TẠP CHÍ KHOA HỌC
TRƯỜNG ĐẠI HỌC SƯ PHẠM TP HỒ CHÍ MINH
Tập 20, Số 7 (2023): 1180-1189
Website: https://journal.hcmue.edu.vn
ISSN: 2734-9918

HO CHI MINH CITY UNIVERSITY OF EDUCATION
JOURNAL OF SCIENCE
Vol. 20, No. 7 (2023): 1180-1189
https://doi.org/10.54607/hcmue.js.20.7.3616(2023)

Bài báo nghiên cứu

ĐIỀU TRA SỐ ỨNG DỤNG DROPBOX TRÊN CÁC MÁY TÍNH CHẠY HỆ ĐIỀU HÀNH WINDOWS 10

***Văn Thiên Hoàng*[1], *Trần Văn Đan Trường*[2*], *Đặng Văn Thành Nhân*[3]**

[1]*Trường Đại học Công nghệ Thành phố Hồ Chí Minh, Việt Nam*

[2]*Công ty Cổ phần Mạng xã hội Du lịch Hahalolo, Việt Nam*

[3]*Trường Đại học Quốc tế Sài Gòn, Việt Nam*

[*]*Tác giả liên hệ: Trần Văn Đan Trường – Email: truongtlt147@gmail.com*

Ngày nhận bài: 11-10-2022; ngày nhận bài sửa: 20-7-2023; ngày duyệt đăng: 27-7-2023

TÓM TẮT

Trong thế giới kết nối Internet ngày nay, các máy tính ngày được sử dụng nhiều hơn để truy cập dịch vụ lưu trữ đám mây, dịch vụ cho phép người dùng truy cập dữ liệu mọi lúc, mọi nơi. Tuy nhiên, các thiết bị này là mục tiêu được nhắm đến bởi tội phạm mạng để thực hiện các hoạt động độc hại, chẳng hạn như xâm nhập dữ liệu, cài đặt phần mềm độc hại, đánh cắp danh tính, vi phạm bản quyền, khủng bố mạng. Do đó, máy tính là một nguồn bằng chứng quan trọng trong việc các cơ quan điều tra tìm ra tội phạm. Trong bài báo này, chúng tôi thực hiện điều tra số ứng dụng Dropbox, một dịch vụ lưu trữ đám mây phổ biến, trên nền tảng hệ điều hành Windows 10 (một trong những hệ điều hành phổ biến và có số lượng người sử dụng nhiều nhất). Chúng tôi cố gắng xác định các dữ liệu còn sót lại mà cơ quan điều tra có thể quan tâm, chẳng hạn như thông tin được tạo ra trong quá trình đăng nhập, tải lên, tải xuống, xóa và chia sẻ tệp. Những phát hiện cũng như kết quả mà chúng tôi đạt được có thể hỗ trợ cho cơ quan chức năng dễ dàng lấy được dữ liệu bằng chứng từ ứng dụng DropBox trên Windows 10.

Từ khóa: lưu trữ đám mây; dropBox forensic; điều tra số; Windows forensic

1. Giới thiệu

Ngày nay, với sự phát triển nhảy vọt của ngành công nghệ thông tin, việc lưu trữ kĩ thuật số đang phát triển vô cùng mạnh mẽ và ngày càng có nhiều người dùng chuyển sang các hệ thống lưu trữ đám mây. Số lượng máy tính ngày càng tăng, một phần nhờ vào sự tiến bộ trong công nghệ và kết nối Internet. Mặc dù, các máy tính hiện nay mạnh mẽ hơn, nhưng việc lưu trữ và xử lí phân quyền dữ liệu vẫn là một thách thức cần được xử trong kỉ nguyên dữ liệu lớn này (Quick et al., 2014). Do đó, không đáng ngạc nhiên khi các nhà sản xuất máy tính sử dụng đám mây để thực hiện việc sao lưu hoặc các công việc xử lí chuyên sâu (Gu, 2014). Việc tăng cường sử dụng các dịch vụ lưu trữ đám mây khiến tội phạm dễ dàng lưu

Cite this article as: Van Thien Hoang, Tran Van Dan Truong, & Dang Van Thanh Nhan (2023). Digital forensic analysis of dropbox on Windows 10 devices. *Ho Chi Minh City University of Education Journal of Science, 20*(7), 1180-1189.

trữ và che giấu các tài liệu phạm tội hơn. Nó có thể là thách thức đối với các nhà điều tra trong việc thu giữ các tệp này do tính chất xuyên biên giới của các dịch vụ đám mây. Việc hiểu biết những thông tin còn sót lại trên các thiết bị của người dùng đến việc sử dụng các ứng dụng lưu trữ đám mây trong các cuộc điều tra liên quan sẽ tạo điều kiện cho cơ quan chức năng phát hiện tội phạm (Hale, 2013).

