 53 74 C:\Users\CloudSt
064E7150 6F 72 61 67 65 5C 41 70 70 44 61 74 61 5C 4C 6F orage\AppData\Lo
064E7160 63 61 6C 5C 4D 69 63 72 6F 73 6F 66 74 5C 53 6B cal\Microsoft\S
064E7170 79 44 72 69 76 65 5C 53 6B 79 44 72 69 76 65 2E yDrive\SkyDrive.
064E7180 65 78 65 2C 31 0D 0A 00 FF FF FF FF 82 79 47 11 exe,1...ÿÿÿÿ,yG.

3B1BD080 -----..Cloud Metadata:.. - folder A12FCC3B7AF059C0
3B1BD0C0 !106 'C:\Users\CloudStorage\SkyDrive\Documenti', creationTime=13
3B1BD100 74768113, modTime=1374768113.. - folder A12FCC3B7AF059C0!104
3B1BD140 'C:\Users\CloudStorage\SkyDrive\Immagini', creationTime=13747681
3B1BD180 12, modTime=1374768112.. - folder A12FCC3B7AF059C0!105 'C:\Us
3B1BD1C0 ers\CloudStorage\SkyDrive\Pubblica', creationTime=1374768112, mo
3B1BD200 dTime=1374768112..Cloud Total: 3 folders, 0 files, 0 bytes.....
3B1BD240 -----
3B1BD280 -----..File System:..Scanning 'C:\Users\CloudStorage\Sky
3B1BD2C0 yDrive'.. - file 'C:\Users\CloudStorage\SkyDrive\.lock' ign
3B1BD300 ored, size=0, creationTime=1375446299, modTime=1375446299.. -
3B1BD340 file 'C:\Users\CloudStorage\SkyDrive\desktop.ini' ignored, si
3B1BD380 ze=103, creationTime=1374768202, modTime=1374768391.. - folde
3B1BD3C0 r 'C:\Users\CloudStorage\SkyDrive\Documenti'.. - folder 'C:\U
3B1BD400 sers\CloudStorage\SkyDrive\Immagini'.. - folder 'C:\Users\Clo
3B1BD440 udStorage\SkyDrive\Pubblica'..Folder 'C:\Users\CloudStorage\SkyD
3B1BD480 rive' Total: 3 folders, 0 files..FileSystem Total: 3 folders, 0
3B1BD4C0 files, 0 symLinks, 0 bytes.....-----
```

OneDriveRAM ANALYSIS – BROWSER ACCESS

- If the user was logged with a browser session we found in RAM the username and password in clear
- We can use the string passwd=

```
.....|MW.H"@.  
H.e.H9ž.oudstorageforensics2013@hotmail.com&passwd=C10udSt0rage&  
type=11&PPFT=CpRPuBqngY1NdvPnGtHaRJImVAiAIqLzscmwC7pBZUHv107yx20
```

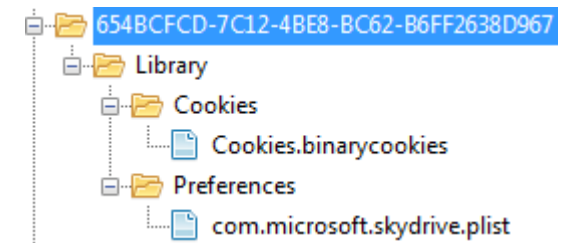
OneDriveDRIVE UNINSTALL

