Forensic Science International: Digital Investigation 45 (2023) 301568

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

DFRWS 2023 USA - Proceedings of the Twenty Third Annual DFRWS Conference

A study on cloud data access through browser credential migration in Windows environment

Uk Hur [a], Soojin Kang [a], Giyoon Kim [a], Jongsung Kim [a, b, *]

[a] *Dept. of Financial Information Security, Kookmin University, 77 Jeongneung-Ro, Seongbuk-Gu, Seoul, 02707, South Korea*
[b] *Dept. of Information Security, Cryptology and Mathematics, Kookmin University, 77 Jeongneung-Ro, Seongbuk-Gu, Seoul, 02707, South Korea*

ARTICLE INFO

Article history:

Keywords:
Cloud forensics
Credential
Data protection

ABSTRACT

Various user data stored in cloud services for data continuity and efficiency is one of the main collection targets in digital forensic investigation. Some forensic tools collect cloud data based on user account and password, or provide data collection functions based on user credentials stored in the web browser. However, because many web services require additional authentication using user devices to protect user data, access using only the account and password is becoming difficult. In the case of credentials generated by auto-login, it does not work or requires re-authentication when moved to the investigator's device. This is so that other devices cannot utilize the credentials that are kept on the device due to security measures. In this paper, we propose a new method to migrate the credentials stored by the web browser to other devices and effectively utilize them, unlike the forensic method that involves using local credentials. Our analysis revealed that the majority of browsers encrypt and store credentials, so we researched credential decryption methods. We proceeded with the migration; move and encrypt the decrypted credentials to the investigator's device, or move the not encrypted credentials simply. As a result, we conducted credentials migration experiments on a total of 28 browsers, among which we have clarified that migration is possible in all browsers except three that do not store data, such as Tor. We verified that it is possible to log in and collect data on 20 types of web services that are frequently used using migrated credentials. Although the approach we propose is straightforward, it allows for effective and efficient cloud data collection in digital forensic investigation.

© 2023 The Author(s). Published by Elsevier Ltd on behalf of DFRWS All rights reserved. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

Cloud computing describes an environment where information technology (IT) services, such as data storage, networking, and content delivery, can be conducted through servers on the internet Mell and Grance (2011). In the meantime, connected devices including personal computers (PCs), smartphones, tablets, and wearable devices emerged with the development of IT. According to Cisco's research, each person has between 1 and 13 devices and connections, and by 2023, it is expected to have an average of more than 3 devices and connections worldwide Cisco (2020). In an environment where multiple devices are used, if the data is stored in local storage on each device, user cannot access the previous data stored in another device. Therefore, cloud services that allow online synchronization have become good alternatives for users to seamlessly access data across multiple devices. For user convenience, an increasing number of businesses and services that provide ubiquitous and synchronized data are emerging. Thus, a considerable amount of user data, which was previously stored in local storage is moving to cloud storage. Among the several cloud services, cloud storage where data are stored, has become one of the main targets in digital forensic investigation. In addition to storing data, cloud storage services like Google Drive, Dropbox, OneDrive, and iCloud also provide several other features like emailing, document editing, file sharing, synchronization, and real-time sharing. These services can be accessed through exclusive programs or web browsers; even today, most tasks can be done with a single browser. However, as the data are stored in a cloud, obtaining user data for digital forensic investigations is getting more and more challenging. When users use cloud storage, it is difficult to determine the exact storage location of the data, and even if the location is identified, collecting the data is challenging.

[*] Corresponding author. Dept. of Financial Information Security, Kookmin University, 77 Jeongneung-Ro, Seongbuk-Gu, Seoul, 02707, South Korea.
E-mail addresses: gjdnr123@kookmin.ac.kr (U. Hur), szin31@kookmin.ac.kr (S. Kang), gi0412@kookmin.ac.kr (G. Kim), jskim@kookmin.ac.kr (J. Kim).

https://doi.org/10.1016/j.fsidi.2023.301568

2666-2817/© 2023 The Author(s). Published by Elsevier Ltd on behalf of DFRWS All rights reserved. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Furthermore, user data can be encrypted, and data collection can be depending on national policies. An intriguing alternative to realistic data collection is the use of credentials, including passwords. For instance, the user password stored in the Chrome browser can be obtained by using *NirSoft's ChromePass* Sofer (2008); and the use of this password can lead to the acquisition of additional data on the websites. However, some websites, like Google, demand additional authentication through a device owned by the user, to log in, making it impossible to access data using just a password. Because of this additional authentication, the credentials[1] generated through auto-login do not work on other devices or require authentication again. As a result, the collected data are not available on the investigator's device. Furthermore, the use of credentials is limited when possession-based or biometric-based authentication is required in addition to the password, which is a knowledge-based authentication factor in, multi-factor authentication. To overcome this limitation, there are various techniques such as cloning a PC for data acquisition, but this approach requires a considerable amount of time and resources. When connecting to a network using a cloned PC, there are concerns about malware infection through the internal network. Furthermore, if the OS and boot images are separated on multiple disks, all of them must be cloned. Therefore, finding an efficient method for data acquisition is our main focus. During our research, we found that data on the trusted device, such as additional authentication through the browser, exists encrypted in a *Cookie*. We expect that if the encrypted data stored in the cookie can be used in other environments, it will be possible to bypass the additional authentication and log in. Therefore, we study how to use cookies by modifying and migrating various data, and consequently propose a data collection method based on this. In this paper, we describe a method to collect the data stored in various services by migrating the main data of various web browsers and bypassing the multi-factor authentication procedure in a more effective way than the full cloning method.

1.1. Our contributions

In this paper, we propose a method of migrating browser data to an investigator device to collect user data from websites using stored credentials in a Windows PC environment. Migrated credentials enable to bypass the authentication process and successfully access cloud-based web services. As a result of our study, migration is possible with simple data movement in some browsers. However, data are typically encrypted in most browsers so that they cannot be used on other devices. To use encrypted credentials on other devices, it is necessary to decrypt and regenerate the credentials to fit other devices. We discovered that 25 different browsers, including some that require data modification, successfully migrate data. Migrated browsers can utilize credentials such as auto-login as before. Overall, to use migrated credentials for digital forensic investigation, we have enumerated websites that can utilize credentials and user data that can be effectively obtained. The following presumptions are necessary to use this study.

o Preparation and Assumption.
 1) The target site's Auto-login or Trust-browser function is enabled.
 2) The live system is accessible.
  2-1) The live system is inaccessible.
   - Collection of Registry Hives (SYSTEM, SECURITY) is required.
   - The user's password is required for Windows account login.

o Impacts on digital forensic investigations (our results).
1) We discovered that data migration is possible in 25 popular browsers running in the Windows environment. Each browser is developed based on three browsers, and we found that browsers developed based on the same browser can easily migrate data in the same manner.
2) We propose a data regeneration method to use encrypted data when it is moved to another device based on the results of our browser migration experiment. We found the encrypted data in a browser developed based on the Chromium browser and showed that the data could be regenerated through decryption and encryption using a data protection application programming interface (DPAPI). Finally, we confirmed that the regenerated data behave exactly the same as before on the migrated device.
3) Through the website credentials, we obtained users' chat history and media data stored in the cloud and showed that it is possible to track the users' real-time locations according to web services.

o Our framework for browser credential migration

We propose a framework for migrating browser credentials (Fig. 1). The proposed framework migrates credentials inside browser data.

2. Background

2.1. How websites remember users

User authentication on each website is implemented by a *Session/Cookie* and *Token* method. The *Session/Cookie* method sends the user ID of the session to the server, checks whether the ID exists in the database (DB) stored on the server, and proceeds with the user authentication Grassi et al. (2016). Credentials such as the session ID are stored in *Cookie* according to settings, and based on this, auto-login is implemented. Meanwhile, the *Token* method conducts a signature algorithm on the user authentication data and related information. Examples of web token methods include JSON web token Jones et al. (2015) and OAuth Hardt (2012). The *Token* is stored on the user's computer, and when the browser sends the *Token* to the server, the server verifies that the *Token* is valid. When a user activates auto-login on a website, an auto-login token is generated and stored on the PC, and based on this, the auto-login is implemented. Auto-login is recommended to be performed on the user's trusted device and is provided under various names such as **Remember me** or **Keep me signed in** (Fig. 2). To properly authenticate on a website, the user does not need to input an ID, and password each time by using the auto-login method, which keeps the credentials in the browser on the device where the user logged in.