Với sự phát triển không ngừng của công nghệ và việc tăng cường sử dụng dịch vụ lưu trữ đám mây, điều này đã đặt ra nhiều thách thức với các cơ quan chức năng khi cố gắng lấy được hoặc khôi phục được các dữ liệu được lưu trữ trong các dịch vụ lưu trữ đám mây (đôi khi dữ liệu này nằm ở nước ngoài). Do đó, điều quan trọng là đảm bảo các cán bộ điều tra phải bắt kịp với những tiến bộ công nghệ – đó là một động lực chính của bài báo này.

Trong bài báo này, chúng tôi áp dụng hướng dẫn phân tích của NIST (Mell & Grance, 2011) (NIST, 2022) và quy trình phân tích đám mây của Choo và Maritni (Martini & Choo, 2012) để tiến hành điều tra và phân tích ứng dụng lưu trữ đám mây phổ biến là Dropbox cho các thiết bị chạy Windows 10. Thách thức đặt ra khi các ứng dụng thay đổi cách lưu trữ cũng như mã hóa khiến cho các dữ liệu khó bị phát hiện hơn. Do đó, chúng tôi tìm cách cung cấp cho nhà phân tích cũng như cơ quan chức năng hiểu biết khái quát về các loại dữ liệu bằng chứng có thể được phục hồi và quy trình lấy được các dữ liệu này từ các thiết bị của người dùng và nhật kí của hệ thống, đây là những đóng góp quan trọng trong quá trình điều tra tội phạm.

2. Nội dung

Nội dung của phần tiếp theo bài báo gồm: phần 2.1 đề cập đến các công trình nghiên cứu liên quan nhằm đưa ra tính khả thi của bài báo, phần 2.2 sẽ trình bày về phương pháp điều tra, phần 2.3 sẽ tiến hành điều tra ứng dụng DropBox qua các thao tác của người dùng, cuối cùng chúng tôi sẽ trình bày về kết quả đạt được cũng như hướng phát triển của nghiên cứu này ở phần 3.

2.1. Các công trình liên quan

Chung và cộng sự đã đề xuất một mô hình điều tra và phân tích cho các ứng dụng lưu trữ đám mây, sử dụng mô hình này đối với các dịch vụ Amazon S3, Dropbox, Evernote và Google Docs trên các thiết bị của Motorola (Android phiên bản 2.2.2), iPhone 4 (iOS phiên bản 4.3.5), máy Mac và máy Windows (Chung, Park, Lee, & Kang, 2012). Các tác giả có thể khôi phục dữ liệu còn sót lại như tên người dùng, các tệp dữ liệu được tải xuống và tải lên. Một dự án nghiên cứu khác đã trình bày cách lấy dữ liệu từ Amazon EC2 bằng cách sử dụng các công cụ phân tích hiện có (tức là EnCase và AccessData FTK) trên các máy ảo chạy Eucalyptus (Dykstra & Sherman, 2012).

Hale đã chứng minh rằng các thông tin của dữ liệu như đường dẫn cài đặt, các thông tin đăng kí hệ thống (ví dụ như phiên bản, hình ảnh icon…), và các hoạt động tải lên/tải xuống có thể được khôi phục từ máy tính sử dụng Windows XP sau khi nó đã được sử dụng để truy cập dịch vụ đám mây của Amazon (Hale, 2013). Sau khi sử dụng Dropbox, Box và

SugarSync trên các thiết bị chạy Android phiên bản 2.1 và iOS phiên bản 3, một số dữ liệu hiển nhiên có thể được phục hồi trước đó (Grispos, Glisson, & Storer, 2013). Tương tự, trong một phân tích khác về một máy chủ ownCloud và các thiết bị khách truy cập các dịch vụ đám mây riêng của ownCloud, tác giả đã chứng minh rằng nhiều thông tin (ví dụ: thông tin xác thực, nội dung tệp và thời gian tạo, thời gian sửa đổi…) có thể được phục hồi từ cả máy khách và máy chủ (Martini & Choo, 2013).

Wen và cộng sự (Wen, Man, Le, & Shi, 2013) đã đề xuất một giải pháp để tiến hành điều tra và nghiên cứu dịch vụ lưu trữ trên đám mây. Họ đã thực hiện công việc bằng cách sử dụng National Software Reference Library (NSRL) để lọc nội dung điển hình từ các tệp được tạo bởi trình cài đặt. Sử dụng Amazon EC2, họ xác định rằng giải pháp này có thể tiết kiệm đến 87% thời gian phân tích. Nhật kí được ghi nhận từ các nguồn khác nhau như kết nối mạng, cơ sở dữ liệu và các quá trình điều tra, phân tích; tuy nhiên, việc thu thập nhật kí từ đám mây có thể là một thách thức. Họ đề xuất ghi nhật kí an toàn dưới dạng dịch vụ (SecLaaS) để lưu trữ nhật kí trong khi vẫn bảo mật thông tin của người dùng sử dụng đám mây. Sau đó, họ đã triển khai giải pháp trên OpenStack (Zawoad, Dutta, & Hasan, 2013).

