101 - Darkverse

Team Information

Team Name : LuckyVicky

Team Member : Eungchang Lee, Hyun Yi, Juho Heo, Dongkyu Lee

Email Address : dfc_luckyvicky@googlegroups.com

Instructions

Description The target is the head-mounted display (HMD) image.

Target	Hash (MD5)
DEVICE#01.ad1	bd3a0f624f2f66bbb10ef181f79bfff6
DEVICE#02.ad1	69a251582ce74e99d12c8708614ddb9d

Questions

1) What is email address of mobile phone owner? (10 points)
2) What is a serial number of the HMD? (15 points)
3) What is timestamp of the screenshot taken with HMD? (15 points)
4) What are the names of people who exchanged messages with the device owner? (20 points)
5) Submit the link sent from the device owner, and the usage of the link. (20 points)
6) What was the last wearing time of HMD? (20 points)

Teams must:

- Develop and document the step-by-step approach used to solve this

problem to allow another examiner to replicate team actions and results.

- Specify all tools used in deriving the conclusion(s).

Tools used:

Name:	FTK Imager	Publisher:	AccessData® FTK® Imager
Version:	4.7.1.2		
URL:	https://go.exterro.com/l/43312/2023-05-03/fc4b78		

Name:	ALEAPP	Publisher:	ALEAPP team
Version:	3.1.8		
URL:	https://github.com/abrignoni/ALEAPP		

Name:	DB Browser for SQLite	Publisher:	sqlitebrowser
Version:	3.12.2		
URL:	https://sqlitebrowser.org/		

Name:	HashTab	Publisher:	Implbits Software
Version:	6.0.0		
URL:	https://implbits.com		

Step-by-step methodology:

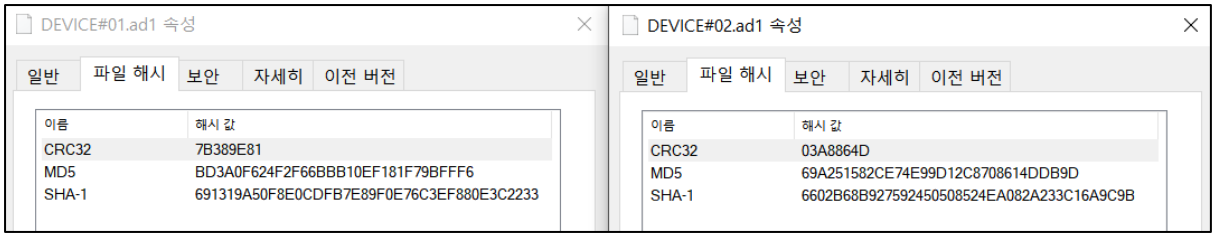


그림 1 target 파일의 md5 해시 값 확인

다운로드받은 target 파일의 md5 해시 값이 일치함을 확인하였습니다.

1) What is email address of mobile phone owner? (10 points)

전반적인 아티팩트 분석 및 확인을 위해 FTK imager를 통해 ad1파일을 로드한 다음, Export Files를 통해 파일을 export하였습니다.