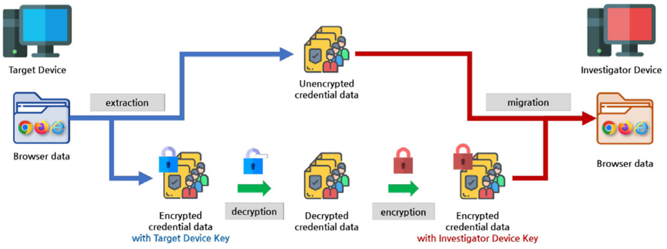
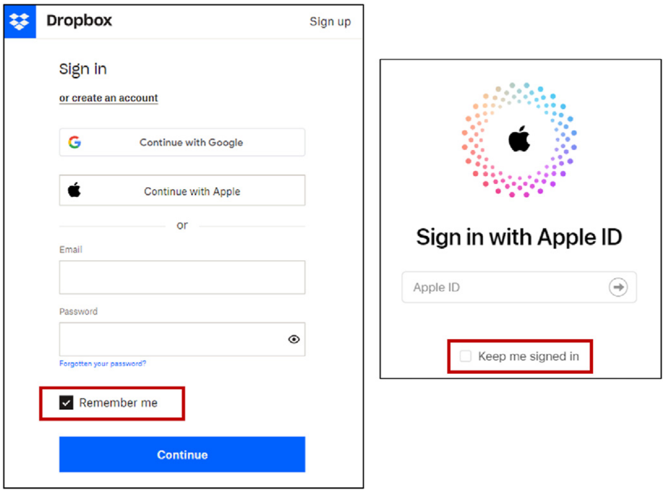

Target Device
Investigator Device
extraction
Unencrypted credential data
migration
Browser data
Browser data
Encrypted credential data with Target Device Key
decryption
Decrypted credential data
encryption
Encrypted credential data with Investigator Device Key

Fig. 1. Our framework for browser credential migration.

[1] Data that can identify and authenticate users is called credentials Grassi et al. (2020).



Dropbox Sign up

Sign in

or create an account

Continue with Google

Continue with Apple

or

Email

Password

Forgotten your password?

☑ Remember me

Continue

Sign in with Apple ID

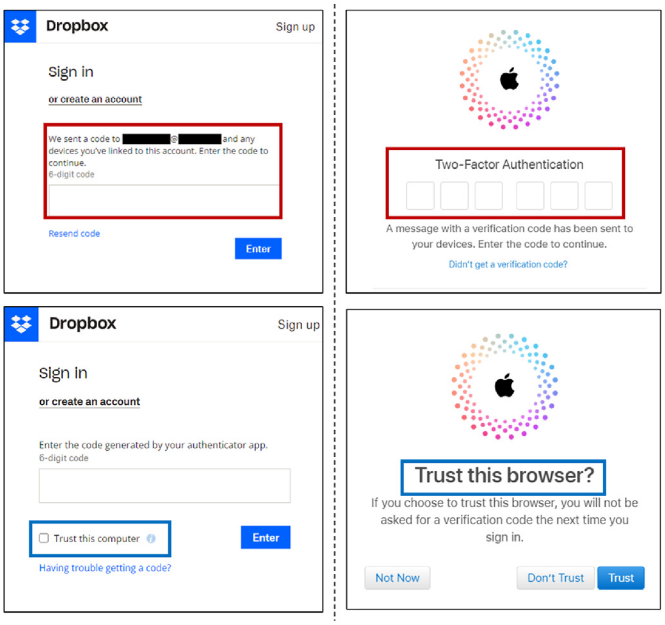
Apple ID

□ Keep me signed in

Fig. 2. Auto-login settings screen of Dropbox and Apple's iCloud website.

Moreover, certain websites recommend that users to use additional authentication (multi-factor authentication, 2-step verification, or 2-factor authentication) as well as credentials to protect user data. The additional authentication process is slightly different for each website. In general, it is done by sending an authentication number to a user-controlled email and entering it, or by sending the authentication number to another trusted device owned by the user and utilizing that as a token (Fig. 3).

For user convenience, certain websites provide an option to omit additional authentication. For instance, options such as **Trust the computer** or **Trust the browser?** Are options that trust the browser or environment in which the user is login in, and the user only needs to enter the ID and password. However, when a user logs in for the first time with additional authentication using the aforementioned option, the related data are stored in the user's PC. Therefore, it is not necessary to conduct additional authentication when logging in later.



Dropbox Sign up

Sign in

or create an account

We sent a code to [redacted]@[redacted] and any devices you've linked to this account. Enter the code to continue.

6-digit code

Resend code

Enter

Two-Factor Authentication

A message with a verification code has been sent to your devices. Enter the code to continue.

Didn't get a verification code?

Dropbox Sign up

Sign in

or create an account

Enter the code generated by your authenticator app.

6-digit code

□ Trust this computer

Enter

Having trouble getting a code?

Trust this browser?

If you choose to trust this browser, you will not be asked for a verification code the next time you sign in.

Not Now Don't Trust Trust

Fig. 3. 2-Step Verification of Dropbox and Apple's iCloud website.

2.2. DPAPI

DPAPI is an application programming interface (API) provided for data protection in Windows operating systems since Windows 2000 Satran et al. Particularly, the DPAPI is included in CryptoAPI and consists of two functions: *CryptProtectData* and *CryptUnprotectData*. The DPAPI uses a device-dependent encryption key such that only a user with the same Windows logon credentials as the user who encrypted the data can decrypt the data. As a result, data encrypted with DPAPI cannot be decrypted when moved to another device. Because, when data are protected using DPAPI, information used for encryption and encryption key are encrypted and stored together. The Data Encryption Key (DEK), a random data, is generated to encrypt the data. The DEK is encrypted and stored as a master key (Key Encryption Key, KEK) dependent on a Windows account. A DPAPI binary large object (DPAPI BLOB), which refers to the data encrypted using the DPAPI, has a particular structure and is encoded with ASN.1 (Fig. 4).

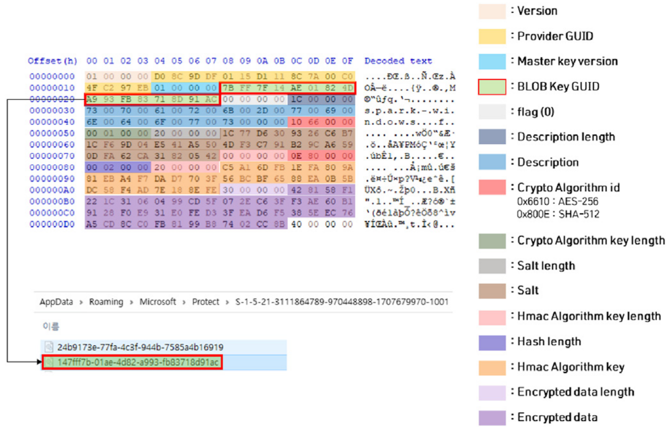
The blob key data (DEK) is stored in the following paths with the globally unique identifier (GUID) of each key value as the file name.

o %AppData%\Microsoft\Protect\<UserSID>
o %windir%\system32\Microsoft\Protect\<UserSID>

The decryption of encrypted data using the DPAPI should be preceded by a KEK acquisition and DEK decryption. The KEK is created based on the Windows account, thus if it is possible to acquire the memory of the live system, the KEK can also be acquired through a tool such as the mimikaz Delpy (2020). In particular, the DEK can be acquired through the data in both the *Protect path* and the *system32 path*. Additionally, the DataProtectionDecryptor Sofer (2017), a tool that decrypts data encrypted using DPAPI, exists. Fig. 5 shows the entire operation process of the DPAPI.