Hệ thống tệp XtreemFS đã được phân tích để xác định phương pháp hiệu quả nhất trong việc thu thập dữ liệu từ một hệ thống tệp phức tạp bởi Martini và cộng sự. Trong nghiên cứu này, các tác giả đã sử dụng API của vCloud để khôi phục dữ liệu và siêu dữ liệu (metadata). Họ xác định rằng có thể thu thập một loạt dữ liệu thông qua API (Martini & Choo, 2014).

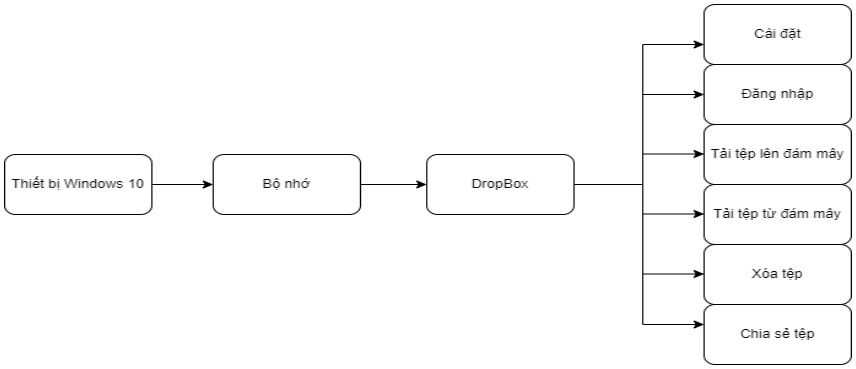
Shariati và cộng sự đã tiến hành các thử nghiệm để xác định dữ liệu còn sót lại của UbuntuOne trên Windows 8.1, OS X và iOS (Shariati, Dehghantanha, Martini, & Choo, 2018). Các tác giả đã thử nghiệm để khôi phục một loạt các dữ liệu từ bộ nhớ của thiết bị và thông tin lưu lượng mạng. Nhóm nghiên cứu chứng minh được dữ liệu có thể được trích xuất rõ ràng từ các thiết bị Mac OS X, Android và iOS sau khi ứng dụng SugarSync được sử dụng trên các thiết bị này (Shariati, Dehghantanha, & Choo, 2016). Các ứng dụng Dropbox, OneDrive và ownCloud Android đã được tiến hành kiểm tra và phân tích, bằng cách sử dụng phương pháp được đề xuất trên thì dữ liệu có thể được phục hồi từ bộ nhớ trong và thẻ SD (Martini, Do, & Choo, 2015).

Các nhà nghiên cứu như Choo và Smith (Choo, 2008; Choo & Smith, 2008) đã cho rằng tội phạm có tổ chức và tội phạm mạng luôn đổi mới và sẽ liên tục tìm cách đổi mới để trốn tránh sự giám sát và tiếp cận của cơ quan thực thi pháp luật, chẳng hạn như bằng cách sử dụng các dịch vụ lưu trữ đám mây khác để lưu trữ bằng chứng buộc tội. Hơn nữa, hiện nay có hơn 1.4 tỉ người dùng sử dụng các thiết bị chạy hệ điều hành Windows 10 trong hơn 200 quốc gia và vùng lãnh thổ (Microsoft, 2022). Do đó, trong bài báo này, chúng tôi muốn đóng góp vào hiểu biết về dịch vụ lưu trữ đám mây phổ biến DropBox đang chạy trên nền tảng Windows 10.

2.2. Phương pháp phân tích

Trong bài báo này, chúng tôi áp dụng phương pháp điều tra và phân tích bốn bước từ NIST (Mell & Grance, 2011) để tiến hành quá trình phân tích này. Quá trình phân tích được mô tả như sau:

