A Study on Cloud Data Acquisition through Browser Credential Migration

Uk Hur, Soojin Kang,
Giyoon Kim, Jongsung Kim
Kookmin UNIV.

DFRWS USA 2023
2023.07.10

KOOKMIN UNIVERSITY

DF&C Lab.
Digital Forensic & Cryptanalysis
KOOKMIN UNIVERSITY

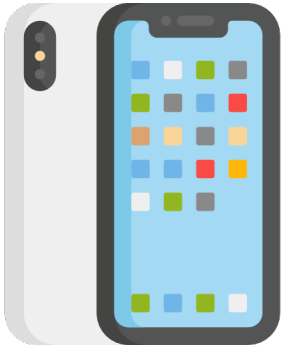
INDEX

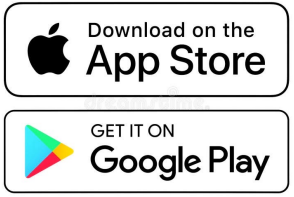
01 Introduction

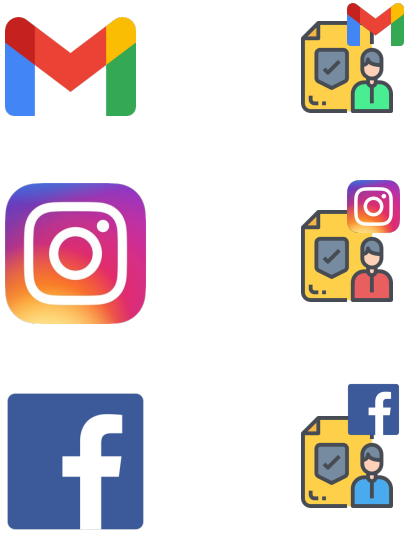
DF&C Lab.
Digital Forensic & Cryptanalysis
KOOKMIN UNIVERSITY

Why analyze browser?

- Web-based application



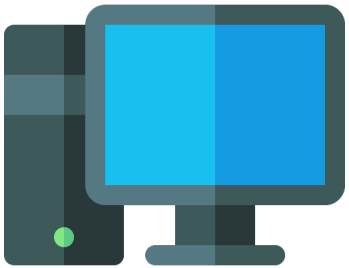


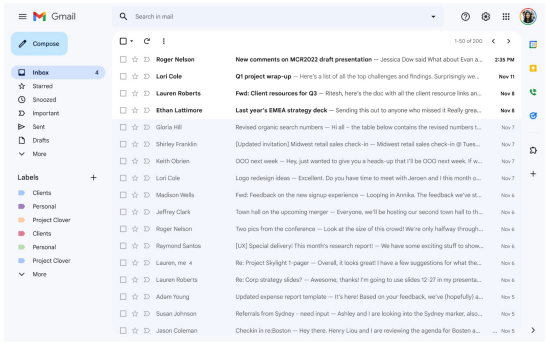


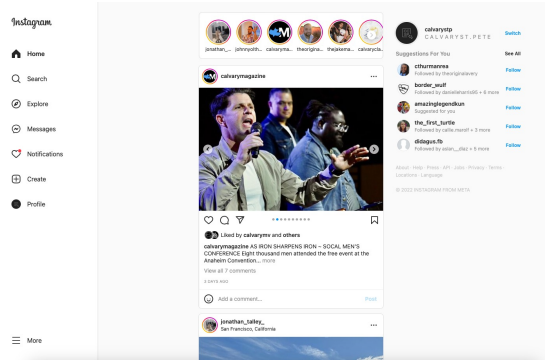
DF&C Lab.
Digital Forensic & Cryptanalysis
KOOKMIN UNIVERSITY

Why analyze browser?

- Web-based application







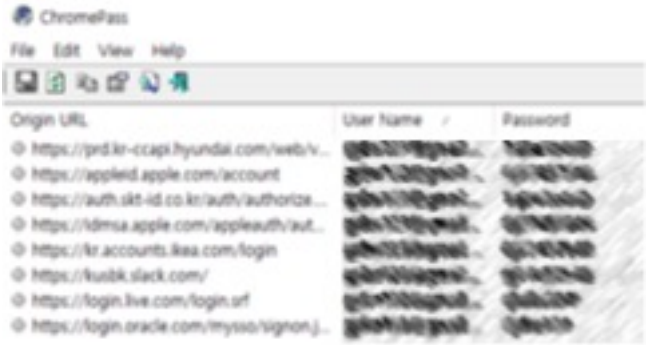
Existing research in browser forensics

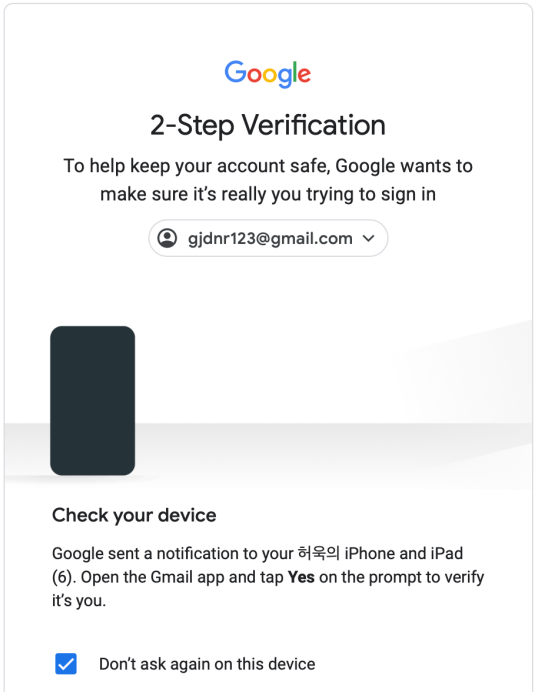
- Focused on local data
  - History (URL, Search)
  - Saved password
  - Bookmark
  - Cache data

