Informatyka kryminalistyczna w kontekście usług przechowywania danych w chmurze obliczeniowej

Paweł Olber[1]

[1] 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 użytownika 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 zawartości 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_ha_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@gooqlemail.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\%3AAACJ-_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 rozwinie 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 formy 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 zapisywane są natomiast dodatkowe informacje. W celu ustalenia całej zawartości dysku wirtualnego użytkownika należy odczytać informacje opatrzone znacznikami „event_type":.

Podgląd zawartości pliku

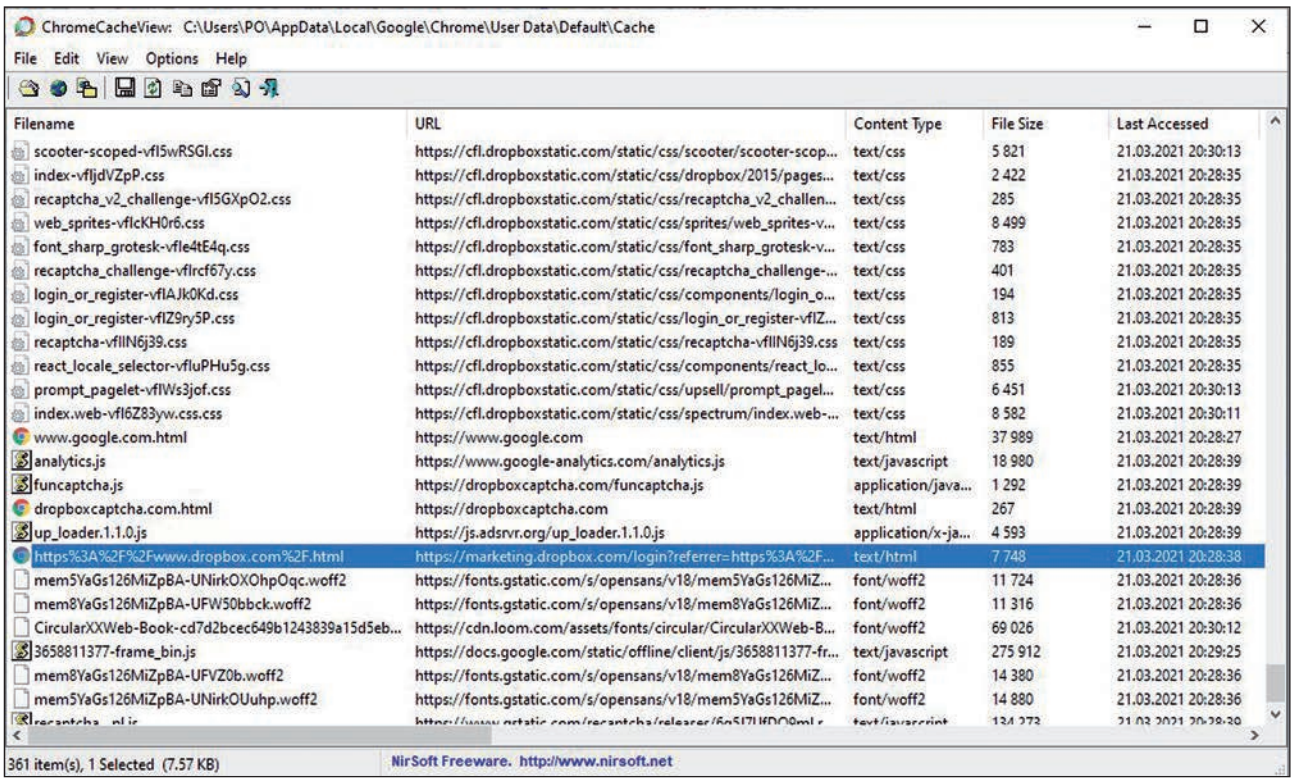
Z badań Horsmana (2020) wynika, że w przypadku wyświetlenia zawartości pliku graficznego na dysku wirtualnym jest on buforowany przez przeglądarkę internetową i zapisywany w pamięci podręcznej, podobnie jak po wyświetleniu podglądu pliku w oknie głównym. Nazwa pliku jest bardzo charakterystyczna, ponieważ 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. Dodatkowe informacje dotyczące przeglądanych plików graficznych są zapisywane w pliku tekstowym o nazwie: is_xhr=trueactivity_context=3activity_context_data=%2FFILENAME.txt.