- Nhận dạng và thu thập: Các dữ liệu chứng cứ được thu thập từ ổ đĩa bộ nhớ của thiết bị máy tính ASUS VivoBook S510UQR, chạy hệ điều hành Windows 10 Pro phiên bản 2004. Bên cạnh đó, việc thu thập dữ liệu thông qua phần mềm Magnet AXIOM phiên bản 5.4 (Magnet Forensic, 2022) cũng như phần mềm SQLiteStudio phiên bản 3.3.3 (SQLiteStudio, 2022).
- Xác thực: Mã hóa MD5 của các tệp dữ liệu đều được tính toán và sau đó sẽ tiến hành kiểm tra xác thực.
- Tiến hành điều tra và phân tích: Mục đích của bước kiểm tra này là phát hiện các thông tin bằng chứng còn sót lại của các ứng dụng lưu trữ đám mây của người dùng trên thiết bị của họ. Trọng tâm của bài báo này chỉ là về giai đoạn kiểm tra. Trong nghiên cứu này, dữ liệu thô đã thu thập được tìm kiếm bằng cách sử dụng các từ khóa xác định trước để xác định những dữ liệu còn sót lại có thể có thông tin đăng nhập của người dùng.
- Báo cáo: Trình bày tóm tắt các thông tin đã tìm thấy cũng như các nội dung đã phân tích được từ máy tính.



Hình 1. *Sơ đồ khối phạm vi phân tích của nghiên cứu*

Mục tiêu của nghiên cứu này là phát hiện những dữ liệu còn sót lại của người dùng khi khi thực hiện các thao tác được đề xuất như trong Hình 1. Một số thử nghiệm đã được thiết kế và thực thi trên các thiết bị Windows 10 để cố gắng đạt được mục tiêu này.

2.3. Kiểm tra và phân tích số ứng dụng DropBox

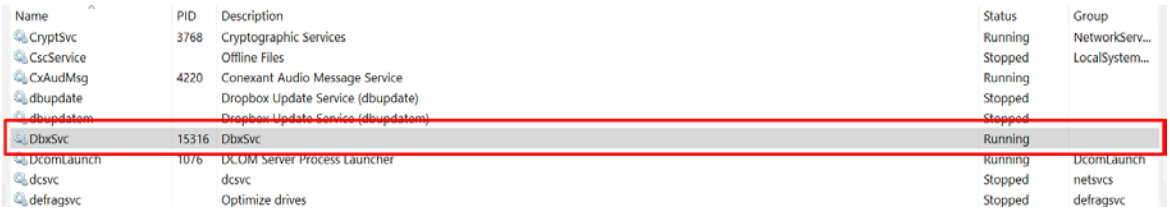
Trong phần này, chúng tôi sẽ trình bày về các nội dung đã điều tra và phân tích được đối với ứng dụng DropBox.

2.3.1. Phân tích quá trình cài đặt

Khi bắt đầu cài đặt ứng dụng Dropbox trên Windows 10, chương trình sẽ tự động tạo ra các thư mục có tên "DropBox" tại các địa chỉ như "C:\Users\[username]\", "C:\User\[username]\AppData\Local", "C:\User\[username]\AppData\Roaming", "C:\Program Files (x86)". Những thư mục này sẽ chứa thông tin dữ liệu đi kèm với các cài

đặt của DropBox.

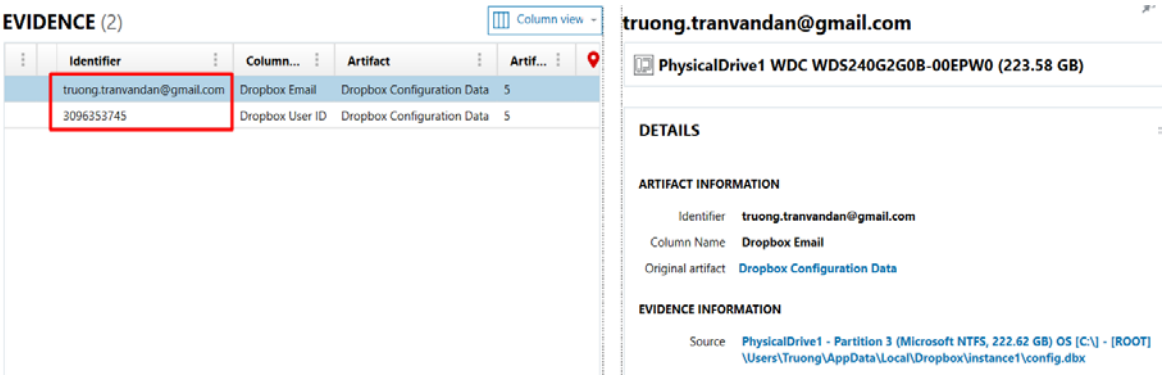
Trong quá trình cài đặt diễn ra, có nhiều thay đổi đối với hệ thống máy tính cần chú ý như việc đăng kí mới các tiến trình. Ví dụ, tiến trình có tên DbxSvc ở Hình 2, đây là tiến trình quan trọng của ứng dụng DropBox được dùng để sao lưu và truy vấn dữ liệu đến và đi từ Internet.



Hình 2. *Tiến trình DbxSvc được tạo ra khi cài đặt ứng dụng DropBox*

2.3.2. Phân tích quá trình đăng nhập

Việc đăng nhập được tiến hành tự động khi mở máy tính sau lần đăng nhập đầu tiên. Với công cụ Magnet AXIOM, chúng tôi tiến hành phân tích tích tệp tin "config.dbx" trong thư mục "%AppData%/Local/DropBox/Instance1" thì phát hiện được ứng dụng DropBox đã lưu trữ thông tin về tài khoản của người dùng như Hình 3 bên dưới. Có thể dễ dàng thấy được tài khoản người dùng sử dụng đăng nhập là "truong.tranvandan@gmail.com", và người dùng này có ID là "3096353745". Như vậy, DropBox đã không lưu giữ lại mật khẩu của người dùng trên máy tính cá nhân, tuy nhiên, việc lưu trữ ID người dùng lại rất có ích khi có thể điều tra các thông tin khác có liên quan đến ID này.

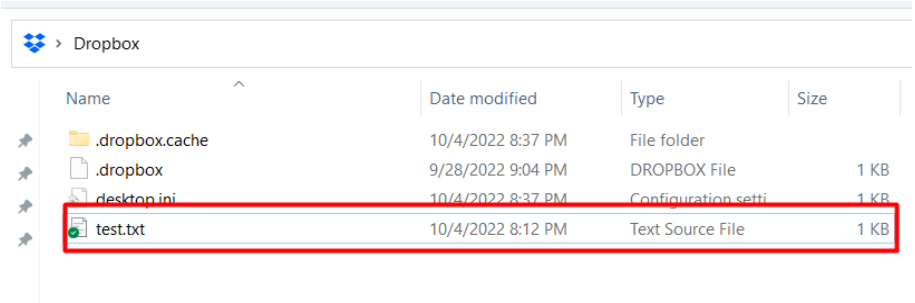


Hình 3.*Thông tin người dùng còn lưu trữ trên máy tính cá nhân*

2.3.3. Phân tích quá trình tải dữ liệu lên đám mây

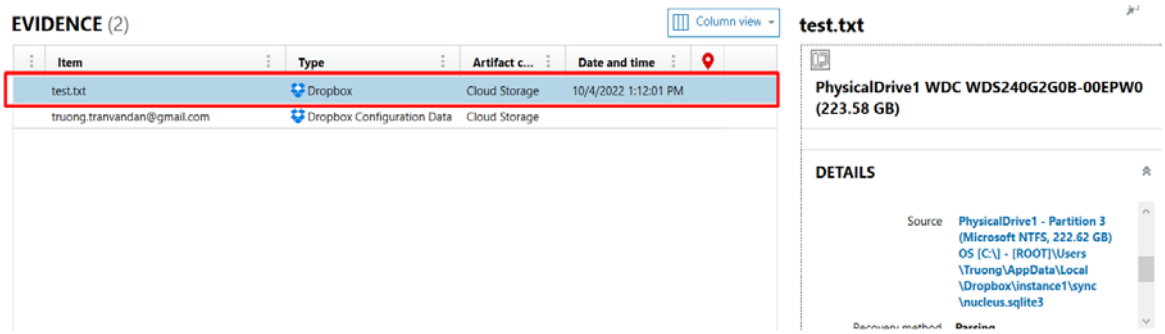
Để tiến hành việc điều tra và phân tích các quá trình tải tệp lên, tải tệp xuống từ máy chủ DropBox, cũng như việc chia sẻ tệp, chúng tôi sử dụng một tệp chung là "test.txt".

Sau khi sao chép tệp tin trên vào thư mục đồng bộ DropBox trên máy tính thì tệp này cũng sẽ được tự động tải lên máy chủ đám mây của DropBox. Việc tải lên thành công rất dễ nhận biết khi tệp tin này có dấu tích màu xanh bên cạnh như Hình 4.