3. Related work

With the emergence of various cloud services, various data collection studies on the use of exclusive applications and web browsers are being performed. For example, Chung et al. analyzed Amazon S3, Google Docs, Dropbox, and Evernote, which are cloud storage services that store and manage data in the cloud Chung et al. (2012). Specifically, in this study, to acquire cloud data, the user ID and password and the issuance of a seizure warrant were emphasized. They specifically obtained and arranged the artifacts produced by each application's use in the Windows, macOS, iOS, and Android environments, assuming the aforementioned



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0  ....ÐŒ.ß..Ñ.Œz.À
00000010  4F C2 97 EB 01 00 00 00 7B FF 7F 14 AE 01 82 4D  OÂ—ë....{ÿ..®.‚M
00000020  A9 93 FB 83 71 8D 91 AC 00 00 00 00 1C 00 00 00  ©"ûƒq.'¬........
00000030  73 00 70 00 61 00 72 00 6B 00 2D 00 77 00 69 00  s.p.a.r.k.-.w.i.
00000040  6E 00 64 00 6F 00 77 00 73 00 00 00 10 66 00 00  n.d.o.w.s....f..
00000050  00 01 00 00 20 00 00 00 1C 77 D6 30 93 26 C6 B7  .... ....wÖ0"&Æ·
00000060  1C F6 9D 04 E5 41 A5 50 4D F3 C7 91 B2 9C A6 59  .ö..åA¥PMóÇ'²œ¦Y
00000070  0D FA 62 CA 31 82 05 42 00 00 00 00 0E 80 00 00  .úbÊ1‚.B.....€..
00000080  00 02 00 00 20 00 00 00 C5 A1 6D FB 1E FA 80 9A  .... ...Å¡mû.ú€š
00000090  81 EB A4 F7 DA D7 70 3F 56 BC BF 65 88 EA 0B 5B  .ë¤÷Ú×p?V¼¿eˆê.[
000000A0  DC 58 F4 AD 7E 18 8E FE 30 00 00 00 42 81 58 F1  ÜXô.~.Žþ0...B.Xñ
000000B0  22 1C 31 06 04 99 CD 5F 07 2E C6 3F F3 AE 60 B1  ".1..™Í_..Æ?ó®`±
000000C0  91 28 F0 E9 31 E0 FE D3 3F EA D6 F5 38 5E EC 76  '(ðé1àþÓ?êÖõ8^ìv
000000D0  A5 CD 8C C0 FB 81 99 B8 74 02 CC 8B 40 00 00 00  ¥ÍŒÀû.™¸t.Ì‹@...
```

AppData › Roaming › Microsoft › Protect › S-1-5-21-3111864789-970448898-1707679970-1001

이름

24b9173e-77fa-4c3f-944b-7585a4b16919

147fff7b-01ae-4d82-a993-fb83718d91ac

Fig. 4. Structure of the data encrypted using the DPAPI.

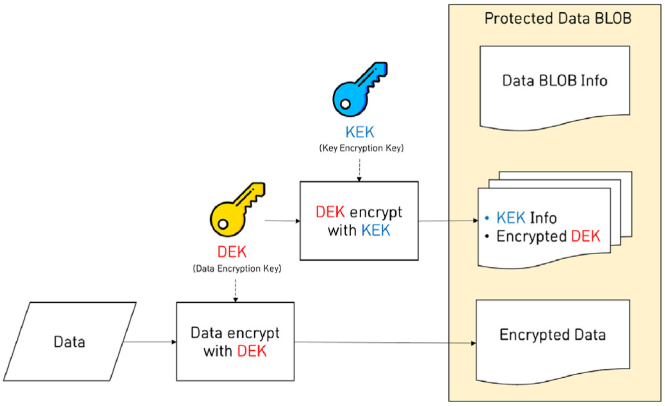


Fig. 5. The operation process of the DPAPI.

environment. However, as described in the paper, it is challenging to obtain the user ID and password, and the environment for obtaining them is a limited assumption. In addition, Quick et al. proposed a method to collect data without obtaining the user ID and password using the virtual forensic computing software, which utilizes the user credentials Quick and Choo (2014). They checked user data stored in Google Drive through synchronized account information. Furthermore, cho et al. conducted a study to log in to a user account using tokens generated for user authentication during auto-login in an Android environment Cho et al. (2018). They collected the credentials of Starbucks applications and anonymous social networking applications well-known in Korea and performed a case study to obtain the user data from the server. Roussev et al. investigated data collection methods for four different kinds of cloud storage: Google Drive, Dropbox, Onedrive, and Box Roussev et al. (2016a,b). They acquired the data in the storage by utilizing the API provided by the cloud storage and proposed a using method for digital forensic investigations. Yang et al. have enhanced collecting method by utilizing the suggested API Yang et al. (2022). They proposed a hybrid data acquisition method using both open and internal APIs, and based on this, improved the cloud data acquisition method. Moussa et al. proposed a model for cloud forensics Moussa et al. (2019). They outlined the limitations of the previously suggested cloud forensic model and suggested an approach to overcome them. In addition, they examined how well the cloud forensics process model requirements were followed via a survey. These articles undoubtedly share aspects with our paper, such as the usage of user credentials or cloud-based data acquisition. However, there is a unique distinction in terms of credentials, which is the focus of this paper. Prior research assumed that the user ID and password were collected or cloned credentials for auto-login. However, in this paper, we focus on securing and utilizing credentials. Therefore, it is anticipated that our study's findings will complement those of earlier research.

4. Methodology of browser data migration

In general, browsers store various user data such as visit history, search history, and credentials. In this paper, we aim to log in from other devices by using certain credentials among various data. The method of storing credentials may be different for each browser. As a result, we propose a generalized browser credential utilization method. More precisely, the methodology we performed in this paper is as follows.

4.1. Data collection step

Browser data operating in the Windows environment is stored in two locations: one is where the browser is installed, and the other is a subpath of %Userprofile%\AppData. Except for information on program execution and setup, all the data stored in the two paths mentioned above are acquired. Subsequently, the collected data are inserted into other devices. If the user has enabled synchronization, the rest of the data can be regenerated by successful auto-login using the credentials. However, in some cases, synchronization may not be set, and there may be organizationally linked data for credential use. Therefore, we aim to collect all data for effective analysis.

4.2. Data migration step

The collected data from the target device is inserted into another device (e.g., an investigator device) and the result is adequately examined. Note that prior to installing the browser on the investigator device during migration, it is crucial to check the version of the browser installed on the target device. Particularly, depending on the version, data might be not compatible as browser updates and data structures change. Therefore, to prevent compatibility issues, the investigator device should use the same or a similar version of the browser as the target device. Our experiments have shown that if there are little version changes, none of the browsers cause problems. However, credentials could not be useable if the main version is changed because of incompatibility issues. When the browser is ready, the basic migration can be completed by inserting the collected data. Following this, whether or not auto-login is possible depends on the browser's security policy for credentials. In particular, moved credentials worked as expected for browsers with weak security rules. More precisely, the study on such browsers is achieved in this step. However, if the credentials do not operate normally, the next **Data analysis and regeneration** step should be conducted. As a result of our study, most browsers required the following additional processes to utilize credentials.

4.3. Data analysis and regeneration step

