# 151 – Android Live

## Team Information

**Team Name: kimbabasaksaksak**

**Team Member: Jaeheon Kim, Donghyun Kim, Soyoung Yoo, Minhee Lee**

**Email Address : uaaoong@gmail.com**

## Instructions

**Description** Analyze provided Android live acquisition data and answer questions.

| Target | Hash (MD5) |
|---|---|
| SM-F721N_Live.zip | F2F4D387879E2CAF854DB8247C6D421B |

**Questions**

1) What are the user's Google, YouTube, and Instagram account names? (30 points)
2) What is the SSID and location (latitude, longitude coordinates) of the wireless network to which the evidence smartphone is connected? (30 points)
3) Which photos taken with a smartphone have an edited EXIF timestamp? (30 points)
4) Which photos uploaded to Instagram were not taken on the evidence smartphone? (30 points)
5) What smartphone were the photo files found in question 4 taken on? (30 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).

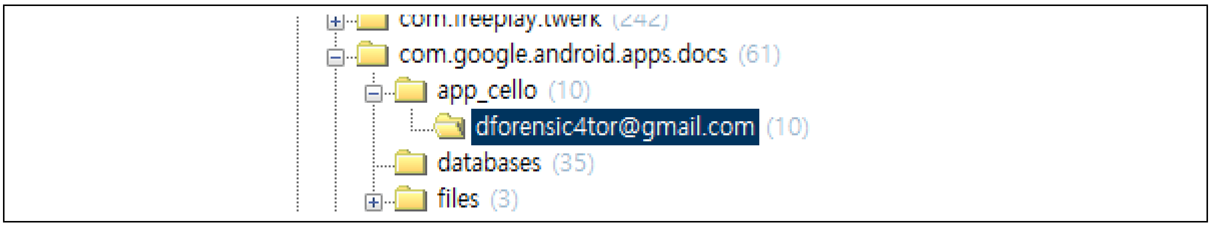
## Tools used:

| | | | |
|---|---|---|---|
| Name: | X-Ways Forensics | Publisher: | X-Ways |
| Version: | 20.2 | | |
| URL: | https://www.x-ways.net | | |

## Step-by-step methodology:

### 1. What are the user's Google, YouTube, and Instagram account names?

**[Google account account name]**



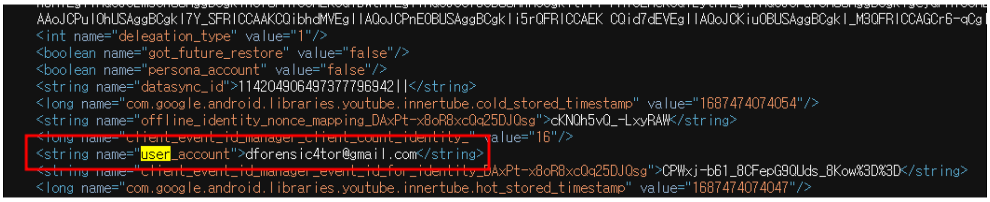
```
com.freeplay.twerk (242)
com.google.android.apps.docs (61)
  app_cello (10)
    dforensic4tor@gmail.com (10)
  databases (35)
  files (3)
```

[그림 1-1] Google account name – dforensic4tor@gmail.com

구글 계정명으로 생성되는 [1]폴더 경로에서 계정명 "dforensic4tor@gmail.com" 확인 가능.

