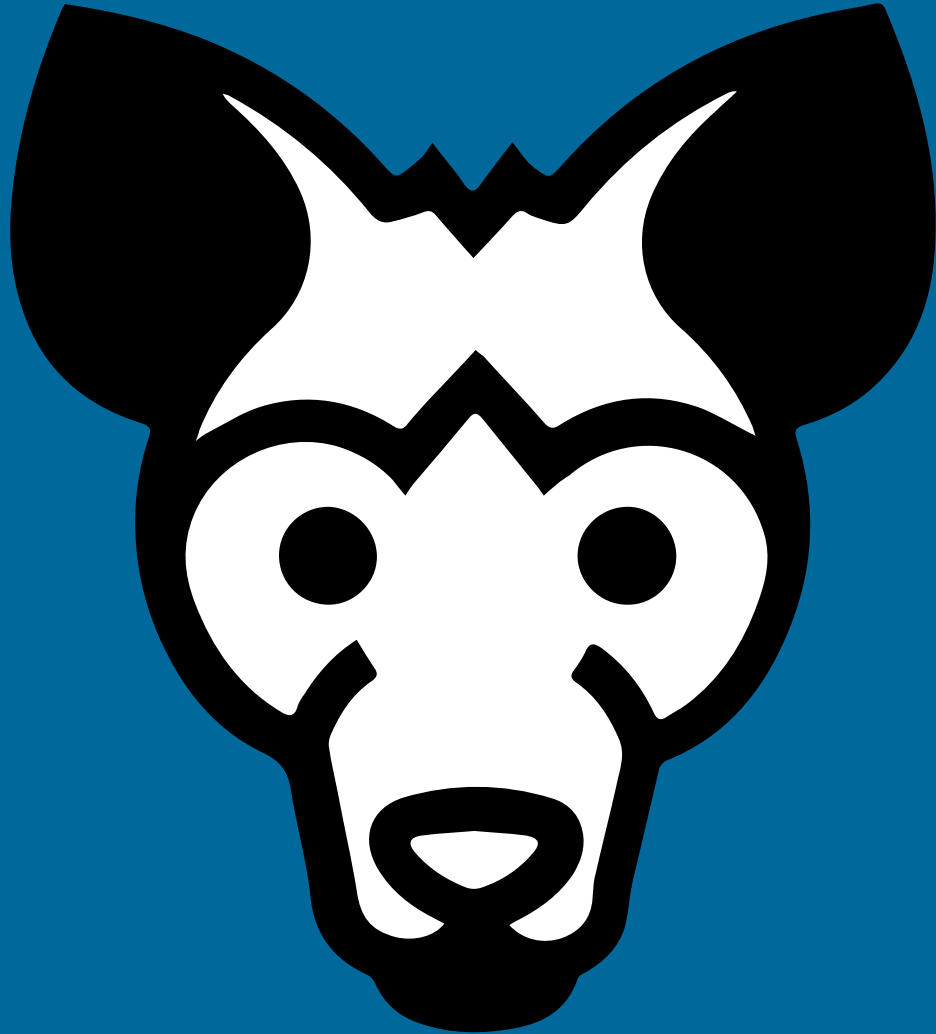




Netherlands Forensic Institute
Ministry of Justice and Security



Aardwolf

A. Boztas, MSc

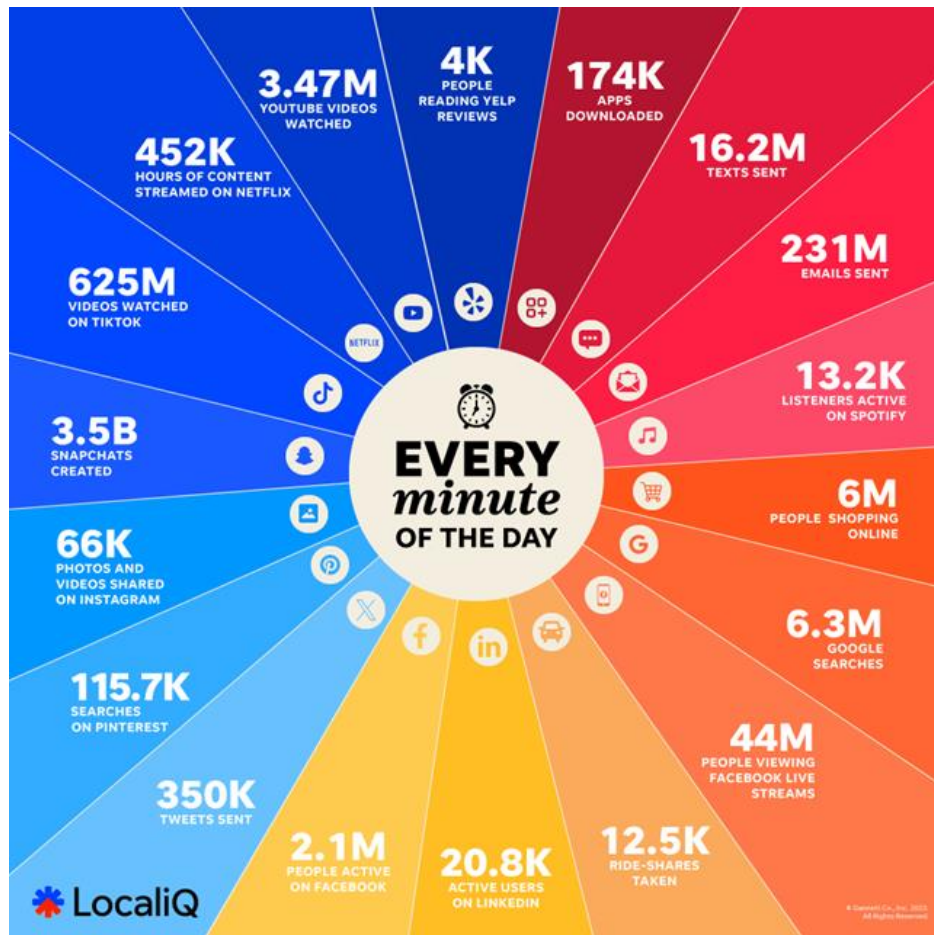


Challenges with app research





Challenges with app research





Netherlands Forensic Institute
Ministry of Justice and Security



Challenges with app research