In the data analysis step, credentials are identified within the collected data, and how to use them is studied. Credentials are usually stored as cookies or tokens in the form of plaintext or encrypted text. First, data that is inferred as a credential is classified through the signature value and extension; encrypted data are also classified as an analysis target. For the classified data, we proceed to identify the structure and format of the detailed data. To evaluate whether plaintext data can be modified, it should specifically be checked for information on the device and information on user credentials. However, as a result of our study to date, plaintext data can be migrated without modification. More so, when there is a browser that encrypts credentials, we discovered the encryption process through reverse engineering. We confirmed that browsers use different encryption keys depending on the PC through reverse engineering. Therefore, when migrating encrypted data, a regeneration process is required to decrypt the data and re-encrypt it with the target device key.

4.4. Verification step

We examine whether auto-login is possible using existing or regenerated credentials. The successful migration of the auto-login previously set on the target device to the investigator device is confirmed through this process. If auto-login is working on the investigator device, verify whether the synchronization account that exists in each browser is also operating normally. Next, when synchronization is operating normally, we collect additional data and conduct real-time monitoring. As a result, we determined the types of information that can be acquired by using credentials for each browser and each website. However, if auto-login is not activated, we decided that the migration failed and moved to the **Data analysis and regeneration** step and reanalyzed.

5. Browser data migration process

Based on the data of StatCounter, which provides web traffic analysis information, we conducted an experiment on browser data migration for a total of 27 browsers with high usage operating in a Windows environment as of 2022 StatCounter (2022). In particular, the browsers we selected for our study were all developed based on Chromium, Firefox, and Internet Explorer (Fig. 6). In addition, in the case of browsers that operate only in incognito mode, including Tor browser, migration is not possible because user data is not saved.

5.1. Chromium-based browser

This is a browser developed based on the Chromium browser, an open-source browser project developed by Google (Google). Representative browsers include Google's Chrome and Microsoft Edge, officially released in January 2020 support (c). Interestingly, the majority of the most popular browsers used today were built using the Chromium, except for Firefox and Safari used in Apple OS.

5.2. Firefox-based browser

This is a browser developed based on the Mozilla Foundation's open-source web browser, Firefox Mozilla. Representative browsers include the Firefox browser and Tor browser which is primarily used to access the dark web.

5.3. Internet Explorer-based browser

This is a browser developed based on Internet Explorer provided by default in Windows. Particularly, the development of Internet Explorer was stopped after Windows' default browser was changed to Chromium-based Edge. Representative browsers include Internet Explorer 11, the last version before development was terminated, and the Edge legacy browser developed later. Intriguingly, Internet Explorer-based browsers are still used to access services developed long ago.

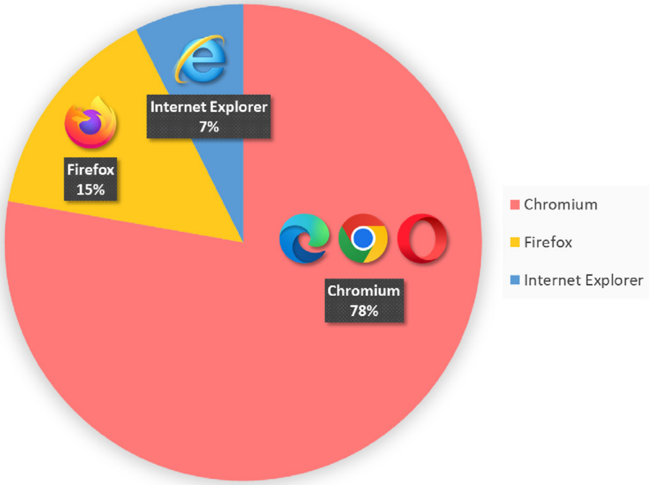


Fig. 6. Classification of types by browser.

As a result of our study, browsers based on the same browser have similar data structures. Furthermore, data migration was possible in the same way. In particular, we discovered six types of browsers that can be migrated only by simple data migration; 19 types of browsers that need to be migrated after modifying data; and two types of browsers that operate only in incognito mode and do not store data. Additionally, all browsers that required data modification were Chromium-based, and the only browsers that could be transferred were those that relied on Firefox and Internet Explorer. Table 1 shows the data migration experiment result for each browser.

Meanwhile, in cases where migration is possible by moving data without suitable modification, the migration process is completed simply by collecting files and subsequently moving them to another device. Thus, we describe the detailed process of data migration of Chromium-based browsers that require analysis and modification of the data. The entire process of browser migration is shown in Fig. 7.

5.4. Migration method for chromium-based browser credentials

5.4.1. Decryption method for chromium-based browser credentials

The user data path of the Chromium-based browser (CBB) is as follows. Depending on the CBB, data can exist in either path, or both paths. If both paths exist, the location where the “User Data” directory exists is the user data path.

o %LocalAppData%\[Browserprovidername]\ [Browsername]
o%AppData%\[Browserprovidername]\[Browsername]

Moreover, under “User Data” of the CBB, data are divided and stored for each browser account. The data of the default account is stored in the “Default” folder, and the data of the accounts registered by the user are stored in the “Profile *N*” folder sequentially. Credentials used in each user account are stored in a different location depending on the Chromium version. Particularly, depending on the Chromium version, credentials are stored in the “Default”, “Profile *N*” folder, otherwise these are stored under “Default\Network”, “Profile *N*|Network”. As for the Chromium development version 80.0.3947.0, credentials are stored within a database in the form of a SQLite database and encrypted in a separate way. The encryption process for each version is as follows.

5.4.1.1. Case 1. version 80 and lower versions.

Fig. 8 is the encrypted data stored in the old version cookies.

All data stored in each column is in the form of a DPAPI blob. The DPAPI blob can be decrypted in different ways depending on the state of the PC to be collected. Specifically, if the target device is available and a Windows user account is accessible, decryption is possible without the need for any additional information through the *CryptUnprotectData* function provided by Windows. Otherwise, additional information is required to decrypt the DPAPI blob: Two folders (see. Section 2.2) where the encrypted key is stored are the Registry Hives (SYSTEM, SECURITY) files for using master key information, and the user login information. Additionally, when the DPAPI BLOB is decrypted using these data, the plaintext of the data needed to activate the session can be obtained.

Table 1
List of browsers used in the migration experiment and results.

Browser name	type	version	User Data path	Migration
Avast Secure Browser	Chromium	108.0.19667.125	%LocalAppdata%\AVAST Software\Browser	✓
Brave	Chromium	109.1.47.171	%LocalAppdata%\BraveSoftware\Brave-Browser	✓
Chromium	Chromium	111.0.5501.0	%LocalAppdata%\Chromium	✓
Chrome	Chromium	108.0.5359.125	%LocalAppdata%\Google\Chrome	✓
Comodo Dragon	Chromium	108.0.5359.95	%LocalAppdata%\Comodo\Dragon	✓
Epic Privacy Browser	Chromium	104.0.5112.81	Incognito mode only	–
FlashPeak Slimjet (64 bit)	Chromium	107.0.5304.62	%LocalAppdata%\Slimjet	✓
Iridium	Chromium	2022.04	Incognito mode only	–