[1] ₩data₩com.google.android.apps.docs₩dforensic4tor@gmail.com

**[Yotube account name]**



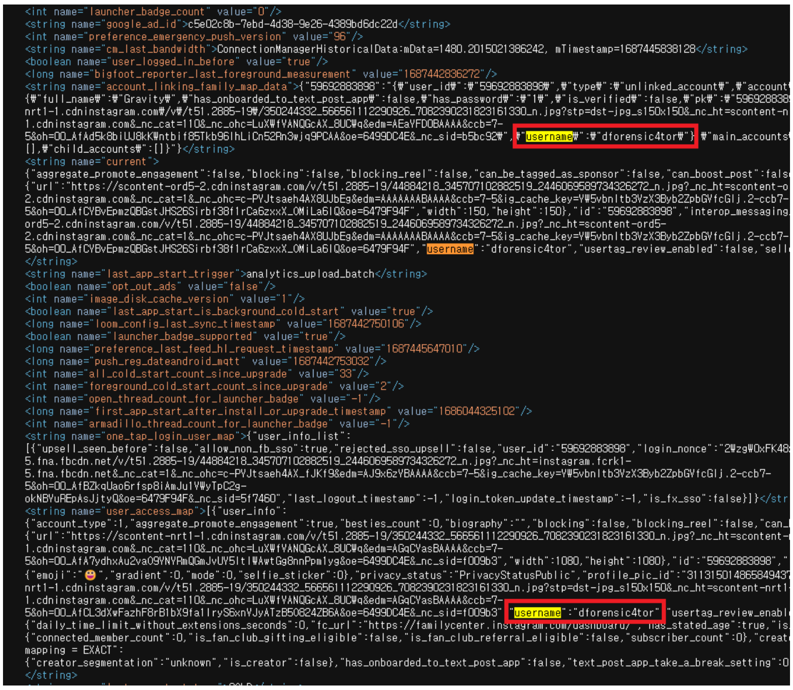
```
AAoJCPuIOhUSAggBCgkI7Y_SFRICCAAKCQibhdMVEgIIAQoJCPnEOBUSAggBCgkIi5rQFRICCAEK CQid7dEVEgIIAQoJCKiuOBUSAggBCgkI_M3QFRICCAGCr6-qCg
<int name="delegation_type" value="1"/>
<boolean name="got_future_restore" value="false"/>
<boolean name="persona_account" value="false"/>
<string name="datasync_id">114204906497377796942||</string>
<long name="com.google.android.libraries.youtube.innertube.cold_stored_timestamp" value="1687474074054"/>
<string name="offline_identity_nonce_mapping_DAxPt-x8oR8xcQq25DJQsg">cKNQh5vQ_-LxyRAW</string>
<long name="client_event_id_manager_client_count_identity_" value="16"/>
<string name="user_account">dforensic4tor@gmail.com</string>
<string name="client_event_id_manager_event_id_for_identity_DAxPt-x8oR8xcQq25DJQsg">CPWxj-b61_8CFepG9QUds_8Kow%3D%3D</string>
<long name="com.google.android.libraries.youtube.innertube.hot_stored_timestamp" value="1687474074047"/>
```

[그림 1-2] Youtube account name – dforensic4tor@gmail.com

유튜브 계정명이 존재하는 [1]아티팩트(youtube.xml)에서 계정명 "dforensic4tor@gmail.com" 확인 가능.