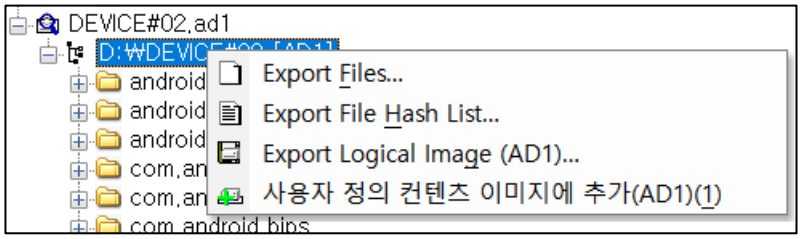


그림 2 Export Files for DEVICE#02.ad1

그 후, zip파일로 export한 패키지들을 압축한 다음 ALEAPP을 통해 전반적인 아티팩트 분석을 수행하였습니다. ALEAPP을 통해, 문제에서 찾는 mobile phone 주인의 이메일 주소를 사용자 Gmail 관련 정보가 포함된 아티팩트인 com.google.android.gm₩shared_prefs₩Gmail.xml에서 다음과 같이 찾을 수 있었습니다.

```
▼<map>
   <string name="app_theme">19</string>
   <boolean name="confirm-send" value="false"/>
   <string name="active-account">joshua.dfc2024@gmail.com</string>
   <string name="removal-action">archive</string>
   <boolean name="conversation-overview-mode" value="true"/>
   <boolean name="confirm-delete" value="false"/>
   <string name="joshua.dfc2024@gmail.com-account-alias">joshua.dfc2024@gmail.com</string>
   <int name="welcome_tour_version" value="1"/>
   <boolean name="force_show_welcome_tour" value="false"/>
   <boolean name="mail-enable-threading" value="true"/>
   <string name="cache-google-accounts-synced">joshua.dfc2024@gmail.com</string>
   <boolean name="confirm-archive" value="false"/>
</map>
```

그림 3 mobile phone owner's email address

답 : joshua.dfc2024@gmail.com

2) What is a serial number of the HMD? (15 points)

DEVICE#02.ad1에서 확인가능한 com.oculus.twilight 폴더에서 RKStorage sqlite3 db파일을 db browser for SQLite로 열었을 때 catalystLocalStorage 테이블에서 Device가 Meta Quest 2임을 확인하였습니다. 그 후, 참고 reference[1]를 통해 deviceSelected key에서 DEVICE_SERIAL 값이 HMD 기기의 serial number임을 확인할 수 있습니다.


```
[{"areConsentsPending":false,"deviceManifest":{"deviceId":"0fb54f7498a39eb1",
"creationTime":1721460072,"displayedDeviceName":"Meta Quest 2","hardware":[],"id":
"395098807013776","lastSyncTime":1721541993,"supports_eye_tracking":false,
"supports_face_tracking":false,"supports_spatial_data":false,"userDefinedDeviceName":
null,"horizon_version":"67.0.0.260.449"},"serialNumber":"1WMHH831ZV0512","type":
"HOLLYWOOD"}]
```


그림 4 HMD 기기의 이름과 serial number 확인

답 : 1WMHH831ZV0512

[1] https://www.sciencedirect.com/science/article/pii/S2666281723001208

3) What is timestamp of the screenshot taken with HMD? (15 points)

DEVICE#01.ad1에 존재하는 Oculus\Screenshots에서 다음과 같이 하나의 사진을 발견할 수 있습니다.

[그림 5] com.oculus.shellenv-20240720-162325.jpg

앞서 살펴본 reference에 따르면, 해당 폴더 내 저장되는 사진의 이름은 {Package_name}-{YYYYMMDD}-{HHMMSS} 형태로 저장되고 (Package Name, Timestamp)로 구성된다고 명시되어 있으므로, 해당 기기에서 찍은 스크린샷의 timestamp는 20240720-162325로 볼 수 있습니다.

답 : 20240720-162325

4) What are the names of people who exchanged messages with the device owner? (20 points)

DEVICE#02.ad1 내 com.oculus.twilight₩databases₩ 폴더에서 메신저 관련 db파일인 messengervr_msys_database_380363178490960 파일을 db browser for SQLite로 확인해보았습니다. 확인 결과, 해당 db 파일 내 contacts 테이블에서 메시지를 주고 받은 사람들에 대한 정보를 다음과 같이 확인할 수 있었습니다.

테이블(T): contacts

	id	ɔic	re.	ɔfile_picture_url_expiration_timestamp_r	name	first_name	normalized_name_for
	필터	…	…	필터	필터	필터	필터
1	380363178490960	…	…	1724050390	Joshua	NULL	joshua
2	315083558365988	…	…	1724052453	Alice	NULL	NULL