Komentarze użytkowników

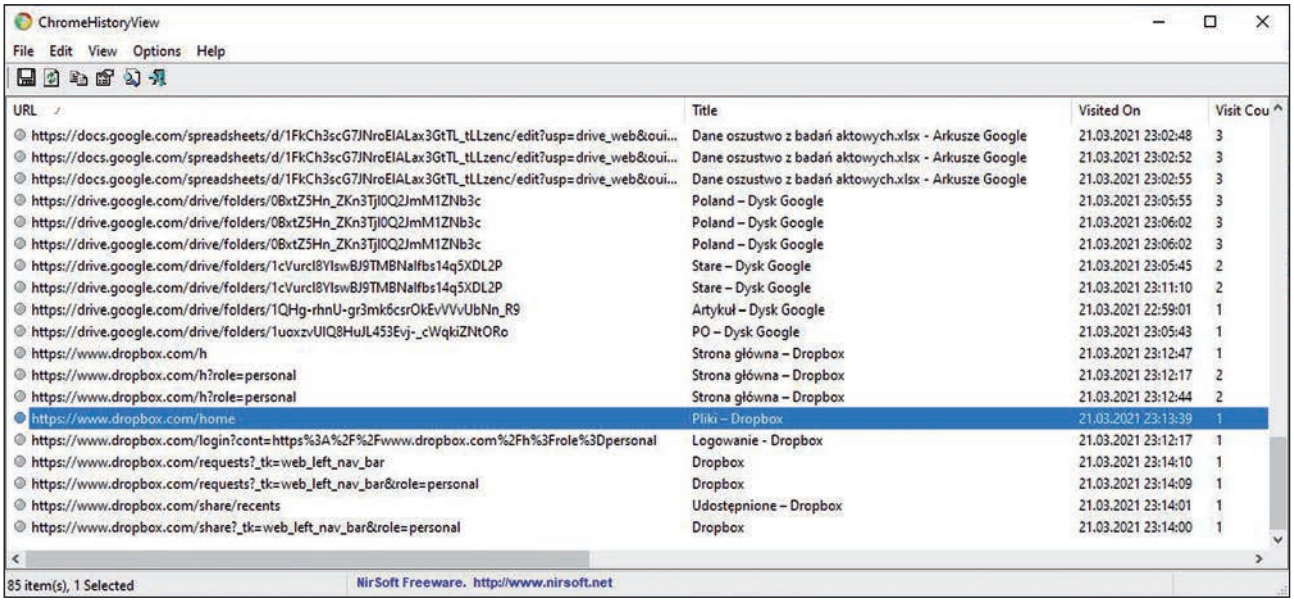
Użytkownik usługi Dropbox ma możliwość dodawania komentarzy do plików znajdujących się na dysku. Komentarze mogą być również dodawane przez innych użytkowników, którzy posiadają dostęp do określonego zasobu. Wstawienie komentarza skutkuje zapisaniem dodatkowych informacji, opatrzonych znacznikiem „comment":, 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