Challenges with app research

- Relevant for each case
- Too many apps
- Limited time





Netherlands Forensic Institute
Ministry of Justice and Security



Challenges with app research





Project goals

- Platform
- Collaboration
- Sharing knowledge

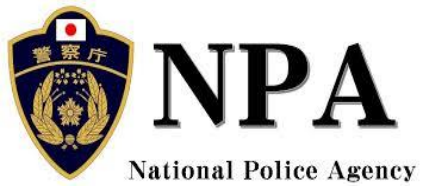




Netherlands Forensic Institute
Ministry of Justice and Security



International collaboration

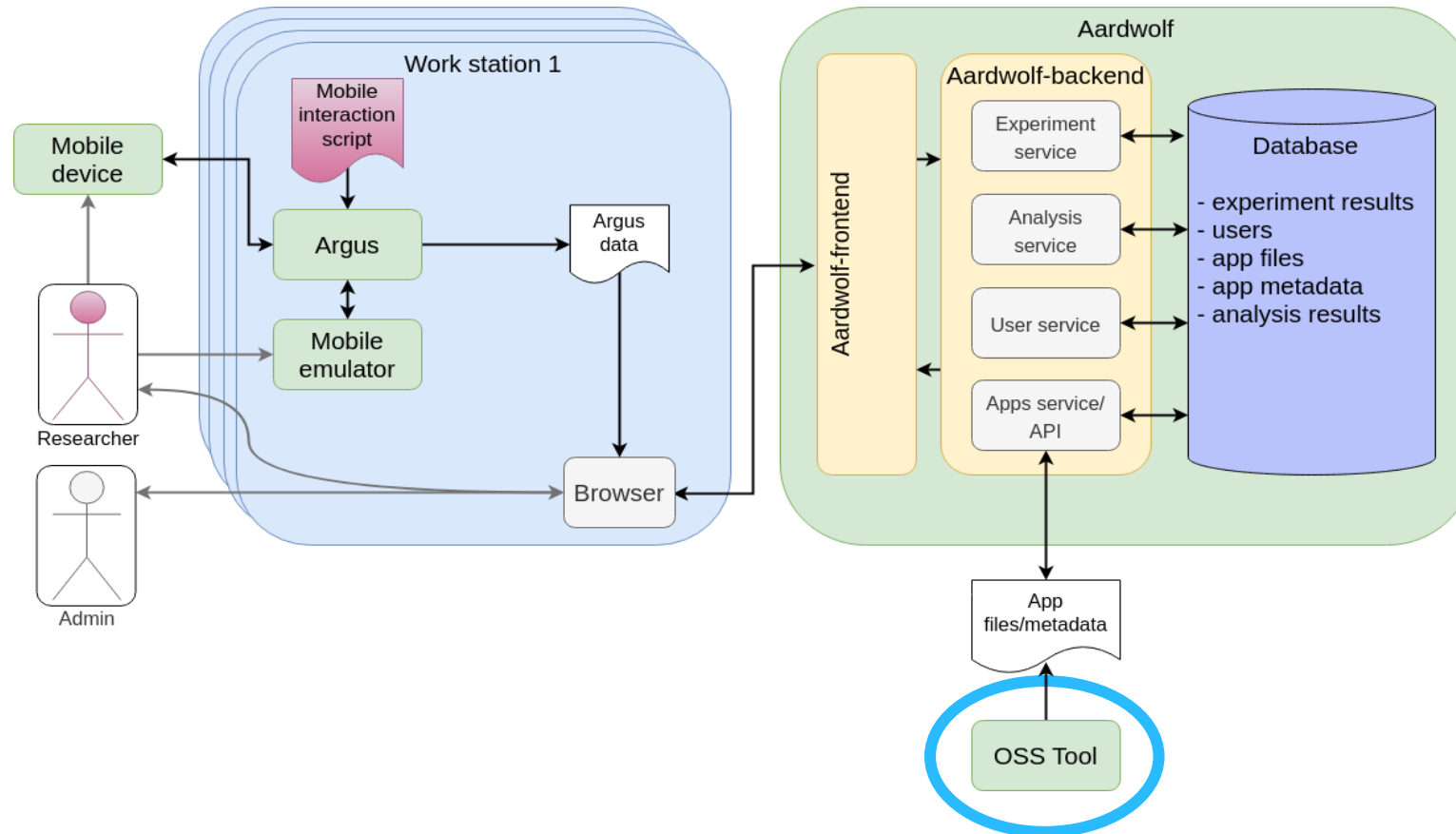


National Bureau of Investigation
Keskusrikospoliisi
Centralkriminalpolisen





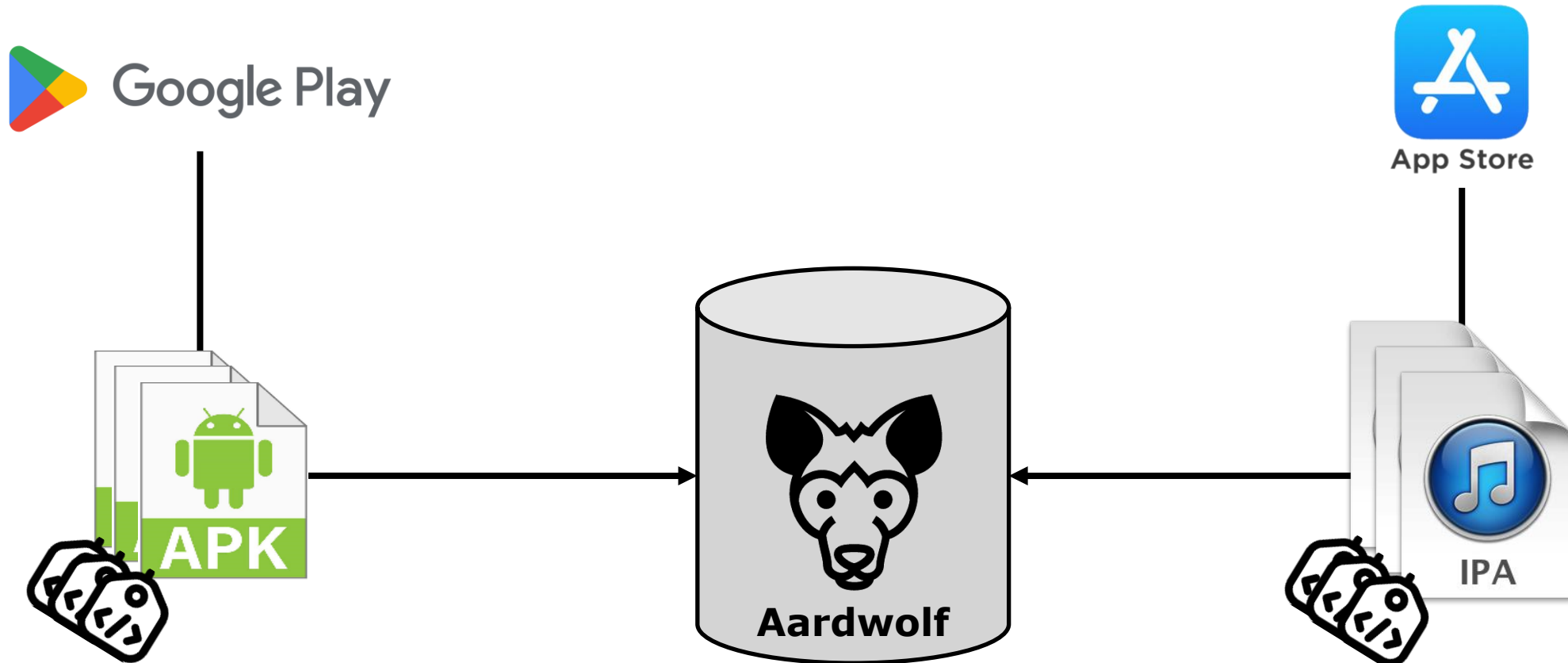
Architecture





Online Store Scraper (OSS tool)

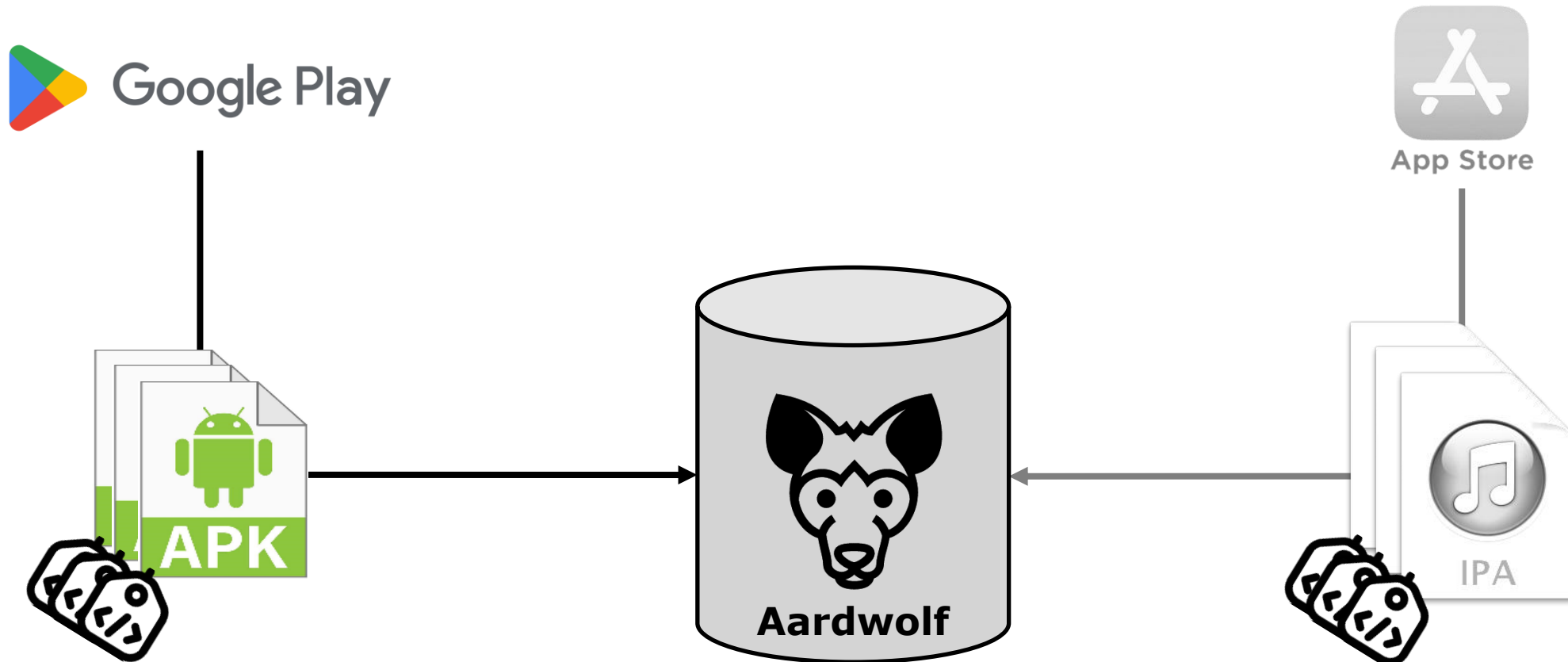
Store and share new versions of applications