[그림 6] 앱 내 message를 주고받은 사람들에 대한 정보

또한, prefs_db 파일에서 앱 내 사용된 메신저 user ID를 나타내는 MetaProfileGenericAuthMap key의 userID와 contacts 테이블 내 id가 같으며, 앞서 1번 문제에서 확인한 이메일 내 이름을 통해 device owner는 380363178490960 id를 가진 joshua로 아래의 그림을 통해 판단할 수 있습니다. 따라서, device owner와 메시지를 교환한 사람은 Alice로 파악됩니다.


```
{"Communicator":{"userID":"380363178490960","token":
"FRLAeea0ZAmP8B9eRC0rToxbFjGLK4JlHrxT4Xj4ZB3ZBVVuRqtAlEUgCHDIJONIjZAl22DuGhU5wPEPV6Udu5
lMynMLkpbTZAPrbwHnaD6eF5W69FigHepXGByPPzHCoCG1OJnX6wSbkE6kbLJEKEjZBbeOGxszTkHZCpZBhIftS
4ZD"}}
```


[그림 7] messenger User ID 확인

또한, 차후 5번 문제에 서술되는 대화 내용에서도 sender id는 device onwer인 joshua와 alice밖에 보이지 않아 대화를 나눈 사람은 Alice만으로 파악됩니다.

답 : Alice

5) Submit the link sent from the device owner, and the usage of the link. (20 points)

4번 문제에서 살펴본 메신저 관련 db 파일에서 messages 테이블을 살펴보면, 다음과 같이 대화를 나눈 기록을 확인할 수 있습니다.

테이블(T): messages

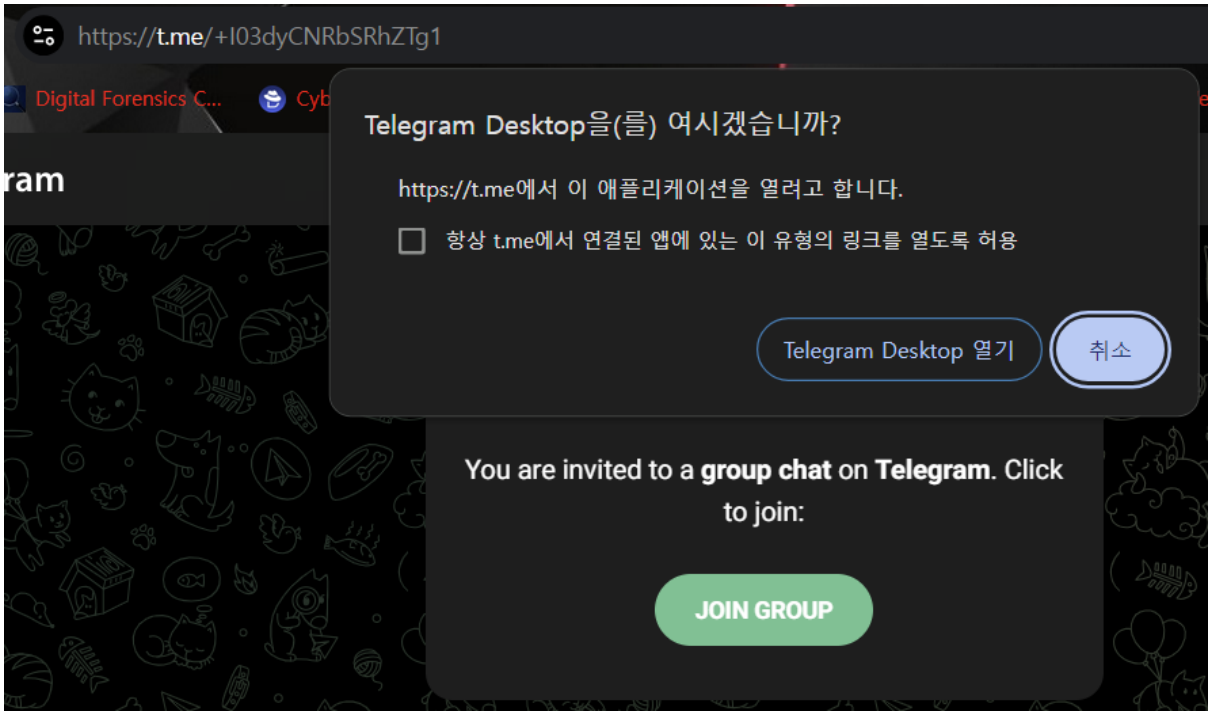
		offline_threading_id	text	sender_id
		필터	필터	필터
1		7220342804141531210	Hello···	380363178490960
2		7220343311232977870	You can now invite each other to parties, send photos, ···	315083558365988
3		7220343369076736677	Hello, Who are you?	315083558365988
4	a2qdyy	7220344042052770994	Nice to meet you. I am Joshua, and I want to be your ···	380363178490960
5		7220344575331057928	Umm Okay, I usually play Horizon Worlds. Did you play it,···	315083558365988
6		7220344845974754560	Sure!	380363178490960
7		7220344975242638744	When you have time, we can meet in Horizon Worlds.	380363178490960
8		7220345363676431484	Cool!	315083558365988
9		7220675472436474342	Hi Alice	380363178490960
10		7220675711597938352	I would like to invite you to our group.	380363178490960
11		7220675915756436736	Hi Joshua	315083558365988
12		7220676004450771104	I am looking forward to it!	315083558365988
13		7220676412036876050	Okay, First you need to join our telegram.	380363178490960
14	;g-···	7220676582167490951	Conversations on this platform are very limited.	380363178490960
15	)likz7Z	7220676762094747353	Understood.	315083558365988
16		7220678605628151790	Here is the link for join group.	380363178490960
17		7220679015982082949	https://bit.ly/3Yebc0U	380363178490960
18		7220679333337687506	Is it working?	315083558365988

[그림 8] - 대화 기록1

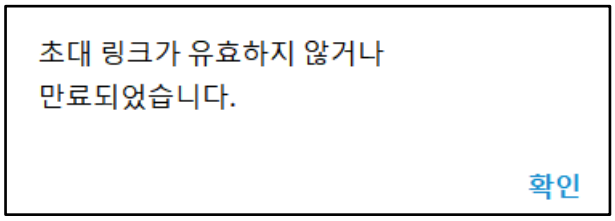
7220679401345037622	Not to me.	315083558365988
7220679440490238045	Let me check.	380363178490960
7220679630465100957	You need to remove last forward-slash.	380363178490960
7220679699442532574	Got it.	315083558365988
7220679771676574220	And you need to passcode for join group.	380363178490960
7220680134658803211	Passcode is 374692	380363178490960
7220680299158410989	NULL	315083558365988

[그림 9] - 대화 기록2

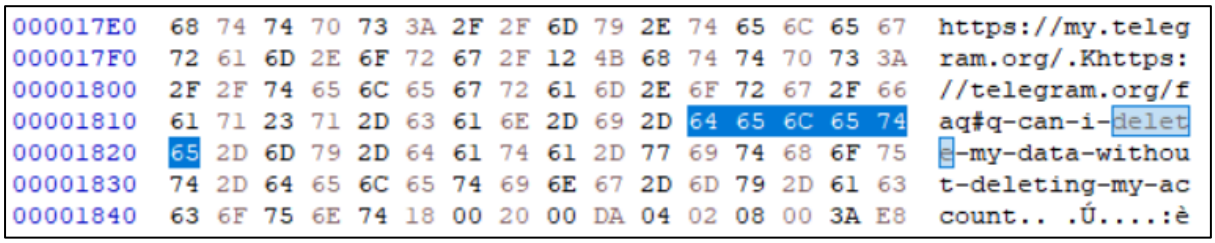
device owner로 판단되는 joshua가 **https://bit.ly/3Yebc0U**라는 링크를 보냈고, 이는 **https://t.me/+I03dyCNRbSRhZTg1**로 리다이렉트되며 대화에서 나눈 텔레그램 그룹 챗 초대 주소임을 알 수 있습니다. Joshua가 Passcode까지 제공하였지만, 아래 Alice의 마지막 대화 내역은 NULL로 확인할 수 없었습니다.