Maelstrom	Chromium	42.0.1.36	%LocalAppdata%\Maelstrom	✓
Edge	Chromium	109.0.1518.52	%LocalAppdata%\Local\Microsoft\Edge	✓
Opera	Chromium	94.0.4606.38	%Appdata%\Opera Software\Opera Stable	✓
Tungsten	Chromium	2.14	%Appdata%\Tungsten	✓
UC Browser	Chromium	6.0.1308.1016	%LocalAppdata%\Maxthon\Application	✓
Vivaldi	Chromium	5.6.2867.50	%LocalAppdata%\Vivaldi	✓
Yandex	Chromium	23.1.0.2539	%LocalAppdata%\Yandex\YandexBrowser	✓
Whale	Chromium	3.18.154.7	%LocalAppdata%\Naver\Naver Whale	✓
360 Safe Browser	Chromium	13.1.6410.0	%Appdata%\360se6	✓
QQ Browser	Chromium	11.5	%LocalAppdata%\Tencent\QQBrowser	✓
Coc Coc	Chromium	114.0.140	%LocalAppdata%\CocCoc\Browser	✓
Sogou Explorer	Chromium	11.0.1.34700	%Appdata%\SogouExplorer\Webkit	✓
Maxthon	Chromium	6.2.0.2000	%LocalAppdata%\Maxthon\Application	✓
Firefox	Firefox	108.0.1	%LocalAppdata%\Maxthon\Application	✓
Comodo ice dragon	Firefox	65.0.2.15	%LocalAppdata%\Comodo\IceDragon	✓
SeaMonkey	Firefox	2.53.14	%LocalAppdata%\Mozilla\SeaMonkey	✓
Pale Moon	Firefox	31.4.2	%LocalAppdata%\Moonchild Productions\Pale Moon	✓
Tor	Firefox	12.0.4	Incognito mode only	–
Internet Explorer 11	IE	11.0.18362.997	%LocalAppdata%\Microsoft\Windows	✓
Edge Lagacy	IE	44.19041.610.0	%LocalAppdata%\Microsoft\Windows	✓

*'✓': Successfully migrated, '-': Supports only incognito mode and does not save data.

5.4.1.2. Case 2. version 80 and upper versions. Fig. 9 is the encrypted data in a changed form.

Encrypted data of version 80 or upper is stored as BLOB data starting after the string "v10".

As a result of our analysis, the data are encrypted with the AES-GCM. More specifically, the encryption key used for encryption is a 32-byte random value generated through pseudorandom number generator (PRNG), and the encryption key is encrypted and stored in the "LocalState" file in the "User Data" directory. The "LocalState" file is in JSON format, and the encryption key is stored in JSON object name "encrypted_key". The value stored in "encrypoted_key" is a DPAPI blob that has been Base64 encoded. Therefore, if the "encrypted_key" value is decrypted in the same way as Case 1 after Base64 decoding, it is possible to obtain an encryption key (Fig. 10).

Furthermore, the GCM nonce uses the upper 12-bytes of the encrypted data and the lower 16-bytes are the GCM tag. By using the acquired encryption key and nonce, encrypted data can be decrypted.

5.4.2. Regeneration method for chromium-based browser credentials

To decrypt the DPAPI blob, the Windows account information used during encryption is required. As a result, it is impossible to decrypt data simply by moving data (Fig. 11).

For migration, it is necessary to decrypt the DPAPI blob in advance on the target device. After moving the decrypted data to the investigator device, the migration is completed by encrypting the data using DPAPI in the investigator device (Fig. 12).

5.4.2.1. Case 1. version 80 and lower versions. The decrypted data stored in each column is encrypted with a *CryptProtectData* function provided by Windows. There is no need for additional information for this process, which is carried out on the investigator device. Fig. 13 is the result of running the browser after encrypting the actual data. Additionally, we confirmed that using our migration strategy, it is possible to successfully log in from a device that has never done so before.

5.4.2.2. Case 2. version 80 and upper versions. Migration from version 80 consists of the following process. First, generate a random GCM key and nonce. Afterwards, the decrypted data is encrypted with the GCM key and nonce. In particular, the GCM key used for encryption is encrypted with the *CryptProtectData* function provided by Windows, Base64 encoded and stored in "LocalState". There was no additional validation of the plaintext data, GCM key, or nonce. Therefore, migration is possible by decrypting only the GCM key in the **Data collection** step and encrypting only the GCM key after moving all data.

5.5. Migration method for other browsers' credentials

Browsers based on Firefox and Internet Explorer do not have encrypted credentials. Therefore, migration was possible with simple data movement. In particular, the migrated credentials contain information about computers, such as encrypted Security identifiers (SID). To modify the encrypted data, a protocol analysis with the web page is necessary. In this paper, the migration process was carried out without modifying the encrypted data. Accordingly, when the migrated credentials are used, the session operates as if it were operating on the target device. However, there is a possibility that the session could be terminated if the device information is incompatible when upgrading the session on the target device or terminating the session. Additionally, migrated credentials will not be available even after the expiration time of the session. As a result of our study, properly migrated credentials were able to use all functions such as access history, auto-complete data, and stored passwords in addition to the used auto-login. Further, it should be noted that if the browser's synchronization feature is activated, the user data may also be collected after the point of collection.

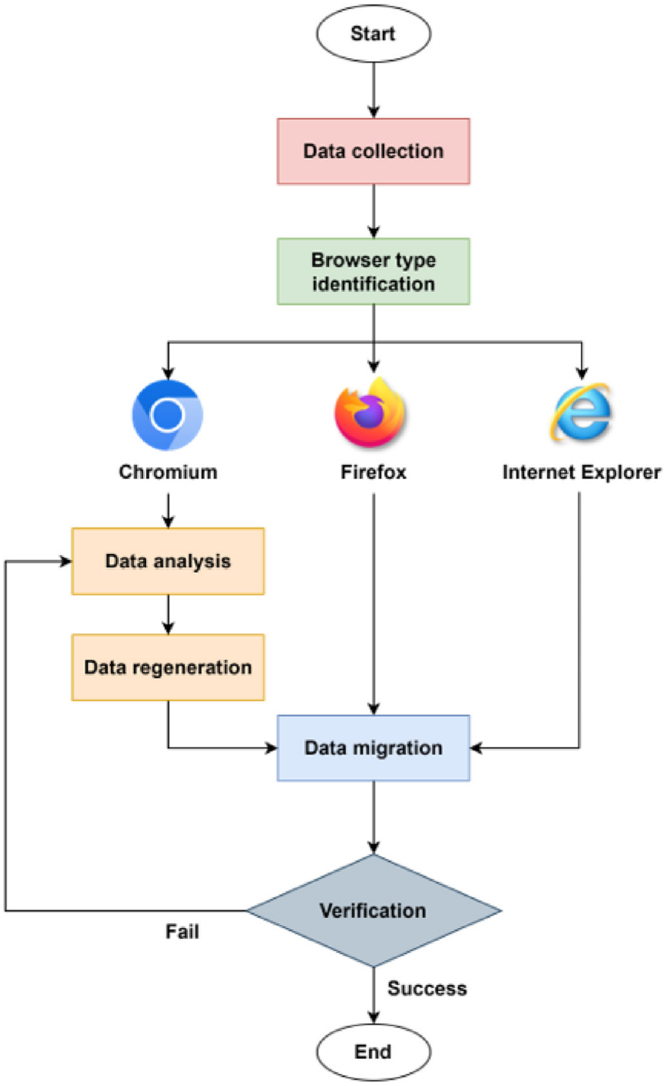
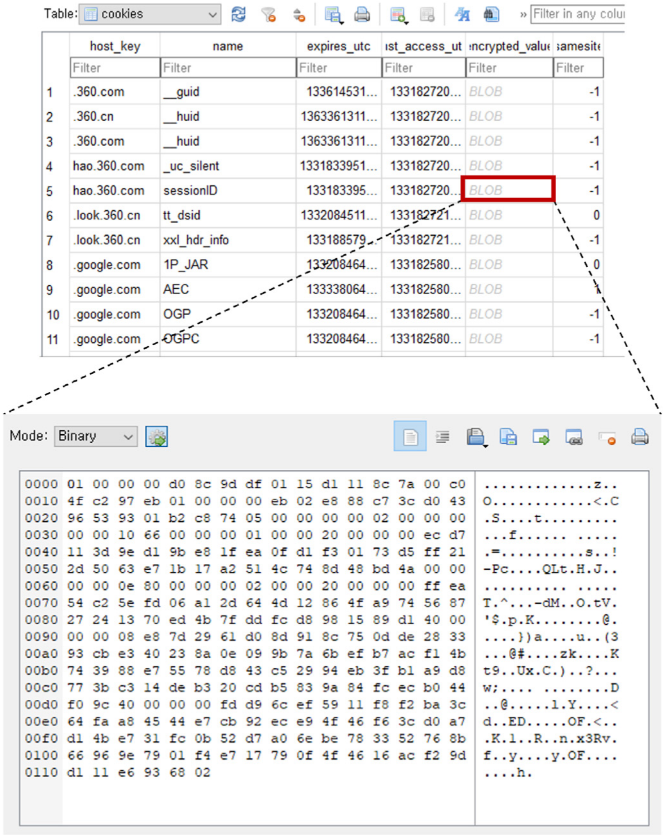


Fig. 7. The entire process of browser migration.

6. Utilization of browser data migration in digital forensic investigations

We can effectively collect the data stored in the cloud from various services through the credentials stored in the browser that has completed migration. Depending on the service provided by the website, collectible data may contain a variety of user information, including emails that users exchange and files stored in the cloud. More so, it is even possible to track user locations through real-time location information on user devices provided on the homepage, such as Microsoft, Google, and Apple. Furthermore, if synchronization is set for each browser, even after the data collection point, the data generated through another device (not the target device) with synchronization enabled can be additionally obtained. Finally, we summarized elements that can be used in digital investigation by the website with credentials obtained through browser data migration. The list of websites that can be auto-logged into is as follows (Table 2).

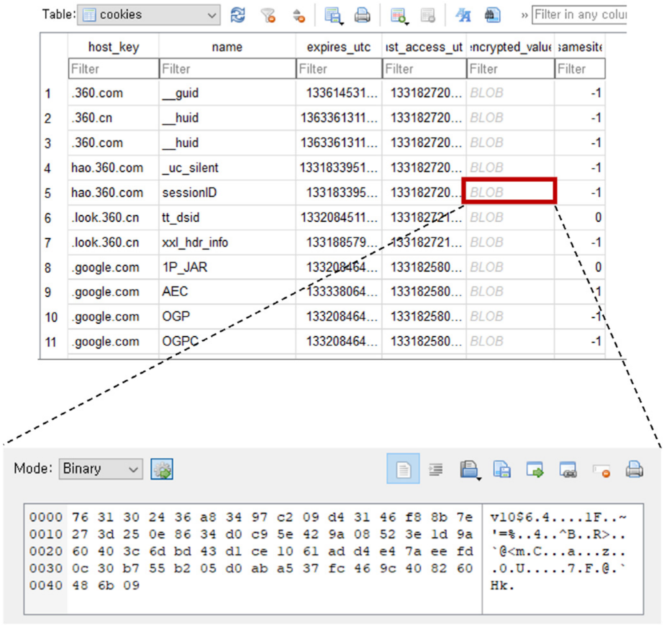
6.1. Browser synchronization account



	host_key	name	expires_utc	ıst_access_ut	ıncrypted_valuı	;amesitı
	Filter	Filter	Filter	Filter	Filter	Filter
1	.360.com	__guid	133614531...	133182720...	BLOB	-1
2	.360.cn	__huid	1363361311...	133182720...	BLOB	-1
3	.360.com	__huid	1363361311...	133182720...	BLOB	-1
4	hao.360.com	_uc_silent	1331833951...	133182720...	BLOB	-1
5	hao.360.com	sessionID	133183395...	133182720...	BLOB	-1
6	.look.360.cn	tt_dsid	1332084511...	133182721...	BLOB	0
7	.look.360.cn	xxl_hdr_info	133188579...	133182721...	BLOB	-1
8	.google.com	1P_JAR	133208464...	133182580...	BLOB	0
9	.google.com	AEC	133338064...	133182580...	BLOB	1
10	.google.com	OGP	133208464...	133182580...	BLOB	-1
11	.google.com	OGPC	133208464...	133182580...	BLOB	-1

```
0000 01 00 00 00 d0 8c 9d df 01 15 d1 11 8c 7a 00 c0   .............z..
0010 4f c2 97 eb 01 00 00 00 eb 02 e8 88 c7 3c d0 43   O............<.C
0020 96 53 93 01 b2 c8 74 05 00 00 00 00 02 00 00 00   .S....t.........
0030 00 00 10 66 00 00 00 01 00 00 20 00 00 00 ec d7   ...f...... .....
0040 11 3d 9e d1 9b e8 1f ea 0f d1 f3 01 73 d5 ff 21   .=..........s..!
0050 2d 50 63 e7 1b 17 a2 51 4c 74 8d 48 bd 4a 00 00   -Pc....QLt.H.J..
0060 00 00 0e 80 00 00 00 02 00 00 20 00 00 00 ff ea   .......... .....
0070 54 c2 5e fd 06 a1 2d 64 4d 12 86 4f a9 74 56 87   T.^...-dM..O.tV.
0080 27 24 13 70 ed 4b 7f dd fc d8 98 15 89 d1 40 00   '$.p.K........@.
0090 00 00 08 e8 7d 29 61 d0 8d 91 8c 75 0d de 28 33   ....})a....u..(3
00a0 93 cb e3 40 23 8a 0e 09 9b 7a 6b ef b7 ac f1 4b   ...@#....zk....K
00b0 74 39 88 e7 55 78 d8 43 c5 29 94 eb 3f b1 a9 d8   t9..Ux.C.)..?...
00c0 77 3b c3 14 de b3 20 cd b5 83 9a 84 fc ec b0 44   w;.... ........D
00d0 f0 9c 40 00 00 00 fd d9 6c ef 59 11 f8 f2 ba 3c   ..@.....l.Y....<
00e0 64 fa a8 45 44 e7 cb 92 ec e9 4f 46 f6 3c d0 a7   d..ED.....OF.<..
00f0 d1 4b e7 31 fc 0b 52 d7 a0 6e be 78 33 52 76 8b   .K.1..R..n.x3Rv.
0100 66 96 9e 79 01 f4 e7 17 79 0f 4f 46 16 ac f2 9d   f..y....y.OF....
0110 d1 11 e6 93 68 02                                 ....h.
```

Fig. 8. Chromium cookie data of the version 80 and lower.

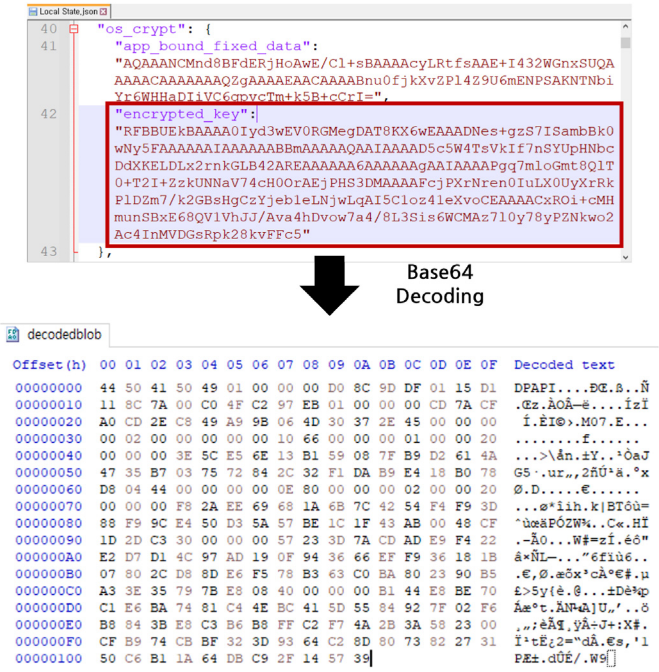


	host_key	name	expires_utc	ıst_access_ut	ıncrypted_valuı	;amesitı
	Filter	Filter	Filter	Filter	Filter	Filter
1	.360.com	__guid	133614531...	133182720...	BLOB	-1
2	.360.cn	__huid	1363361311...	133182720...	BLOB	-1
3	.360.com	__huid	1363361311...	133182720...	BLOB	-1
4	hao.360.com	_uc_silent	1331833951...	133182720...	BLOB	-1
5	hao.360.com	sessionID	133183395...	133182720...	BLOB	-1
6	.look.360.cn	tt_dsid	1332084511...	133182721...	BLOB	0
7	.look.360.cn	xxl_hdr_info	133188579...	133182721...	BLOB	-1
8	.google.com	1P_JAR	133208464...	133182580...	BLOB	0
9	.google.com	AEC	133338064...	133182580...	BLOB	1
10	.google.com	OGP	133208464...	133182580...	BLOB	-1
11	.google.com	OGPC	133208464...	133182580...	BLOB	-1