[1] ₩data₩com.google.android.youtube₩shared_prefs₩youtube.xml

**[Instagram account name]**



```
<int name="launcher_badge_count" value="0"/>
<string name="google_ad_id">c5e02c8b-7ebd-4d38-9e26-4389bd6dc22d</string>
<int name="preference_emergency_push_version" value="96"/>
<string name="cm_last_bandwidth">ConnectionManagerHistoricalData:mData=1480.2015021386242, mTimestamp=1687445838128</string>
<boolean name="user_logged_in_before" value="true"/>
<long name="bigfoot_reporter_last_foreground_measurement" value="1687442836272"/>
<string name="account_linking_family_map_data">{"59692883898":"{₩"user_id₩":₩"59692883898₩",₩"type₩":₩"unlinked_account₩",₩"account₩
{₩"full_name₩":₩"Gravity₩",₩"has_onboarded_to_text_post_app₩":false,₩"has_password₩":₩"1₩",₩"is_verified₩":false,₩"pk₩":₩"596928838
nrt1-1.cdninstagram.com₩/v₩/t51.2885-19₩/350244332_566561112290926_7082390231823161330_n.jpg?stp=dst-jpg_s150x150&_nc_ht=scontent-n
1.cdninstagram.com&_nc_cat=110&_nc_ohc=LuX₩fVANQGcAX_8UC₩q&edm=AEaYFDOBAAAA&ccb=7-
5&oh=00_AfAd5k8biUJ8kK₩ntbif85Tkb96IhLiCn52Rn3wjq9PCAA&oe=6499DC4E&_nc_sid=b5bc92₩",₩"username₩":₩"dforensic4tor₩"},₩"main_accounts₩
[],₩"child_accounts₩":[]}"}</string>
<string name="current">
{"aggregate_promote_engagement":false,"blocking":false,"blocking_reel":false,"can_be_tagged_as_sponsor":false,"can_boost_post":fals
{"url":"https://scontent-ord5-2.cdninstagram.com/v/t51.2885-19/44884218_345707102882519_2446069589734326272_n.jpg?_nc_ht=scontent-o
2.cdninstagram.com&_nc_cat=1&_nc_ohc=c-PYJtsaeh4AX8UJbEg&edm=AAAAAAABAAAA&ccb=7-5&ig_cache_key=Y₩5vbnltb3VzX3Byb2ZpbGVfcGlj.2-ccb7-
5&oh=00_AfCYBvEpmzQBGstJHS26Sirbf38f1rCa6zxxX_OMiLa6lQ&oe=6479F94F","width":150,"height":150},"id":"59692883898","interop_messaging
ord5-2.cdninstagram.com/v/t51.2885-19/44884218_345707102882519_2446069589734326272_n.jpg?_nc_ht=scontent-ord5-
2.cdninstagram.com&_nc_cat=1&_nc_ohc=c-PYJtsaeh4AX8UJbEg&edm=AAAAAAABAAAA&ccb=7-5&ig_cache_key=Y₩5vbnltb3VzX3Byb2ZpbGVfcGlj.2-ccb7-
5&oh=00_AfCYBvEpmzQBGstJHS26Sirbf38f1rCa6zxxX_OMiLa6lQ&oe=6479F94F","username":"dforensic4tor","usertag_review_enabled":false,"sell
</string>
<string name="last_app_start_trigger">analytics_upload_batch</string>
<boolean name="opt_out_ads" value="false"/>
<int name="image_disk_cache_version" value="1"/>
<boolean name="last_app_start_is_background_cold_start" value="true"/>
<long name="loom_config_last_sync_timestamp" value="1687442750106"/>
<boolean name="launcher_badge_supported" value="true"/>
<long name="preference_last_feed_hl_request_timestamp" value="1687445647010"/>
<long name="push_reg_dateandroid_mqtt" value="1687442753032"/>
<int name="all_cold_start_count_since_upgrade" value="33"/>
<int name="foreground_cold_start_count_since_upgrade" value="2"/>
<int name="open_thread_count_for_launcher_badge" value="-1"/>
<long name="first_app_start_after_install_or_upgrade_timestamp" value="1686044325102"/>
<int name="armadillo_thread_count_for_launcher_badge" value="-1"/>
<string name="one_tap_login_user_map">{"user_info_list":
[{"upsell_seen_before":false,"allow_non_fb_sso":true,"rejected_sso_upsell":false,"user_id":"59692883898","login_nonce":"2₩zg₩OxFK48
5.fna.fbcdn.net/v/t51.2885-19/44884218_345707102882519_2446069589734326272_n.jpg?_nc_ht=instagram.fcrk1-
5.fna.fbcdn.net&_nc_cat=1&_nc_ohc=c-PYJtsaeh4AX_fJKf9&edm=AJ9x6zYBAAAA&ccb=7-5&ig_cache_key=Y₩5vbnltb3VzX3Byb2ZpbGVfcGlj.2-ccb7-
5&oh=00_AfBZkqUao6rfsp8iAmJu1V₩yTpC2g-
okNBYuREpAsJjtyQ&oe=6479F94F&_nc_sid=5f7460","last_logout_timestamp":-1,"login_token_update_timestamp":-1,"is_fx_sso":false}]}</str
<string name="user_access_map">[{"user_info":
{"account_type":1,"aggregate_promote_engagement":true,"besties_count":0,"biography":"","blocking":false,"blocking_reel":false,"can_
{"url":"https://scontent-nrt1-1.cdninstagram.com/v/t51.2885-19/350244332_566561112290926_7082390231823161330_n.jpg?_nc_ht=scontent-
1.cdninstagram.com&_nc_cat=110&_nc_ohc=LuX₩fVANQGcAX_8UC₩q&edm=AGqCYasBAAAA&ccb=7-
5&oh=00_AfA7ydhxAu2va09YNYRmQGmJvUY5ltI₩AwtGg8nnPpm1yg&oe=6499DC4E&_nc_sid=f009b3","width":1080,"height":1080},"id":"59692883898","
{"emoji":"😛","gradient":0,"mode":0,"selfie_sticker":0},"privacy_status":"PrivacyStatusPublic","profile_pic_id":"311315014865849437
nrt1-1.cdninstagram.com/v/t51.2885-19/350244332_566561112290926_7082390231823161330_n.jpg?stp=dst-jpg_s150x150&_nc_ht=scontent-nrt1-
1.cdninstagram.com&_nc_cat=110&_nc_ohc=LuX₩fVANQGcAX_8UC₩q&edm=AGqCYasBAAAA&ccb=7-
5&oh=00_AfCL3dXwFazhF8rB1bX9fallryS6xnVJyATzB50824ZB6A&oe=6499DC4E&_nc_sid=f009b3","username":"dforensic4tor","usertag_review_enabl
{"daily_time_limit_without_extensions_seconds":0,"fc_url":"https://familycenter.instagram.com/dashboard/","has_stated_age":true,"is
{"connected_member_count":0,"is_fan_club_gifting_eligible":false,"is_fan_club_referral_eligible":false,"subscriber_count":0},"creat
mapping = EXACT":
{"creator_segmentation":"unknown","is_creator":false},"has_onboarded_to_text_post_app":false,"text_post_app_take_a_break_setting":0
</string>
```