- During the uninstall process the **client config folder** is removed
 - We found **Log** entries from unallocated space
- The **prefetch** files are not deleted
- The key **NTUSER\Software\SkyDrive** is still present but without values

- **Local file** are not deleted
- If the user deleted the local file we can try to carve it
- We can also recover information from:
 - Registry keys about recent files
 - LNK files
 - Browser history and cache
 - Thumbnails
 - Restore points/ Volume Shadow Copies
 - Pagefile.sys
 - Hiberfil.sys

OneDrive iOS APP

- The SkyDrive iOS App is stored in
\\var\\mobile\\Applications\\654BCFCD-7C12-4BE8-BC62-B6FF2638D967
- It contains 3 sub folders
 - Documents
 - Library
 - Caches
- The Preferences folder contains a file named **com.microsoft.Skydrive.plist** with
 - User email
- The cache folder contains the **cached copy** of the opened files, but it can be extracted only if we can perform a physical dump



```
<dict>
  <key>DrxWillSendDocumentToOtherApp</key>
  <false/>
  <key>bErrorReportingUUID</key>
  <string>E76B29B6-A07C-445B-88FB-0CB22E94BB83</string>
  <key>needpopsigninview_(null)</key>
  <string>no</string>
  <key>needpopsigninview_mattiaep@hotmail.it</key>
  <string>no</string>
</dict>
</plist>
```

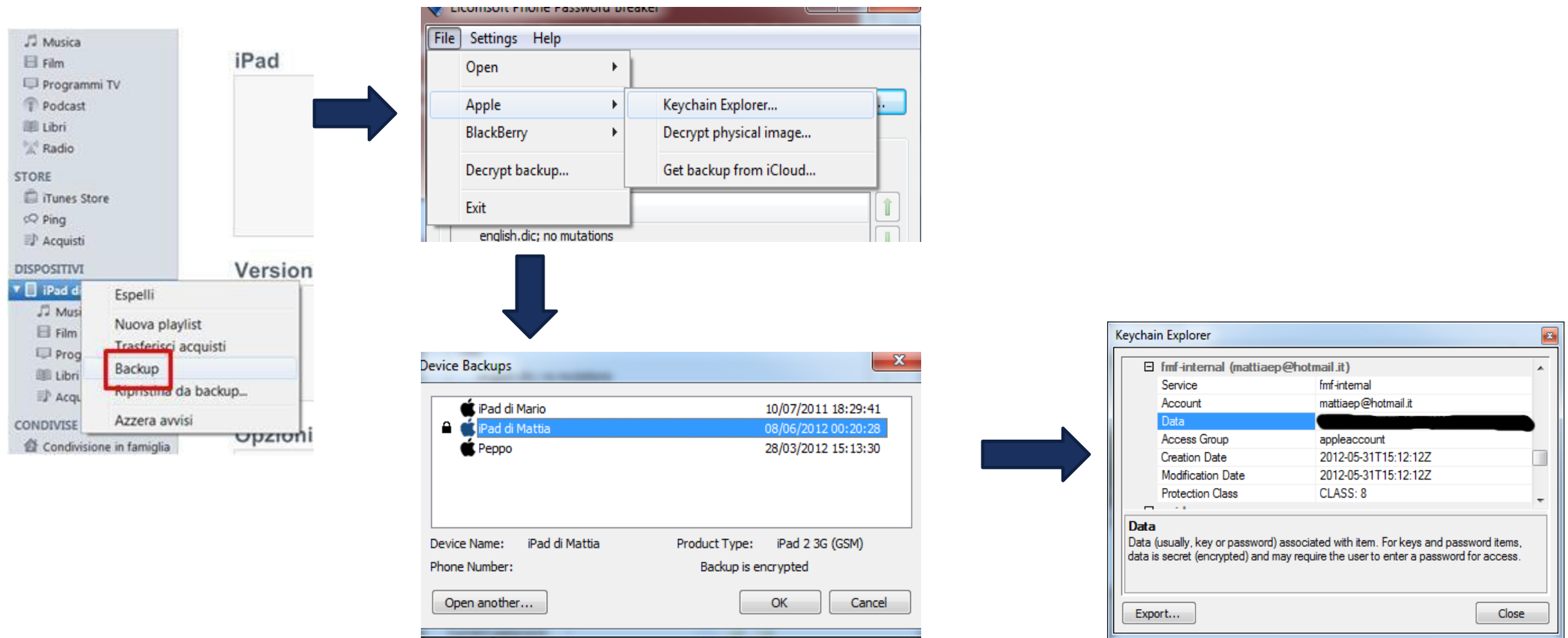
ICLOUD

- Using iTunes we can make a **backup of an iOS device**
- In order to perform the backup it is needed that:
 - The phone is not protected by a lock code, or
 - Knowing the lock code, or
 - Obtaining the synchronization certificates for the device from a trusted computer
- The **keychain file** stores **WiFi, e-mail and third-party applications password**
- If the backup is **not encrypted** → keychain file is encrypted using a key hard-coded into the device
- If the backup is **password protected** → keychain file is encrypted using the **user-chosen password**

ICLOUD