Online Store Scraper (OSS tool)

Store and share new versions of applications



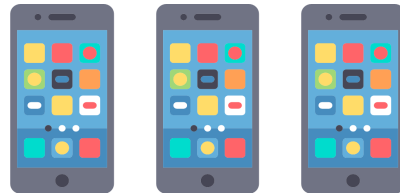


Online Store Scraper (OSS tool)

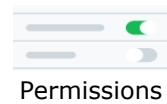
1. Update all apps



2. Updated apps



3. Get metadata



4. Store in AARDWOLF





- Home
- App search
- File search
- Data import
- Audit trail
- User Management
- Help

Search for Marketplace

Other App Store Play Store

Showing 30 versions of 1 app from a total of 145 apps in the database

Showing 30 versions

Applications

| App Name | Package Name | Version | Publisher | Marketplace | Number of experiments | Installation File |
|----------|---------------------|------------------|-----------|-------------|-----------------------|---------------------------|
| ▼ X | com.twitter.android | 10.1.0-release.0 | X Corp. | Play Store | 0 | arm64-v8a |

Description

The X app is the trusted digital town square for everyone. With X, you can: - Post content for the world to see and join public conversations - Stay up to date on breaking news - Go live with Spaces for audio or stream with Direct Messages - Subscribe to Blue to expand your reach, get a blue checkmark, and more - Earn a living creating exclusive content for your paid subscribers and share in the ad revenue generated in replies Communities around topics and interests, from sports to music to technology - Upload and watch videos up to 3 hours in length - Write and read long form posts - Connect directly with your customers to help your

Uploaded by

oss - 2023-08-02 04:37:52 UTC

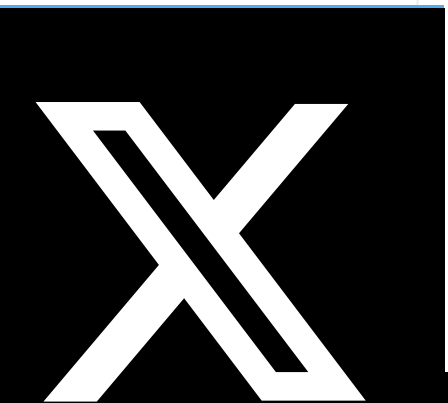
Last Modified

oss - 2023-08-02 04:37:52 UTC

| | | | | | | |
|-----------|---------------------|------------------|---------------|------------|---|---------------------------|
| ▼ Twitter | com.twitter.android | 9.71.0-release.0 | Twitter, Inc. | Play Store | 0 | arm64-v8a |
|-----------|---------------------|------------------|---------------|------------|---|---------------------------|