[그림 1-3] Instagram account name – dforensic4tor

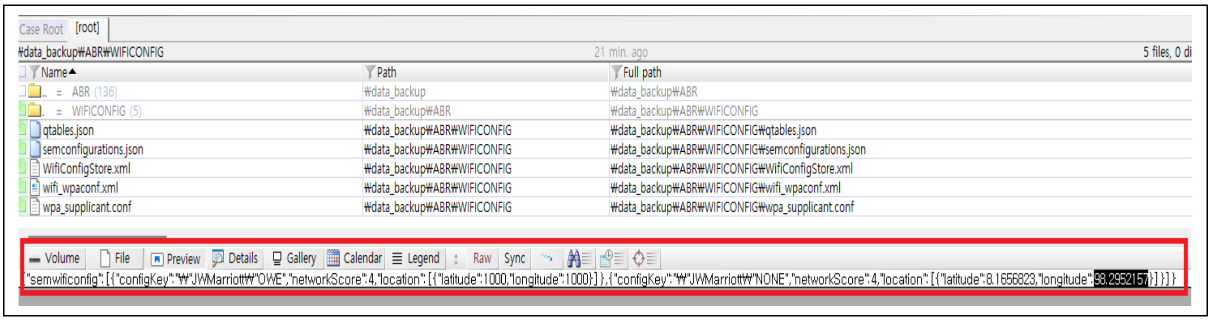
인스타그램 계정명 정보가 존재하는 [1]아티팩트(com.instagram.android_preferences.xml)에서 계정명 "dforensic4tor" 식별 가능.

[1] ₩data₩com.instagram.android₩shared_prefs₩com.instagram.android_preferences.xml

**[1번 답안]**

| Platform | Account Name |
|---|---|
| Google | dforensic4tor@gmail.com |
| Youtube | dforensic4tor@gmail.com |
| Instagram | dforensic4tor |

## 2. What is the SSID and location (latitude, longitude coordinates) of the wireless network to which the evidence smartphone is connected?



₩data_backup₩ABR₩WIFICONFIG

| Name▲ | Path | Full path |
|---|---|---|
| .. = ABR (136) | ₩data_backup | ₩data_backup₩ABR |
| . = WIFICONFIG (5) | ₩data_backup₩ABR | ₩data_backup₩ABR₩WIFICONFIG |
| qtables.json | ₩data_backup₩ABR₩WIFICONFIG | ₩data_backup₩ABR₩WIFICONFIG₩qtables.json |
| semconfigurations.json | ₩data_backup₩ABR₩WIFICONFIG | ₩data_backup₩ABR₩WIFICONFIG₩semconfigurations.json |
| WifiConfigStore.xml | ₩data_backup₩ABR₩WIFICONFIG | ₩data_backup₩ABR₩WIFICONFIG₩WifiConfigStore.xml |
| wifi_wpaconf.xml | ₩data_backup₩ABR₩WIFICONFIG | ₩data_backup₩ABR₩WIFICONFIG₩wifi_wpaconf.xml |
| wpa_supplicant.conf | ₩data_backup₩ABR₩WIFICONFIG | ₩data_backup₩ABR₩WIFICONFIG₩wpa_supplicant.conf |

```
"semwificonfig":[{"configKey":"₩"JWMarriott₩"OWE","networkScore":4,"location":[{"latitude":1000,"longitude":1000}]},{"configKey":"₩"JWMarriott₩"NONE","networkScore":4,"location":[{"latitude":8.1656823,"longitude":98.2952157}]}]}
```