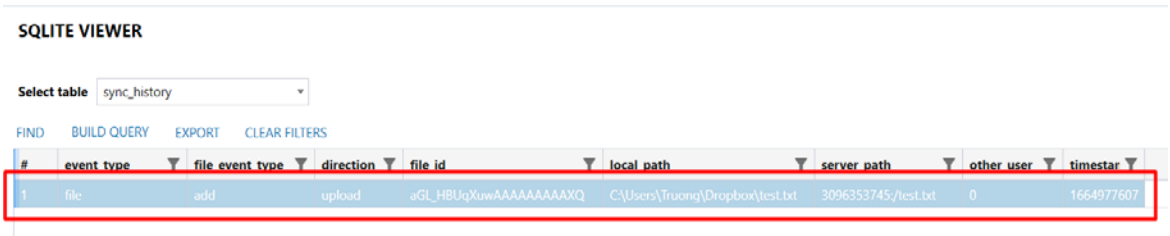


Hình 4. *Tệp "test.txt" đã được đánh dấu tích đồng bộ*

Ngoài ra, chúng tôi còn tiến hành điều tra thư mục DropBox ở máy tính cá nhân và phát hiện rằng việc đồng bộ tệp tin "test.txt" đã được lưu trữ. Thông tin này được chúng tôi phát hiện khi phân tích tệp tin "nucleus.sqlite3" trong thư mục "..\instance1\sync", Hình 5. Tương tự, chúng tôi cũng phát hiện việc lưu trữ thông tin này ở tệp "sync_history.db" trong thư mục "..\instance1\". Thông tin chúng tôi phân tích được bao gồm đường dẫn tệp, đường dẫn máy chủ, thời gian thực hiện… như trong Hình 6. Ở đây, có thể thấy đường dẫn ở máy chủ bắt đầu với chuỗi kí tự số, đó là ID của người dùng. Việc lưu lại thông tin như tên tệp, nội dung, thời gian rất có ích cho việc điều tra khi chỉ cần đọc lại những thông tin được lưu trong cơ sở dữ liệu.



Hình 5. *Thông tin tệp "test.txt" được lưu trữ trong tệp tin "nucleus.sqlite3"*

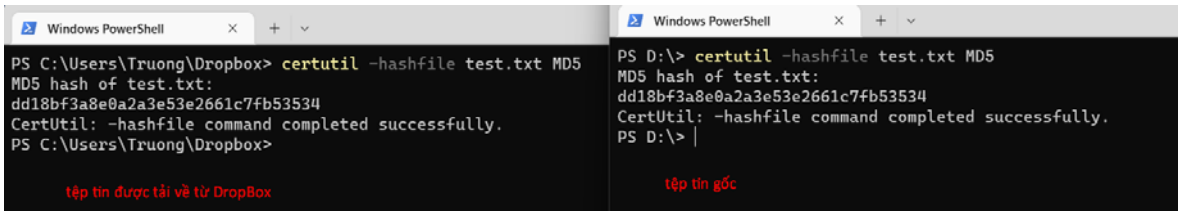


Hình 6. *Thông tin tệp "test.txt" được lưu trữ trong tệp tin "sync_history.db"*

2.3.4. Phân tích quá trình tải xuống dữ liệu từ đám mây

Chúng tôi tiến hành tải tệp "test.txt" từ máy chủ DropBox về máy tính cá nhân, sau đó thực hiện kiểm tra checksum đối với tệp gốc và tệp được tải về từ máy chủ DropBox, kết quả checksum của cả hai tệp đều là "dd18bf3a8e0a2a3e53e2661c7fb53534" như Hình 7. Như vậy, có thể kết luận rằng, việc tải dữ liệu lên máy chủ DropBox sẽ không làm thay đổi

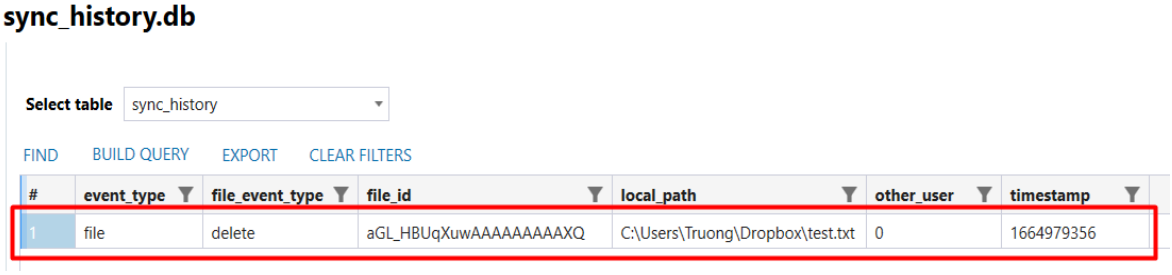
nội dung dữ liệu, hay metadata của những tệp tin đó. Điều này sẽ hỗ trợ rất nhiều trong quá trình điều tra khi tội phạm cố tình thay dữ liệu ở máy cá nhân nhưng chưa cập nhật lên DropBox thì những chứng cứ quan trọng vẫn được lưu lại trên máy chủ và không bị thay đổi.