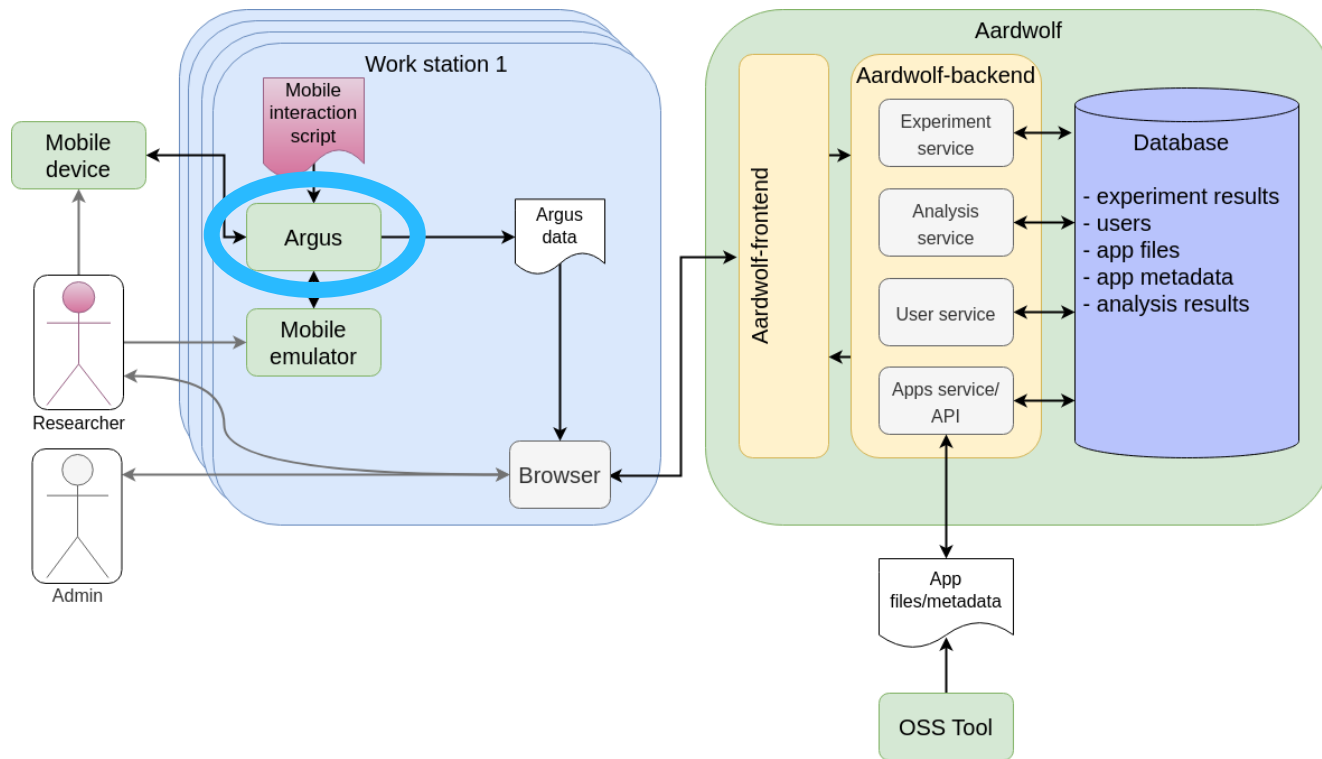
Description

Join the conversation! Expand your social network and stay updated on what's trending now. Retweet, chime in on a thread, go viral, or just scroll through the Twitter timeline to stay on top of what's happening, who's trending around the world. Twitter is your go-to social media app and the new media source for what's going on around the globe. Jump into the conversation with sound! Twitter Spaces is a new way to have live audio with the human voice. Engage authentically with fans and followers, listen and learn about your favorite creators, influential people and activists on their live Spaces. From tweeting to talking, Join, listen, and speak in live audio on trending topics in media, or get to know thought-leaders in the areas that matter to you; whether your interests range from celebrity tweets to politics, news updates, best podcast recommendations or football, you can connect with people or your friends alike. Every voice can impact the world. Follow your interests. Tweet, Retweet, Reply to Tweets, Share or Like - Twitter is the #1 social media app for latest news & updates. Trending Topics Get real-time insights on hashtags and trending topics to stay in the know. Follow the tweets of your favorite influencers and crime podcast hosts, alongside hundreds of interesting Twitter users, and read their content at a glance. Share your thoughts with noteworthy links, photos and videos. DM your friends or reply in a thread. Whether you chat privately or go viral, your voice makes a difference. Get noticed. Twitter allows you to find interesting people or build your network in you. Beyond chatting with friends, Twitter allows influencers to build a personal connection with their fans. Speak directly to the people who influence you - you may be surprised by how many answer back. ✓





Argus

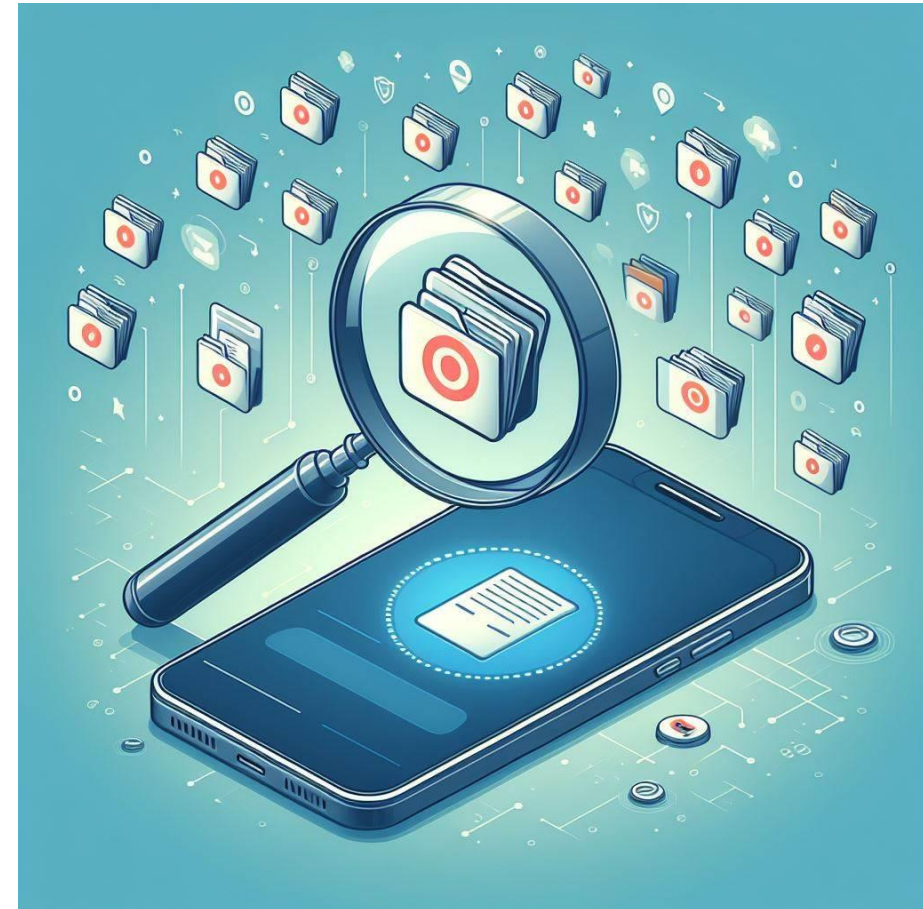




Argus

- Given an action performed using an app, which files are affected (created/modified/deleted)?
- Given information on a file, which app could have been involved in this?