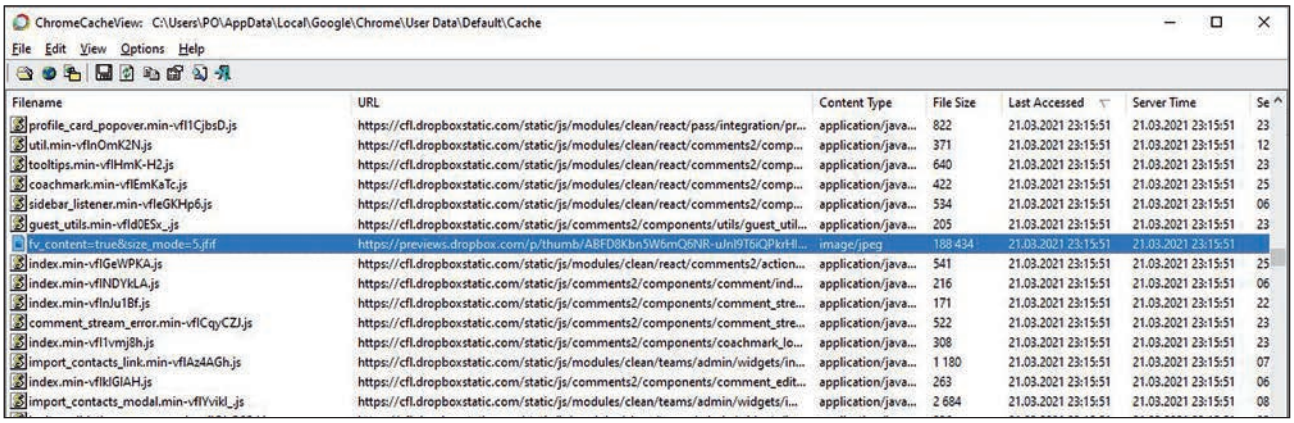
Przejście użytkownika usługi do zakładki zawierającej zasoby udostępnione innym użytkownikom znajduje odzwierciedlenie w historii przeglądania stron internetowych: https://www.dropbox.com/share. Wyświetlenie



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



Ryc. 3. Historia przeglądania stron internetowych.



Ryc. 4. Wskazanie pliku fv_content=true&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.

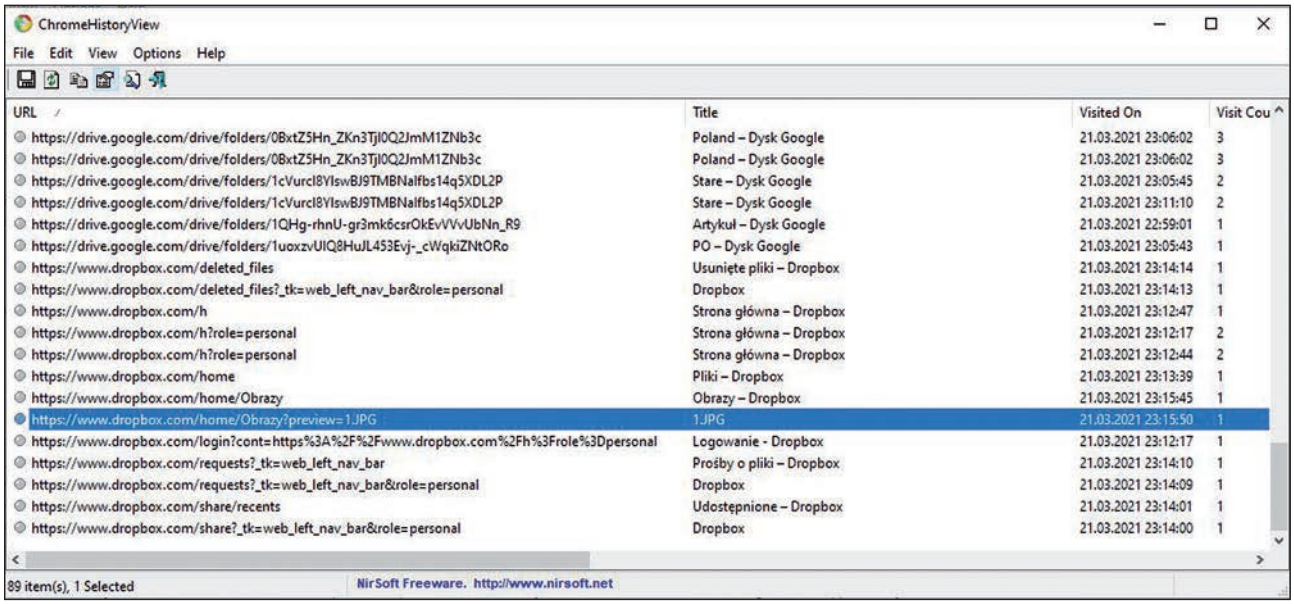
Wyniki badań własnych

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 ustaleniami 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.