[그림 2-1] SSID and location

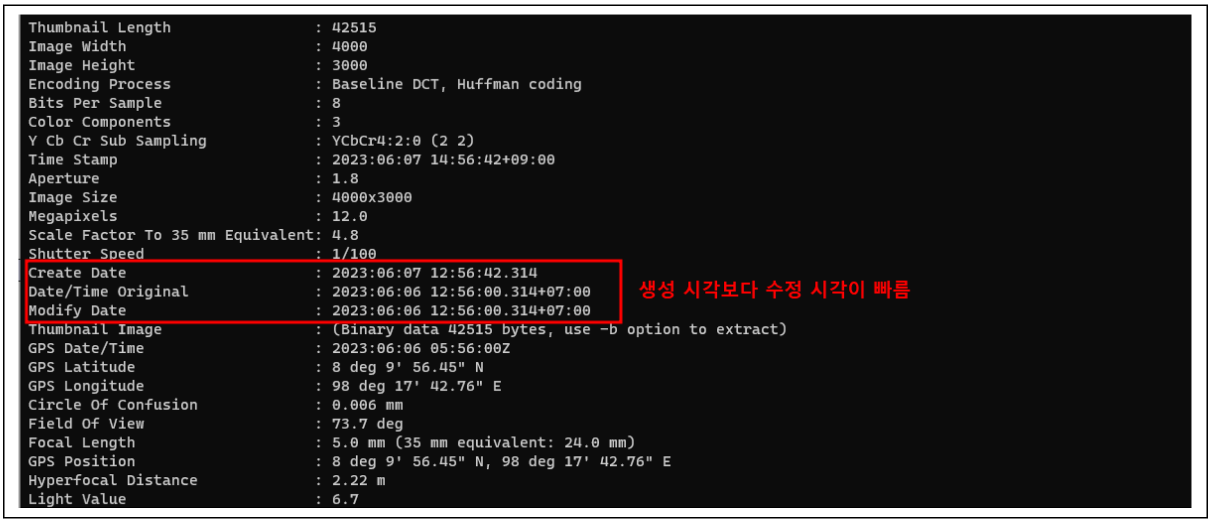
SSID와 위치 정보 값이 존재하는 [1]아티팩트 경로에서 식별 가능함.

[1] ₩data_backup₩ABR₩WIFICONFIG₩

### [2번 답안]

| Artifact | Type | Value |
|---|---|---|
| wap_supplicant.conf | SSID | JWMarriott |
| Semconfigurations.json | Location | Latitude - 8.1656823<br>Longitude – 98.2952157 |

## 3. Which photos taken with a smartphone have an edited EXIF timestamp?



```
Thumbnail Length                : 42515
Image Width                     : 4000
Image Height                    : 3000
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Time Stamp                      : 2023:06:07 14:56:42+09:00
Aperture                        : 1.8
Image Size                      : 4000x3000
Megapixels                      : 12.0
Scale Factor To 35 mm Equivalent: 4.8
Shutter Speed                   : 1/100
Create Date                     : 2023:06:07 12:56:42.314
Date/Time Original              : 2023:06:06 12:56:00.314+07:00
Modify Date                     : 2023:06:06 12:56:00.314+07:00
Thumbnail Image                 : (Binary data 42515 bytes, use -b option to extract)
GPS Date/Time                   : 2023:06:06 05:56:00Z
GPS Latitude                    : 8 deg 9' 56.45" N
GPS Longitude                   : 98 deg 17' 42.76" E
Circle Of Confusion             : 0.006 mm
Field Of View                   : 73.7 deg
Focal Length                    : 5.0 mm (35 mm equivalent: 24.0 mm)
GPS Position                    : 8 deg 9' 56.45" N, 98 deg 17' 42.76" E
Hyperfocal Distance             : 2.22 m
Light Value                     : 6.7
```

생성 시각보다 수정 시각이 빠름

[그림 3-1] Suspect image file information (20230607_125642.jpg)

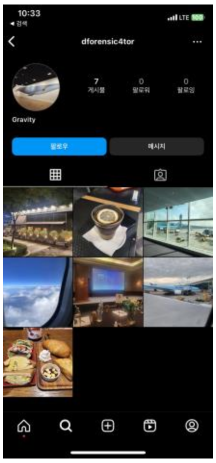
스마트폰에 존재하는 이미지 중 단 하나의 [1]이미지(20230607_125642.jpg)에서만 생성 시각보다 수정된 시각이 빠르게 설정된 것을 확인할 수 있음.