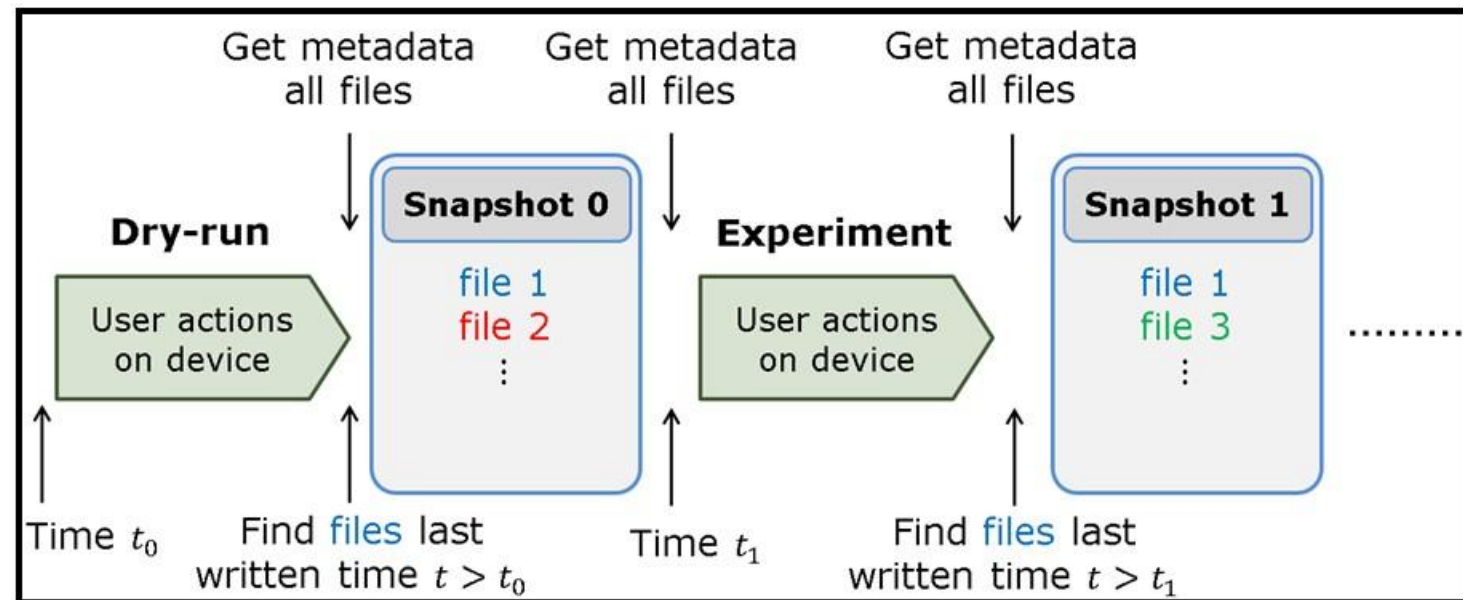
Apps ↔ Files/Traces





Argus

- Original approach, making images of phones:
 - Multiple images per experiment
 - Costs a lot of time/space
- Argus: uses metadata:
files created/modified/deleted
during a time frame





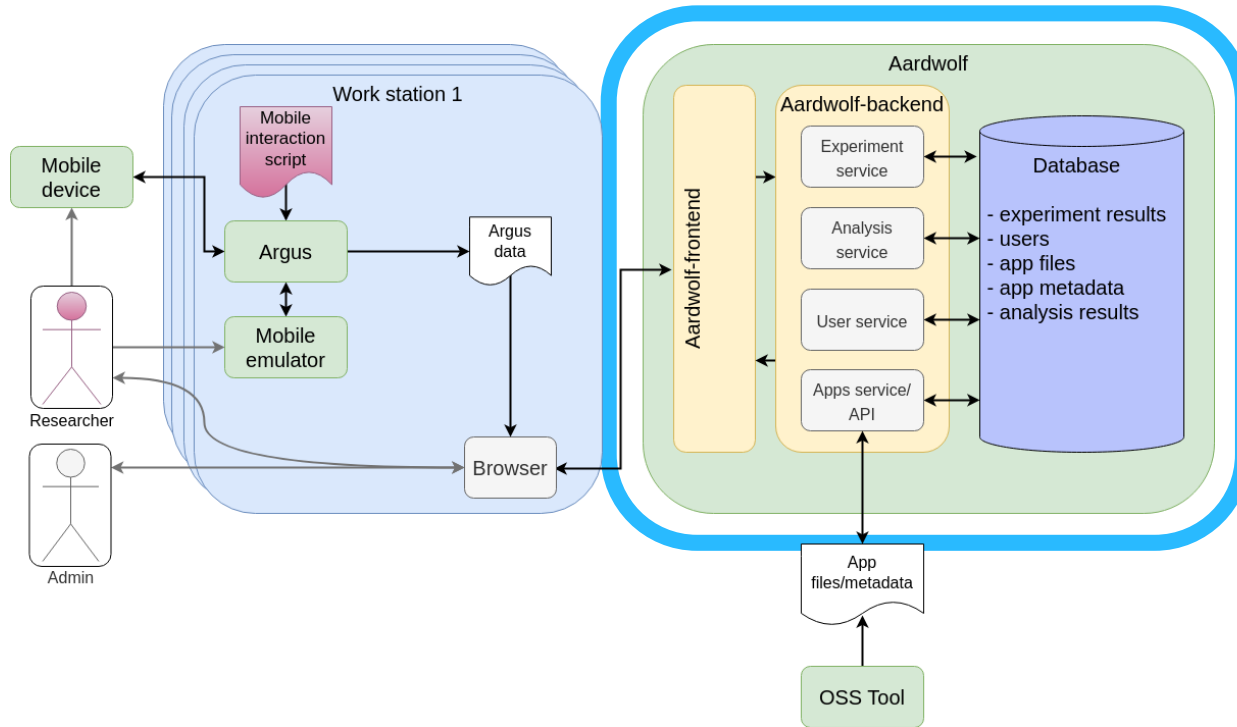
Argus

| Manual experiment Files metadata analysis | Scripted experiment – Roadmap | Additional Analysis - Roadmap |
|--|---|-----------------------------------|
| Android on Linux & Windows | Android (on Linux & Windows) | Ram acquisition & analysis |
| iOS on Linux & Windows | iOS (ONLY on MacOS) need of developer account (\$99 / year) | Network acquisition & analysis |
| | | Correlium automation |