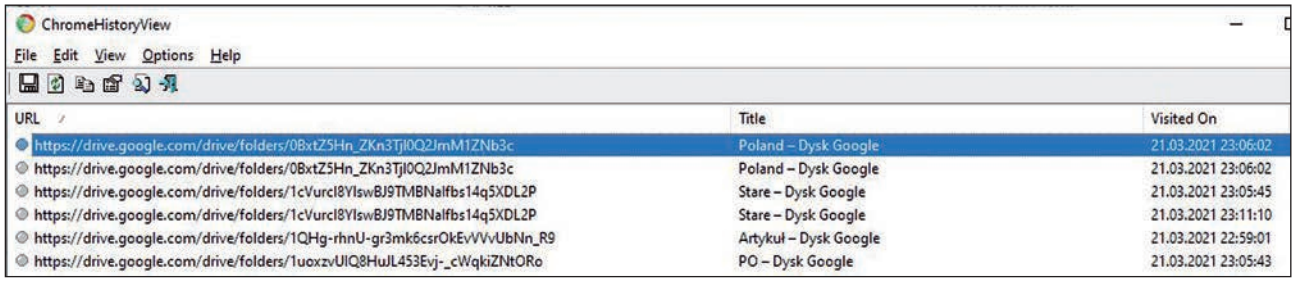
Usługa Google Drive

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-CihkhmywOek1Gak4ySlhnQkk.

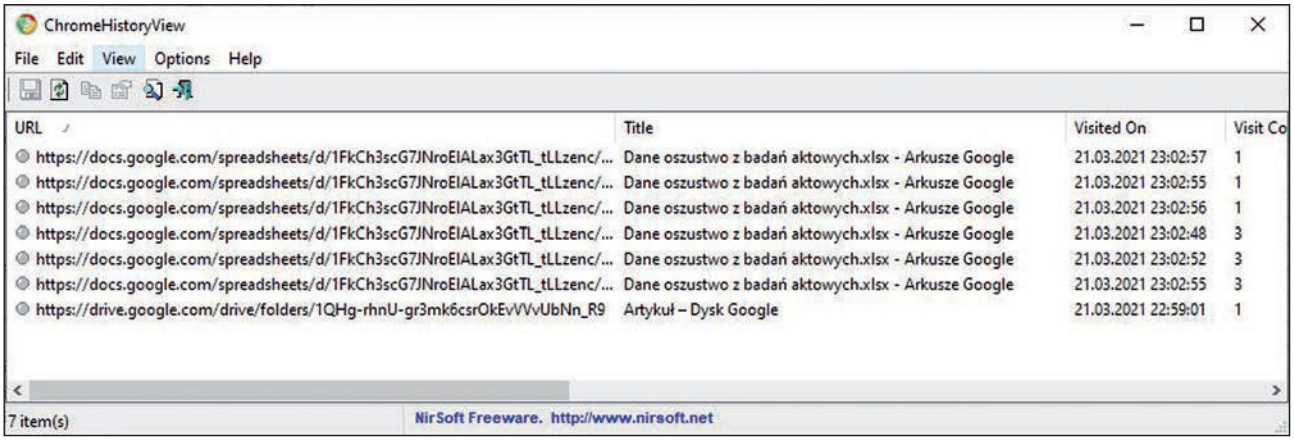
Wyniki badań własnych

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.

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



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

1. 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.
2. 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.
3. 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.
4. Herman, M., Iorga, M., Salim, A.M., Jackson, R.H., Hurst, M.R., Leo, R., … Sardinas, R. (2014). *NIST Cloud Computing Forensic Science Challenges*. Gaithersburg: National Institute of Standards and Technology.
5. 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).
6. 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.
7. 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. 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.
9. 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.
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.
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.