```
0000 76 31 30 24 36 a8 34 97 c2 09 d4 31 46 f8 8b 7e   v10$6.4....1F..~
0010 27 3d 25 0e 86 34 d0 c9 5e 42 9a 08 52 3e 1d 9a   '=%..4..^B..R>..
0020 60 40 3c 6d bd 43 d1 ce 10 61 ad d4 e4 7a ee fd   `@<m.C...a...z..
0030 0c 30 b7 55 b2 05 d0 ab a5 37 fc 46 9c 40 82 60   .0.U.....7.F.@.`
0040 48 6b 09                                          Hk.
```

Fig. 9. Chromium cookie data of the version 80 and upper.

Each browser provides a function to synchronize data through a user account. When users use the synchronization function, data including access history from various devices can be integrated and managed. Furthermore, it is possible to additionally collect data on user actions that take place after the data collection point and data produced by another device.



```
"os_crypt": {
  "app_bound_fixed_data":
  "AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAcyLRtfsAAE+I432WGnxSUQA
  AAAACAAAAAAAQZgAAAAEAACAAAABnu0fjkXvZPl4Z9U6mENPSAKNTNbi
  Yr6WHHaDIiVC6gpvcTm+k5B+cCrI=",
  "encrypted_key":
  "RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAADNes+gzS7ISambBk0
  wNy5FAAAAAAIAAAAAABBmAAAAAQAAIAAAAD5c5W4TsVkIf7nSYUpHNbc
  DdXKELDLx2rnkGLB42AREAAAAAA6AAAAAAgAAIAAAAPgq7mloGmt8QlT
  0+T2I+ZzkUNNaV74cH0OrAEjPHS3DMAAAAFcjPXrNren0IuLX0UyXrRk
  PlDZm7/k2GBsHgCzYjebleLNjwLqAI5Cloz4leXvoCEAAAACxROi+cMH
  munSBxE68QVlVhJJ/Ava4hDvow7a4/8L3Sis6WCMAz7l0y78yPZNkwo2
  Ac4InMVDGsRpk28kvFFc5"
},
```

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  44 50 41 50 49 01 00 00 00 D0 8C 9D DF 01 15 D1  DPAPI....ÐŒ.ß..Ñ
00000010  11 8C 7A 00 C0 4F C2 97 EB 01 00 00 00 CD 7A CF  .Œz.ÀOÂ—ë....ÍzÏ
00000020  A0 CD 2E C8 49 A9 9B 06 4D 30 37 2E 45 00 00 00   Í.ÈI©›.M07.E...
00000030  00 02 00 00 00 00 00 10 66 00 00 00 01 00 00 20  ........f......
00000040  00 00 00 3E 5C E5 6E 13 B1 59 08 7F B9 D2 61 4A  ...>\ån.±Y..¹ÒaJ
00000050  47 35 B7 03 75 72 84 2C 32 F1 DA B9 E4 18 B0 78  G5·.ur„,2ñÚ¹ä.°x
00000060  D8 04 44 00 00 00 00 0E 80 00 00 00 02 00 00 20  Ø.D.....€......
00000070  00 00 00 F8 2A EE 69 68 1A 6B 7C 42 54 F4 F9 3D  ...ø*îih.k|BTôù=
00000080  88 F9 9C E4 50 D3 5A 57 BE 1C 1F 43 AB 00 48 CF  ˆùœäPÓZW¾..C«.HÏ
00000090  1D 2D C3 30 00 00 00 57 23 3D 7A CD AD E9 F4 22  .-Ã0...W#=zÍ.éô"
000000A0  E2 D7 D1 4C 97 AD 19 0F 94 36 66 EF F9 36 18 1B  â×ÑL—...”6fïù6..
000000B0  07 80 2C D8 8D E6 F5 78 B3 63 C0 BA 80 23 90 B5  .€,Ø.æõx³cÀº€#.µ
000000C0  A3 3E 35 79 7B E8 08 40 00 00 00 B1 44 E8 BE 70  £>5y{è.@...±Dè¾p
000000D0  C1 E6 BA 74 81 C4 4E BC 41 5D 55 84 92 7F 02 F6  Áæºt.ÄN¼A]U„’..ö
000000E0  B8 84 3B E8 C3 B6 B8 FF C2 F7 4A 2B 3A 58 23 00  ¸„;èÃ¶¸ÿÂ÷J+:X#.
000000F0  CF B9 74 CB BF 32 3D 93 64 C2 8D 80 73 82 27 31  Ï¹tË¿2=“dÂ.€s‚'1
00000100  50 C6 B1 1A 64 DB C9 2F 14 57 39                 PÆ±.dÛÉ/.W9
```

Fig. 10. DPAPI BLOB stored in LocalState

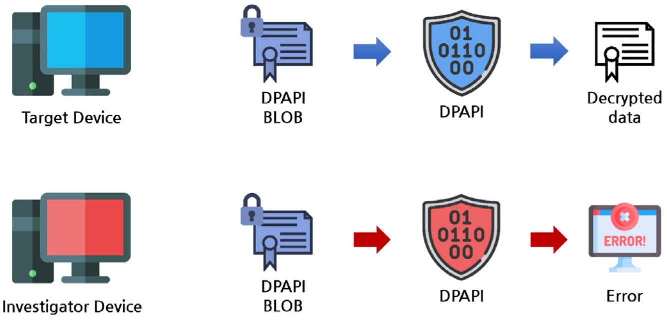


Fig. 11. Reasons for migration failure.

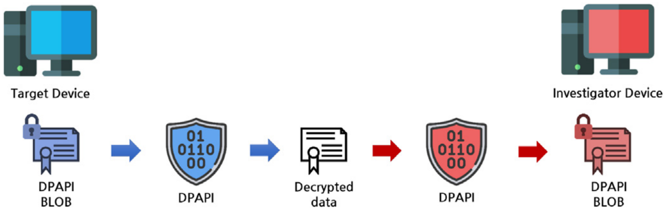


Fig. 12. Regeneration process of the DPAPI BLOB.

6.2. OS provider's website

OS providers such as Microsoft, Google, and Apple collect various information from devices using their OS and services. In particular, information collected by the OS can be partly obtainable through each website (e.g., Microsoft, Google, and iCloud). User device information logged in with the same account can be obtained, and location information of Windows, macOS, Android, and iOS devices can be inquired based on the user settings (Fig. 14).

In addition, Microsoft, Google, and iCloud sites provide useful information in digital investigations. According to Microsoft, the default storage location of the recovery key for Bitlocker data decryption is the Microsoft account; and it can be obtained through the website login support (d). Furthermore, Google provides information not only on Android devices, but also on devices using the Chrome browser support (a). Meanwhile, Apple can also access a variety of data, such as synchronized contacts, calendars, and downloaded files, via iCloud support (b). Additionally, the websites for Microsoft, Google, and iCloud sites provide e-mail, cloud storage, and productivity services (documents, memos, and so on), which will be described later. As a result, various types of data can be collected together.

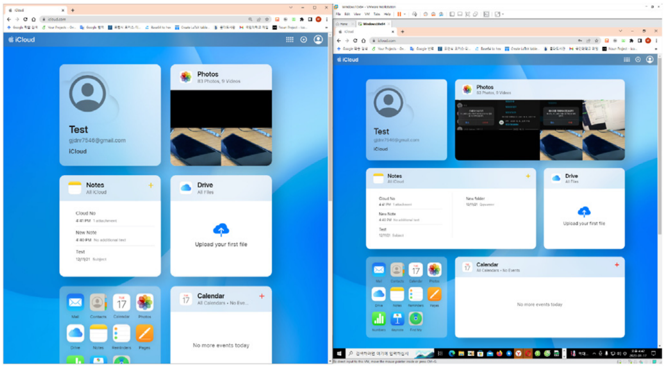


Fig. 13. Migration results for Chrome browser (left: target device, right: migrated virtual device).

6.3. Email service

Most e-mail services used in the Windows environment provide services through web pages without programs. In particular, e-mail exchanged through web pages is not stored locally except when used in conjunction with programs such as Outlook, such that cloud data collection is required. Additionally, the majority of e-mails are sent using a secure protocol that allows end-to-end encryption like PGP, thus even if the data stored on the server is collected, decryption is impossible. As a result, security features like additional authentication can be bypassed if access to an e-mail account is available using credentials stored in the web browser.