DF&C Lab.
Digital Forensic & Cryptanalysis
KOOKMIN UNIVERSITY

Existing research in browser forensics

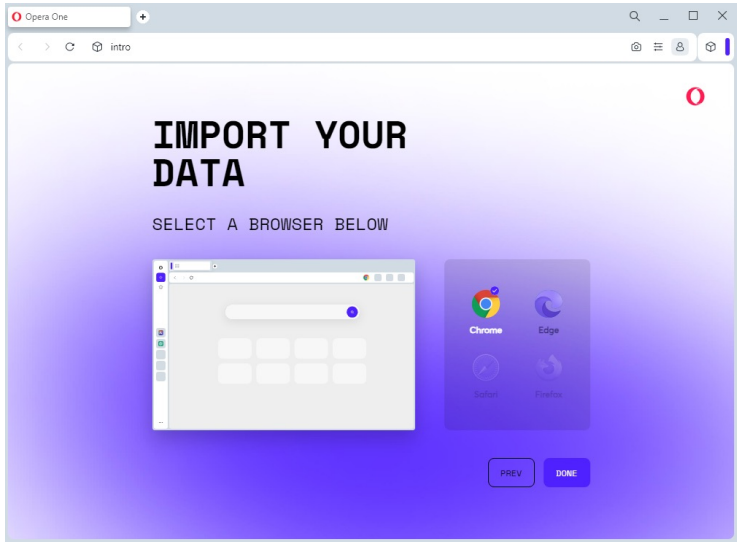
- Limitaton of existing research

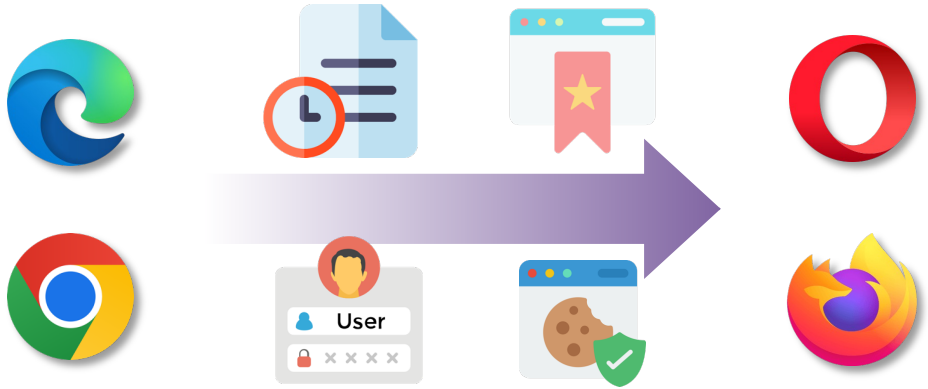




Motivation

- Browser data import function





Existed browser

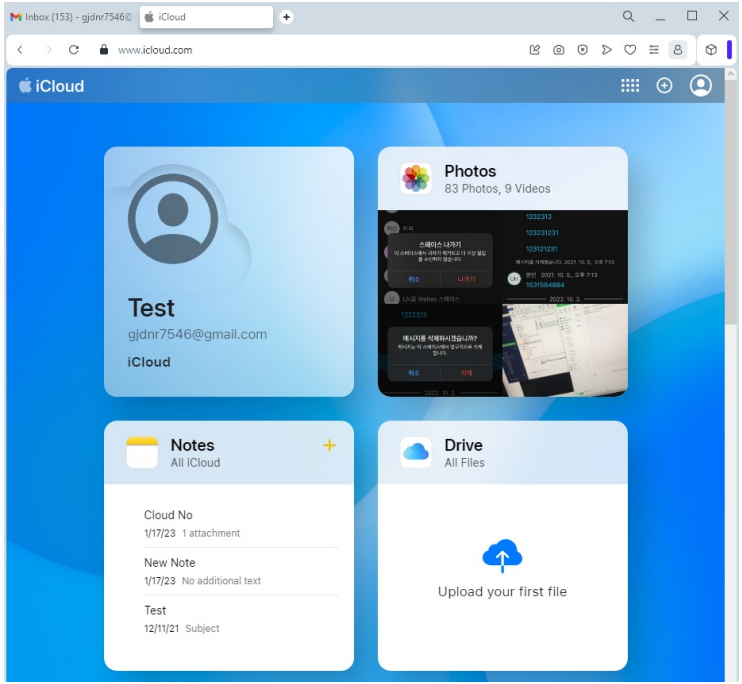
History, Bookmark
Auto fill data
Cookie

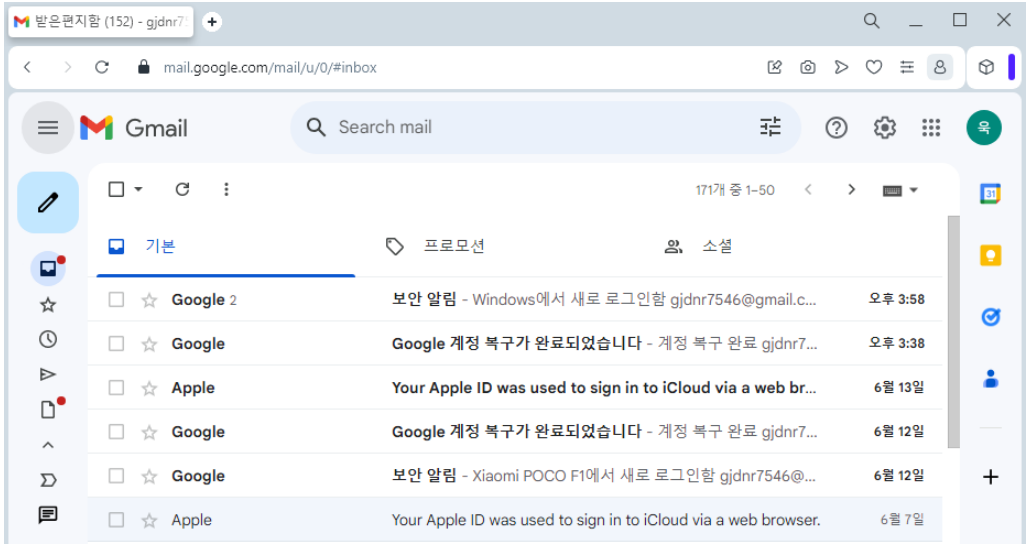
Another browser

DF&C Lab.
Digital Forensic & Cryptanalysis
KOOKMIN UNIVERSITY

Motivation

- After import data..