[그림 10] 초대링크 리다이렉션 확인



[그림 11] 초대링크 만료



[그림 12] com.android.vending₩cache₩streamdatastore₩streamdatastore.db 내 흔적

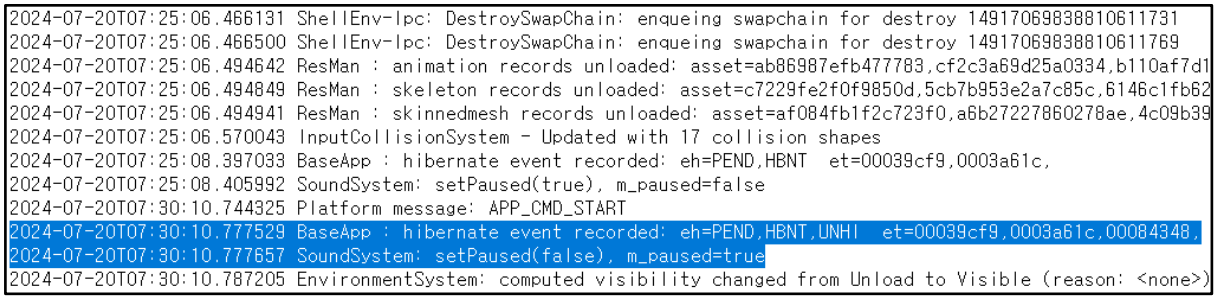
다만, 위 그림들을 통해 device owner가 건넨 link는 현재 만료되었으며, 텔레그램을 통해 메시지를 주고 받았다면 org.telegram.messenger 패키지 내 아티팩트가 존재해야 하지만 없는 것으로 확인됩니다. 또한, 그림 12와 같이 streamdatastore.db 내 데이터 삭제 여부와 관련된 질문으로 미루어 볼 때, 간접적으로 흔적을 남기지 않은 것으로 유추됩니다. 따라서, 문제를 직역하여 링크의 사용처나 용도를 의미하는 것이라면 Joshua의 **텔레그램 그룹 초대 입장 링크로** 보이며, 링크의 사용 여부를 묻는 것이라면 **링크의 사용여부는 알 수 없는 것으로 판단됩니다.**

6) What was the last wearing time of HMD? (20 points)

HMD의 마지막 착용 시간은 각주 1의 reference를 참고해보았을 때, DEVICE#01 내 com.oculus.shellenv에서 확인할 수 있습니다.

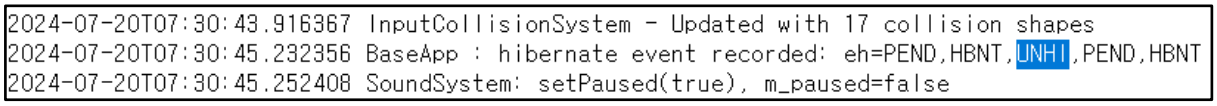
[그림 13] com.oculus.shellenv₩files₩log 내 파일들

해당 로그 파일들에서 user가 HMD를 착용해제했을 때 hibernate 상태(로 돌입하고, 다시 착용하였을 때는 unhibernate 상태로 기록된다. 4개의 shellenv.log 파일 중 가장 최근 로그를 기록하는 shellenv.log 파일에서 마지막으로 착용한 시간을 다음과 같이 확인할 수 있습니다.



[그림 14] shellenv.log 내 가장 마지막 unhibernate log 확인

[그림 15] unhibernate 이후 PENDING



[그림 16] PENDING 이후 다시 hibernate log 확인

위 그림들을 통해 가장 마지막으로 기록된 unhibernate log를 확인하였습니다. 각주 1의 reference와는 조금 다른 로그이지만 [그림 13]의 BaseApp에서 eh 파라미터에 UNHI라는 문자가 기록되었고, SoundSystem의 이벤트 타입에서는 기존에 Unhibernate log에서 보이는 setPaused(false), m_paused=true가 기록되어 있습니다. 그 후, [그림 14]와 [그림 15]를 통해 UNHI 이후 PEND, HBNT가 순차적으로 기록되며 다시 hibernate에 돌입하는 것으로 볼 때, HMD를 마지막으로 착용한 시간은 user의 local zone에 맞춰지는 타임스탬프에 따라 2024-07-20T07:30:10으로 파악됩니다.

답: 2024-07-20T07:30:10