

THE JOURNAL OF  
**DIGITAL FORENSICS,  
SECURITY AND LAW**

**Journal of Digital Forensics,  
Security and Law**

---

Volume 15 | Number 1

Article 3


---

June 2020

## **What's in the Cloud? - An examination of the impact of cloud storage usage on the browser cache.**

Graeme Horsman  
Teesside University, g.horsman@tees.ac.uk

Follow this and additional works at: <https://commons.erau.edu/jdfsl>

 Part of the [Computer Law Commons](#), and the [Information Security Commons](#)

---

### **Recommended Citation**

Horsman, Graeme (2020) "What's in the Cloud? - An examination of the impact of cloud storage usage on the browser cache.," *Journal of Digital Forensics, Security and Law*: Vol. 15 : No. 1 , Article 3.

DOI: <https://doi.org/10.15394/jdfsl.2020.1592>

Available at: <https://commons.erau.edu/jdfsl/vol15/iss1/3>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact [commons@erau.edu](mailto:commons@erau.edu).



(c)ADFSL



# WHAT'S IN THE CLOUD? - AN EXAMINATION OF THE IMPACT OF CLOUD STORAGE USAGE ON THE BROWSER CACHE

Graeme Horsman  
Teesside University  
g.horsman@tees.ac.uk

## ABSTRACT

Cloud storage is now a well established and popular service adopted by many individuals and organizations, often at a scaled cost, with free accounts also available. It provides users with the ability to store content on a cloud service provider's infrastructure, offering the benefit of redundancy, reliability, security, the flexibility of access, and the potential assumed the liability of the provider for data loss within the contexts of a licensing agreement. Consequently, this form of remote storage provides a regulatory challenge as content which once resided upon a seized digital exhibit, available for scrutiny during a digital forensic investigatory, may no longer be present where attempting to acquire access to it creates costing and juridical difficulties. This article offers a digital forensic examination of trace-evidence left in the Internet browser cache following cloud storage account usage and interaction. Following interactions with Dropbox and Google Drive in the Chrome browser, testing demonstrates the possibility to recover data capable of facilitating a partial reconstruction of a user's cloud storage account, with results offered and contextualized.

**Keywords:** Digital Forensics, Cloud Storage, Investigation, Cache, Dropbox, Google Drive

## 1. INTRODUCTION

Cloud computing is now revolutionizing the way individuals create, access, and store digital content (Ruan et al., 2011). The 'Cloud' (a term often used to encapsulate all cloud technology service variants) is multifaceted, with options available to the user which range from simple storage facilities, to access to specialist software and hardware platforms (Birk et al., 2011). While an in-depth discussion of cloud technologies is beyond the scope of this work (see Hayes (2008); Mell

and Grance, (2011); Ruparelia, (2016); for a dialogue on this content), defining the Cloud and its coverage is necessary despite not being straightforward due to its multiple areas of coverage, of which attention is drawn toward Mell, and Grance's (2011 p.3) proposed interpretation.

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with min-

imal management effort or service provider interaction." (Mell and Grance, 2011 p.3)

One of the many benefits offered by cloud service providers is the ability for users to store their digital content within a Cloud infrastructure, which has even seen law enforcement utilize such platforms to store large quantities of video footage generated as part of their investigations, for later review (Microsoft, 2016). This is typically referred to as 'cloud storage' where currently, a reported 1.9 billion consumers to have accounts (Statista, 2018c). While forms of a local digital data storage continue to play an important role in the configuration of many computing and mobile systems (a position which is unlikely to drastically change in the immediate future), there are now many cost-effective (in some cases, free) cloud service provider options available for a user who wishes to place their data beyond the confines of their current device's local storage facilities. In doing so, the user acquires the benefit of redundancy, reliability, security, flexibility of access, and the potential assumed liability of the provider for data loss within the contexts of a licensing agreement. Consequently, due to its increasing popularity of using this form of remote data storage creates a regulatory concern, particularly for those involved in the investigation of digital offenses.

Typically, a 'traditional' DF investigation commences with an examination of lawfully seized digital devices and any form of digital storage media which they contain. Prior to cloud technologies, an examination of locally resident content would arguably often result in the ability to determine the way in which a user has interacted with their device and what content they possess, or have created and interacted with. Yet, despite increases in storage media capacities, which are also now more affordable, non-local cloud storage facilities offer an alternative and popular option for robust and secure storage of personal

data. Currently, it is estimated that approximately 3.6 billion users utilize cloud storage services in 2018 (Statista, 2018a), with Dropbox alone claiming 500 million users in 2016 (Dropbox, 2016). While cloud storage maintains many clear benefits for the user, such platforms are abused (Choo and Dehghan-tanha, 2016), where those tasked with investigating such events are posed with a number of investigatory challenges. Those who choose to implement cloud technology as part of any suspected offense create an issue for those tasked with investigating a suspected offense (Grispos et al., 2012; Zargari and Benford, 2012; Thethi and Keane, 2014), where Dykstra and Sherman (2011, p47) note, cloud storage may be used as an 'an accessory to a crime'.

Acknowledgment of the potential for abusing cloud storage technology has long been noted (BBC News, 2011). Any form of remote storage beyond the direct access and scrutiny of law enforcement arguably creates regulatory concerns. As a result, attention is placed on the provider and any mechanisms in place designed to detect abuse of their services. In reality, this is an impossible task, and although service provider agreements make users concede not to utilize their cloud technology for illegal acts, there are those who seek to misuse these services where prohibiting these acts is difficult. While protocols to identify known or notable files may be in place, beyond the knowledge of the user, obfuscation of key files via encryption prior to upload would likely render the provider powerless to detect that illegal content is being stored by a user. One of the main concerns of cloud storage providers is the ability to store images depicting child sexual abuse (IDCSA) (Europol, 2014) with cloud storage reportedly being utilized to store and share IDCSA on a number of occasions (BBC News, 2013; BBC News, 2017; O'Connell, 2018).

This article offers a forensic examination of the impact of cloud storage usage via an Internet browser on the cache to identify the existence and interpretation of digital trace evidence to support law enforcement investigations. Section 2 provides a discussion surrounding the challenges posed by the Cloud, where Section 3 presents an examination of the browser cache following Dropbox usage with Section 4, examining the impact of Google Drive on the browser cache. Finally, conclusions are drawn.

## 2. PROBLEMS WITH THE CLOUD

Anyone involved in criminal acts where liability will ensue if illegal content is found within their possession will likely view cloud storage as a method of protecting themselves by storing content in a place that may not be easily identified. One of the fundamental issues that cloud storage facilities provide is a lack of direct and immediate physical access to content (Dykstra and Sherman, 2012; Zawoad and Hasan, 2013; Simou et al., 2014), where different challenges are encountered depending on the service model which is implemented by the user (Alqahtany et al., 2015). In the context of a user who has access to a cloud storage facility, digital data which formerly resided on a local device may no longer be present following its transfer to the Cloud and any further accesses to it might occur remotely through a cloud storage portal (browser-based or mobile application, etc.). Further, traces of any digital data prior to it being moved to the Cloud may no longer be available on a local device. In each case the challenge of any forensic investigation where a cloud storage account has been used is twofold; first, identifying that a cloud storage service is being used by a suspect and second, identifying what is in there in order

to ascertain potential accountability for criminal acts (Zawoad and Hasan, 2012; Quick et al., 2013; Daryabar et al., 2017). A concern exists that it may not be possible for an investigating practitioner to establish either of these points following a forensic examination of any seized devices.

### 2.1 Access to the Cloud

Assuming that a DF practitioner can identify that a suspect has operated a cloud storage account, they may seek (with appropriate guidance and authority as part of an investigation) to examine content stored within it. To achieve this, they may attempt to acquire credentials to access a cloud account (either from a seized device or suspect, accompanied by relevant legal authority) or seek legal disclosure of account information from the provider directly. Such processes can be time-consuming, expensive, and have varying rates of success due to procedural irregularities or non-compliance (Dykstra and Sherman, 2011; Marturana et al., 2012). Figure 1 provides a high-level overview of the decisions involved in the investigation of a cloud storage account believed to be involved in a suspect offense.

There are three investigatory paths to proceed with acquiring access to a cloud storage account. The first follows a request directly to the cloud service provider following the correct disclosure requirements have been met, accompanied by the necessary legal authority. Procedural requirements are often defined within a provider's terms and conditions and legal guidance, which is often supplied on their websites. In some cases, a law enforcement portal is available specifically for request purposes. Following a submission request, the provider determines its validity taking into account their licensing agreements and operational arrangements before deciding whether to make an account information disclosure. Where a provider exists beyond the jurisdiction in which the current

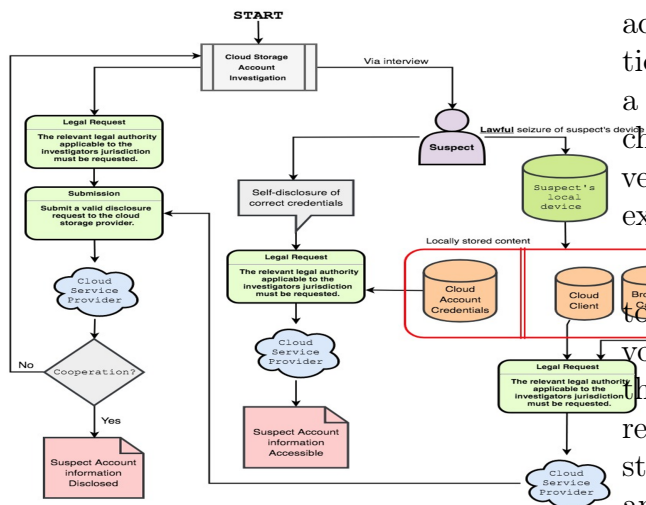


Figure 1. The high-level stages involved during an investigation involving a suspected cloud storage account.

investigation is taking place, difficulties can arise due to, in some cases, a lack of legal enforcement issues and compliance. While a disclosure request is likely to be the main option for obtaining a complete depiction of a suspect’s cloud storage account, the timely cooperation by a service provider along with procedural efficiencies and costs has raised concerns (James and Gladyshev, 2016; Parliamentary Office of Science and Technology, 2016; Casey et al., 2018).

Second, a suspect may choose to self-disclose the content of their accounts or provide access to it. Subject to requisite legal authority to access and utilized such disclosed content, the practitioner may be able to extract and examine content within cloud storage. Finally, following an investigation of any of a suspect’s seized items (computer, mobile device, etc.) it may be possible to extract cloud storage account credentials and utilize them to attain a remote login to the cloud storage account (see tools such as Magnet AXIOM Cloud) (Martini et al., 2016). Again, while the required legal authority is needed, this option provides potentially the quickest

access to a suspect account. While this option may offer a quicker route to accessing a cloud account, providers can update and change the way their service operates, preventing such methods from being forensically exploited.

Despite these three options being available to law enforcement, prior to any stages involved with securing access to the account, those involved must first have some form of reasonable grounds first to suspect that cloud storage facilities have been used as part of an offense, and second, maintain some indication as to what they expect to be stored within the account or how they believe it has been used. Access to a cloud account can be a resource-intensive process. Therefore a decision to pursue access should be made following information which provides some form of reasonable suspicion that content within it will be of evidentiary value to a current investigation. While legal requirements differ between jurisdictions and service providers, typically, such requirements are in place to prevent unnecessary privacy breached and collateral intrusion. In the UK, the Regulation of Investigatory Powers Act 2000 provides the power to compel suspects to disclose their passwords (see RIPA section 49), with the recent case of Stephen Nicholson demonstrating prosecution for failing to provide access to his Facebook account (Sky News, 2018). Such methods may be seen as a way to potentially circumvent the difficulties associated with seeking disclosure from a service provider.

Given the issues noted previously in sections 1 and 2, establishing such evidence-of-use may be an issue. In the last eight years, academic literature has focused on documenting the forensic challenges posed by cloud platforms (see, for example, Aminzhad et al., 2013), but minimal attention to the browser cache has been paid.

## 2.2 The Cache

Providing private modes have not been utilized, the Internet browser cache on most mainstream browsing applications provides an insight into the content hosted on the sites visited by the user. The browser cache is frequently acknowledged but rarely the sole focus of digital forensics research (see Horsman, 2018a; 2018b for some examples of cache-focused work). In the context of the Cloud, this is also often the case, where for example Malik et al., (2015) focus on cloud storage application artifacts omitting an analysis of the cached content from basic browser-based interaction with a cloud storage account, which can be a potential source of content cached from a result of their visit and interaction with their storage account. Section 3 and 4 demonstrates the potential value of the browser cache as part of an investigation into cloud storage usage.

## 3. METHODOLOGY

The testing undertaken followed the Framework for Reliable Experimental Design (FRED) research model (Horsman, 2018c). All testing carried out within this article was completed using test Dropbox and Google Drive accounts with uniquely identifiable data (both in terms of content; pre-hashed for identification purposes, and filename) to examine account usage behaviors in the cache. Interaction with these accounts was carried out on a clean install of the Windows 10 operating system with logins and access to the cloud storage accounts undertaken through the Chrome Internet browser (version 67.0.3396.99) due to its reported dominant share of the market in terms of users. Subsequent analysis of the Chrome cache following cloud storage account activity was carried out utilizing Nirsoft's (2018) 'Chrome-CacheView v1.77', a cache parsing application. Testing was iterative, examining indi-

vidual account actions, then repeating test results for reliability purposes.

### 3.1 Dropbox

This section explores the impact on the Internet browser cache following user interaction with a Dropbox cloud storage account.

#### 3.1.1 Dropbox 'On-Landing':- Account Metadata

An examination of the cache following landing on the `www.dropbox.com` site, the `www.dropbox.com.html` file is of interest (see Figure 2). Here, details of the cached site HTML structure is available for query. While this file does not render when placed back into the browser window itself allowing a visual inspection of the site's elements (a typical process implemented in forensic investigations in order to force the browser to re-render a cached site's architecture), its internal HTML code can still support the identification of Dropbox content when a user has viewed their account online using Chrome.

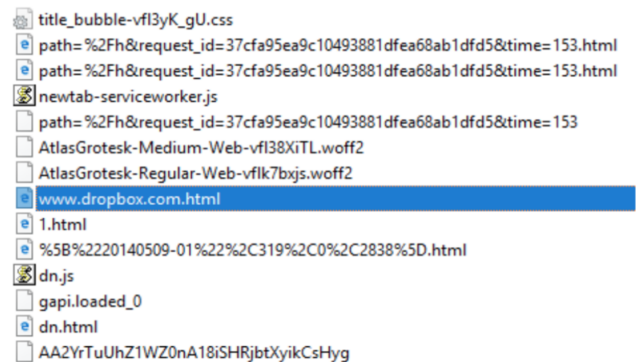


Figure 2. Chrome cache content following a visit to `www.dropbox.com`.

To commence, following an examination of the `\\www.dropbox.com.html\\$` file and its contents (an example content is captured and provided below for reference), the "PAGE\_LOAD\_TIME": tag entry denotes a UNIX Epoch timestamp which following testing indicates the time the page was last

loaded. Following a live examination of the *Dropbox* homepage source code indicates this value is also updated when the page is refreshed. Therefore the value reflects a 'last load time,' which could be either an initial visit or page refresh. In the case of the former, this time may be cross-referenceable against Internet history timestamp information if present. As a result, this time stamp allows a practitioner to determine what files were in the Dropbox account at a given time, taking into account the information discussed in the following sections of this article.

Also, data contained in the { "LOCALE": } parenthesis depicts metadata surrounding the account, which has been accessed through the web browser (shown below). The `display_name`: tag value reflects the 'Name' value assigned to the account (defined by the account holder during sign-up). The `id`: tag value provides an account identifier, which can also be attributed to account activity (see Section 3.1.2 for further details). The `email`: tag value provides the email address of the account signed in during the Dropbox session, and the `photo_circle_url`: tag value contains the URL for the profile picture assigned to the account. A third party can access this URL to display the image if it remains hosted on the *Dropbox* servers. If no profile image has been set, this value is set to NULL.

```
{\"LOCALE\": \"GB\", \"prompt_hiding\": true, \"viewer_properties\": {\"display_name\": \"GREY JOY\", \"can_moderate_comments\": false, \"deprecated_first_user_in_the_cookie_id\": 77837232, \"is_reseller_session\": false, \"is_team_assume_user_session\": false, \"is_assume_user_session\": false, \"user_data\": [\"initials_url\": \"https://ac.dropboxstatic.com/account_photo/get_initials?initials=GJ\\u0026size=128x128\\u0026vers=0\", \"user
```

```
_root_permissions\": \"edit\", \"has_never_set_password\": false, \"id\": 77837232, \"sso_required\": false, \"display_name\": \"Grey Joy\", \"_authenticated\": true, \"home_ns_id\": 126648836, \"lname\": \"JOY\", \"role\": \"personal\", \"is_email_verified\": true, \"fname\": \"GREY\", \"cdm_path\": \"\", \"email\": \"grey.joy@googlemail.com\", \"is_paper_disabled\": false, \"account_id\": \"dbid:AAAAz7mAv7FT0-BYzKWNpC1uj3FaJ1wVfBA\", \"is_cdm_member\": false, \"nid\": \"01529833775757704936\", \"is_dropbox_admin\": false, \"paid\": 0, \"root_ns_id\": 126648836, \"photo_url\": null, \"is_team_admin\": false, \"familiar_name\": \"GREY\", \"is_team\": false, \"photo_circle_url\": \"https://dl-web.dropbox.com/account_photo/get/dbaphid/%3AAACJ-_rJyCoDzFXXbB8MDaBqtStmlN-pZdY?circle_crop=1\\u0026size=128x128\\u0026vers=1530383091362\"}], \"DEFAULT_ROOT_NAME\": \"Dropbox\", \"PERSONAL_ROLE_STRING\": \"Personal\"}
```

### 3.1.2 Home Screen Activity

The `www.dropbox.com.htm` file also maintains structural information regarding the Dropbox web pages visited by a user, with the starting point for analysis being the Dropbox 'Homepage'. The Dropbox 'Homepage' maintains by default a list of the 10 most recent activities undertaken by the user. However, this list does offer a user the chance to expand this view. Figure 3 provides an example of the Dropbox Homepage, where key page artifacts have been highlighted. This demonstrates how this data are presented in the `www.dropbox.com.html` file and the meaning of associated metadata retained.

Every single entry on the 'Recent' list on the Dropbox homepage is structured within the `www.dropbox.com.html` file as follows:-

```
\"recent_activities\": [{\"when_milli\
```

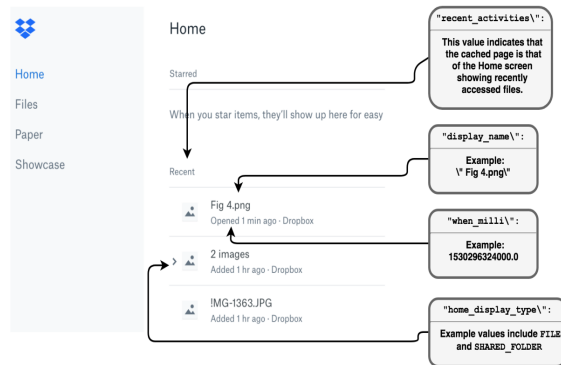


Figure 3. The Dropbox ‘Home’ screen showing recent user activity.

```
": 1530296324000.0, \"resource_id\":
\"id:WftHZCn1cXAAAAAAAAACXg\", \"rela
ted_activity_keys\": [\"RmlsZUFjdG12aX
R50ldmdEhaQ24xY1hBQUFBQUFBQUFDWc6Zml
sZV9vYmpfa2V5\"], \"iewing_user\": {
\"id\": 77837232}, \"recent_event_ty
pe\": 0, \"activity_key\": \"UmVjZW50
QWN0aXZpdHk6MDoxNTMwMjk2MzIOLjA6Yjgz
ZWlYzTY4MjA4YTUxODQyMjYxMmVlNjM5ZyYw
ZmQ\", \"id_type\": \"ENCODED_FILE_OBJ
_ID\", \"activity_data\": {\"home_dis
play_type\": \"FILE\"}, \"skeleton_
data\": {\"context_display_name\": \"P
ersonal\", \"context_display_path\": \"
\", \"filter_types_by_key\": {\"RmlsZUFj
dG12aXR50ldmdEhaQ24xY1hBQUFBQUFBQUFDW
Gc6ZmlsZV9vYmpfa2V5\": 1}, \"display_
name\": \"Scre-en Shot 2018-05-19 at
21.12.40.png\", \"icon\": \"page_whit
e_picture\"}}}
```

The "when\_milli" timestamp reflects the 'informal' value displayed to the user. For example, in Figure 3 where Fig 4.png is shown to have been opened '1 minute ago', the "when\_milli" UNIX Epoch timestamp when converted depicts the actual time stamp. Whenever an entry on the Recent list is interacted with (a file/folder is opened, viewed, etc.), this timestamp is dynamic and updates to reflect the time of this interaction,

therefore depending on the time that the `www.dropbox.com.html` file is cached by the browser, further accesses may have occurred but not have been reflected in the cached data. The "activity\_key" is a Base64 encoded value which when decoded is typically formatted as follows - *RecentActivity:9:1530369097.0:b83eb2e68208a518422612ee639c60fd*. Following testing, the RecentActivity timestamp was shown to be the same as "when\_milli" timestamp. Although there appears to be a hash-type alphanumeric string (seemingly of structure type MD5) value, this value changes when the same file (identical, verified by hash) is uploaded and when file names are changed and therefore testing suggests this value cannot be used as a unique identifier for the file which has been accessed on the account. The "viewing\_user" value corresponds to the account ID (shown in section 3.1.1 regarding account metadata). The "home\_display\_type" value indicates the type of artifact where FILE indicates a stored file, and SHARED/\_FOLDER indicates a shared folder item.

Finally, the "display\_name" value corresponds to the file/folder name shown to the user, which has been assigned to the file when uploaded.

If the user expands a Recent event which contains one or more files (typically images, see for example in Figure 3 where 2 images are stated indicating two images are stored within an expandable menu), a 100\*100 preview image will be displayed to the user of each file (see Figure 4). Following testing, when a user expands these menus within their browser window, these preview images are cached with typical file names structured as `size=100x100size_mode=4.jfif` indicating that it is an expanded menu previewed file which has been cached, and therefore files cached with this name can be attributed to this form of Dropbox activity. When the



browser cache is parsed, the cached file's associated URL contains the file's original filename; therefore, it is possible to identify the filename given to the file by the user, which has been cached.

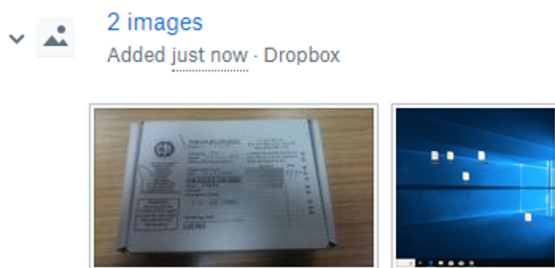


Figure 4. An example expanded preview on the Dropbox Homepage.

### 3.1.3 'Files' View

When a user navigates to the 'Files' page (which lists all files in the user's Dropbox account) in their Dropbox account (a URL of <https://www.dropbox.com/home> is recorded in the address bar and Internet history), a home.html file is cached denoting the structure of the 'Files' Dropbox page. When attempting to determine the contents of this page, the event\_type parenthesis contains information regarding each item shown to be in the Dropbox account onscreen, with a typical structure shown below. Figure 5 demonstrates how this metadata is visually linked to a typical Dropbox page.

```
{\"event_type\": 1, \"beacon_context\": \"AAB8jgVq61LHPiMD6YF4zX8v44x_N2VWkQ8M\", \"href\": \"//www.dropbox.com/pri/get/fig/%204.png?_subject_uid=1023627536\\u0026w=AAAEDd5K1A1-duu09ccAm_1evI1KPlpnJ1brSTb14RZ8vQ\", \"is_dir\": false, \"thumbnail_url_tmpl\": \"https://photos.dropbox.com/t/2/AABriBxPofqyc7onrTIpCz8jC4Rngx2egmWGatv398FafA/12/1023627536/png
```

```
/32x32/1/_/1/9/fig/%204.png/EKCxq9oKGDUGAigC/BHWu3g9fdmJx3Q8jvCrer6wyjxqgFwqz8aGQqcJOJIgtK_P3ZoDGQ7i28B7mUqml1uRwaj91cg0ufX5_orq8B2MM4nX2bTqQD5jRmYf2g4S15VSRpEwPmjJ4Wto6ewHcOLc?size=32x32\\u0026size_mode=1\", \"is_cloud_doc\": false, \"is_in_team_folder_tree\": false, \"user_id\": 1023627536, \"fq_path\": \"/Fig4.png\", \"ts\": 1530266052, \"previous_type\": \"photo\", \"sjid\": 47, \"size\": \"13.08KB\", \"type\": 1, \"ns_path\": \"/Fig4.png\", \"direct_blockserver_link\": \"//dleb.dropbox.com/get/fig/%204.png?_subject_uid=1023627536\\u0026w=AAAEDd5K1A1-duu09ccAm_1evI1KPlpnJ1brSTb14RZ8vQ\", \"sort_key\": [\"Mzk1BA8GCEdDNQENAdwMAA==\"], \"is_unmounted\": false, \"file_id\": \"id:1go40NUabqAAAAAAAAAAQw\", \"is_symlink\": false, \"icon\": \"page_white_picture_32\", \"ago\": \"29/6/201810:54\", \"bytes\": 13399, \"preview_url\": \"https://photos-6.dropbox.com/t/2/AABriBxPofqyc7onrTIpCz8jC4Rngx2egmWGatv398FafA/12/1023627536/png/32x32/1/_/1/9/fig/%204.png/EKCxq9oKGDUGAigC/BHWu3g9fdmJx3Q8jvCrer6wyjxqgFwqz8aGQqcJOJIgtK_P3ZoDGQ7i28B7mUqml1uRwaj91cg0ufX5_orq8B2MM4nX2bTqQD5jRmYf2g4S15VSRpEwPmjJ4Wto6ewHcOLc?preserve_transparency=1\\u0026size=32x32\\u0026size_mode=1\", \"ext\": \".png\", \"revision_id\": \"2fab4ad8a0\", \"ns_id\": 2873809056}
```

### 3.1.4 Viewing an Individual File

When an individual picture file is viewed from within Dropbox (for example, a picture is clicked upon expanding the user's view of it as shown in Figure 6), this previewed file is cached by the browser with a filename struc-



Figure 5. An example of a typical 'Files' Dropbox page indicating which metadata is cached.

ture of `size=32x32size_mode=5.jfif`. Files with this naming structure can be attributed to the act of viewing an individual file on Dropbox. As noted above, with the caching of expandable menu previewed files, the cached file's associated URL maintains the original file name of the cached image, which the user has attributed to this file on the Dropbox account (for example, `www.dropbox.com/home?preview=FILENAME\AME.png`). Metadata regarding individually viewed files is cached in a text file which the following testing has the following naming convention where `%2FFILENAME` reflects the name of the file on Dropbox, and therefore, metadata can be correlated to it - `is_xhr=trueactivity_context=3activity_context_data=%2FFILENAME.txt`. This file is typically structured as follows:-

```
{
  "status": "ok",
  "payload": {
    "can_edit_feedback": true,
    "resolved_comment_count": 0,
    "feedback_off": false,
    "users_to_notify": [
      {
        "dbx_account_id": "dbid:AADHAYZBkFdb6WkH63Kk_th-sjvKcj1Gq7Y",
        "initials_url": "https://ac.dropboxstatic.com/account_photo/get_initials?initials=GJ\u0026size=64x64\u0026vers=0",
        "id": 1023627536,
        "photo_url": null,
        "display_name": "Grey Joy",

```

```

    "lname": "Joy",
    "role": "personal",
    "photo_circle_url": null,
    "fname": "Grey",
    "email": "",
    "unique_id": "dbid:AADHAYZBkFdb6WkH63Kk_th-sjvKcj1Gq7Y"}
  ],
  "latest_revision": {
    "direct_blockserver_link": null,
    "rev_owner": null,
    "preview_link": null,
    "when": 1527771969.0,
    "revision_id": "BHX_hi0zgCXy4-p6eC24vvjrGN5PLYS01DsBmq7FVv3yMmUF6ZoTN4RE3d2VRQpk0_rcrLwGthE79-hPoSieEdeZhdKY0hjd5gBUwiAvWcFNxfSHCBgRpPxSlL4X2mMH1mo"},
    "file_icon": "page_white_picture",
    "owner": {
      "dbx_account_id": "dbid:AADHAYZBkFdb6WkH63Kk_th-sjvKcj1Gq7Y",
      "initials_url": "",
      "email": "",
      "lname": "",
      "role": "personal",
      "photo_circle_url": null,
      "fname": "",
      "display_name": "",
      "id": 1023627536,
      "unique_id": "dbid:AADHAYZBkFdb6WkH63Kk_th-sjvKcj1Gq7Y",
      "photo_url": null},
    "is_dir": false,
    "fq_path": "/Fig 5.png",
    "when_milli": 1527771969000,
    "comment_activity_dicts": [],
    "name": "Fig 5.png",
    "context_data": "/Fig 5.png",
    "when": 1527771969,
    "actor": {
      "dbx_account_id": "dbid:AADHAYZBkFdb6WkH63Kk_th-sjvKcj1Gq7Y",
      "initials_url":

```



Figure 6. A demonstration of an individual file preview showing comment information and file metadata.

A Dropbox user can also comment on the files they have uploaded to their account, and in turn, if the file has been shared with another user, they can also make comments. When comments are made (shown in Figure 6), the `s\_xhr=true&activity_cont=3activity_context_data=%2FFILENA-`

ME.txt file maintains addition "comment": tags. Examples of comments and comment metadata are provided below.

```
"comment": {"resolved": false,
"comment_meta_json": null,
"comment_text": "LOTS OF COMMENT TEXT",
"client_id": null, "when_mses":
1530907487537, "commenter_dict":
{"dbx_account_id":
"dbid:AADHAYZBkF
db6WkH63Kk_th-sjvKcj1Gq7Y",
"initials_url":
"https://ac.dropboxstatic.com
/account_photo
/get_initials?initials
=GJ\u0026size=64x64
\u0026vers=0", "id": 1023627536,
"photo_url": null, "display_name":
"Grey Joy", "lname": "Joy", "role":
"personal", "photo_circle_url": null,
"fname": "Grey", "email": "",
"unique_id": "dbid:AADHAYZBkF
db6WkH63Kk_th-sjvKcj1Gq7Y"},
"comment_gid":
"c3650FsrDbAAAAAAAAAABg",
"when": 1530907487,
"reply_to_activity_key":
null, "raw_comment_text":
"LOTS OF COMMENT TEXT"},
```

Comments can be replied to directly by a third party account where the original owner of the file directly links their account to a comment. Where a third party replies, `display_name`, `lname` and `fname` tags will reflect the third party's account details. No email address information is available for

the third party commenter, and the "id": tag does not maintain the account holder's unique id, rather the value is typically set to 0. As a result, while a 3rd party account can be partially identified, it may not be possible to identify the actual account (or submit a disclosure request to Dropbox) if account name metadata has been changed

### 3.1.5 File Sharing and Deleted Files

Each Dropbox account also has a 'Sharing' page (visits to this page generate the URL <https://www.dropbox.com/share> in the Internet history), which depicts the files and folders which have been shared with the user's account. When a user interacts with this page, following an examination of the cache, no records of the page content and shared files could be located. Similarly, Dropbox maintains deleted files for 30 days where a user can view and restore this content. No records attributable to deleted file records could be identified in the browser cache during test visits to the deleted files pages. As a result, the browser cache is unlikely to provide any records of content from a user account that has been deleted or shared.

## 4. GOOGLE DRIVE

Section 4 provides an analysis of 'Google Drive', a cloud storage service comparable to that of Dropbox. Those who have a Google account also have access to Google's cloud storage facility 'Google Drive,' and at the time of writing, Google offers 15 GB of storage free to account holders. Forensic analysis of Google Drive demonstrates that despite being a comparative platform to Dropbox, the behavior of this service within the web browser cache presents a greater challenge to those seeking to investigate the usage of cloud storage accounts of this type. In contrast to Dropbox analysis, the Chrome browser cache retains limited information depicting a user's

interaction with their Google Drive account with the remainder of this section demonstrating this.

As a starting point for analysis, the Google Drive Home screen is examined. The Home URL for a Google Drive visit is structured as <https://drive.google.com/drive/my-drive> with Figure 7 depicting the Home screen site structure.

The 'My Drive' link documents a scrollable list of all contents within the Google Drive account. Unlike Dropbox, on-landing, site stratal .html content is not locally cached, and therefore no metadata regarding stored files visible to the user onscreen can be extracted and examined from the browser cache (unlike Dropbox). As a result, from the cache alone, testing indicated that it was not possible to ascertain the names and associated metadata of content stored in the account. While this, compared to Dropbox, is a limiting factor for practitioners who are tasked with a cloud storage account investigation, some image caching does occur. The Google Drive Home screen maintains two types of thumbnail image, 'Quick Access' (files typically cached with a file name of w300-k) and 'File List' thumbnails (files typically cached with a file name of w32-h32-p-k-nu) (shown in Figure 7). Following testing, no user assigned and attributable file name information was available.

An examination of all files cached (cache content was captured using Nirsoft's (2018) 'ChromeCacheView v1.77' and keyword searched for file names (uniquely attributed to test data) and associated onscreen visible metadata) following a visit to the Google Drive Home screen failed to identify file related metadata of cloud storage content. This indicates that Google Drive account metadata content is not cached on the local device.

The URL associated with Google Drive activity also offers limited information. When

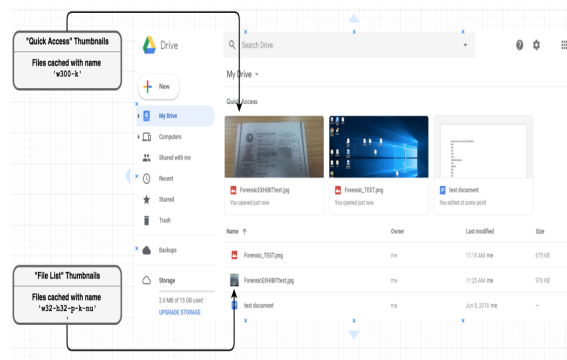


Figure 7. The Google Drive Home screen structure.

an image is previewed from the Home screen, the URL does not change (it remains - <https://drive.google.com/drive/my-drive>). However, previewed images are cached with a typical file name of w1366-h662), meaning analysis of Internet history is unlikely to reveal significant information regarding account content. When a user navigates to a folder they have created within their account; the URL is typically structured as <https://drive.google.com/drive/folders/OBy-Cihkhmyw0ek1Gak4ySlhnQkk>. The bolded section appears encoded and does not change when the folder is renamed, indicating that it is unlikely to hold obfuscated folder name information. As a result, an analysis of internet history is unlikely to reveal account usage behavior.

Google Drive is also part of Google's suite of tools offered to a Google account holder, where a user who has files of the type that can be placed under the umbrella term of 'office documents', can automatically utilize Google Slides, Docs, and Sheets to open, view and edit them. When a user selects an office document of any type and is directed to an appropriate Google facility (either Docs, Sheets or Slides), testing showed that the content of these documents is not cached by Chrome (following extraction of the Chrome

cache and the utilization of keyword and file carving techniques).

## 5. RESULTS AND CONCLUDING THOUGHTS

The use of cloud storage facilities now means that digital forensic practitioners face an increased likelihood that localized forms of data storage may not contain all of a user's owned and potentially evidentiary digital content. Whilst procedures are in place to request account content disclosure from a service provider and to seek account credentials for future access; such methods are not a guaranteed way of establishing access to a user's account (see, for example, Google's (2017) Transparency Report documenting acts of compliance to requests and disclosure of account data). It is key to note that often a request for account access must be made following some form of a reasonable belief that content within the account may be relevant to an investigation where measures are often in place both jurisdictionally and in the terms of service of many providers to protect a user's privacy in the context of using such services. Acquiring such reasonable belief requires an investigation of the surrounding facts of a case and information available to an investigator, of which one key source (dependent on the platform in use) may be that of the Internet browser cache. Localized forms of cached cloud storage activity have been overlooked by current academic research in digital forensics and cloud storage investigations. Yet, testing demonstrated in this article reveals that the act of accessing Dropbox via the Chrome web browser leads to what can be arguably considered comprehensive caching of their account content and its associated metadata. While the same level of caching was not witnessed with Google Drive, testing

demonstrates that even though the value of the browser cache in cloud storage investigations varies depending upon the service in use by a suspect, it should not be wholly disregarded as a source of potentially evidentiary information. Subject to the deletion of cache content (either through a browser's inbuilt cleaning features or via 3rd party deletion applications), cached content may influence law enforcement decision making as to whether to pursue a potentially time consuming and costly disclosure request to a service provider.

### 5.1 A Comparison of Platform Results

As each platform displays different caching behavior, it is necessary to offer the following breakdown of recoverable cached data as a result of the use of each service.

Dropbox:

**File Listings:** Information regarding files listed in the user's Dropbox account, including any files within sub-folders, can be recovered from cached content. This includes not only file names assigned by the user but also timestamp information.

**Images:** Both thumbnail images and previewed images are cached.

Account information: Metadata, including account holder information, email, and account identification, can all be retrieved from cached .html files denoting the Dropbox account site's structure.

**File Comment information:** Where a comment has been left on a file within the Dropbox account, comment content is cached.

**Descriptive Internet History:** Where a user accesses folders on their account, the URL denotes the file and folder names associated with this content (for example- `www.dropbox.com/home/TESTFOLDERNAME`).

Google Drive:

**Images:** Both thumbnail images and pre-

viewed images are cached.

Despite a difference in the volume of content cached between both services, it is critical to note that in both cases caching in some form does take place and therefore offers some use to a practitioner examining a device. Particularly as noted in Section 1, where cloud storage providers have been utilized to store IDCSA when a user visits their account, testing suggests that image caching of viewable content (see Horsman (2018d) for a discussion of the browser cache and viewable content onscreen) including preview thumbnails will occur on both platforms. In such cases, this may be enough for an examination to identify that an account holds potentially relevant information providing that they can attribute the cached files to an act of viewing a cloud storage account through the browser. This should be achievable by examining the chronological timings of Internet history and, as noted above, acknowledging files with the naming conventions previously highlighted and acknowledging that these have come from a cached cloud storage account visit.

## 5.2 Limitations and Future Work

Chrome remains a reported market-leading Internet browser and, therefore, a chosen target of this work (Statista, 2018b). The results depicted may be transferable to other web browsing applications, where further testing is required, but due to the exhaustive number of services and browser platforms, it was not feasible to achieve this within this work. As a result, this work provides an entry analysis into this form of investigation to inform practitioners of the potential presence of such content and to incorporate this within their investigation processes. The depiction of cached cloud storage content is also subject to changes over time, and as cloud service providers update and adapt their platform, el-

ements may no longer be cached locally, or in some cases, additional content may be cached. As a result, cache analysis in this context is a moving target with multiple variables that may impact the success of determining how someone is using their account. This work has demonstrated that caching of cloud storage artifacts can occur, and therefore it is argued that the browser cache should not be disregarded when investigations of this type are being undertaken. Future work must involve the sustained research of Internet browser cache behavior in this context, incorporating both different browser platforms.

## REFERENCES

- [1] Alqahtany, S., Clarke, N., Furnell, S. and Reich, C., 2015, April. Cloud forensics: a review of challenges, solutions and open problems. In *Cloud Computing (ICCC), 2015 International Conference on* (pp. 1-9). IEEE.
- [2] Aminnezhad, A., Dehghantanha, A., Abdullah, M.T. and Damshenas, M., 2013. Cloud forensics issues and opportunities. *International Journal of Information Processing and Management*, 4(4), p.76.
- [3] BBC News (2011) 'Are there criminals hiding in the cloud?' Available at: [http://news.bbc.co.uk/1/hi/programmes/click\\_online/9477968.stm](http://news.bbc.co.uk/1/hi/programmes/click_online/9477968.stm) (Accessed: 1 August 2018)
- [4] BBC News (2013) 'Ian Watkins child abuse inquiry appeal prompts new leads' Available at: <https://www.bbc.co.uk/news/uk-wales-25159467> (Accessed: 1 August 2018)
- [5] BBC News (2017) 'British teacher held in Spain over child sexual images' Available at: <https://www.bbc.co.uk/>

- news/uk-40847761 (Accessed: 1 August 2018)
- [6] Birk, D. and Wegener, C., 2011, May. Technical issues of forensic investigations in cloud computing environments. In *Systematic Approaches to Digital Forensic Engineering (SADFE)*, 2011 IEEE Sixth International Workshop on (pp. 1-10). IEEE.
- [7] Casey, E., Geradts, Z. and Nikkel, B., 2018. Transdisciplinary strategies for digital investigation challenges. *Digital Investigation* 25 pp.1-4
- [8] Choo, K.K.R. and Dehghantanha, A. eds., 2016. *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*. Syngress.
- [9] Daryabar, F., Dehghantanha, A. and Choo, K.K.R., 2017. Cloud storage forensics: MEGA as a case study. *Australian Journal of Forensic Sciences*, 49(3), pp.344-357.
- [10] Dropbox (2016) 'Celebrating half a billion users' Available at: <https://blogs.dropbox.com/dropbox/2016/03/500-million/> (Accessed: 1 August 2018)
- [11] Dykstra, J. and Sherman, A.T., 2011, May. Understanding issues in cloud forensics: two hypothetical case studies. In *Proceedings of the Conference on Digital Forensics, Security and Law* (pp. 45-54).
- [12] Dykstra, J. and Sherman, A.T., 2012. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, 9, pp.S90-S98.
- [13] Europol, E.C.C., 2014. *The Internet Organised Crime Threat Assessment (IOCTA)*. Available at: [https://www.europol.europa.eu/sites/default/files/documents/europol\\_iocta\\_web.pdf](https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web.pdf) (Accessed: 1 August 2018)
- [14] Google (2017)' Requests for user information' Available at: [https://transparencyreport.google.com/user-data/overview?hl=en&user\\\_requests\\\_report\\\_period=series:requests,accounts;authority;time:Y2015H2&lu=user\\_requests\\_report\\\_period](https://transparencyreport.google.com/user-data/overview?hl=en&user\_requests\_report\_period=series:requests,accounts;authority;time:Y2015H2&lu=user_requests_report\_period) (Accessed: 27 August 2018)
- [15] Grispos, G., Storer, T. and Glisson, W.B., 2012. Calm before the storm: The challenges of cloud computing in digital forensics. *International Journal of Digital Crime and Forensics (IJDCF)*, 4(2), pp.28-48.
- [16] Hayes, B., 2008. Cloud computing. *Communications of the ACM*, 51(7), pp.9-11.
- [17] Horsman, G., 2018a. I didn't see that! An examination of internet browser cache behaviour following website visits. *Digital Investigation*, 25 105-113
- [18] Horsman, G., 2018b. Reconstructing streamed video content: A case study on YouTube and Facebook Live stream content in the Chrome web browser cache.
- [19] Horsman, G., 2018c. Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics. *Computers Security*, 73, pp.294-306.
- [20] Horsman, G., 2018d. I didn't see that! An examination of internet browser

- cache behaviour following website visits. Digital Investigation.
- [21] James, J.I. and Gladyshev, P., 2016. A survey of mutual legal assistance involving digital evidence. *Digital Investigation*, 18, pp.23-32.
- [22] Malik, R., Shashidhar, N. and Chen, L., 2015. Cloud Storage Client Application Analysis. *International Journal of Security*, 9(1), p.1.
- [23] Martini, B., Do, Q. and Choo, K.K.R., 2015. Mobile cloud forensics: An analysis of seven popular Android apps. arXiv preprint arXiv:1506.05533.
- [24] Martini, B., Do, Q. and Raymond Choo, K.K., 2016. Digital forensics in the cloud era: The decline of passwords and the need for legal reform. *Trends Issues in Crime Criminal Justice*, (512).
- [25] Marturana, F., Me, G. and Tacconi, S., 2012, October. A case study on digital forensics in the cloud. In *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2012 International Conference on (pp. 111-116). IEEE.
- [26] Mell, P. and Grance, T., 2011. The NIST definition of cloud computing.
- [27] Microsoft (2016) 'London's police officers get new tool to fight crime – Microsoft Azure' Available at: <https://news.microsoft.com/en-gb/2016/12/01/35558/> (Accessed August 10 2018)
- [28] Nirsoft (2018) 'ChromeCacheView v1.77 - Cache viewer for Google Chrome Web browser' Available at: [https://www.nirsoft.net/utils/chrome\\_cache\\_view.html](https://www.nirsoft.net/utils/chrome_cache_view.html) (Accessed August 10 2018)
- [29] O'Connell, Gerard (2018) 'Vatican diplomat sentenced to five years in prison for child pornography crimes' Available at: <https://www.americamagazine.org/faith/2018/06/23/vatican-diplomat-sentenced-five-years-prison-child-pornography-crimes> (Accessed: 1 August 2018)
- [30] Parliamentary Office of Science and Technology (2016) 'Digital Forensics and Crime' POSTnote 520 March 2016 Available at: <http://researchbriefings.files.parliament.uk/documents/POST-PN-0520/POST-PN-0520.pdf> (Accessed 19 July 2018)
- [31] Quick, D., Martini, B. and Choo, R., 2013. *Cloud storage forensics*. Syngress.
- [32] Ruan, K., Carthy, J., Kechadi, T. and Crosbie, M., 2011, January. Cloud forensics. In *IFIP International Conference on Digital Forensics* (pp. 35-46). Springer, Berlin, Heidelberg.
- [33] Ruparelia, N.B., 2016. *Cloud computing*. Mit Press.
- [34] Simou, S., Kalloniatis, C., Kavakli, E. and Gritzalis, S., 2014, June. Cloud forensics: identifying the major issues and challenges. In *International Conference on Advanced Information Systems Engineering* (pp. 271-284). Springer, Cham.
- [35] Sky News (2018) 'Lucy McHugh murder suspect jailed for refusing to reveal Facebook password' Available at: <https://news.sky.com/story/lucy-mchugh-murder-suspect-jailed-for-refusing-to-reveal-facebook-password-11486507> (Accessed 3 September 2018)



- [36] Statista (2018a) 'Number of consumer cloud-based service users worldwide in 2013 and 2018 (in billions)' Available at: <https://www.statista.com/statistics/321215/global-consumer-cloud-computing-users/> (Accessed 17 August 2018)
- [37] Statista (2018b) 'Global market share held by the leading web browser versions as of February 2018' Available at: <https://www.statista.com/statistics/268299/most-popular-internet-browsers/> (Accessed 3 September 2018)
- [38] Statista (2018c) 'Forecast number of personal cloud storage consumers/users worldwide from 2014 to 2020 (in millions)' Available at: <https://www.statista.com/statistics/499558/worldwide-personal-cloud-storage-users/> (Accessed 3 September 2018)
- [39] Thethi, N. and Keane, A., 2014, February. Digital forensics investigations in the cloud. In Advance Computing Conference (IACC), 2014 IEEE International (pp. 1475-1480). IEEE.
- [40] Zargari, S. and Benford, D., 2012, September. Cloud forensics: Concepts, issues, and challenges. In Emerging Intelligent Data and Web Technologies (EIDWT), 2012 Third International Conference on (pp. 236-243). IEEE.
- [41] Zawoad, S. and Hasan, R., 2013. Digital forensics in the cloud. ALABAMA UNIV IN BIRMINGHAM.
- [42] Zawoad, S. and Hasan, R., 2012, December. I have the proof: Providing proofs of past data possession in cloud forensics. In Cyber Security (CyberSecurity), 2012 International Conference on (pp. 75-82). IEEE.