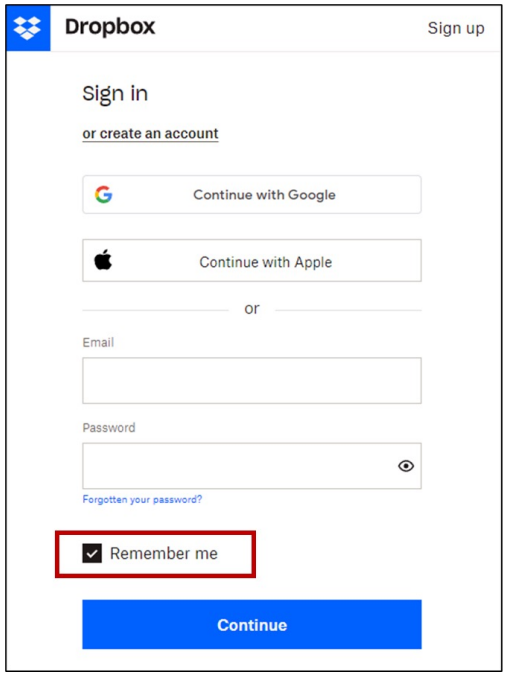


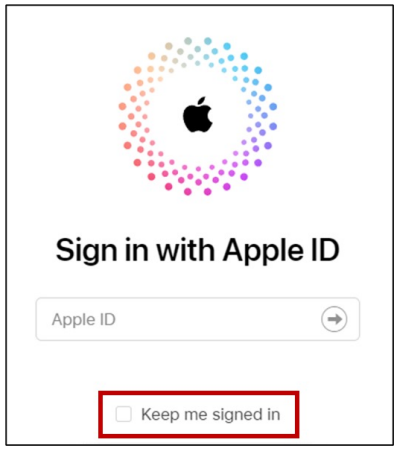


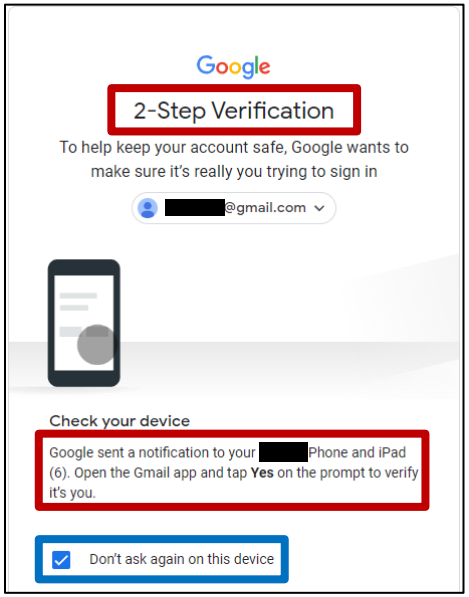
DF&C Lab.
Digital Forensic & Cryptanalysis
KOOKMIN UNIVERSITY

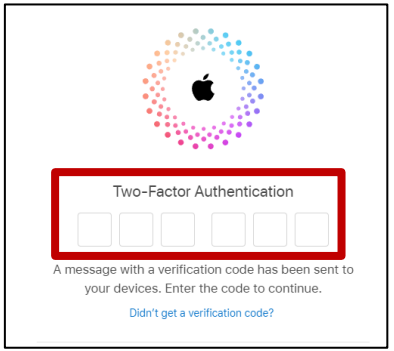
Background

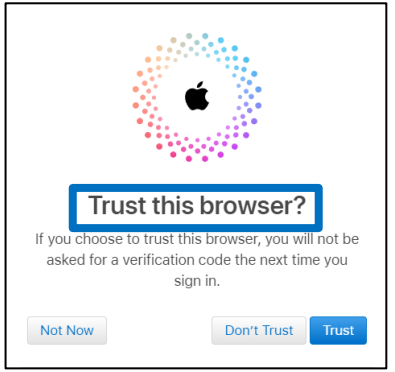
- Keep me signed in and Trust browser











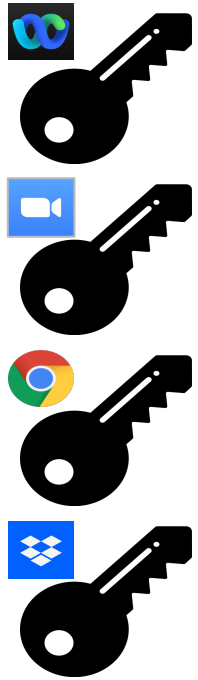
DF&C Lab.
Digital Forensic & Cryptanalysis
KOOKMIN UNIVERSITY

Background

- DPAPI

Windows Login Password

Master Key

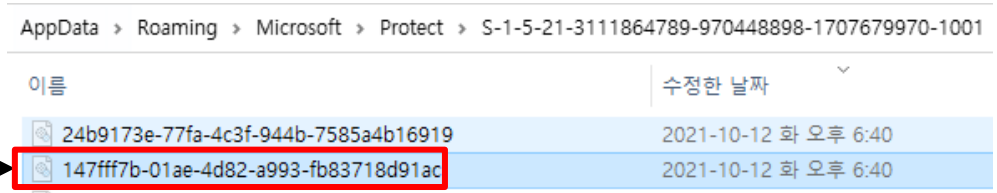


BLOB Keys

Background

- DPAPI BLOB

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‹@...
000000E0	15	6E	C2	D8	1F	57	E0	57	AD	E8	02	38	94	E4	BA	48	.nÂØ.WàW.è.8"ä°H
000000F0	44	79	BC	AD	D1	38	5D	BC	E1	F8	7C	1A	2E	32	38	9A	Dy¼.Ñ8]¼áø|..28š
00000100	AE	1D	95	30	D7	99	A2	3F	4E	55	BA	50	F2	7B	E3	17	®.•0×™¢?NU°Pò{ã.
00000110	ED	81	7E	92	14	1D	0E	F4	7D	CF	D5	ED	2E	3A	4D	76	í.~'...ô}ÏÕí.:Mv

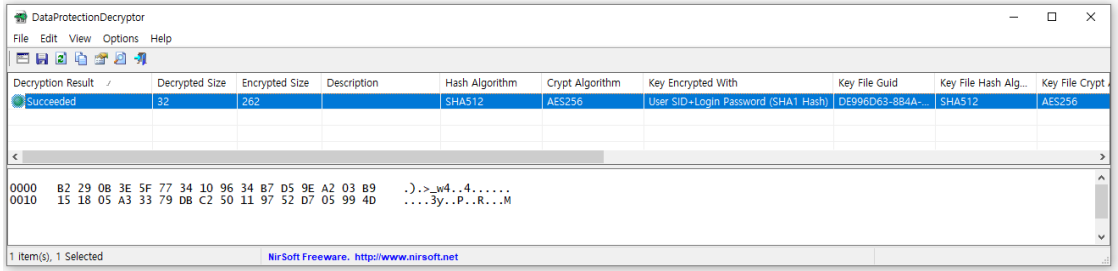


: BLOB Key GUID
: Description length
: Description
: Crypto Algorithm id
0x6610 : AES-256
0x800E : SHA-512
: Encrypted data

BLOB Key

Background

- DPAPI Tools
  - Mimikatz
  - DataProtectionDecryptor



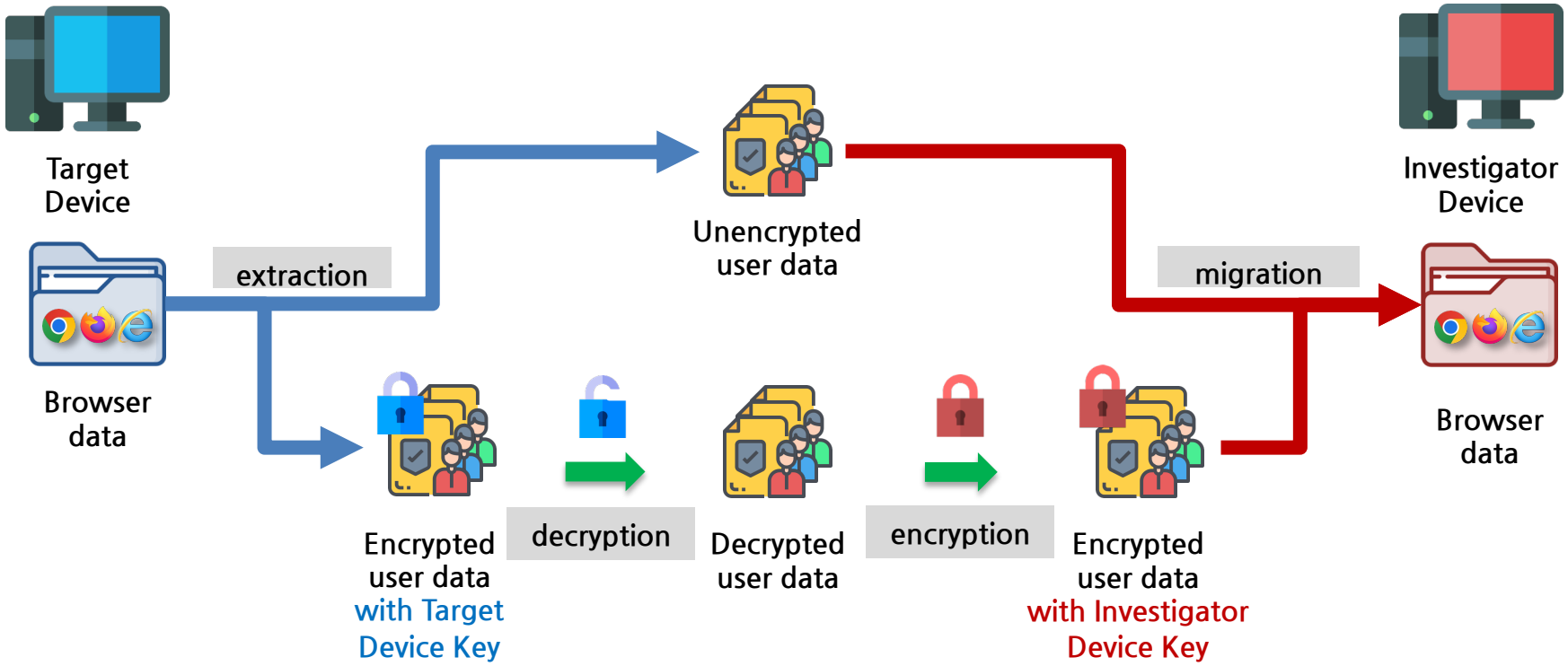
  - Python module – win32crypt

```
import win32crypt
import base64

def decrypt(b64string):

    b64decodedstring = base64.b64decode(b64string)

    clear = win32crypt.CryptUnprotectData(b64decodedstring, None, None, None, 0)

    return clear[1].decode("utf-16-le")
```

02 Our goal and analysis

Our goal

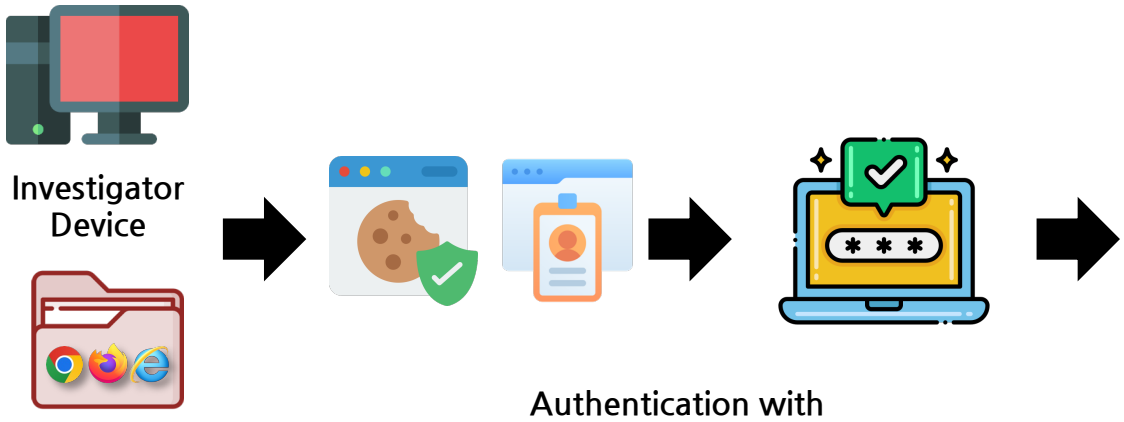
- Browser data migration to another device

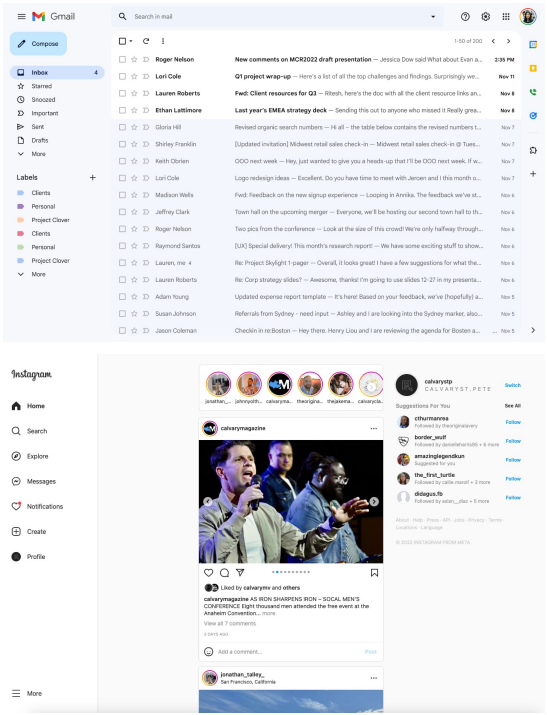


DF&C Lab.
Digital Forensic & Cryptanalysis
KOOKMIN UNIVERSITY

Our goal

- Acquiring Cloud Data Using Browser Credentials



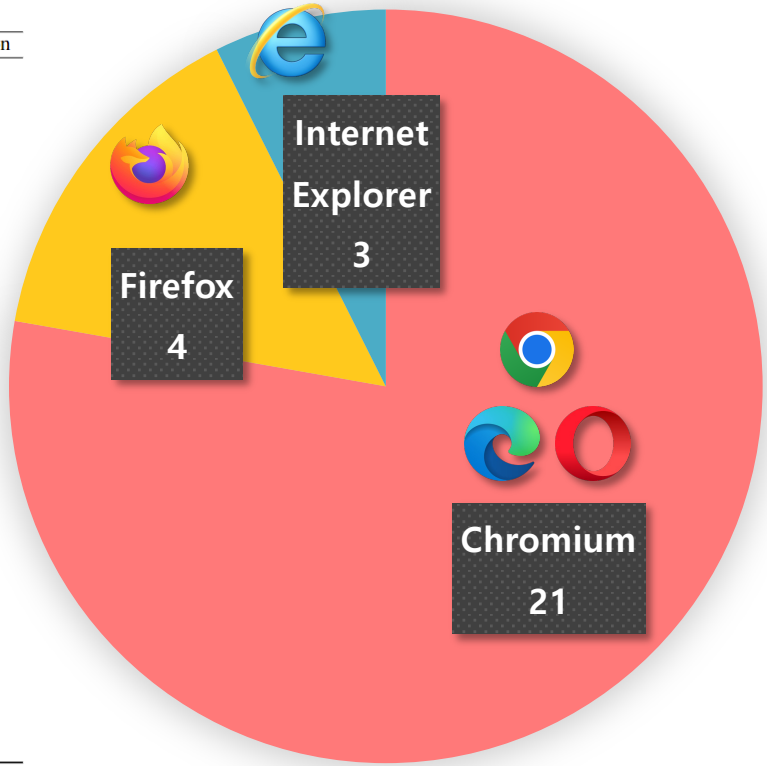


List of analyzed browser

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

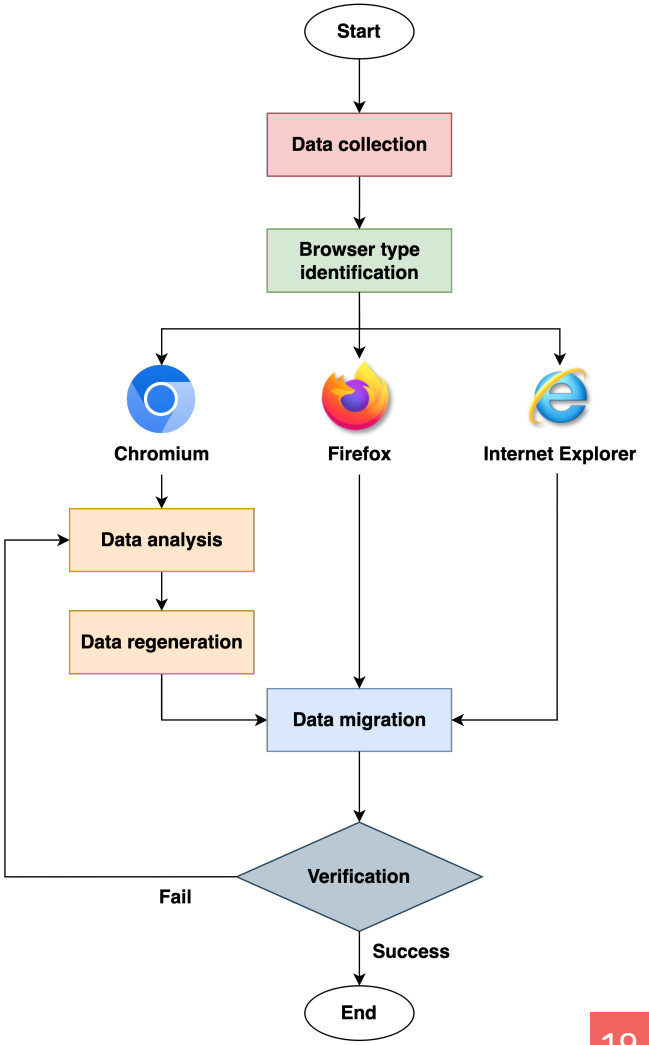


03 Our proposed migration process

DF&C Lab. Digital Forensic & Cryptanalysis KOOKMIN UNIVERSITY

Entire process of browser migration

- Data collection
  - Copy browser data
- Chromium browser
  - Data regeneration process required
- Firefox and IE based browser
  - Paste the data into the same location



DF&C Lab. Digital Forensic & Cryptanalysis KOOKMIN UNIVERSITY

Data protection of Chromium based browser

- DPAPI + AES-GCM hybrid protection
  - Password and Cookie data encrypted with AES-GCM

Table: cookies

	host_key	name	expires_utc	ıst_access_ut	ıncrypted_value	samesite
	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

Mode: Binary

```
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.
```

DF&C Lab. Digital Forensic & Cryptanalysis KOOKMIN UNIVERSITY

Data protection of Chromium based browser

- DPAPI + AES-GCM hybrid protection
  - Encryption Key is Protected with DPAPI

DF&C Lab.
Digital Forensic & Cryptanalysis
KOOKMIN UNIVERSITY

Data protection of Chromium based browser

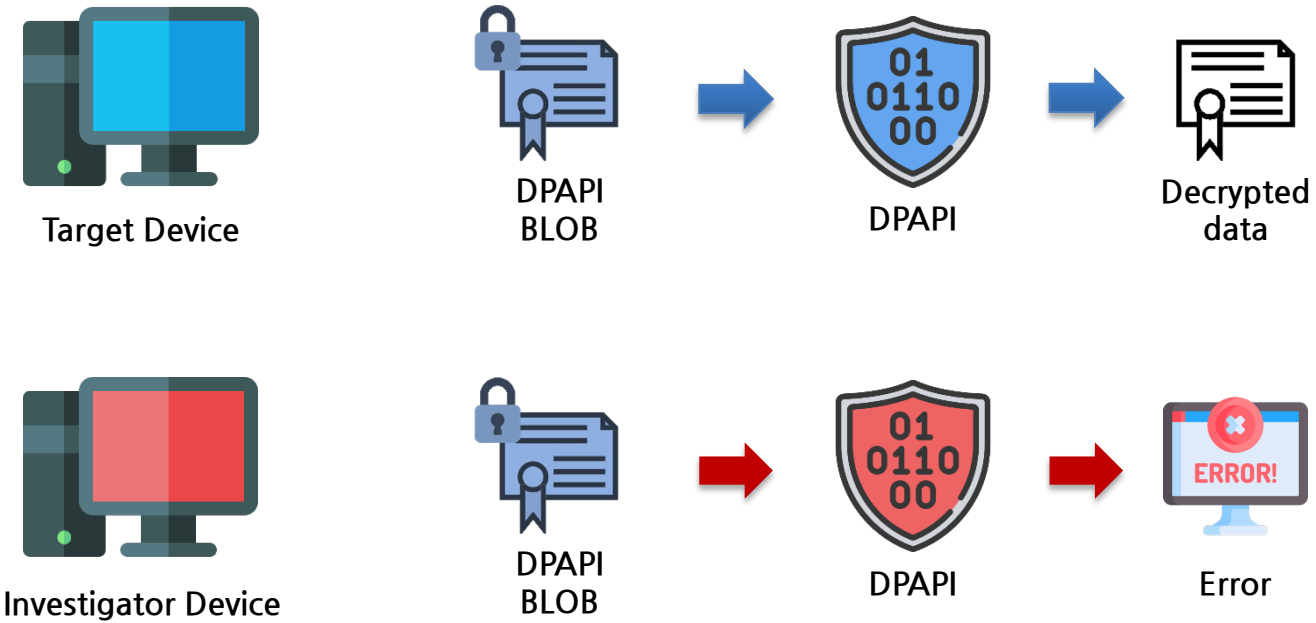
- DPAPI + AES-GCM hybrid protection
  - Encryption Key is Protected with DPAPI

무제1

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	63	6D	99	.Œz.ÀOÂ—ë....cm™
00000020	DE	4A	8B	EC	42	94	4C	9D	80	DD	2E	B8	B2	00	00	00	ÞJ‹ìB”L.€Ý.¸²...
00000030	00	02	00	00	00	00	00	10	66	00	00	00	01	00	00	20	........f......
00000040	00	00	00	01	B6	AF	6A	0F	4A	9B	6F	65	5C	8D	D9	D5	....¶¯j.J›oe\.ÙÕ
00000050	4F	A3	97	51	F2	B5	20	BA	89	94	A4	4C	78	5A	F5	BE	O£—Qòµ °‰”¤LxZõ¾
00000060	EE	09	1A	00	00	00	00	0E	80	00	00	00	02	00	00	20	î.......€......
00000070	00	00	00	96	C5	5C	E1	C1	CB	AC	7C	0D	35	B6	AB	D6	...–Å\áÁË¬|.5¶«Ö
00000080	FB	7D	00	4E	24	8B	D8	C3	59	BA	23	91	31	63	D8	39	û}.N$‹ØÃY°#‘1cØ9
00000090	03	B3	5F	30	00	00	00	33	FF	1F	97	01	CF	7B	95	5F	.³_0...3ÿ.—.Ï{•_
000000A0	56	B5	44	0F	D2	96	C6	06	6C	A2	10	09	8A	BC	B8	ED	VµD.Ò–Æ.l¢..Š¼¸í
000000B0	77	18	F1	D4	4C	62	36	E9	B2	BA	4C	DA	B7	00	C3	A4	w.ñÔLb6é²ºLÚ·.Ã¤
000000C0	8F	4A	C3	E9	F6	10	A3	40	00	00	00	6D	68	54	7F	0C	.JÃéö.£@...mhT..
000000D0	BD	92	10	BE	38	23	58	9E	A6	82	7A	7F	CF	97	47	83	½’.¾8#Xž¦‚z.Ï—Gƒ
000000E0	30	5A	23	7F	67	FD	2F	C9	0B	63	EF	93	90	FC	83	F0	0Z#.gý/É.cï“.üƒð
000000F0	9C	C9	4D	9A	D3	A4	FE	C0	E9	A9	D2	C7	0C	4A	2C	96	œÉMšÓ¤þÀé©ÒÇ.J,–
00000100	E0	86	93	3D	46	BD	23	14	D4	6A	8F						à†“=F½#.Ôj.

Data protection of Chromium based browser

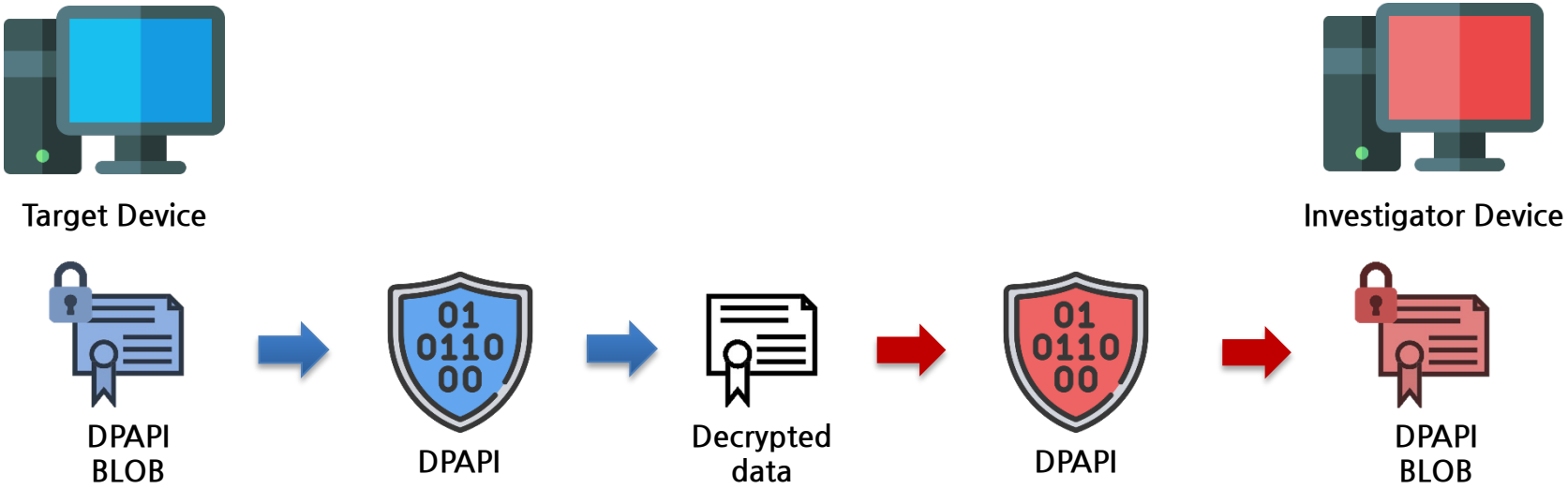
- When a DPAPI blob is moved to another device



DF&C Lab.
Digital Forensic & Cryptanalysis
KOOKMIN UNIVERSITY

Data protection of Chromium based browser

- DPAPI BLOB regeneration process
  - Regeneration only DPAPI BLOB in LocalState



DF&C Lab. Digital Forensic & Cryptanalysis KOOKMIN UNIVERSITY

Old Version Chromium

- Each data is directly protected by DPAPI
- version 80 and lower versions

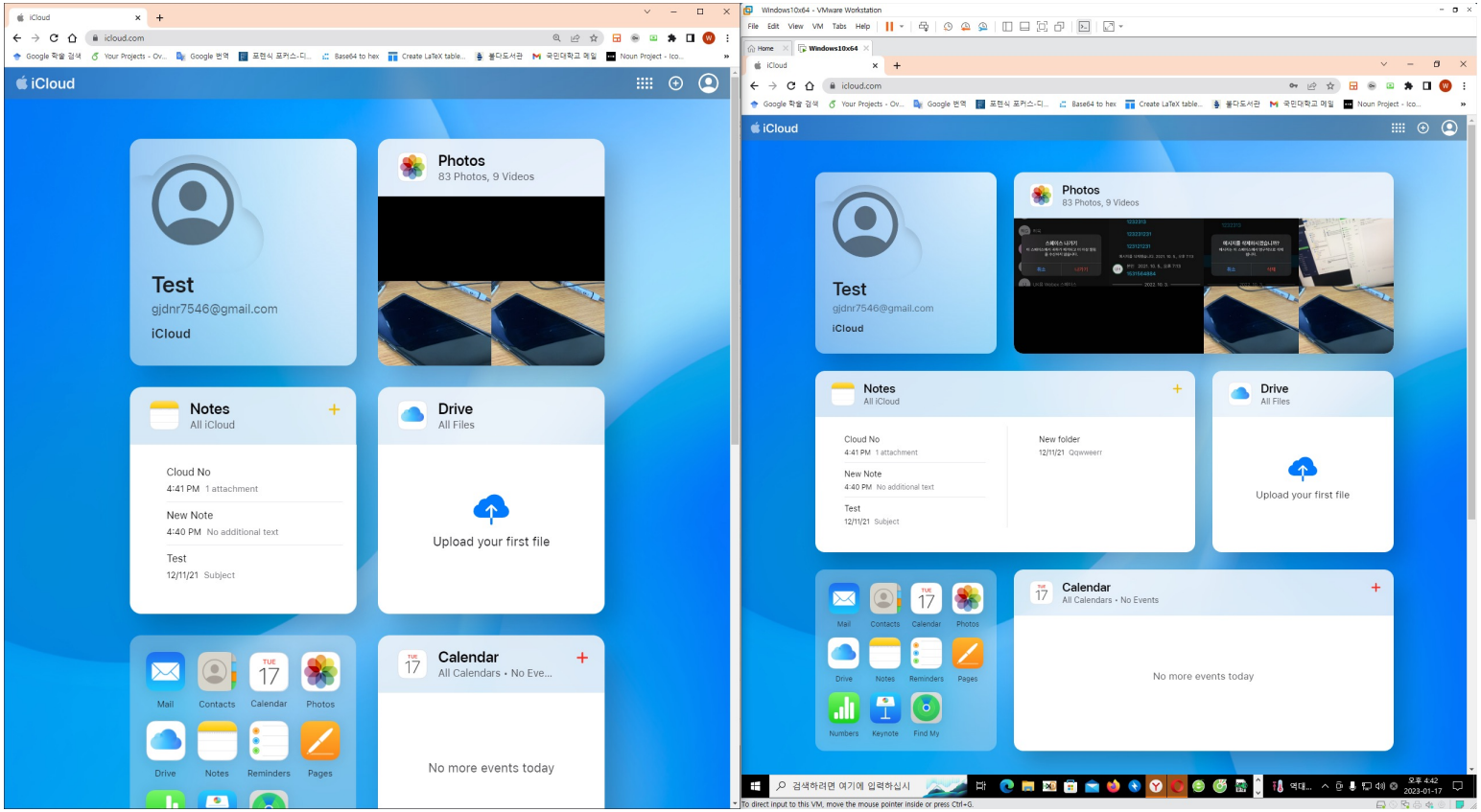
Table: cookies

	host_key	name	expires_utc	ıst_access_ut	ıncrypted_valu	samesite
	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

Mode: Binary

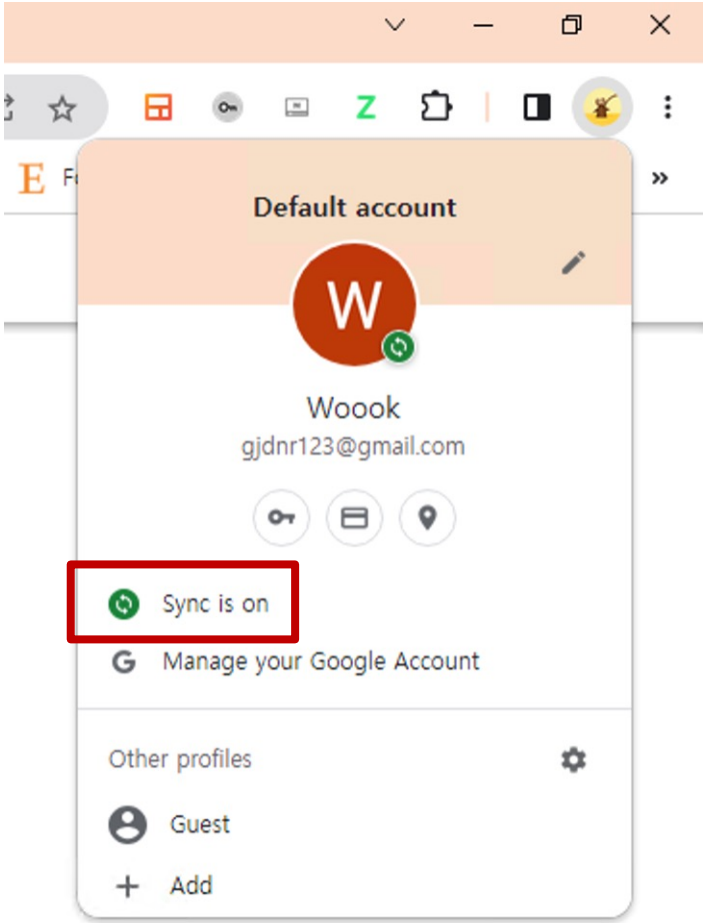
```
0000 01 00 00 00 d0 8c 9d df 01 15 d1 11 8c 7a 00 c0  ............z..
0010 4f c2 97 eb 01 00 00 00 eb 02 e8 88 c7 3c d0 43  O............<.C
0020 96 53 93 01 b2 c8 74 05 00 00 00 00 02 00 00 00  .S....t.........
0030 00 00 10 66 00 00 00 01 00 00 20 00 00 00 ec d7  ...f...... .....
0040 11 3d 9e 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.
```

Migration result



One more Thing..