- If an attacker can get his hands on an unlocked phone, he can:
 - Make a backup by choosing the password he wants
 - «Crack» the backup....with the choosen password 😊
 - Access data stored on the phone....and the passwords stored in the keychain

ICLOUD



ICLOUD

- Researchers at the Russian software company Elcomsoft have analyzed the communication protocol between iDevice and Apple iCloud
- They were able to **emulate the correct commands to retrieve the contents of a user's iCloud storage**
<http://cansecwest.com/slides/2013/Cracking%20and%20Analyzing%20Apple%20iCloud.ppt>
- The download operations are **completely transparent to the device owner**, so an attacker can **monitor user activities every time a new backup is created online**

ICLOUD



ICLOUD

Sign In X

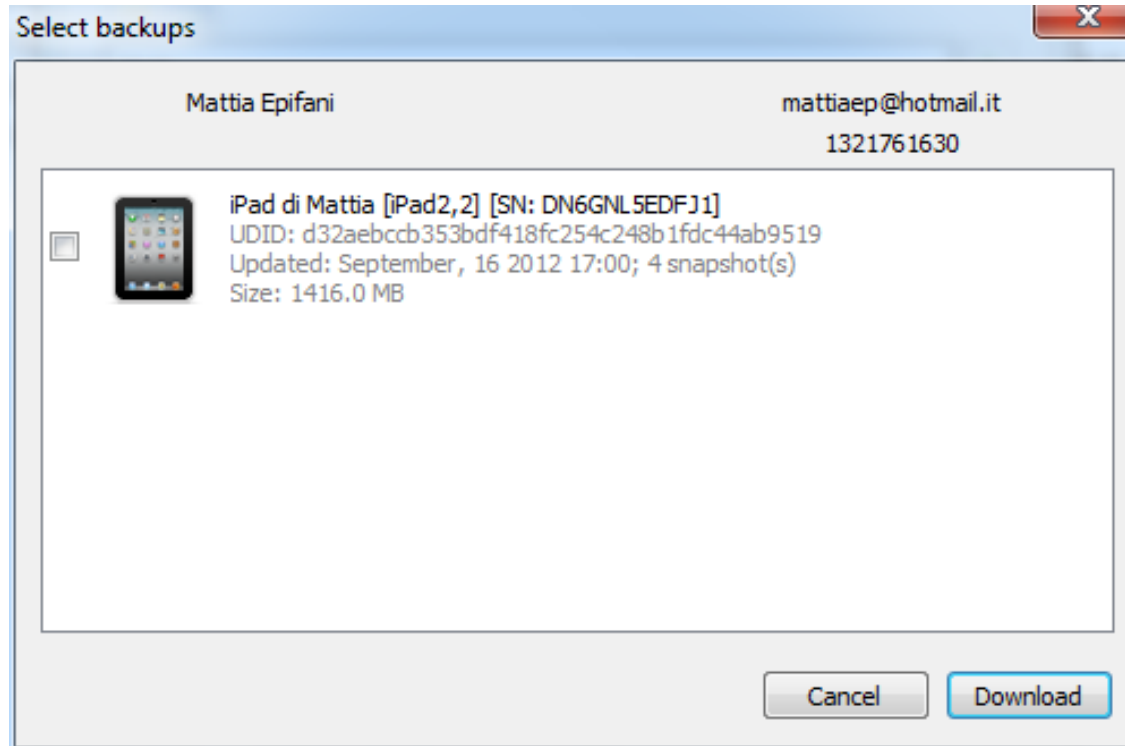
☒ Sign in with Apple ID

Apple ID:

Password:

☐ Use authentication token (base64)

ICLOUD



CONCLUSIONS

- A lot of useful information can be found by analyzing artifacts left by Cloud Storage clients
- Dropbox and Google Drive use Sqlite databases to store information about files
- Dropbox databases are encrypted but in some cases can be easily decrypted (Dropbox Decryptor, IEF)
- Google Drive databases are in clear and contain information about file still present in the storage
- Google Drive Sync_log.log is useful to obtain information about deleted files
- SkyDrive uses a binary file (usercontent.dat) to store information about files still present in the storage
- SkyDrive usercontent.dat file can be analyzed with Internet Evidence Finder or with a Hex editor
- SkyDrive log files are useful to obtain information about deleted files
- Ram analysis is useful to obtain information about client configuration
- Interesting information can be found by analyzing traditional Windows artifacts (LNK, Browser, Thumbnails, Hiberfil, etc.)



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk