

# Informatyka kryminalistyczna w kontekście usług przechowywania danych w chmurze obliczeniowej

Paweł Olber<sup>1</sup>

<sup>1</sup> Wyższa Szkoła Policji w Szczytnie, p.olber@wspol.edu.pl

## Streszczenie

Rola i możliwości informatyki kryminalistycznej w środowisku chmury obliczeniowej nadal pozostają nierozwiązanym i niedostatecznie zbadanym obszarem badań naukowych. Rosnąca popularność usług przechowywania danych w chmurze sprawia, że zabezpieczanie dowodów zlokalizowanych w Internecie stanowi jedno z wyzwań informatyki kryminalistycznej. Istniejące bariery prawne w większości przypadków uniemożliwiają uzyskiwanie bezpośredniego dostępu do zasobów w chmurze w celu zabezpieczenia danych. W wielu sytuacjach wymagana jest pomoc zagranicznych organów ścigania i wymiaru sprawiedliwości. Uzasadnieniem podjęcia współpracy międzynarodowej mogą być ustalenia dokonywane w ramach kryminalistycznych badań informatycznych, które pozwalają na odtworzenie aktywności użytkownika w zakresie korzystania z usług przechowywania danych w chmurze obliczeniowej. Istotna jest więc znajomość potencjalnych źródeł informacji, umożliwiających odtworzenie aktywności użytkownika usług chmur obliczeniowych, a także świadomość aktualnego stanu wiedzy i badań naukowych w tym zakresie.

**Słowa kluczowe:** chmura obliczeniowa, dysk wirtualny, informatyka kryminalistyczna, badania informatyczne

## Wstęp

Technologia chmury obliczeniowej umożliwia uzyskiwanie nieograniczonego dostępu do zasobów obliczeniowych, takich jak serwery i pamięci masowe, które dostarczane są przy minimalnej interakcji z dostawcą usług. Niewątpliwie jedną z głównych zalet rozwiązań oferowanych w chmurze jest łatwy i szybki dostęp do zasobów, do których można sięgnąć na żądanie z dowolnego miejsca na świecie (Mell, Grance, 2011).

Rosnąca popularność usług przechowywania danych w chmurze obliczeniowej oraz możliwość wykorzystania tych rozwiązań do celów przestępczych przyciągają uwagę naukowców i praktyków zajmujących się informatyką kryminalistyczną (Sharma, Arora, Sakthivel, 2018). Jednym z powodów takiego stanu rzeczy jest fakt, że cechy chmury obliczeniowej potęgują trudności związane z zabezpieczaniem i analizą dowodów cyfrowych (Samy i in., 2018). Szczegółowy przegląd istniejących wyzwań i problemów informatyki kryminalistycznej w zakresie pozyskiwania i analizy danych z chmur obliczeniowych został udokumentowany w raporcie amerykańskiej organizacji standaryzacyjnej NIST (Herman i in., 2014). Duża liczba otwartych wyzwań przedstawionych we wspomnianym dokumencie potwierdza, że rola i możliwości informatyki kryminalistycznej w środowisku chmury obliczeniowej pozostają nadal nierozwiązanym i niedostatecznie zbadanym obszarem badań naukowych (Martini, Choo, 2014). W celu zniwelowania istniejących problemów część naukowców zwraca uwagę na artefakty pozostałe w pamięci zabezpieczanych do badań cyfrowych

nośników danych, które mogą mieć istotne znaczenie w kontekście zasobów przechowywanych w środowisku chmury obliczeniowej.

Celem artykułu jest przedstawienie i podsumowanie aktualnego stanu wiedzy na temat śladów aktywności użytkowników usług przechowywania danych w chmurze, zapisywanych w pamięci cyfrowych nośników danych.

Biorąc pod uwagę cel artykułu, zdefiniowano następujące pytanie badawcze: jakiego rodzaju ślady aktywności użytkownika usług przechowywania danych w chmurze obliczeniowej zapisywane są w pamięci cyfrowych nośników danych?

W związku z postawionym pytaniem badawczym przyjęto hipotezę, według której informacje na temat aktywności użytkownika usług zdalnego przechowywania danych w chmurze internetowej zapisywane są w pamięci cyfrowych nośników danych. Informacje te mogą pomóc w ustaleniu zawartości zasobów znajdujących się w środowisku chmury obliczeniowej.

Przyjęta hipoteza badawcza zdeterminowała strukturę publikacji. W odrębnych częściach artykułu przedstawiono wyniki dotychczasowych badań naukowych dotyczących informatyki kryminalistycznej oraz usług przechowywania danych w chmurze. Następnie szczegółowo opisano istniejące możliwości identyfikacji śladów aktywności użytkownika aplikacji Dropbox i Google Drive.

Badania przeprowadzono metodą monograficzną z wykorzystaniem metody krytycznej analizy literatury. Posłużono się również metodą empiryczną, zastosowaną do weryfikacji opublikowanych badań dotyczących

usług Dropbox i Google Drive. Wnioski przedstawiono w zakończeniu.

### Przegląd literatury

Usługi przetwarzania danych w chmurze w kontekście kryminalistycznych badań informatycznych są przedmiotem wielu badań naukowych. Niewielu jednak naukowców zajęło się badaniami dotyczącymi możliwości ujawniania w pamięci urządzeń lokalnych śladów aktywności użytkowników usług przechowywania danych w chmurze.

Dehghantanha i Dargahi (2017) podjęli się analiz związanych z dwiema usługami: CloudMe oraz Qihoo 360 Yunpan. CloudMe to europejska usługa chmurowa powstała w 2012 roku, której właścicielem jest firma CloudMe AB. Oferuje ona bezpieczne przechowywanie danych w chmurze, synchronizację plików oraz oprogramowanie klienckie do zdalnego zarządzania danymi. Z kolei Qihoo 360 Yunpan to chińska usługa przechowywania danych w chmurze, którą wyróżnia największy bezpłatny dysk online na świecie. W przeprowadzonych badaniach autorzy wykorzystali różne systemy operacyjne: Windows 8.1, Android KitKat 4.4.2 oraz Apple iOS 8.0. W ich wyniku stwierdzili, że analiza zawartości dysku, pamięci RAM, pamięci wewnętrznej urządzeń mobilnych oraz zabezpieczonego ruchu sieciowego pozwala na odczytanie danych uwierzytelniających, nazw urządzeń oraz nazw plików przechowywanych na dyskach wirtualnych. Badania te dowodzą, że korzystanie z usług chmurowych pozostawia wiele śladów w pamięci cyfrowych nośników danych. Wynika z nich także, że ślady powstały w wyniku wykonywania różnych operacji na plikach zlokalizowanych w chmurze, ale również podczas instalacji/deinstalacji aplikacji klienckiej. Badacze zwrócili również uwagę na kwestię szyfrowania danych w każdej ze wspomnianych usług. Stwierdzili, że w przypadku usługi Qihoo 360 Yunpan bezpieczeństwo danych podczas transferu jest bardzo niskie. Autorzy łatwo zgromadzili i przeanalizowali dane dotyczące ruchu sieciowego w celu zebrania wymaganych dowodów. Usługa CloudMe znacznie lepiej chroni prywatność użytkowników. Deinstalacja aplikacji klienckiej CloudMe, choć pozostawiła pliki konfiguracyjne, to nie zmieniła kluczy rejestru i wykorzystuje szyfrowanie danych podczas transferu.

Mohtasebi i in. (2017) przeprowadzili badania związane z trzema kolejnymi usługami: SpiderOak, JustCloud i pCloud. Naukowcy zlokalizowali i opisali różne artefakty kryminalistyczne łączące się z wykorzystaniem wspomnianych usług za pośrednictwem trzech przeglądarek internetowych: Internet Explorer, Mozilla Firefox oraz Google Chrome, a także aplikacji klienckiej zainstalowanej w systemie Windows 8.1 oraz w urządzeniu iPhone 5S z systemem iOS 8.1.1. Dane ujawnione i odzyskane w trakcie badań zawierały adresy e-mail, identyfikator i nazwę utworzonego konta oraz nazwy przesyłanych i pobieranych plików.

Teing, Dehghantanha i Choo (2018) zbadali możliwości ujawnienia śladów aktywności użytkownika dysku internetowego CloudMe. Analizy autorów obejmowały różne systemy operacyjne: Windows 8.1 Professional, Linux (dystrybucja Ubuntu 14.04.1 LTS), Apple Mac OS X Mavericks 10.9.5, a także urządzenia mobilne: iPhone 4 z systemem iOS 7.1.2 oraz telefon HTC One z systemem Android KitKat 4.4.4. Przedmiotowe badania uwzględniały instalację/deinstalację aplikacji klienckich CloudMe, a także wysyłanie, pobieranie, przeglądanie, usuwanie, synchronizację i udostępnianie zasobów. Wspomniani autorzy podkreślają, że w badaniach informatycznych dotyczących usługi CloudMe należy zwrócić uwagę na pliki bazodanowe: Cache.db, db.sdb oraz logi, pliki konfiguracyjne aplikacji, a także pamięć podręczną przeglądarki internetowej. Analiza historii przeglądania stron internetowych umożliwiła im bowiem zidentyfikowanie unikatowych adresów internetowych, które pomogły w ustaleniu czynności wykonywanych przez użytkownika usługi CloudMe, takich jak logowanie/wylogowanie, uzyskiwanie dostępu do plików/folderów i pobieranie danych. Pomimo że połączenie z usługą CloudMe za pośrednictwem przeglądarki internetowej było szyfrowane, badacze odzyskali zawartość katalogu głównego aplikacji z pamięci podręcznej przeglądarki. Katalog aplikacji obejmował pliki użytkownika, metadane oraz pliki opisu OpenSearch zawierające informacje o znacznikach czasowych i hasła do udostępnionych zasobów.

Istniejące możliwości ujawnienia śladów aktywności użytkowników usługi pCloud w pamięci ulotnej RAM opisali Ahmad i in. (2020), którzy zilustrowali istniejące możliwości identyfikacji śladów w systemie Windows 7 Ultimate. Naukowcy ocenili możliwość ujawnienia danych dotyczących interakcji użytkownika z dyskiem wirtualnym na podstawie różnych scenariuszy, obejmujących przesyłanie danych oraz otwieranie i przeglądanie ich zawartości. W przeprowadzonym badaniu analizie poddano zawartość pamięci ulotnej RAM, jak również pamięć podręczną przeglądarki internetowej Google Chrome. Wynika z niego, że w przypadku usługi pCloud istnieje możliwość odczytania wszystkich danych uwierzytelniających oraz wszystkich informacji o plikach przechowywanych na dysku wirtualnym. Przedmiotowe badania potwierdzają wyniki wcześniejszych eksperymentów (Dargahi, Dehghantanha, Conti, 2017), których autorzy skoncentrowali się na usłudze pCloud i zaprezentowali możliwości ujawnienia wielu śladów w systemach operacyjnych: Microsoft Windows, Android, iOS oraz Linux. Wykazali, że istnieje możliwość odczytania danych uwierzytelniających użytkowników usługi pCloud oraz informacji o plikach przechowywanych na dysku.

Z powyższego przeglądu literatury wynika, że analiza zawartości cyfrowych nośników danych umożliwia (z zasady) ujawnienie informacji wskazujących na korzystanie przez użytkownika urządzenia/systemu z usług przechowywania danych w chmurze

obliczeniowej oraz dodatkowych informacji, w tym wartości wirtualnych zasobów, danych identyfikujących użytkownika oraz danych uwierzytelniających. Przeprowadzone badania koncentrują się na wielu różnych usługach, takich jak: CloudMe, Qihoo 360 Yunpan, SpiderOak, JustCloud, pCloud, które nie wyczerpują katalogu istniejących rozwiązań w zakresie zdalnego przechowywania danych. Zbiór ten można rozszerzyć chociażby o dwie popularne usługi: Dropbox i Google Drive, które były przedmiotem badań Horsmana (2020). Z uwagi na dużą popularność powyższych usług oraz aktualność wspomnianych badań ich wyniki zostaną przedstawione i zweryfikowane w dalszej części artykułu.

### Metodologia badań

W celu dokonania wstępnej oceny możliwości ujawnienia śladów aktywności użytkownika usług Dropbox i Google Drive przeprowadzono analizę wyników wspomnianych badań. W eksperymentach Horsmana (2020) wykorzystano system operacyjny Microsoft Windows 10 oraz przeglądarkę internetową Google Chrome (wersja 67.0.3396.99). Pamięć podręczna przeglądarki internetowej została odczytana za pomocą programu ChromeCacheView v1.77 firmy Nirsoft. W trakcie powtarzania procedury badawczej Horsmana (2020) posłużono się nowszą wersją przeglądarki internetowej Google Chrome (wersja 89.0.4389.90) oraz aktualnymi programami firmy Nirsoft: ChromeCacheView v2.25, ChromeHistoryView v1.42.

### Usługa Dropbox

Z badań przeprowadzonych przez Horsmana (2020) wynika, że w przypadku korzystania z usługi Dropbox za pośrednictwem przeglądarki internetowej Google Chrome w pamięci podręcznej przeglądarki zapisywany jest plik o nazwie `www.dropbox.com.html`. Plik ten nie otwiera się w oknie przeglądarki internetowej. Wymagane jest przeprowadzenie analizy kodu źródłowego. Czynność ta pozwala na odczytanie podstawowych informacji o użytkowniku usługi oraz identyfikację zawartości dysku wirtualnego. Informacje zapisane w pliku `www.dropbox.com.html` zawierają następujące dane:

- nazwę konta użytkownika (znacznik „display\_name”);
- identyfikator konta (znacznik: „id”);
- adres e-mail użytkownika (znacznik „email”);
- adres URL zdjęcia profilowego użytkownika (znacznik: „photo\_circle\_url”).

Fragment kodu zapisanego w pliku `www.dropbox.com.html` przedstawia rycina 1.

### Główne okno programu

Plik `www.dropbox.com.html` zawiera dodatkowe zapisy wskazujące na aktywność użytkownika na stronie głównej usługi Dropbox. Domyślnie na stronie głównej dysku znajduje się lista ostatnich działań podjętych przez użytkownika. Każdy wpis na liście ostatnich aktywności znajduje odzwierciedlenie w strukturze pliku `www.dropbox.com.html`. Lista ostatnich aktywności

```

\{"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"}
"user_root_permissions":
"edit", "has_never_set_password": false,
"id": 77837232, "sso_required": false,
"display_name": "Grey Joy",
"authed": 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:AAAAz7mAv7FTO-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%3A%ACJ- rJyCoDzFXXbB8MDaBqtS/
"DEFAULT_ROOT_NAME": "Dropbox",
"PERSONAL_ROLE_STRING": "Personal"}
}

```

Ryc. 1. Fragment kodu pliku `www.dropbox.com.html`.

zapisywana jest w znacznikach: „recent\_activities”:. Znaczniki zawierają czas interakcji (np. otwieranie folderu/pliku), który jest zapisany w formacie UNIX. Jeżeli użytkownik rozwinię ostatnie zdarzenie, które zawiera jeden lub więcej plików (zazwyczaj graficznych), to dla każdego pliku wyświetla się podgląd obrazu. Skutkuje to zapisywaniem w pamięci przeglądarki internetowej plików, których nazwy są bardzo charakterystyczne, na przykład: size=100x100size\_mode=4.jfif. W razie ujawnienia w pamięci podręcznej przeglądarki internetowej plików o podobnych nazwach należy utożsamiać je z powyższą formą aktywności na dysku Dropbox.

### Podgląd zawartości dysku

W przypadku kiedy użytkownik usługi Dropbox wyświetla wszystkie pliki zapisane na dysku, w historii przeglądarki internetowej zapisywany jest adres URL: <https://www.dropbox.com/home>. W pliku [www.dropbox.com/html](https://www.dropbox.com/html) zapisywane są natomiast dodatkowe informacje. W celu ustalenia całej zawartości dysku wirtualnego użytkownika należy odczytać informacje opatrzone znacznikami „event\_type”:

### Podgląd zawartości pliku

Z badań Horsmana (2020) wynika, że w przypadku wyświetlenia zawartości pliku graficznego na dysku wirtualnym jest on buforowany przez przeglądarkę internetową i zapisywany w pamięci podręcznej, podobnie jak po wyświetleniu podglądu pliku w oknie głównym. Nazwa pliku jest bardzo charakterystyczna, ponieważ zawiera informacje o jego rozmiarze:

size=32x32size\_mode=5.jfif. Oryginalna nazwa pliku jest natomiast zapisywana w adresie URL i można ją odczytać z historii przeglądarki internetowej: [www.dropbox.com/home?preview=FILENAME.png](https://www.dropbox.com/home?preview=FILENAME.png). Dodatkowe informacje dotyczące przeglądanych plików graficznych są zapisywane w pliku tekstowym o nazwie: `is_xhr=trueactivity_context=3activity_context_data=%2FFILENAME.txt`.

### Komentarze użytkowników

Użytkownik usługi Dropbox ma możliwość dodawania komentarzy do plików znajdujących się na dysku. Komentarze mogą być również dodawane przez innych użytkowników, którzy posiadają dostęp do określonego zasobu. Wstawienie komentarza skutkuje zapisaniem dodatkowych informacji, opatrzonych znacznikiem „comment”: w pliku tekstowym `is_xhr=trueactivity_context=3activity_context_data=%2FFILENAME.txt`. Jeżeli osoba trzecia odpowie na zamieszczony komentarz, wówczas nazwa konta tej osoby zostanie zapisana w znacznikach: `display_name`, `lname` oraz `fname`. W metadanych brak jest natomiast adresu e-mail oraz identyfikatora konta osoby odpowiadającej na komentarz, w związku z czym identyfikacja rzeczywistego konta osoby trzeciej wydaje się niemożliwa.

### Udostępnianie i usuwanie plików

Przejście użytkownika usługi do zakładki zawierającej zasoby udostępnione innym użytkownikom znajduje odzwierciedlenie w historii przeglądania stron internetowych: <https://www.dropbox.com/share>. Wyświetlenie

Filename	URL	Content Type	File Size	Last Accessed
scooter-scoped-vf15wRSGI.css	https://cfl.dropboxstatic.com/static/css/scooter/scooter-scop...	text/css	5 821	21.03.2021 20:30:13
index-vf1jdVZpP.css	https://cfl.dropboxstatic.com/static/css/dropbox/2015/pages...	text/css	2 422	21.03.2021 20:28:35
recaptcha_v2_challenge-vf15GXpO2.css	https://cfl.dropboxstatic.com/static/css/recaptcha_v2_challen...	text/css	285	21.03.2021 20:28:35
web_sprites-vf1cKH0r6.css	https://cfl.dropboxstatic.com/static/css/sprites/web_sprites-v...	text/css	8 499	21.03.2021 20:28:35
font_sharp_grotesk-vf1e4E4q.css	https://cfl.dropboxstatic.com/static/css/font_sharp_grotesk-v...	text/css	783	21.03.2021 20:28:35
recaptcha_challenge-vf1rcf67y.css	https://cfl.dropboxstatic.com/static/css/recaptcha_challenge-...	text/css	401	21.03.2021 20:28:35
login_or_register-vf1AJk0Kd.css	https://cfl.dropboxstatic.com/static/css/components/login_o...	text/css	194	21.03.2021 20:28:35
login_or_register-vf1Z9y5P.css	https://cfl.dropboxstatic.com/static/css/login_or_register-vf1Z...	text/css	813	21.03.2021 20:28:35
recaptcha-vf1IN6j39.css	https://cfl.dropboxstatic.com/static/css/recaptcha-vf1IN6j39.css	text/css	189	21.03.2021 20:28:35
react_locale_selector-vf1uPHu5g.css	https://cfl.dropboxstatic.com/static/css/components/react_lo...	text/css	855	21.03.2021 20:28:35
prompt_pagelet-vf1wS3jof.css	https://cfl.dropboxstatic.com/static/css/upsell/prompt_pagel...	text/css	6 451	21.03.2021 20:30:13
index.web-vf16Z83yw.css	https://cfl.dropboxstatic.com/static/css/spectrum/index.web-...	text/css	8 582	21.03.2021 20:30:11
www.google.com.html	https://www.google.com	text/html	37 989	21.03.2021 20:28:27
analytics.js	https://www.google-analytics.com/analytics.js	text/javascript	18 980	21.03.2021 20:28:39
funcaptcha.js	https://dropboxcaptcha.com/funcaptcha.js	application/java...	1 292	21.03.2021 20:28:39
dropboxcaptcha.com.html	https://dropboxcaptcha.com	text/html	267	21.03.2021 20:28:39
up_loader.1.1.0.js	https://js.adsrvr.org/up_loader.1.1.0.js	application/x-ja...	4 593	21.03.2021 20:28:39
https%3A%2F%2Fwww.dropbox.com%2F.html	https://marketing.dropbox.com/login?referrer=https%3A%2F...	text/html	7 748	21.03.2021 20:28:38
mem5YaGs126MiZpBA-UNirkOXOhpOqc.woff2	https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZ...	font/woff2	11 724	21.03.2021 20:28:36
mem8YaGs126MiZpBA-UFW50bbck.woff2	https://fonts.gstatic.com/s/opensans/v18/mem8YaGs126MiZ...	font/woff2	11 316	21.03.2021 20:28:36
CircularXXWeb-Book-cd7d2bcec649b1243839a15d5eb...	https://cdn.loom.com/assets/fonts/circular/CircularXXWeb-B...	font/woff2	69 026	21.03.2021 20:30:12
3658811377-frame_bin.js	https://docs.google.com/static/offline/client/js/3658811377-fr...	text/javascript	275 912	21.03.2021 20:29:25
mem8YaGs126MiZpBA-UFW50bbck.woff2	https://fonts.gstatic.com/s/opensans/v18/mem8YaGs126MiZ...	font/woff2	14 380	21.03.2021 20:28:36
mem5YaGs126MiZpBA-UNirkOUuhp.woff2	https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZ...	font/woff2	14 880	21.03.2021 20:28:36
recaptcha_nli...	https://www.gstatic.com/recaptcha/releases/6nS17HMD0mlr...	text/javascript	124 272	21.03.2021 20:28:30

Ryc. 2. Okno programu ChromeCacheView z zawartością pamięci podręcznej przeglądarki.

URL	Title	Visited On	Visit Cou
https://docs.google.com/spreadsheets/d/1FKCh3scG7JNroEIALax3GtTL_tLlZenc/edit?usp=drive_web&ou...	Dane oszustwo z badań aktowych.xlsx - Arkusze Google	21.03.2021 23:02:48	3
https://docs.google.com/spreadsheets/d/1FKCh3scG7JNroEIALax3GtTL_tLlZenc/edit?usp=drive_web&ou...	Dane oszustwo z badań aktowych.xlsx - Arkusze Google	21.03.2021 23:02:52	3
https://docs.google.com/spreadsheets/d/1FKCh3scG7JNroEIALax3GtTL_tLlZenc/edit?usp=drive_web&ou...	Dane oszustwo z badań aktowych.xlsx - Arkusze Google	21.03.2021 23:02:55	3
https://drive.google.com/drive/folders/0BxtZ5Hn_ZKn3TjJ0Q2mM1ZNb3c	Poland – Dysk Google	21.03.2021 23:05:55	3
https://drive.google.com/drive/folders/0BxtZ5Hn_ZKn3TjJ0Q2mM1ZNb3c	Poland – Dysk Google	21.03.2021 23:06:02	3
https://drive.google.com/drive/folders/0BxtZ5Hn_ZKn3TjJ0Q2mM1ZNb3c	Poland – Dysk Google	21.03.2021 23:06:02	3
https://drive.google.com/drive/folders/1cVurcl8YlswBJ9TMBNalfbs14q5XDL2P	Stare – Dysk Google	21.03.2021 23:05:45	2
https://drive.google.com/drive/folders/1cVurcl8YlswBJ9TMBNalfbs14q5XDL2P	Stare – Dysk Google	21.03.2021 23:11:10	2
https://drive.google.com/drive/folders/1QhG-rhnU-gr3mk6csr0KevVVvUbNn_R9	Artykuł – Dysk Google	21.03.2021 22:59:01	1
https://drive.google.com/drive/folders/1uoxzvUIQ8HuJL453Evj_-cWqkiZnORo	PO – Dysk Google	21.03.2021 23:05:43	1
https://www.dropbox.com/h	Strona główna – Dropbox	21.03.2021 23:12:47	1
https://www.dropbox.com/h?role=personal	Strona główna – Dropbox	21.03.2021 23:12:17	2
https://www.dropbox.com/h?role=personal	Strona główna – Dropbox	21.03.2021 23:12:44	2
https://www.dropbox.com/home	Pliki – Dropbox	21.03.2021 23:13:39	1
https://www.dropbox.com/login?cont=https%3A%2F%2Fwww.dropbox.com%2Fh%3Frole%3Dpersonal	Logowanie - Dropbox	21.03.2021 23:12:17	1
https://www.dropbox.com/requests?_tk=web_left_nav_bar	Dropbox	21.03.2021 23:14:10	1
https://www.dropbox.com/requests?_tk=web_left_nav_bar&role=personal	Dropbox	21.03.2021 23:14:09	1
https://www.dropbox.com/share/recents	Udostępnione – Dropbox	21.03.2021 23:14:01	1
https://www.dropbox.com/share?_tk=web_left_nav_bar&role=personal	Dropbox	21.03.2021 23:14:00	1

Ryc. 3. Historia przeglądania stron internetowych.

Filename	URL	Content Type	File Size	Last Accessed	Server Time	Se
profile_card_popover.min-vf11CjbsD.js	https://cfl.dropboxstatic.com/static/js/modules/clean/react/pass/integration/pr...	application/java...	822	21.03.2021 23:15:51	21.03.2021 23:15:51	23
util.min-vf1nOmK2N.js	https://cfl.dropboxstatic.com/static/js/modules/clean/react/comments2/comp...	application/java...	371	21.03.2021 23:15:51	21.03.2021 23:15:51	12
tooltips.min-vf1HmK-H2.js	https://cfl.dropboxstatic.com/static/js/modules/clean/react/comments2/comp...	application/java...	640	21.03.2021 23:15:51	21.03.2021 23:15:51	23
coachmark.min-vf1EmKaTc.js	https://cfl.dropboxstatic.com/static/js/modules/clean/react/comments2/comp...	application/java...	422	21.03.2021 23:15:51	21.03.2021 23:15:51	25
sidebar_listener.min-vf1eGKHp6.js	https://cfl.dropboxstatic.com/static/js/modules/clean/react/comments2/comp...	application/java...	534	21.03.2021 23:15:51	21.03.2021 23:15:51	06
guest_utils.min-vf1d0ESx.js	https://cfl.dropboxstatic.com/static/js/comments2/components/utills/guest_util...	application/java...	205	21.03.2021 23:15:51	21.03.2021 23:15:51	23
fv_content=true&size_mode=5.jfif	https://previews.dropbox.com/p/thumb/ABFD8Kbn5W6mQ8NR-ujn9T6QPkrHl...	image/jpeg	188-434	21.03.2021 23:15:51	21.03.2021 23:15:51	
index.min-vf1GeWPKA.js	https://cfl.dropboxstatic.com/static/js/modules/clean/react/comments2/action...	application/java...	541	21.03.2021 23:15:51	21.03.2021 23:15:51	25
index.min-vf1NDYkLA.js	https://cfl.dropboxstatic.com/static/js/modules/clean/react/comments2/component/ind...	application/java...	216	21.03.2021 23:15:51	21.03.2021 23:15:51	06
index.min-vf1nu1Bf.js	https://cfl.dropboxstatic.com/static/js/comments2/components/comment_stre...	application/java...	171	21.03.2021 23:15:51	21.03.2021 23:15:51	22
comment_stream_error.min-vf1CqyCZj.js	https://cfl.dropboxstatic.com/static/js/comments2/components/comment_stre...	application/java...	522	21.03.2021 23:15:51	21.03.2021 23:15:51	23
index.min-vf1vmj8h.js	https://cfl.dropboxstatic.com/static/js/comments2/components/coachmark_lo...	application/java...	308	21.03.2021 23:15:51	21.03.2021 23:15:51	23
import_contacts_link.min-vf1A24AGh.js	https://cfl.dropboxstatic.com/static/js/modules/clean/teams/admin/widgets/in...	application/java...	1 180	21.03.2021 23:15:51	21.03.2021 23:15:51	07
index.min-vf1kGIAH.js	https://cfl.dropboxstatic.com/static/js/comments2/components/comment_edit...	application/java...	263	21.03.2021 23:15:51	21.03.2021 23:15:51	06
import_contacts_modal.min-vf1yvikl.js	https://cfl.dropboxstatic.com/static/js/modules/clean/teams/admin/widgets/...	application/java...	2 684	21.03.2021 23:15:51	21.03.2021 23:15:51	08

Ryc. 4. Wskazanie pliku fv\_content=true&amp;size\_mode=5.jfif.

listy zasobów udostępnianych nie skutkuje zapisaniem dodatkowych informacji w pamięci podręcznej przeglądarki internetowej. Podobnie jest w przypadku plików usuniętych. Usługa Dropbox przechowuje usunięte pliki przez 30 dni, a użytkownik może je przywracać i przeglądać. W pamięci podręcznej przeglądarki internetowej nie będzie jednak jakichkolwiek rekordów, które można przypisać do czynności usunięcia danych.

### Wyniki badań własnych

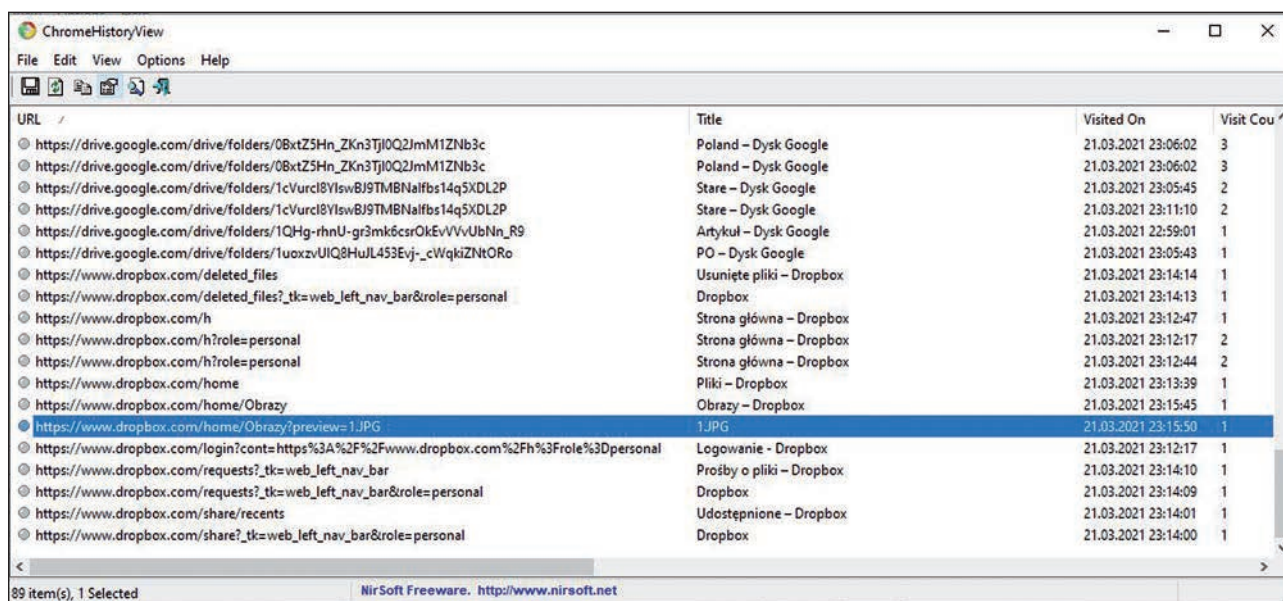
W wyniku powtórzenia procedury badawczej Horsmana (2020) uzyskano odmienne wyniki. Stwierdzono mianowicie, że wyświetlenie zawartości dysku wirtualnego Dropbox powoduje zapisanie w pamięci podręcznej przeglądarki internetowej Google Chrome pliku o nazwie: <https://www.dropbox.com/>.html, którego nazwa jest zakodowana. Plik ten wskazano na rycinie 2.

Ustalono, że plik <https://www.dropbox.com/>.html nie zawiera żadnych danych identyfikujących użytkownika usługi Dropbox. W przeprowadzonym badaniu

potwierdzono, że aktywność użytkownika usługi znajduje odzwierciedlenie w historii przeglądania stron internetowych. W przypadku wyświetlenia przez użytkownika usługi Dropbox całej zawartości dysku w historii przeglądarki internetowej (zgodnie z ustawieniami Horsmana) zapisywany jest adres URL: <https://www.dropbox.com/home>. Podobnie w historii przeglądarki internetowej zapisywane są adresy internetowe wskazujące na inne aktywności użytkownika, takie jak na przykład: wyświetlanie zasobów udostępnionych, otwieranie listy próśb o pliki oraz otwieranie listy plików usuniętych.

Przeprowadzone badanie potwierdziło, że wyświetlenie w usłudze Dropbox zawartości pliku graficznego skutkuje zapisaniem go w pamięci podręcznej przeglądarki internetowej w formacie JFIF. W omawianym przykładzie plik graficzny został zapisany pod nazwą: `fv_content=true&size_mode=5.jfif`.

Oryginalna nazwa pliku została zapisana w adresie URL i można ją odczytać z historii przeglądania stron



Ryc. 5. Wskazanie pliku 1.JPG.

internetowych. W omawianym przykładzie jest to plik o nazwie 1.JPG.

Przeprowadzone badanie nie potwierdziło ustaleń Horsmana (2020), według których podgląd zawartości pliku graficznego oraz dodanie komentarza w usłudze Dropbox powoduje zapisanie dodatkowych informacji w plikach tekstowych.

### Usługa Google Drive

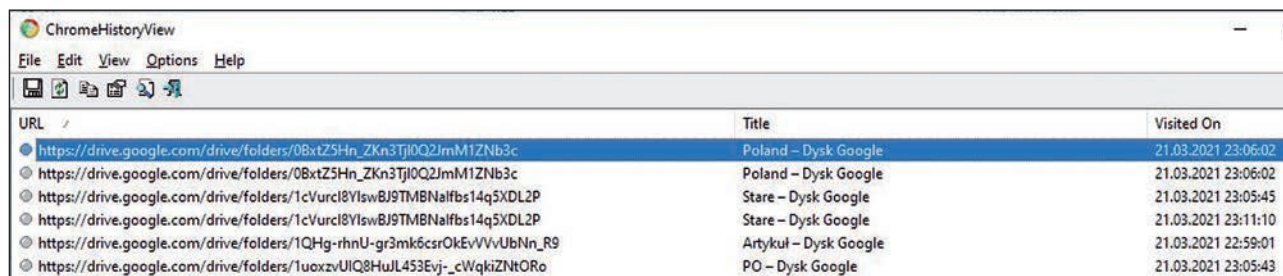
W pamięci podręcznej przeglądarki internetowej Google Chrome znajdują się ograniczone informacje dotyczące interakcji użytkownika z usługą Google Drive. Z badań przeprowadzonych przez Horsmana (2020) wynika, że pamięć podręczna przeglądarki internetowej Google Chrome nie zawiera plików identyfikujących użytkownika lub opisujących zawartość dysku wirtualnego Google Drive. Oznacza to, że informacje dotyczące usługi Google Drive nie są buforowane, odmiennie niż w przypadku usługi Dropbox. W pamięci przeglądarki internetowej zapisywane są jedynie pliki graficzne, przeglądane z poziomu dysku Google Drive. Przeglądane pliki zapisywane są pod charakterystyczną nazwą, na przykład: W1366-H662. Właściwość ta nie dotyczy dokumentów tekstowych,

arkuszy kalkulacyjnych oraz prezentacji multimedialnych przeglądanych z poziomu dysku.

Zdaniem Horsmana (2020) adresy internetowe zapisane w historii przeglądania stron internetowych, powiązane z aktywnością użytkownika, zawierają ograniczone informacje. Przykładowo podgląd zawartości pliku graficznego na dysku wirtualnym nie zmienia adresu URL: <https://drive.google.com/drive/my-drive>. Z kolei wyświetlenie zawartości konkretnego folderu zmienia adres internetowy w sposób, który nie pozwala na ustalenie nazwy zasobu: <https://drive.google.com/drive/folders/0By-CihkhmywOek1Gak4ySilhnQkk>.

### Wyniki badań własnych

W wyniku przeprowadzonych badań stwierdzono, że wnioski Horsmana (2020) dotyczące usługi Google Drive wymagają uzupełnienia w zakresie możliwości identyfikacji nazw folderów zapisanych na dysku wirtualnym. Każdorazowe wyświetlenie zawartości folderu powoduje zmianę adresu URL, który nie pozwala na ustalenie nazwy zasobu. Jednakże wyświetlenie historii przeglądania stron internetowych za pośrednictwem aplikacji ChromeHistoryView v1.42 umożliwia ustalenie nazw folderów na dysku Google Drive, które były otwierane przez



Ryc. 6. Nazwy folderów dysku wirtualnego w tytułach stron internetowych.

Filename	URL	Content Type	File Size	Last Accessed
2524158713-waffle_js_prod_conditionalformat_pljs	https://docs.google.com/static/spreadsheets2/client/js/2524158713-waffle_js_pr...	text/javascript	12 764	21.03.2021 23:06:06
w1280-h881-ft_jfif	https://lh3.googleusercontent.com/ffe/ABSRIpbj8h-m3l_f0tZesdGjsEBLTYfgoT...	image/jpeg	160 627	21.03.2021 23:06:02
d-logo-blue-bkg%254032h.png	https://lh3.googleusercontent.com/-Vj8PcttrOE/XfoJf-rJ7m/AAAAAAAAAV9Q/q...	image/png	871	21.03.2021 23:06:02
docId=0BxtZ5Hn_ZKn3QmNiN0ZEak9XclE&revisionId&u...	https://blobcomments-pa.clients5.google.com/v1/metadata?docId=0BxtZ5Hn_...	application/json	671	21.03.2021 23:06:01
416349405-docos_binary_i18n_pljs	https://docs.google.com/static/comments/client/js/416349405-docos_binary_i1...	text/javascript	383 971	21.03.2021 23:06:01
w1280-h881-iv2.html	https://lh3.googleusercontent.com/0/d/0BxtZ5Hn_ZKn3QmNiN0ZEak9XclE=w1280-h881-...	text/html	0	21.03.2021 23:06:01
docId=0BxtZ5Hn_ZKn3M0trRfHWMjhlbkE&revisionId&u...	https://blobcomments-pa.clients5.google.com/v1/metadata?docId=0BxtZ5Hn_...	application/json	670	21.03.2021 23:06:01
HT8XDe	https://drive.google.com/_drive_fe/_js/k=drive_fe.main.pl.8ziDbkY0pCY.O/am...	text/javascript	279	21.03.2021 23:06:01
sywc,aW3pY,syyz,sy114,sy10n,syzy,sy11b,sy115,syw7,sy10...	https://drive.google.com/_drive_fe/_js/k=drive_fe.main.pl.8ziDbkY0pCY.O/am...	text/javascript	7 150	21.03.2021 23:06:01
sywg,sywh,sy2z,syz3,syz4,sy10j,sy12m,sy12j,sy12n,sy12o,t...	https://drive.google.com/_drive_fe/_js/k=drive_fe.main.pl.8ziDbkY0pCY.O/am...	text/javascript	1 469	21.03.2021 23:06:00
v-sprite35.svg	https://ssl.gstatic.com/docs/common/viewer/v3/v-sprite35.svg	image/svg+xml	10 011	21.03.2021 23:06:00

Ryc. 7. Plik graficzny w1280-h881-ft.jfif zapisany w pamięci podręcznej przeglądarki.

URL	Title	Visited On	Visit Co
https://docs.google.com/spreadsheets/d/1FkCh3scG7JNroEIALax3GtTL_tLLzenc/...	Dane oszustwo z badań aktowych.xlsx - Arkusze Google	21.03.2021 23:02:57	1
https://docs.google.com/spreadsheets/d/1FkCh3scG7JNroEIALax3GtTL_tLLzenc/...	Dane oszustwo z badań aktowych.xlsx - Arkusze Google	21.03.2021 23:02:55	1
https://docs.google.com/spreadsheets/d/1FkCh3scG7JNroEIALax3GtTL_tLLzenc/...	Dane oszustwo z badań aktowych.xlsx - Arkusze Google	21.03.2021 23:02:56	1
https://docs.google.com/spreadsheets/d/1FkCh3scG7JNroEIALax3GtTL_tLLzenc/...	Dane oszustwo z badań aktowych.xlsx - Arkusze Google	21.03.2021 23:02:48	3
https://docs.google.com/spreadsheets/d/1FkCh3scG7JNroEIALax3GtTL_tLLzenc/...	Dane oszustwo z badań aktowych.xlsx - Arkusze Google	21.03.2021 23:02:52	3
https://docs.google.com/spreadsheets/d/1FkCh3scG7JNroEIALax3GtTL_tLLzenc/...	Dane oszustwo z badań aktowych.xlsx - Arkusze Google	21.03.2021 23:02:55	3
https://drive.google.com/drive/folders/1QHg-rhnU-gr3mk6csrOkEvVVvUbNn_R9	Artykuł - Dysk Google	21.03.2021 22:59:01	1

Ryc. 8. Nazwy plików otwieranych przez użytkownika usługi Google Drive.

użytkownika. Nazwy folderów zawarte są w tytułach stron internetowych, co zostało ukazane na rycinie 6.

Przeprowadzone badania potwierdziły, że podgląd zawartości pliku graficznego na dysku Google Drive powoduje, iż jest on buforowany i zapisywany w pamięci podręcznej przeglądarki internetowej Google Chrome. Na rycinie 7 zaznaczono plik graficzny w1280-h881-ft.jfif, którego zawartość została wyświetlona na dysku.

Wyświetlenie zawartości dokumentów tekstowych, arkuszy kalkulacyjnych oraz prezentacji multimedialnych zapisanych na dysku wirtualnym Google Drive nie skutkuje zapisaniem dodatkowych informacji w pamięci podręcznej przeglądarki. Istnieje jednak możliwość ustalenia nazw plików otwieranych przez użytkownika. Informacje takie dostępne są w oknie programu ChromeHistoryView, co zostało pokazane na rycinie 8.

## Wyniki i dyskusja

Z przeprowadzonej analizy opublikowanych badań oraz powtórzonej procedury badawczej wynika, że interakcje użytkownika z usługami Dropbox i Google Drive skutkują zapisywaniem informacji w pamięci urządzeń lokalnych. Najwięcej informacji zapisywanych jest podczas korzystania z usługi Dropbox. W tym jednak przypadku badania własne zakończyły się uzyskaniem wyników odmiennych od rezultatów Horsmana (2020). Różnice te wynikają najprawdopodobniej

z wykorzystania różnych wersji przeglądarki internetowej Google Chrome oraz bezpłatnych programów: ChromeHistoryView v1.42 i ChromeCacheView v2.25. Należy również wskazać na istniejącą możliwość ustalenia zawartości dysku Google Drive na podstawie tytułów stron internetowych, wyświetlanych za pośrednictwem wymienionych powyżej aplikacji, co nie zostało opisane w badaniu Horsmana (2020).

## Podsumowanie

Przypuszczać można, że popularność usług przechowywania danych w chmurze obliczeniowej będzie stale rosła, co wynika z wielu zalet tych rozwiązań. Zwiększa się więc prawdopodobieństwo, że wiele danych istotnych z punktu widzenia prowadzonych postępowań karnych będzie zlokalizowanych w chmurze, w tym na dyskach wirtualnych. Istniejące bariery prawne w większości przypadków uniemożliwiają jednak uzyskiwanie bezpośredniego dostępu do tego rodzaju zasobów. W tych sytuacjach niezbędne jest korzystanie z pomocy zagranicznych organów ścigania i wymiaru sprawiedliwości. Uzasadnieniem wniosków kierowanych do podmiotów zagranicznych mogą być ustalenia biegłych z zakresu badań informatycznych. Analizy biegłych mogą potwierdzać fakt korzystania z usług przechowywania danych w chmurze, jak również pomóc w ustaleniu danych uwierzytelniających

oraz zawartości zasobów, co może być istotne w prowadzonym postępowaniu karnym.

Pomimo że prezentowana publikacja ma charakter głównie poglądowy, zawiera opis i wyniki badań własnych, potwierdzających przyjętą hipotezę. Badania własne zostały zrealizowane za pomocą aktualnych wersji aplikacji, co tłumaczy różnice w uzyskanych wynikach. Przykład ten potwierdza również, że każde badanie informatyczne ma charakter indywidualny.

W przyszłych badaniach naukowych, dotyczących problematyki ujawniania śladów aktywności użytkownika usług chmur obliczeniowej, należy dążyć do korzystania z bardziej zaawansowanych programów, stosowanych w kryminalistycznych badaniach informatycznych, takich jak na przykład: X-Ways Forensics, NetAnalysis oraz HstEx.

### Źródło rycin:

**Ryc. 1:** opracowanie własne na podstawie: Horsman, 2020

**Ryc. 2–8:** autor

### Bibliografia

- Ahmad, N.H., Hamid, A.S.S.A., Shahidan, N.S.S., Ariffin, K.A.Z. (2020). Cloud forensic analysis on pCloud: From volatile memory perspectives. W: M.H. Miraz, P. Excell, A. Ware, S. Soomro, M. Ali (red.), *Emerging Technologies in Computing, Third EAI International Conference, iCETiC 2020*. Cham: Springer.
- Dargahi, T., Dehghantanha, A., Conti, M. (2017). Investigating storage as a service cloud platform: pCloud as a case study. W: A. Dehghantanha, K.-K.R. Choo (red.), *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*. Amsterdam–Boston i in.: Elsevier, <https://doi.org/10.1016/B978-0-12-805303-4.00012-5>.
- Dehghantanha, A., Dargahi, T. (2017). Residual cloud forensics. W: A. Dehghantanha, K.-K.R. Choo (red.), *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*. Amsterdam–Boston i in.: Elsevier, <https://doi.org/10.1016/B978-0-12-805303-4.00014-9>.
- Herman, M., Iorga, M., Salim, A.M., Jackson, R.H., Hurst, M.R., Leo, R., ... Sardinias, R. (2014). *NIST Cloud Computing Forensic Science Challenges*. Gaithersburg: National Institute of Standards and Technology.
- Horsman, G. (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*, 15(1).
- Martini, B., Choo, K.-K.R. (2014). Cloud forensic technical challenges and solutions: A snapshot. *IEEE Cloud Computing*, 1(4), <https://doi.org/10.1109/MCC.2014.69>.
- Mell, P.M., Grance, T. (2011). *The NIST Definition of Cloud Computing*. Gaithersburg: National Institute of Standards and Technology.
- Mohtasebi, S.H., Dehghantanha, A., Choo, K.-K.R. (2017). Cloud storage forensics. W: A. Dehghantanha, K.-K.R. Choo (red.), *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications* (s. 205–246). Amsterdam–Boston i in.: Elsevier, <https://doi.org/10.1016/B978-0-12-805303-4.00013-7>.
- Samy, G.N., Shanmugam, B., Maarop, N., Magalingam, P., Perumal, S., Albakri, S.H. (2018). Digital forensic challenges in the cloud computing environment. W: F. Saeed, N. Gazem, S. Patnaik, A.S. Saed Balaid, F. Mohammed (red.), *Recent Trends in Information and Communication Technology*. Cham: Springer, [https://doi.org/10.1007/978-3-319-59427-9\\_69](https://doi.org/10.1007/978-3-319-59427-9_69).
- Sharma, P., Arora, D., Sakthivel, T. (2018). Mobile cloud forensic: Legal implications and counter measures. W: S.C. Satapathy, A. Joshi (red.), *International Conference on Information and Communication Technology for Intelligent Systems*. Cham: Springer, [https://doi.org/10.1007/978-3-319-63673-3\\_64](https://doi.org/10.1007/978-3-319-63673-3_64).
- Teing, Y.-Y., Dehghantanha, A., Choo, K.-K.R. (2018). CloudMe forensics: A case of big data forensic investigation. *Concurrency and Computation: Practice and Experience*, 30(5), <https://doi.org/10.1002/cpe.4277>.



# Digital forensics in the context of cloud computing data storage services

Paweł Olber<sup>1</sup>

<sup>1</sup> The Police Academy in Szczytno, p.olber@wspol.edu.pl

---

## Summary

The role and capabilities of digital forensics in the cloud computing environment still remain an unsolved and insufficiently explored scientific area. The growing popularity of cloud-based data storage services makes recovery of evidence on the Internet a major challenge for forensic IT examiners. Existing legal barriers in most cases prevent direct access to cloud stored resources for the purpose of recovering data. In many situations, assistance from foreign law enforcement and judicial authorities is required. Findings made during forensic IT analysis that allow reconstructing user's activities and indicate the act of taking advantage of cloud computing data storage is a justification for undertaking international cooperation. Therefore, it is important to know potential sources of information that enable the reconstruction of the activity of the user in cloud computing services, as well as the awareness of the current state of knowledge and scientific research in this field.

**Key words:** computing cloud, file hosting service, digital forensics, IT examinations

---

## Introduction

Cloud computing technology provides an unlimited access to computing resources such as servers and storage that are delivered with a minimal interaction with the service provider. Undoubtedly, one of the main advantages of cloud solutions is easy and quick access to resources that may be available on demand from anywhere in the world (Mell & Grance, 2011).

The growing popularity of cloud computing data storage services and the possibility of using these solutions for criminal purposes call for efforts on the part of scientists and practitioners in the field of forensic IT (Sharma, Arora, Sakthivel, 2018). One of the reasons for this situation is that cloud computing specifics exacerbate the difficulties in recovering and analysing digital evidence (Samy et al., 2018). A detailed review of the existing challenges and problems of digital forensics in the aspect of obtaining and examining data from cloud computing has been documented in the Report of the American National Institute of Standards and Technology: NIST (Herman et al., 2014). A large number of open challenges presented in the aforementioned document confirms that the role and possibilities of digital forensic in the cloud computing environment remain an unsolved and insufficiently explored area of scientific research (Martini, Choo, 2014). In order to overcome the persisting problems some scientists point to artifacts remaining in the memory of the data carriers recovered for the purpose of forensic examination as they may be important in the context of resources stored in the cloud computing environment.

The aim of the article is to present and summarise the current state of knowledge on the traces of cloud

storage services users activities remaining in the memory of digital data carriers.

In view of the purpose of the article, the following research question was defined: what kind of traces of user activity of cloud computing data storage services stay in the memory of digital data carriers?

In connection with the posed research question a hypothesis was adopted according to which information on the activity of a user of Internet cloud remote file hosting service are stored in the memory of digital data carriers. That information can help to determine the content of resources in the cloud computing environment.

The research hypothesis had determined the structure of this publication. The results of previous research on forensic computing and cloud storage services were presented in separate parts of the article. Then, the existing possibilities of identifying traces of user activity in Dropbox and Google Drive were described in detail.

The research was carried out using the monographic method with critical literature analysis. In addition to that an empirical method was also applied to verify published results of Dropbox and Google Drive services research. Finally, the conclusions were formulated.

## Literature review

Cloud computing services in the context of digital forensics are the subject of many scientific research undertakings. However, few scientists have studied the possibility of revealing traces of activity of users of cloud data storage services in the memory of local devices.

Dehghantanha and Dargahi (2017) endeavoured analyses of two services: CloudMe and Qihoo 360

Yunpan. CloudMe is a European file storage service established in 2012, owned by CloudMe AB. It offers secure cloud storage, file synchronization and remote data management client software. Qihoo 360 Yunpan, on the other hand, is a Chinese file storage service distinguished by the largest free online drive in the world. In the course of research, the authors used various operating systems: Windows 8.1, Android KitKat 4.4.2 and Apple iOS 8.0. As a result, they found that the analysis of the disk content, RAM memory, internal memory of mobile devices and secured network traffic allowed for the reading of authentication data, names of devices, as well as files stored on the on-line drives. These studies show that the use of cloud computing services leaves many traces in the memory of digital data carriers. They also demonstrate that the traces are formed as a result of performing various operations on files located in the cloud, but also during the installation / uninstallation of the client application. The researchers also highlighted the issue of data encryption in each of these services. They found that in the case of the Qihoo 360 Yunpan service, data security during the transfer was very low. The authors easily gathered and analysed network traffic data to recover required evidence. CloudMe protect users' privacy much better. Uninstalling the CloudMe client application, although it retained the configuration files, did not change the registry keys and uses data encryption during the transfer.

Mohtasebi et al. (2017) conducted studies of three more services: SpiderOak, JustCloud and pCloud. The researchers located and described various forensic artefacts connected to the use of these services by three web browsers: Internet Explorer, Mozilla Firefox and Google Chrome, as well as client applications installed on Windows 8.1 and an iPhone 5S with iOS 8.1.1. The data revealed and retrieved during the study included e-mail addresses, the ID and name of the created account, as well as the names of uploaded and downloaded files.

Teing, Dehghantanha, and Choo (2018) investigated the possibility of revealing traces of CloudMe online disk user activity. Their analyses covered various operating systems: Windows 8.1 Professional, Linux (Ubuntu 14.04.1 LTS distribution), Apple Mac OS X Mavericks 10.9.5, as well as mobile devices: iPhone 4 with iOS 7.1.2 and HTC One with Android KitKat 4.4.4. The research included the installation / uninstallation of CloudMe client applications, as well as uploading, downloading, browsing, deleting, synchronizing and sharing resources. Those authors emphasise that during examinations of the CloudMe service, attention should be paid to the database files: Cache.db, db.sdb and logs, application configuration files, as well as the web browser cache. The analysis of web browsing history allowed them to identify unique web addresses that helped to determine the activities performed by the CloudMe user, such as logging in / logging out, accessing files / folders and data downloading. Even though the connection

to CloudMe via the web browser was encrypted, the researchers recovered the contents of the application's root directory from the browser cache. The application directory included user files, metadata, and OpenSearch description files containing timestamp information and passwords for shared resources.

Ahmad et al. (2020) who illustrated the existing trace identification capabilities in Windows 7 Ultimate described the existing possibilities of revealing the traces of pCloud service users' activities in volatile RAM. The scientists verified the possibility of revealing information on user interaction with the online drive based on various scenarios including data transfer with opening and viewing of its contents. In the study, the content of the volatile RAM memory as well as the cache of the Google Chrome web browser were analysed. Consequently, in the case of the pCloud service, it was possible to read all credentials and all information about files stored on the file hosting service. The study in question confirms the results of the previous experiments (Dargahi, Dehghantanha, Conti, 2017), whose authors focused on the pCloud service and presented the possibility of detecting many traces in the following operating systems: Microsoft Windows, Android, iOS and Linux. They showed that it was possible to read the credentials of pCloud users and information about files stored on the disk.

According to the above literature review the analysis of the content of digital data carriers allows (in principle) the disclosure of information indicating the use of cloud computing data storage services by the user of the device / system and additional information, such as: the content of virtual resources, user identification data and credentials. The research projects focus on several different services, including: CloudMe, Qihoo 360 Yunpan, SpiderOak, JustCloud, pCloud, which do not exhaust the catalogue of existing remote data storage solutions. This list may be extended, for example, by two popular services: Dropbox and Google Drive, which were the subject of Horsman's research (2020). Due to the widespread popularity of these services and the timeliness of the study the results will be presented and verified later in the article.

### Methodology

In order to make a preliminary assessment of the possibility of detecting traces of the Dropbox and Google Drive users activities, an analysis of the results of the above-mentioned studies was carried out. Horsman's experiments (2020) used the Microsoft Windows 10 operating system and the Google Chrome web browser (version 67.0.3396.99). The web browser cache was read with Nirsoft's ChromeCacheView v1.77. In the course of repeating the examination procedure of Horsman (2020), a newer version of the Google Chrome web browser (version 89.0.4389.90) and current Nirsoft programs: ChromeCacheView v2.25, ChromeHistoryView v1.42 were used.

### Dropbox service

The research conducted by Horsman (2020) shows that in case of using the Dropbox service via the Google Chrome web browser a file called `www.dropbox.com.html` is saved in the web browser's cache. This file does not open in the web browser window. Source code analysis is required. That procedure allows reading basic information about the service user and identification of the contents of the virtual disk. The information stored in the `www.dropbox.com.html` file comprises the following data:

- User name (tag: „display\_name“:),
- Account identifier (tag: „id“:),
- User's email address (tag: „email“),
- URL address of user's profile picture (tag: „photo\_circle\_url“:).

A fragment of the code recorded in `www.dropbox.com.html` file is presented in Figure 1.

### Main window of the program

The `www.dropbox.com.html` file contains additional records that reflect user's activity on the Dropbox homepage. By default, on the homepage of the drive there is a list the last actions taken by the user. Each entry in the list of recent activities is incorporated in the structure of the `www.dropbox.com.html` file. The list of recent activities is saved under the „recent\_activities“ tags. The tags contain the interaction time (e.g. opening a folder / file), which is saved in UNIX format. If the user unfolds the last event that contains one or more

files (usually graphic ones), a preview of the image is displayed for each file. That results in saving files with very specific names in the memory of the web browser, for example: `size = 100x100size_mode = 4.jfif`. In the event of finding files with similar names in the browser cache it should be concluded they indicate the above form of activity have taken place on the Dropbox drive.

### Preview of drive contents

In the event that the Dropbox user displays all the files saved on the disk, the URL address is saved in the history of the web browser: `https://www.dropbox.com/home`. Additional information is saved in the `www.dropbox.com.html` file. In order to determine the entire contents of the user's virtual disk, read the information marked with „event\_type“: tags.

### Preview of file contents

Horsman's research (2020) shows that when the graphic file content is displayed on the online drive it is cached by the web browser (stays in the cache) similarly to the situation when a file is previewed in the main window. The name of the file is very distinctive because it contains information about its size: `size = 32x32size_mode = 5.jfif`. The original file name is saved in the URL address and can be read from the browser's history: `www.dropbox.com/home?preview=FILENAME.png`. Additional information about viewed image files is saved in a text file named: `is_xhr = trueactivity_context = 3activity_context_data = % 2FFILENAME.txt`.

```

\{"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"}
"user_root_permissions":
"edit", "has_never_set_password": false,
"id": 77837232, "sso_required": false,
"display_name": "Grey Joy",
"authed": 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:AAAAz7mAv7FTO-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%3A%ACJ- rJyCoDzFXXbB8MDaBqtSI
"DEFAULT_ROOT_NAME": "Dropbox",
"PERSONAL_ROLE_STRING": "Personal"}
}

```

Fig. 1. Fragment of `www.dropbox.com.html` file code.

**Users' comments**

A Dropbox user has an option of adding comments to files stored on the drive. Comments can also be added by other users who have access to the specific resource. Making a comment causes saving additional information, marked with the "comment": tag, in the text file is\_xhr = trueactivity\_context = 3activity\_context\_data =% 2FFILENAME.txt. If a third party responds to the comment, the account name of that third party will be saved in the following tags: display\_name, lname and fname. However, the metadata does not include the e-mail address and account ID of the person responding to the comment, so it does not seem possible to identify the actual third party account.

**File sharing and deletion**

When a user goes to the tab containing the resources shared with other users it is reflected in the browsing history of websites: https://www.dropbox.com/share. Viewing a list of shared resources does not cache any additional information in the web browser. The same is true for deleted files. The Dropbox service stores deleted files for 30 days, and during that period the user can restore and view them. However, there will be no records in the web browser's cache that can be assigned to the data wipe action.

**Results of author's own research**

Upon repeating the research procedure of Horsman (2020) the author obtained different results. Namely, it

has been found that when the contents of the Dropbox virtual drive are displayed https://www.dropbox.com/.html file is cached by Google Chrome and its name is encoded. This file is highlighted in Figure 2.

It has been determined that https://www.dropbox.com/.html does not contain any data identifying a Dropbox user. The examinations confirmed that the activity of the service user has its reflection in the website browsing history. If the Dropbox user views the entire disk content, the URL: https://www.dropbox.com/home is saved in the history of the web browser (according to Horsman's findings). Similarly, the web browser history stores web addresses that indicate other user activities, such as: viewing shared resources, opening a list of file requests, and opening a list of deleted files.

The author's examinations confirmed that displaying the content of the graphic file in the Dropbox service results in saving it in the cache of the web browser in JFIF format. In the example under discussion, the graphic file was saved under the name: fv\_content = true & size\_mode = 5.jfif.

The original name of the file was incorporated in the URL address and it can be read in the web browsing history. In the discussed example it is the file named: 1.JPG.

The conducted study did not confirm the findings of Horsman (2020), according to which viewing the content of an image file and adding a comment in the Dropbox service causes saving additional information in text files.

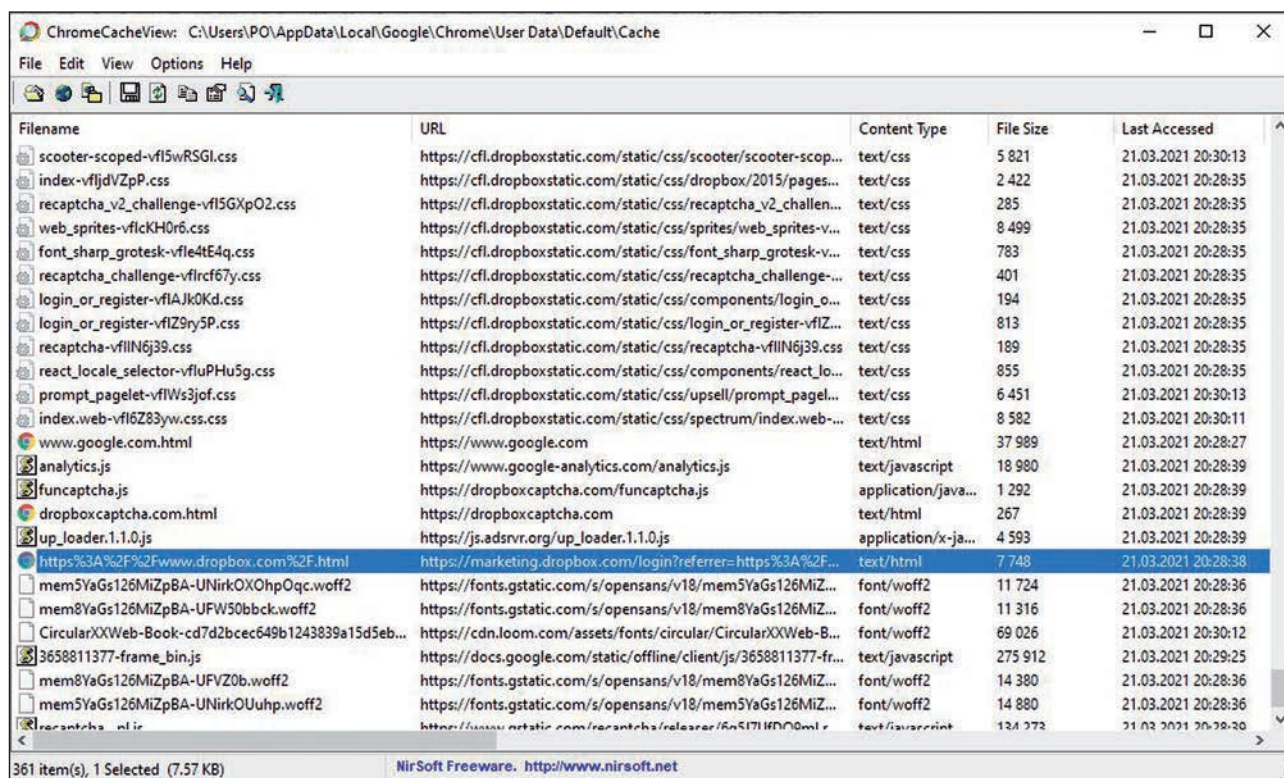


Fig. 2. ChromeCacheView window with the contents of the browser cache.

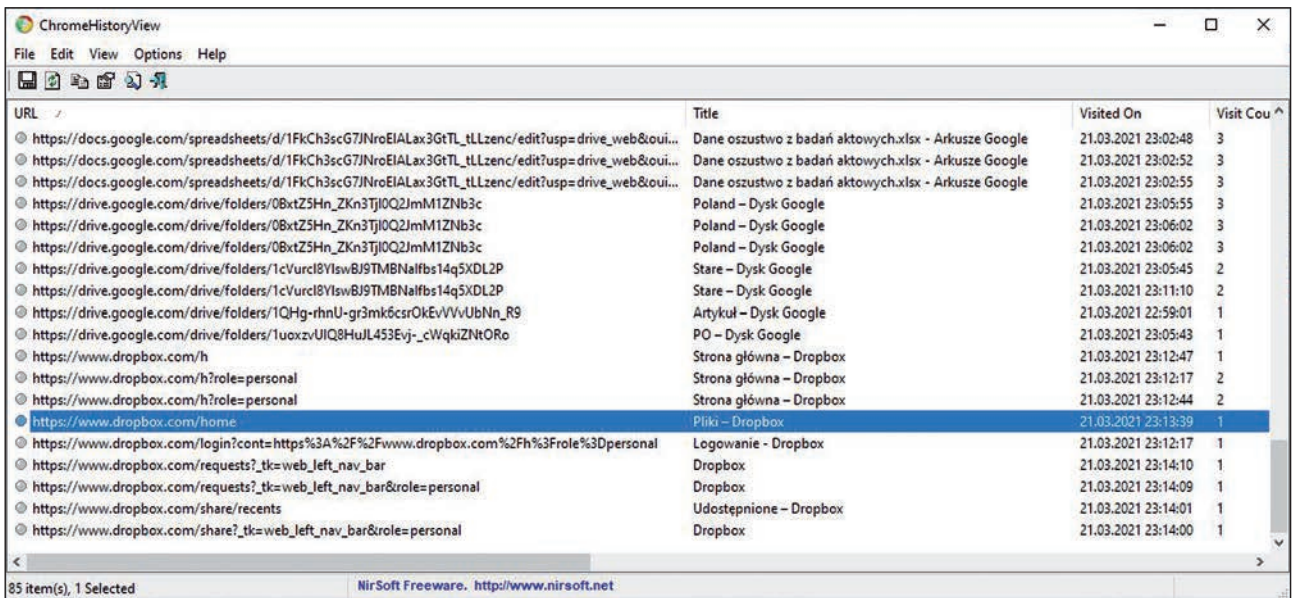


Fig. 3. Web browsing history.

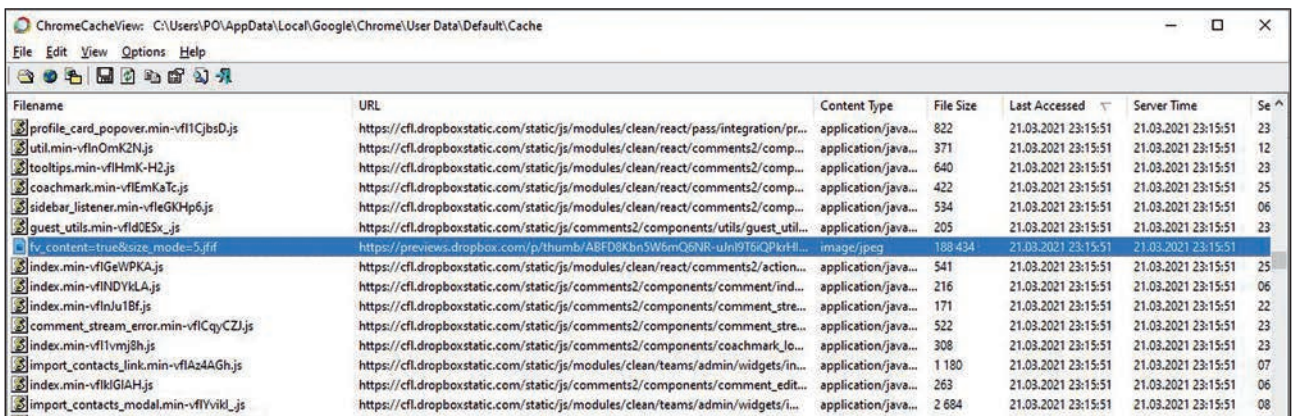


Fig. 4. Indication of fv\_content=true&size\_mode=5.jiff file.

**Google Drive service**

In the cache of the Google Chrome web browser limited information is available regarding the user’s interaction with the Google Drive service. Research by Horsman (2020) shows that Google Chrome web browser cache does not contain files revealing the identity of the user or describing the contents of the virtual Google Drive. This means the information about the Google Drive service is not cached, unlike the Dropbox service. Only graphic files viewed from the Google Drive level are saved in the browser memory. The browsed files are saved under a specific name, for example: W1366-H662. This property does not apply to text documents, spreadsheets and multimedia presentations viewed at the disk level.

According to Horsman (2020) web addresses stored in the history of browsing history and related to the user’s activity contain limited information. For example, previewing the contents of an image file on a virtual drive does not change the URL: https://drive.google.com/drive/my-drive. On the other hand, displaying the

contents of a specific folder alters the web address in a way that does not allow the resource name to be determined: https://drive.google.com/drive/folders/0By-CihkhmywOek1Gak4ySlhnQkk.

**Results of author’s own research**

As a result of his own research the author found that Horsman’s (2020) conclusions regarding the Google Drive service need to be complemented in terms of the possibility of identifying the names of folders stored on a virtual drive. Each time the contents of a directory are displayed, the URL changes, which does not allow the resource name to be determined. However, displaying web browsing history through ChromeHistoryView v1.42 allows to determine the names of Google Drive directories that have been opened by the user. Directories’ names are included in the website titles, as shown in Figure 6.

The conducted research confirmed that the preview of the content of the graphic file on the Google Drive

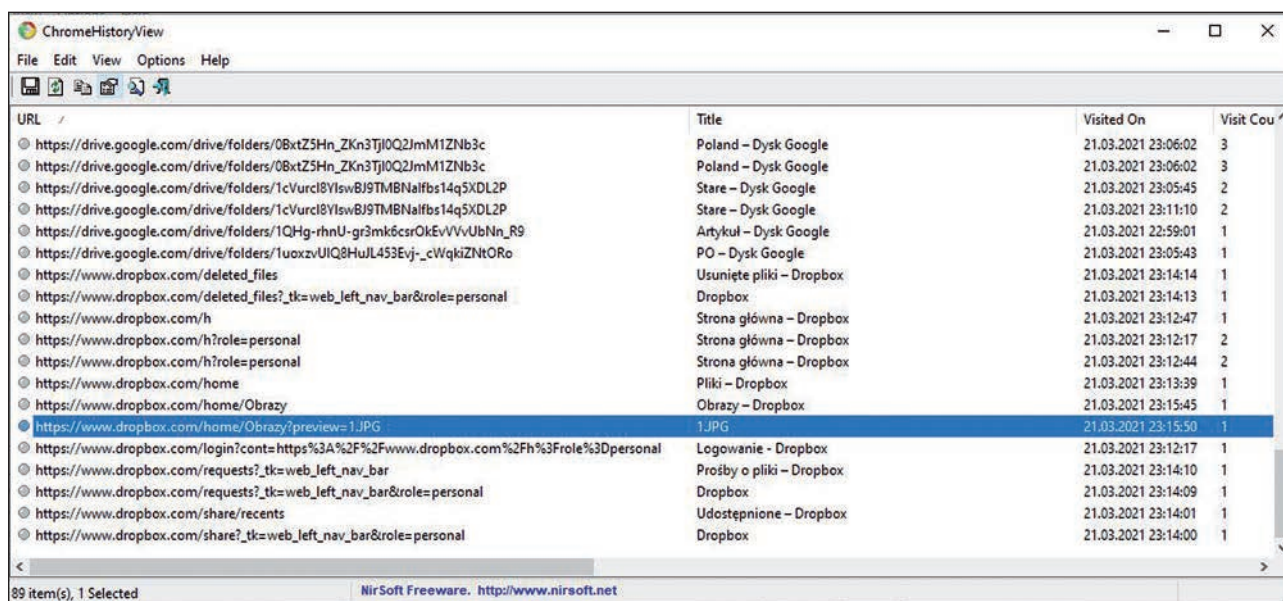


Fig. 5. Indication of 1.JPG file.

causes that it is cached and saved in the cache of the Google Chrome web browser. Figure 7 shows the graphic file w1280-h881-ft.jfif, the content of which has been displayed on the disk.

Displaying the content of text documents, spreadsheets and multimedia presentations saved on a virtual Google Drive does not result in saving additional information in the browser cache. However, it is possible to define the names of files opened by the user. Such information is available in the ChromeHistoryView program window, as shown in Figure 8.

**Results and discussion**

The analysis of published studies and the repeated procedure show that user interactions with Dropbox and Google Drive services result in saving information in the memories of local devices. Most information is saved when the Dropbox service is used. In this case, however, author’s own research led to obtaining results different from the results of Horsman (2020). These differences are most likely due to the use of different versions of Google Chrome browser and free programs: ChromeHistoryView v1.42 and ChromeCacheView v2.25. The possibility of determining the content of

the Google Drive based on the titles of the websites displayed via the above-mentioned applications, which was not described in the Horsman study (2020) should also be mentioned.

**Summary**

It can be assumed that the popularity of cloud computing storage services will continue to grow, which is due to the many advantages of these solutions. Therefore, there is a growing probability that a lot of data significant for criminal proceedings will be located in cloud storage including the virtual drives. However, in most cases the existing legal barriers make it impossible to gain direct access to this type of resources. In these circumstances it is necessary to use the assistance of foreign law enforcement and judicial authorities. The justification for applications addressed to foreign entities may be the findings made by experts in digital forensics. Those analyses may confirm the use of cloud-based data storage services, as well as help in determining credentials and the content of resources, which may be of importance for criminal proceedings.

Although the presented publication has mainly a character of an informative review it does contain

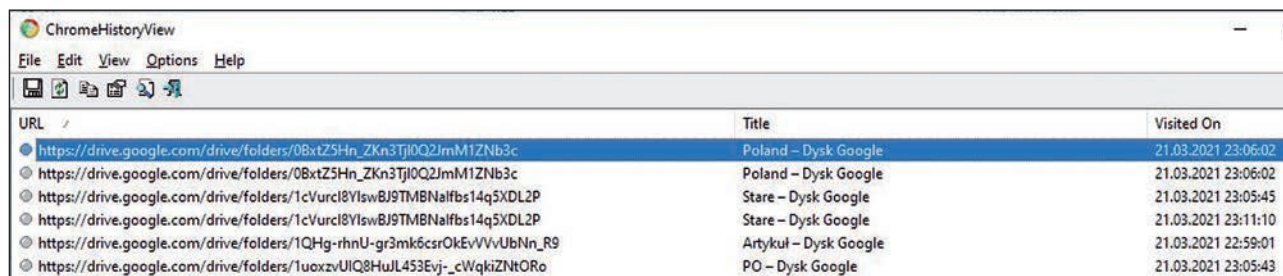


Fig. 6. Virtual disk folder names in web page titles.

Filename	URL	Content Type	File Size	Last Accessed
2524158713-waffle_js_prod_conditionalformat_pljs	https://docs.google.com/static/spreadsheets2/client/js/2524158713-waffle_js_pr...	text/javascript	12 764	21.03.2021 23:06:06
w1280-h881-ft.jiff	https://lh3.googleusercontent.com/ffe/ABSRIpbj8h-m3l_f0tZesdGjsEBLTVfgoT...	image/jpeg	160 627	21.03.2021 23:06:02
d-logo-blue-bkg%254032h.png	https://lh3.googleusercontent.com/-Vj8PcttrOE/XfoJf-jR7m/AAAAAAAAAV9Q/q...	image/png	871	21.03.2021 23:06:02
docId=0BxtZ5Hn_ZKn3QmNiN0ZEak9XclE&revisionId&u...	https://blobcomments-pa.clients5.google.com/v1/metadata?docId=0BxtZ5Hn_...	application/json	671	21.03.2021 23:06:01
416349405-docos_binary_i18n_pljs	https://docs.google.com/static/comments/client/js/416349405-docos_binary_i1...	text/javascript	383 971	21.03.2021 23:06:01
w1280-h881-iv2.html	https://lh3.googleusercontent.com/u/0/d/0BxtZ5Hn_ZKn3QmNiN0ZEak9XclE=w1280-h881-...	text/html	0	21.03.2021 23:06:01
docId=0BxtZ5Hn_ZKn3M0trRFhWMjhbkE&revisionId&u...	https://blobcomments-pa.clients5.google.com/v1/metadata?docId=0BxtZ5Hn_...	application/json	670	21.03.2021 23:06:01
HT8XDe	https://drive.google.com/_drive_fe/_js/k=drive_fe.main.pl.8ziDbkY0pCY.O/am...	text/javascript	279	21.03.2021 23:06:01
sywC,aW3pY,syyz,sy114,sy10n,syzy,sy11b,sy115,syw7,sy10...	https://drive.google.com/_drive_fe/_js/k=drive_fe.main.pl.8ziDbkY0pCY.O/am...	text/javascript	7 150	21.03.2021 23:06:01
sywg,sywh,sy2z,syz3,syz4,sy10j,sy12m,sy12j,sy12n,sy12o,t...	https://drive.google.com/_drive_fe/_js/k=drive_fe.main.pl.8ziDbkY0pCY.O/am...	text/javascript	1 469	21.03.2021 23:06:00
v-sprite35.svg	https://ssl.gstatic.com/docs/common/viewer/v3/v-sprite35.svg	image/svg+xml	10 011	21.03.2021 23:06:00

Fig. 7. W1280-h881-ft.jiff graphic file saved in the browser cache.

URL	Title	Visited On	Visit Co
https://docs.google.com/spreadsheets/d/1FkCh3scG7JNroEIALax3GtTL_tLLzenc/...	Dane oszustwo z badań aktowych.xlsx - Arkusze Google	21.03.2021 23:02:57	1
https://docs.google.com/spreadsheets/d/1FkCh3scG7JNroEIALax3GtTL_tLLzenc/...	Dane oszustwo z badań aktowych.xlsx - Arkusze Google	21.03.2021 23:02:55	1
https://docs.google.com/spreadsheets/d/1FkCh3scG7JNroEIALax3GtTL_tLLzenc/...	Dane oszustwo z badań aktowych.xlsx - Arkusze Google	21.03.2021 23:02:56	1
https://docs.google.com/spreadsheets/d/1FkCh3scG7JNroEIALax3GtTL_tLLzenc/...	Dane oszustwo z badań aktowych.xlsx - Arkusze Google	21.03.2021 23:02:48	3
https://docs.google.com/spreadsheets/d/1FkCh3scG7JNroEIALax3GtTL_tLLzenc/...	Dane oszustwo z badań aktowych.xlsx - Arkusze Google	21.03.2021 23:02:52	3
https://docs.google.com/spreadsheets/d/1FkCh3scG7JNroEIALax3GtTL_tLLzenc/...	Dane oszustwo z badań aktowych.xlsx - Arkusze Google	21.03.2021 23:02:55	3
https://drive.google.com/drive/folders/1QHg-rhnU-gr3mk6csrOkEvVvUbnN_R9	Artykuł - Dysk Google	21.03.2021 22:59:01	1

Fig. 8. Names of files opened by a Google Drive user.

a description and the results of author's own research confirming the adopted hypothesis. The own research was carried out using the latest versions of the application, which explains the differences in the obtained results. This example also confirms that each IT examination is of unique kind.

In future scientific research on the issue of detecting traces of user's activity in cloud computing services, one ought to pursue applying more advanced programmes designed for forensic IT examinations, such as: X-Ways Forensics, NetAnalysis and HstEx.

#### Sources of figures:

Fig. 1: elaborated by author basing on: Horsman, 2020  
Figs. 2–8: author

#### Bibliography

- Ahmad, N.H., Hamid, A.S.S.A., Shahidan, N.S.S., Ariffin, K.A.Z. (2020). Cloud forensic analysis on pCloud: From volatile memory perspectives. In: M.H. Miraz, P. Excell, A. Ware, S. Soomro, M. Ali (ed.), *Emerging Technologies in Computing, Third EAI International Conference, iCETiC 2020*. Cham: Springer.
- Dargahi, T., Dehghantanha, A., Conti, M. (2017). Investigating storage as a service cloud platform: pCloud as a case study. In: A. Dehghantanha, K.-K.R. Choo (ed.), *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*. Amsterdam–Boston et al.: Elsevier, <https://doi.org/10.1016/B978-0-12-805303-4.00012-5>.
- Dehghantanha, A., Dargahi, T. (2017). Residual cloud forensics. In: A. Dehghantanha, K.-K.R. Choo (red.), *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*. Amsterdam–Boston et al.: Elsevier, <https://doi.org/10.1016/B978-0-12-805303-4.00014-9>.
- Herman, M., Iorga, M., Salim, A.M., Jackson, R.H., Hurst, M.R., Leo, R., ... Sardinias, R. (2014). *NIST Cloud Computing Forensic Science Challenges*. Gaithersburg: National Institute of Standards and Technology.
- Horsman, G. (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*, 15(1).
- Martini, B., Choo, K.-K.R. (2014). Cloud forensic technical challenges and solutions: A snapshot. *IEEE Cloud Computing*, 1(4), <https://doi.org/10.1109/MCC.2014.69>.
- Mell, P.M., Grance, T. (2011). *The NIST Definition of Cloud Computing*. Gaithersburg: National Institute of Standards and Technology.

8. Mohtasebi, S.H., Dehghantanha, A., Choo, K.-K.R. (2017). Cloud storage forensics. In: A. Dehghantanha, K.-K.R. Choo (ed.), *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications* (s. 205–246). Amsterdam–Boston et al.: Elsevier, <https://doi.org/10.1016/B978-0-12-805303-4.00013-7>.
9. Samy, G.N., Shanmugam, B., Maarop, N., Magalingam, P., Perumal, S., Albakri, S.H. (2018). Digital forensic challenges in the cloud computing environment. In: F. Saeed, N. Gazem, S. Patnaik, A.S. Saed Balaid, F. Mohammed (red.), *Recent Trends in Information and Communication Technology*. Cham: Springer, [https://doi.org/10.1007/978-3-319-59427-9\\_69](https://doi.org/10.1007/978-3-319-59427-9_69).
10. Sharma, P., Arora, D., Sakthivel, T. (2018). Mobile cloud forensic: Legal implications and counter measures. W: S.C. Satapathy, A. Joshi (red.), *International Conference on Information and Communication Technology for Intelligent Systems*. Cham: Springer, [https://doi.org/10.1007/978-3-319-63673-3\\_64](https://doi.org/10.1007/978-3-319-63673-3_64).
11. Teing, Y.-Y., Dehghantanha, A., Choo, K.-K.R. (2018). CloudMe forensics: A case of big data forensic investigation. *Concurrency and Computation: Practice and Experience*, 30(5), <https://doi.org/10.1002/cpe.4277>.

*Translation Ewa Nogacka*