Hình 7. *Kết quả checksum của hai tệp dữ liệu*

2.3.5. Phân tích quá trình xóa dữ liệu từ đám mây

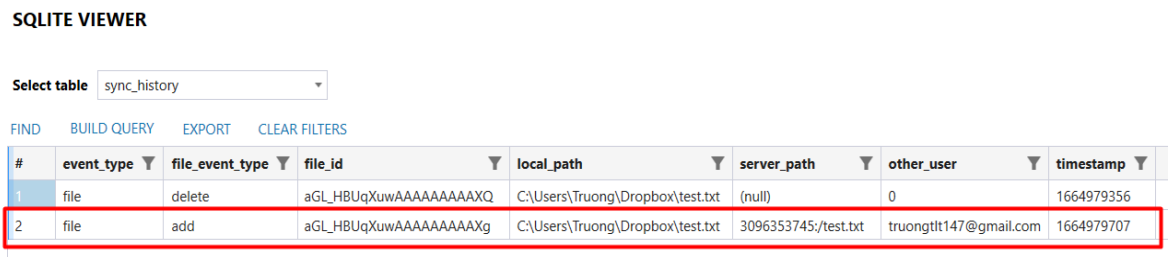
Chúng tôi tiến hành việc xóa tệp tin "test.txt" từ cả phía máy chủ DropBox và thư mục đồng bộ DropBox. Đối với cả hai thao tác, DropBox đã thực hiện việc đồng bộ nên tệp tin đều được xóa ở phía còn lại. Tuy nhiên, việc xóa dữ liệu này đều được ghi nhận lại. Bằng việc điều tra và phân tích tệp "sync_history.db" trong thư mục "..\instance1\sync", chúng tôi phát hiện thông tin tệp bị xóa được ghi lại gồm đường dẫn tệp, thời gian bị xóa như Hình 8. Điều này rất có ích cho quá trình điều tra của các cơ quan chức năng khi tội phạm cố tình xóa tệp tin, nhưng DropBox vẫn ghi lại thông tin này, do đó, bằng cách sử dụng các công cụ khôi phục dữ liệu, họ có thể lấy lại được tệp tin gốc trước khi bị xóa.



Hình 8. *Thông tin xóa tệp "test.txt" được ghi nhận lại*

2.3.6. Phân tích quá trình chia sẻ dữ liệu với người khác

Chúng tôi tiến hành việc chia sẻ tệp tin "test.txt" với người khác, ở đây chúng tôi thực hiện chia sẻ với người dùng có địa chỉ email là "truongtlt147@gmail.com". Sau khi thực hiện việc điều tra và phân tích tệp "sync_history.db", chúng tôi tiếp tục phát hiện rằng thông tin chia sẻ dữ liệu đã được ghi nhận lại, cụ thể như Hình 9. Việc này rất có lợi cho công tác điều tra khi tội phạm chia sẻ dữ liệu với một người khác, bằng việc sử dụng thông tin địa chỉ email của người nhận, họ có thể tiếp tục truy tìm những người có liên quan đến đối tượng điều tra.


SQLITE VIEWER

Select table sync_history

FIND BUILD QUERY EXPORT CLEAR FILTERS

#	event_type	file_event_type	file_id	local_path	server_path	other_user	timestamp
1	file	delete	aGL_HBUqXuwAAAAAAAAAXQ	C:\Users\Truong\Dropbox\test.txt	(null)	0	1664979356
2	file	add	aGL_HBUqXuwAAAAAAAAAXg	C:\Users\Truong\Dropbox\test.txt	3096353745:/test.txt	truongtlt147@gmail.com	1664979707

Hình 9. *Thông tin chia sẻ tệp "test.txt" được ghi nhận lại*

3. Kết luận và kiến nghị

Trong bài báo này, chúng tôi đã đưa ra được một quy trình điều tra và phân tích các dữ liệu chứng cứ còn sót lại trong quá trình sử dụng ứng dụng dịch vụ lưu trữ đám mây DropBox trên thiết bị máy tính chạy hệ điều hành Windows 10. Các quá trình như cài đặt ứng dụng, tải dữ liệu lên, tải dữ liệu xuống từ đám mây, xóa dữ liệu cũng như chia sẻ dữ liệu với người khác là những thao tác thường được sử dụng. Việc đưa ra những phân tích về các quá trình trên giúp ích cho các cơ quan chức năng trong quá trình điều tra tội phạm, họ sẽ dựa vào những nội dung mà chúng tôi đưa ra để có thể nhanh chóng lấy được các thông tin bằng chứng còn sót lại trong máy tính của chúng. Từ đó góp phần đẩy nhanh tiến độ của công tác điều tra, cũng như giảm thiểu tỉ lệ tội phạm trong xã hội. Các kết quả đạt được trong bài báo này đều được thực nghiệm trực tiếp với máy chủ DropBox, do đó có thể chứng minh được tính đúng đắn của của quy trình được đề xuất, nên quy trình này có thể làm cơ sở cho các nghiên cứu tiếp theo cũng như đưa ra sử dụng trong các ứng dụng thực tế. Hướng phát triển tiếp theo của nghiên cứu sẽ ứng dụng quy trình này để thực hiện điều tra và phân tích đối với các ứng dụng lưu trữ đám mây khác như OneDrive, GoogleDrive, Box… và trên các thiết bị khác như máy tính chạy hệ điều hành MacOS, hay trên các thiết bị di động.