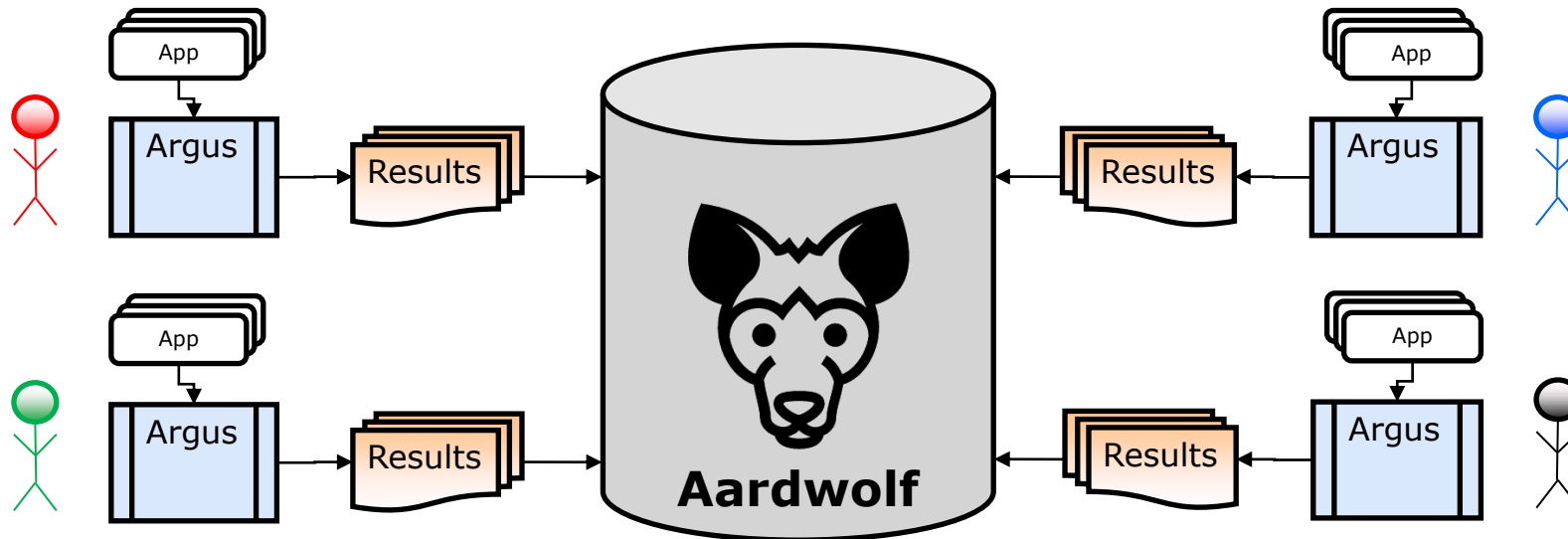


Aardwolf





Aardwolf



Application Analysis Results Directory With Open-source Library Foundation



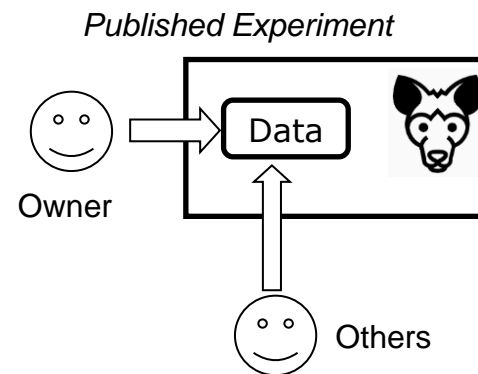
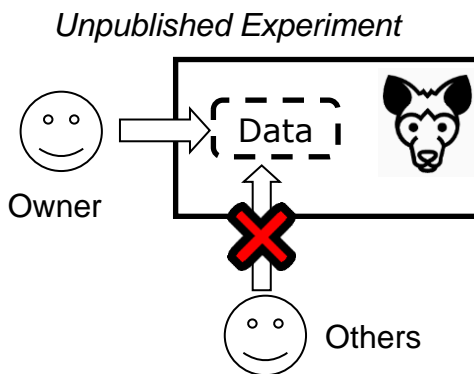
Aardwolf

- Store experiment results in an easily accessible and searchable way
- Having older app versions available facilitates
- Prevents 're-inventing the wheel'
 - Researchers can benefit from each other's work
 - The community can help itself
- Especially useful for (but not limited to) lesser-known apps
 - Popular apps are already supported by commercial tools
 - Support for less popular or regional apps is harder to find



Aardwolf

- The researcher doing the experiments 'owns' the experiment data
- Owners can choose to publish the results to the community (this is encouraged!)
- Experiment data is not visible to anyone but the owner until the result is published





Aardwolf

- Home
- App search
- File search
- Resources
- Data import
- Audit trail
- User Management
- System Info
- Help