- Synchronization account
  - Sync data between devices using the same account
  - User activity after the data collection point is synchronized



DF&C Lab.
Digital Forensic & Cryptanalysis
KOOKMIN UNIVERSITY

One more Thing..

- Synchronization account

Browser name	type	version	Migration	Synchronization account migration
Avast Secure Browser	Chromium	108.0.19667.125	O	O
Brave	Chromium	109.1.47.171	O	-
Chromium	Chromium	111.0.5501.0	O	O
Chrome	Chromium	108.0.5359.125	O	O
Comodo Dragon	Chromium	108.0.5359.95	O	O
Epic Privacy Browser	Chromium	104.0.5112.81	-	-
FlashPeak Slimjet (64 bit)	Chromium	107.0.5304.62	O	O
iridium	Chromium	2022.04	-	-
Maelstrom	Chromium	42.0.1.36	O	X
Edge	Chromium	109.0.1518.52	O	X
Opera	Chromium	94.0.4606.38	O	O
Tungsten	Chromium	2.14	O	X
UC Browser	Chromium	6.0.1308.1016	O	X
Vivaldi	Chromium	5.6.2867.50	O	X
Yandex	Chromium	23.1.0.2539	O	O
Whale	Chromium	3.18.154.7	O	X
360 Safe Browser	Chromium	13.1.6410.0	O	X
QQ Browser	Chromium	11.5	O	X
Coc Coc	Chromium	114.0.140	O	O
Sogou Explorer	Chromium	11.0.1.34700	O	X
Maxthon	Chromium	6.2.0.2000	O	X
Firefox	Firefox	108.0.1	O	O
Comodo ice dragon	Firefox	65.0.2.15	O	O
SeaMonkey	Firefox	2.53.14	O	-
Pale Moon	Firefox	31.4.2	O	-
Internet Explorer 11	IE	11.0.18362.997	O	X
Edge Lagacy	IE	44.19041.610.0	O	X

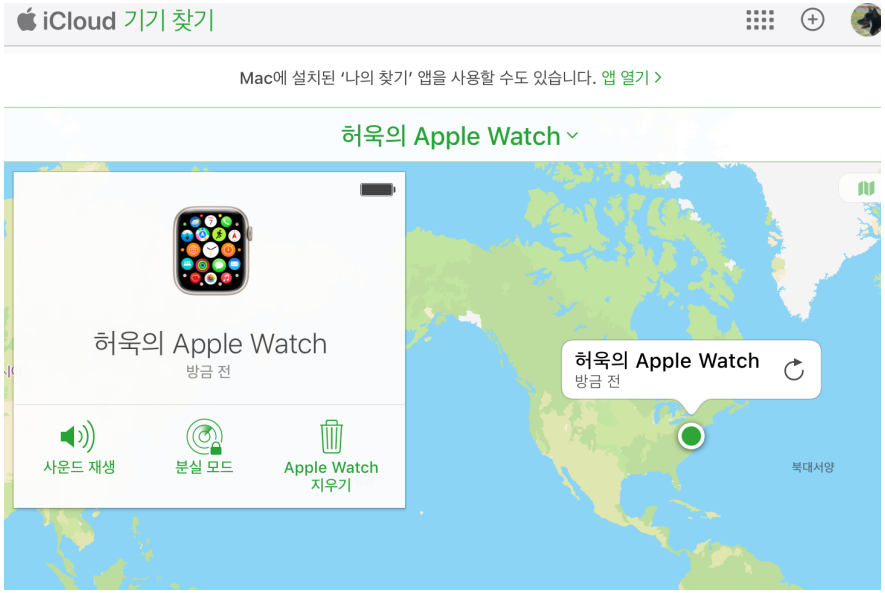
04 Utilize Forensic Investigation

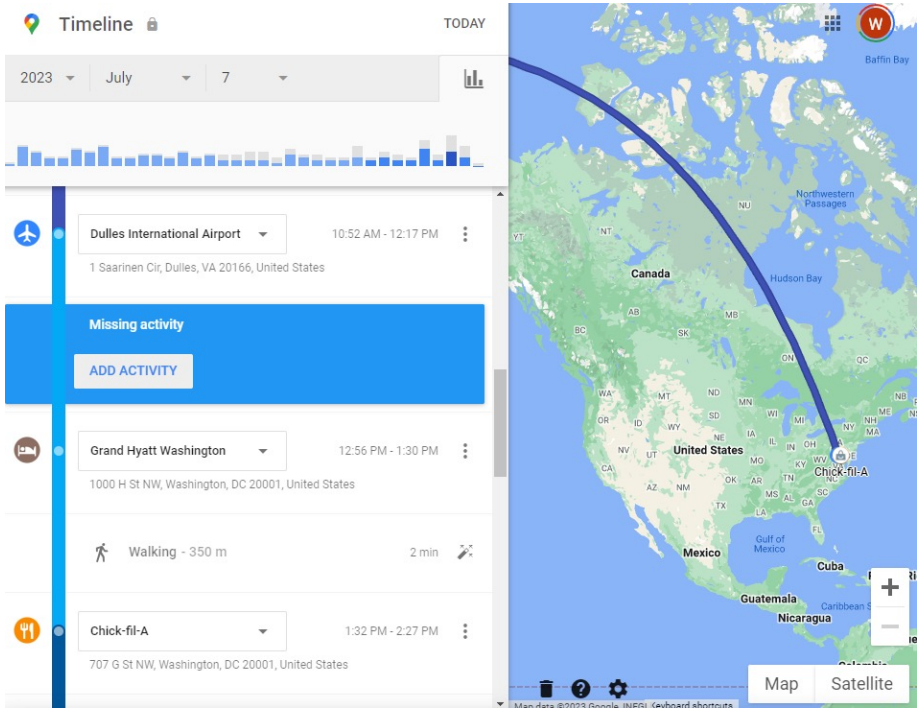
Useful web services that provide auto-login function

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/			✓		

Useful web services that provide auto-login function

- OS Provider (Google, Microsoft, Apple)





Benefits compared to OS drive migration

- Free from drive protection techniques (ex. BitLocker).
- No require storage device and fast (~10GB).
- Relatively free from legal restrictions.

05 Conclusion and future works

Conclusion and future works

- Useful data from various web services can be retrieved through simple browser data migration process.
- A Synchronization account allows to sync user activities on different devices

- Other Windows applications using the same protection mechanism using DPAPI (Zoom, WebEx..)


Q&A