❖ ***Tuyên bố về quyền lợi:*** *Các tác giả xác nhận hoàn toàn không có xung đột về quyền lợi.*

TÀI LIỆU THAM KHẢO

Choo, K. K. R. (2008). Organised crime groups in cyberspace: A typology. *Trends in Organized Crime*, 270-295.

Choo, K. K. R., & Smith, R. (2008). Criminal Exploitation of Online Systems by Organised Crime Groups. *Asian Journal of Criminology*, 37-59.

Chung, H., Park, J., Lee, S., & Kang, C. (2012). Digital forensic investigation of cloud storage services. *Digital Investigation*, 81-95.

Dykstra, J., & Sherman, A. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, S90-S98.

Grispos, G., Glisson, W. B., & Storer, T. (2013). Using Smartphones as a Proxy for Forensic Evidence Contained in Cloud Storage Services. *IEEE*, 4910-4919.

Gu, Q., & Guirguis, M. (2014). *High Performance Cloud Auditing and Applications.* Springer.

Hale, J. (2013). Amazon Cloud Drive forensic analysis. *Digital Investigation*, 259-265.

Magnet Forensic. (2022, 10 9). *Magnet Forensic*. Retrieved from Magnet Forensic: https://www.magnetforensics.com/products/magnet-axiom/

Martini, B., & Choo, K. K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, 71-80.

Martini, B., & Choo, K. K. R. (2013). Cloud storage forensics: ownCloud as a case study. *Digital Investigation*, 287-299.

Martini, B., & Choo, K. K. R. (2014). Remote Programmatic vCloud Forensics: A Six-Step Collection Process and a Proof of Concept. *IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, (pp. 935-942).

Martini, B., Do, Q., & Choo, K.-K. R. (2015). Conceptual evidence collection and analysis methodology for Android devices, 285-307.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *NIST Special Publication 800-145*.

Microsoft. (2022, 10 9). *Microsoft by the Numbers*. Retrieved from https://news.microsoft.com/bythenumbers/en/windowsdevices

NIST. (2022, 10 9). *National Software Reference Library*. Retrieved from National Software Reference Library: https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl

Quick, D., Martini, B., & Choo, K. K. R. (2014). *Cloud storage forensics.* Syngress, an Imprint of Elsevier.

Service, U. F. (n.d.). *Reforestation, Nurseries, and Genetics Resources*. Retrieved from http://www.rngr.net

Shariati, M., Dehghantanha, A., & Choo, K. K. R. (2016). SugarSync forensic analysis. *Australian Journal of Forensic Sciences*, 95-117.

Shariati, M., Dehghantanha, A., Martini, B., & Choo, K. K. R. (2018). Ubuntu One Investigation: Detecting Evidences on Client Machines. *Syngress*, 429-446.

SQLiteStudio. (2022, 10 9). *SQLiteStudio*. Retrieved from SQLiteStudio: https://sqlitestudio.pl/

Wen, Y., Man, X., Le, K., & Shi, W. (2013). Forensics-as-a-Service (FaaS): Computer Forensic Workflow Management and. *The Fifth International Conferences on Pervasive Patterns and Applications*, (pp. 208-214).

Zawoad, S., Dutta, A. K., & Hasan, R. (2013). SecLaaS: secure logging-as-a-service for cloud forensics. *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, (pp. 219-230).

DIGITAL FORENSIC ANALYSIS OF DROPBOX ON WINDOWS 10 DEVICES

Van Thien Hoang[1], Tran Van Dan Truong[2*], Dang Van Thanh Nhan[3]

[1]Ho Chi Minh City University of Technology, Vietnam

[2]Hahalolo Travel Social Network Joint Stock Company, Vietnam

[3]The Saigon International University, Vietnam

[*]Corresponding author: Tran Van Dan Truong – Email: truongtlt147@gmail.com

Received: October 11, 2022; Revised: July 20, 2023; Accepted: July 27, 2023

ABSTRACT

In an Internet-connected world, computers are increasingly used to access cloud storage services, which allow users to access data anytime, anywhere. However, these devices are targeted by cybercriminals to perform malicious activities, such as data intrusion, malware installation, identity theft, cyber terrorism. As a result, computers are an important source of evidence in investigating crimes. In this article, we investigate the digital forensic of Dropbox applications, a popular cloud storage service, on the Windows 10 operating system platform, one of the most popular and widely used operating systems in the world. We attempted to identify residual data that may be of interest to investigative authorities, such as information generated during logins, uploads, downloads, deletions, and file sharing. The findings as well as the results can help the authorities to easily obtain evidence data from the DropBox application on Windows 10.

Keywords: Cloud storage; digital forensic; dropBox forensic; Windows forensic