[1] ₩media₩DCIM₩Camera₩20230607_125642.jpg

**[3번 답안]**

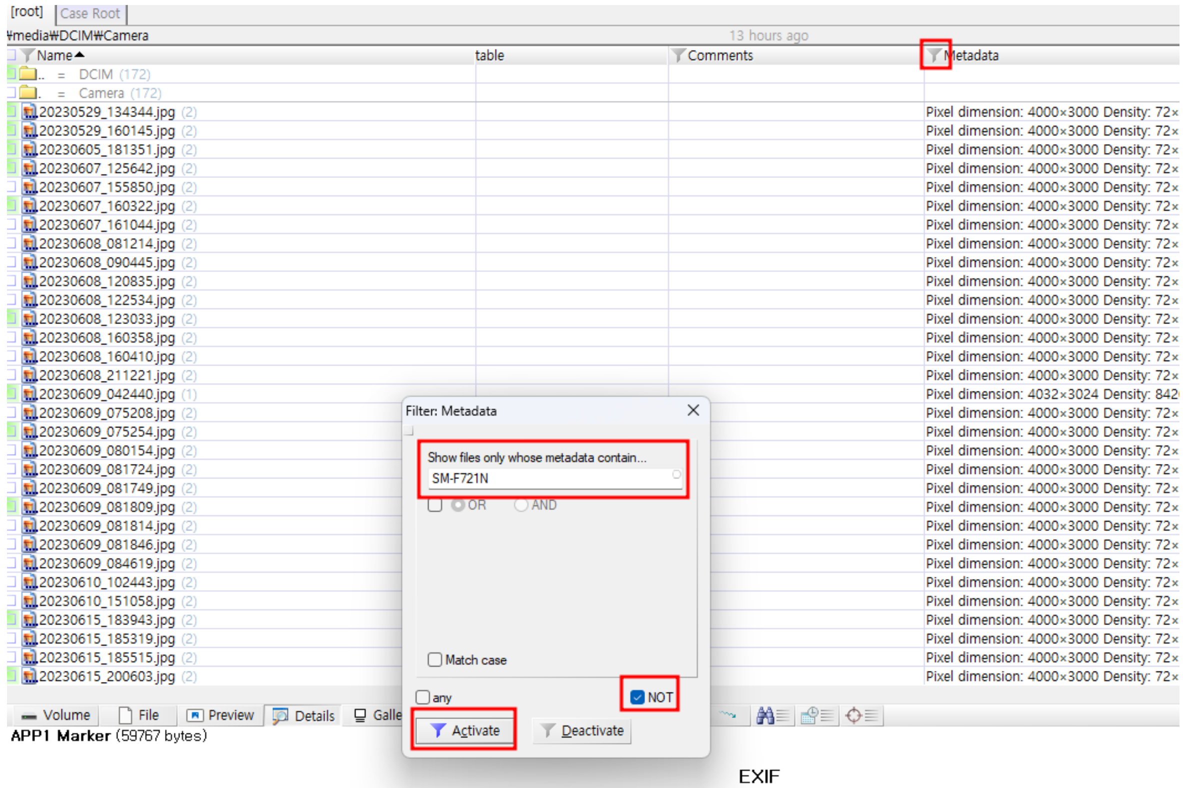
20230607_125642.jpg

## 4. Which photos uploaded to Instagram were not taken on the evidence smartphone?



[그림 4-1] Photos uploaded to Instagram (dforensic4tor)

인스타그램에 업로드한 사진들은 해당 계정에서 식별이 가능함.



¥media₩DCIM₩Camera

| Name | table | Comments | Metadata |
|---|---|---|---|
| .. = DCIM (172) | | | |
| . = Camera (172) | | | |
| 20230529_134344.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230529_160145.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230605_181351.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230607_125642.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230607_155850.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230607_160322.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230607_161044.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230608_081214.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230608_090445.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230608_120835.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230608_122534.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230608_123033.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230608_160358.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230608_160410.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230608_211221.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230609_042440.jpg (1) | | | Pixel dimension: 4032×3024 Density: 842 |
| 20230609_075208.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230609_075254.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230609_080154.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230609_081724.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230609_081749.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230609_081809.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230609_081814.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230609_081846.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230609_084619.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230610_102443.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230610_151058.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230615_183943.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230615_185319.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230615_185515.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |
| 20230615_200603.jpg (2) | | | Pixel dimension: 4000×3000 Density: 72× |

Filter: Metadata

Show files only whose metadata contain...
SM-F721N

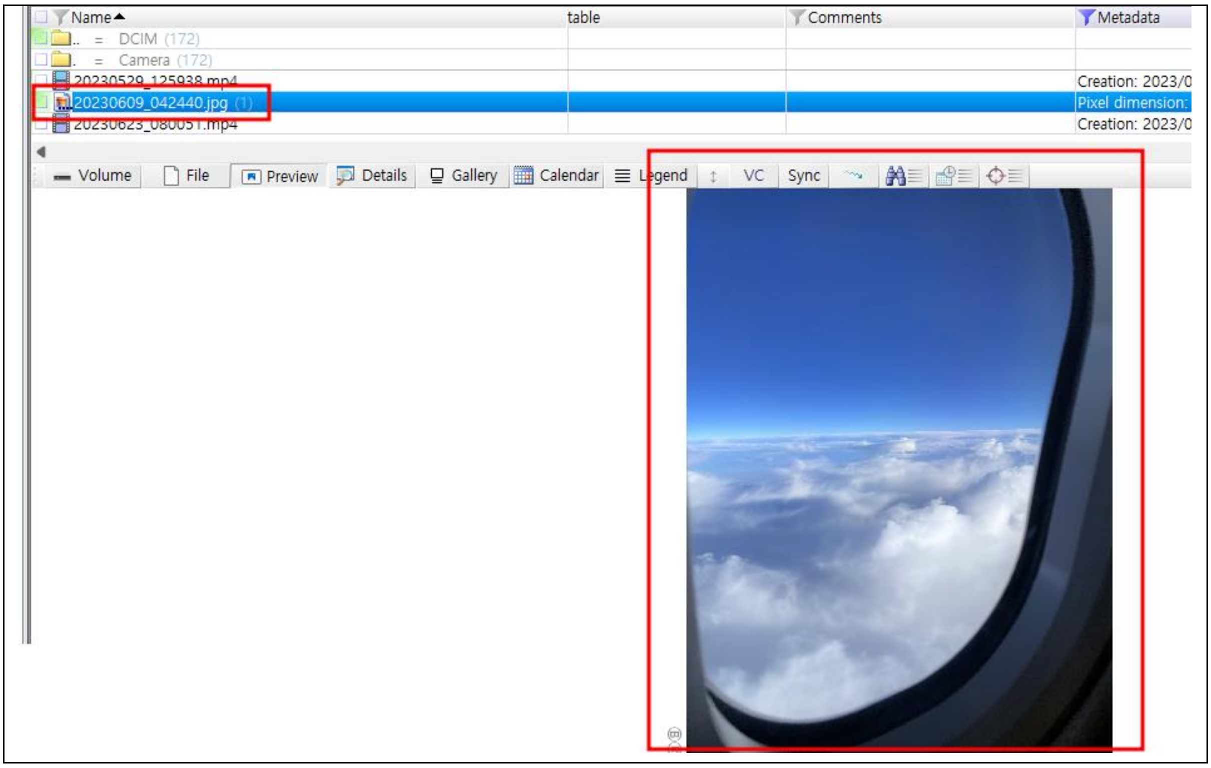
□ ● OR ○ AND

□ Match case

□ any ☑ NOT

APP1 Marker (59767 bytes)

EXIF



| Name | table | Comments | Metadata |
|---|---|---|---|
| .. = DCIM (172) | | | |
| . = Camera (172) | | | |
| 20230529_125938.mp4 | | | Creation: 2023/0 |
| 20230609_042440.jpg (1) | | | Pixel dimension: |
| 20230623_080051.mp4 | | | Creation: 2023/0 |

[그림 4-2] Suspect image file (20230609_042440.jpg)

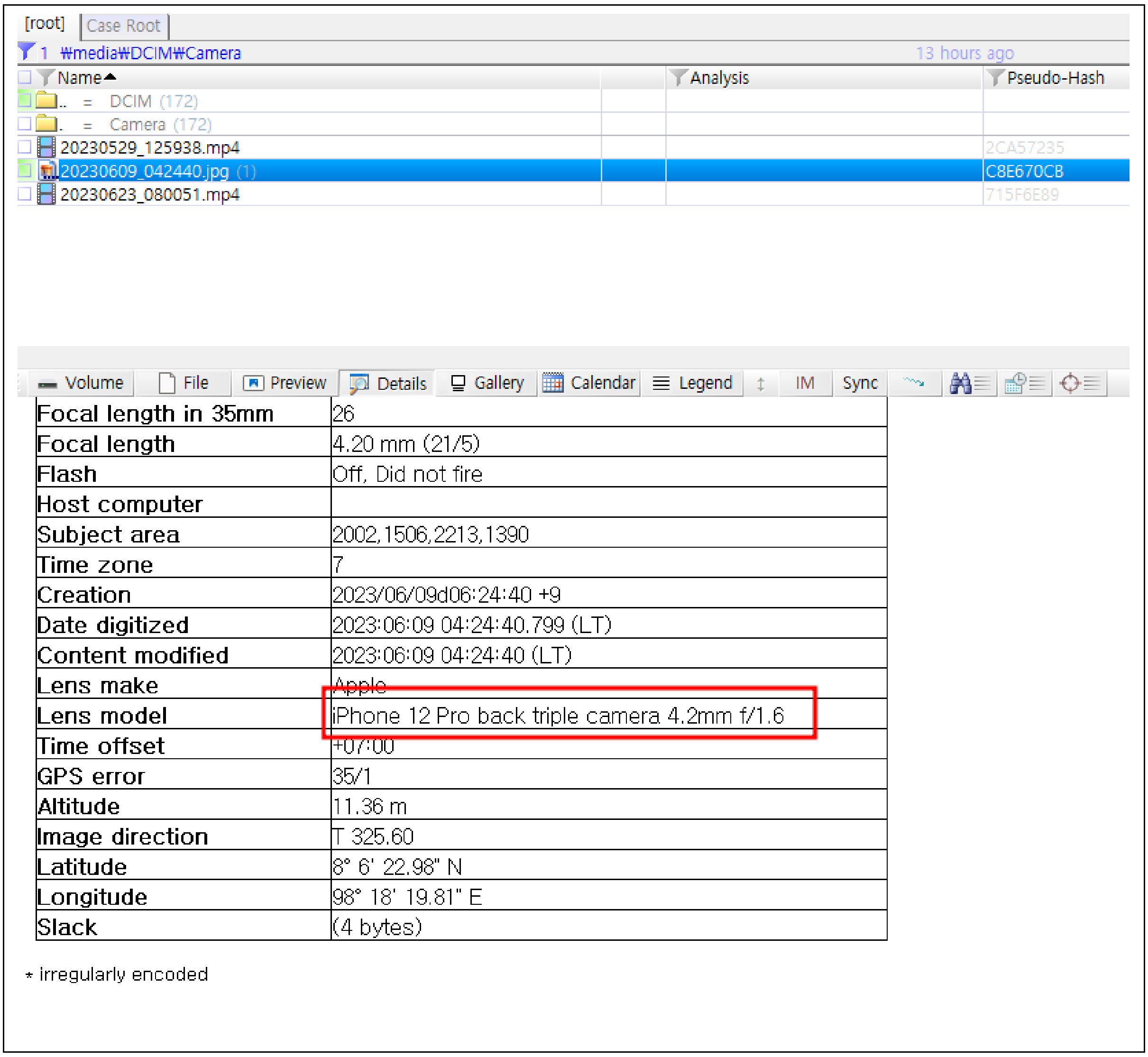
해당 스마트폰 모델(SAMSUNG SM-F721N)로 촬영되지 않은 이미지로 필터를 설정하여 검색하면 인스타그램에 업로드된 이미지 중 하나의 [1]이미지 파일(20230609_042440.jpg)이 검색됨.

[1] ₩media₩DCIM₩Camera₩20230609_042440.jpg

**[4번 답안]**

20230609_042440.jpg

## 5. What smartphone were the photo files found in question 4 taken on?



| Name | Analysis | Pseudo-Hash |
|---|---|---|
| .. = DCIM (172) | | |
| . = Camera (172) | | |
| 20230529_125938.mp4 | | 2CA57235 |
| 20230609_042440.jpg (1) | | C8E670CB |
| 20230623_080051.mp4 | | 715F6E89 |

| | |
|---|---|
| Focal length in 35mm | 26 |
| Focal length | 4.20 mm (21/5) |
| Flash | Off, Did not fire |
| Host computer | |
| Subject area | 2002,1506,2213,1390 |
| Time zone | 7 |
| Creation | 2023/06/09d06:24:40 +9 |
| Date digitized | 2023:06:09 04:24:40.799 (LT) |
| Content modified | 2023:06:09 04:24:40 (LT) |
| Lens make | Apple |
| Lens model | iPhone 12 Pro back triple camera 4.2mm f/1.6 |
| Time offset | +07:00 |
| GPS error | 35/1 |
| Altitude | 11.36 m |
| Image direction | T 325.60 |
| Latitude | 8° 6' 22.98" N |
| Longitude | 98° 18' 19.81" E |
| Slack | (4 bytes) |

[그림 5-1] Lens Model (20230609_042440.jpg)

해당 이미지 파일의 Lens model을 확인하면 iPhone 12 Pro 으로 촬영되었음을 알 수 있으며 실제 동일 기종으로 촬영된 Lens model 값 또한 일치하는 것을 확인하였음.

**[5번 답안]**

iPhone 12 Pro