6.4. Cloud storage

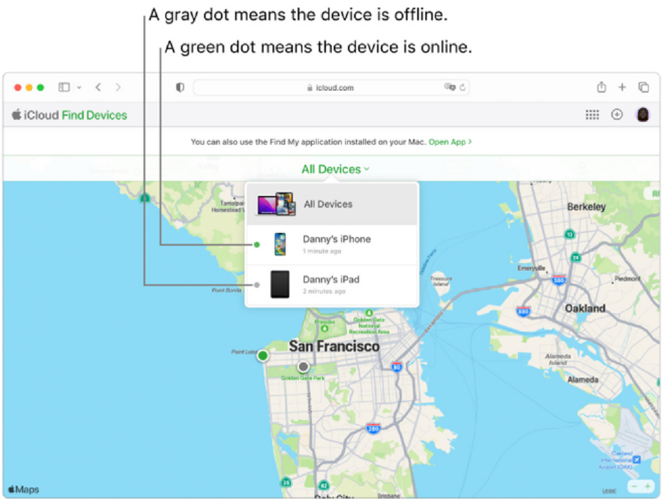
If the cloud storage is accessible, various data including photos, videos, and document data uploaded therein can be acquired. Given that cloud storage often and automatically synchronizes the many types of data generated by user devices, it provided by OS providers can be particularly helpful in digital investigations. In addition to common cloud storage, private network storage such as the network attached storage (NAS) also provides an interface through websites, to ensure it can be utilized in the same way.

6.5. Productivity service

Document tools provided by web pages such as Google Docs and various productivity services that provide functions such as collaboration, video conferencing, and memos, provide interfaces through web pages to respond to various work environments. Particularly, the cloud-based productivity tools provide the ability to import documents from specific points in the past and independently record changes for user convenience. By using this, even if there are deleted items inside the document, the data before it was deleted can be restored from the cloud.

Table 2
The list of websites that can be auto-logged into.

Name	URL	OS	Email	Social	Cloud storage	Productivity
Google	https://www.google.com/	✓	✓	✓	✓	✓
iCloud	https://www.icloud.com/	✓	✓		✓	✓
Microsoft	https://account.microsoft.com/	✓	✓		✓	✓
Proton	https://proton.me/		✓		✓	✓
Naver	https://www.naver.com/		✓	✓	✓	✓
Daum	https://www.daum.net/		✓	✓	✓	
Yandex	https://yandex.com/		✓	✓	✓	
Dropbox	https://www.dropbox.com/				✓	
Box	https://www.box.com/				✓	
Mega	https://mega.io/				✓	
Zoom	https://zoom.us/			✓		
Trello	https://trello.com/					✓
Notion	https://www.notion.so/					✓
Facebook	https://www.facebook.com/			✓		
Instagram	https://www.instagram.com/			✓		
Youtube	https://www.youtube.com/			✓		
Twitter	https://twitter.com/			✓		
Tiktok	https://www.tiktok.com/			✓		
Reddit	https://www.reddit.com/			✓		
Linkedin	https://www.linkedin.com/			✓		


A gray dot means the device is offline.

A green dot means the device is online.

You can also use the Find My application installed on your Mac. Open App ›

Fig. 14. Find devices on iCloud.com.

6.6. *Social networking service*

Social network service (SNS) includes data that is not accessible only to certain users, such as the direct message between users or secret posts, in addition to services through public posts. To obtain those data, it is necessary to access the user account. It is simple to determine whether a user has utilized services like anonymous posting by gaining access to their user account.

Additionally, websites that provide auto-login can utilize migration data in the same way until the credentials expire, as well as the functions mentioned above. Above all, the credentials of websites like Google, Apple, and Facebook, that provide single sign-on (SSO) functions can be used as credentials for other services on their own.

7. Conclusion

As the number of devices used by one person increases, there has been a corresponding increase in services that store data in the cloud to provide a seamless user experience in various devices and environments. In addition, for services provided based on the data stored in the cloud, it is challenging to obtain and analyze data only with the previous digital forensic investigation method, which analyzes the data stored in devices. At this time, credentials remaining in the browser can be used very useful. In this paper, we proposed a method of migrating browser data to the investigator device to utilize credentials stored in the browser data. As a result of our experiment, we were able to migrate the same user environment such as auto-login and password autocomplete through data migration. Furthermore, if the auto-login and browser trust options are enabled, it is possible to log in normally to websites that could not be logged into using only ID and password. Additionally, we were able to obtain various data, which can be efficiently used for digital forensic investigation related to user behavior such as e-mail, chat history, and location information on web pages accessible via auto-login. Overall, we believe that the results of this paper will be useful in digital forensic investigation.

Acknowledgement

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No. 2021-0-00540, Development of Fast Design and Implementation of Cryptographic Algorithms based on GPU/ASIC).

References

Cho, J., Kim, D., Kim, H., 2018. User credential cloning attacks in android applications: exploiting automatic login on android apps and mitigating strategies. IEEE Cons. Electron. Magazine 7, 48–55.
Chung, H., Park, J., Lee, S., Kang, C., 2012. Digital forensic investigation of cloud storage services. Digit. Invest. 9, 81–95.
Cisco, 2020. Cisco annual internet report(2018–2023) white paper. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf. 01-Jau-2023.
Delpy, B., 2020. mimikatz. https://github.com/ParrotSec/mimikatz.
Google. The chromium projects. https://www.chromium.org/chromium-projects/.
Grassi, P., Garcia, M., Fenton, J., 2020. Digital Identity Guidelines. National Institute of Standards and Technology. Technical Report.
Grassi, P.A., Fenton, J.L., Newton, E.M., Perlner, R.A., Regenscheid, A.R., Burr, W.E., Richer, J.P., Lefkovitz, N.B., Danker, J.M., Choong, Y., et al., 2016. Draft Nist Special Publication 800-63b Digital Identity Guidelines. National Institute of Standards and Technology (NIST) 27.
Hardt, D., 2012. The OAuth 2.0 Authorization Framework (Technical Report).
Jones, M., Bradley, J., Sakimura, N., 2015. Json Web Token (Jwt). Technical Report.
Mell, P., Grance, T., et al., 2011. The Nist Definition of Cloud Computing.
Moussa, A.N., Ithnin, N., Almolhis, N., Zainal, A., 2019. A consumer-oriented cloud

forensic process model. In: 2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC). IEEE, pp. 219–224.

Mozilla. Firefox browser. https://www.mozilla.org/en-US/firefox/.

Quick, D., Choo, K.K.R., 2014. Google drive: forensic analysis of data remnants. J. Netw. Comput. Appl. 40, 179–193.

Roussev, V., Ahmed, I., Barreto, A., McCulley, S., Shanmughan, V., 2016a. Cloud forensics–tool development studies & future outlook. Digit. Invest. 18, 79–95.

Roussev, V., Barreto, A., Ahmed, I., 2016b. Forensic Acquisition of Cloud Drives arXiv preprint arXiv:1603.06542.

Satran, M., Sharkey, K., Jacobs, M., Coulter, D., Ashcraft, A.. Cng dpapi. https://learn.microsoft.com/en-us/windows/win32/seccng/cng-dpapi. (Accessed 14 January 2023).

Sofer, N., 2008. Chromepass - chrome browser password recovery for windows. https://www.nirsoft.net/utils/chromepass.html. (Accessed 14 January 2023).

Sofer, N., 2017. DataProtectionDecryptor v1.11. https://www.nirsoft.net/utils/dpapi_data_decryptor.html. (Accessed 14 January 2023).

StatCounter, 2022. Desktop browser market share worldwide. https://gs.statcounter.com/browser-market-share/desktop/worldwide.

support, G., a. Lock or erase your lost phone or computer. https://support.google.com/accounts/answer/7177579?hl=en&ref_topic=7189123.

support, G., b. Lock or erase your lost phone or computer. https://support.apple.com/ko-kr/guide/icloud/mm281e3e7d/1.0/icloud/1.0.

support, M., c. Download the new microsoft edge based on chromium. https://support.microsoft.com/en-us/microsoft-edge/download-the-new-microsoft-edge-based-on-chromium-0f4a3dd7-55df-60f5-739f-00010dba52cf.

support, M., d. Finding your bitlocker recovery key in windows. https://support.microsoft.com/en-us/windows/finding-your-bitlocker-recovery-key-in-windows-6b71ad27-0b89-ea08-f143-056f5ab347d6.

Yang, J., Kim, J., Bang, J., Lee, S., Park, J., 2022. Catch: cloud data acquisition through comprehensive and hybrid approaches. Forensic Sci. Int.: Digit. Invest. 43, 301442.