<< Back Experiment Detail

Search

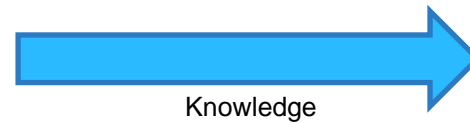
| | | | |
|----------|-------------|---------------------|-------------------------|
| App Name | App Version | Package identifier | User Actions |
| Camera | 2.0.002 | com.android.camera2 | Start app; Take picture |

| | |
|--|---|
| Experiment Description | Experiment Device |
| Scroll up from the android emulator, click on Camera app and take picture. Repeat picture for second experiment. New Argus | Device type: android with OS version: 9 and SDK version: 28 |

| Status | File Name | Filetype | Action | Path Name |
|-----------------------|--|------------|--------|---|
| Created In Snapshot 1 | system_app_strictmode@1699021192609.txt | text/plain | | /data/system/dropbox/system_app_strictmode@1699021192609.txt |
| Created In Snapshot 1 | 26a1273db2e17b5efc50b579e7fdd608482abc38108f17ea74c65645c8cc4483.0 | image/jpeg | | /data/data/com.android.camera2/cache/image_manager_disk_cache/26a1273db2e17b5e... |
| Created In Snapshot 1 | bf2992a70c0544628df2808aaaa450bf6c4e7ee6b361c0d519ed819396692256.0 | image/jpeg | | /data/data/com.android.camera2/cache/image_manager_disk_cache/bf2992a70c054462... |



Aardwolf en AI





Netherlands Forensic Institute
Ministry of Justice and Security



picture
camera : iPhone 12
width : 640
height : 480
original taken on : 2008-07-27T15:21:20.000Z
...



File name : olifant.jpg

path :

//private/var/mobile/Containers/Data/Application/424594F6-7B11-4F47-97B0-03575898CB45/Documents/FolderLockAdvanced/Photos/My Photos/olifant.jpg

/private/var/mobile/Containers/Data/Application/C61F377E-D82A-44F7-ACD5-3ECD4140D0DC/Library/FolderLockAdvanced.sqlite

<< Back Experiment Detail

| | | | |
|--------------|-------------|---------------------------|--------------|
| App Name | App Version | Package identifier | User Actions |
| Calculator # | 3.3.6 | net.newssoftwares.NSVault | Take picture |

| | |
|------------------------|--|
| Experiment Description | Experiment Device |
| | Device type: iOS with OS version: 13.6 |

| Status | Path Name |
|------------------------|--|
| Created In Snapshot 1 | /private/var/mobile/Containers/Data/Application/424594F6-7B11-4F47-97B0-03575898CB45/Documents/FolderLockAdvanced/Photos/My Photos/tmp/Asset_3.png |
| Modified In Snapshot 1 | /private/var/logs/lockdown.log |
| Modified In Snapshot 1 | /private/var/mobile/Containers/Data/Application/424594F6-7B11-4F47-97B0-03575898CB45/Library/Preferences/net.newssoftwares.NSVault.plist |
| Modified In Snapshot 1 | /private/var/mobile/Containers/Data/Application/424594F6-7B11-4F47-97B0-03575898CB45/Library/FolderLockAdvanced.sqlite |

ChatGPT 3.5



Netherlands Forensic Institute
Ministry of Justice and Security



Aardwolf is a database that contains experiments with mobile devices. Experiments are conducted with Argus, a program that runs locally on the computer of a user that is conducting the experiment. Argus records changes in the mobile device and these changes, together with a description of the activity, make and model of the device and recorded changes in the filesystem. Here is an example:

App Name: [net.whatsapp.WhatsApp](#)

App Version: 23.7.83

Device name: iPhone 8

Experiment description: start [whatsapp](#), click on camera, take a picture, click tick and stop without sending it to anyone. Repeat for [exp](#) run.

Experiment device: Device type: iOS with OS version: 12.4.1

| Status | Filename | Pathname | Files |
|--|---|---|----------------------------|
| Modified In Snapshot 1 | LocalKeyValue.sqlite-wal | /private/var/mobile/Containers/Shared/AppGroup/E74ACCC6-8700-42B5-9140-F0EA7EB6F8A2/LocalKeyValue.sqlite-wal | Snapshot 0 |
| | | | Snapshot 1 |
| Modified In Snapshot 1 | 1449A7575E3053912D4910D0271AA4 | /private/var/db/uidtext/F7/1449A7575E3053912D4910D0271AA4 | Snapshot 0 |
| | | | Snapshot 1 |
| Modified In Snapshot 1 | CurrentPowerlog.PLSQL-wal | /private/var/containers/Shared/SystemGroup/C37DC93B-36E1-4C18-AC5B-712626C26FB7/Library/BatteryLife/CurrentPowerlog.PLSQL-wal | Snapshot 0 |
| | | | Snapshot 1 |
| Deleted In Snapshot 1 | E5C4EEA5-71FF-4232-B441-E868305AFB12-export.jpg | /private/var/mobile/Containers/Data/Application/58187339-DA19-4A3D-A8C7-CC4A2E6C42CB/tmp/documents/MediaEditing/E5C4EEA5-71FF-4232-B441-E868305AFB12-export.jpg | Snapshot 0 |
| | | | Snapshot 1 |
| Modified In Snapshot 1 | cache_encryptedB.db-wal | /private/var/root/Library/Caches/locationd/cache_encryptedB.db-wal | Snapshot 0 |
| | | | Snapshot 1 |
| Modified In Snapshot 1 | 052623-0000.log | /private/var/mobile/Library/Logs/com.apple.ioam/ioam_logs/052623-0000.log | Snapshot 0 |
| | | | Snapshot 1 |
| Modified In Snapshot 1 | 5F8FE6A51036E4A388A352A5DA1894 | /private/var/db/uidtext/87/5F8FE6A51036E4A388A352A5DA1894 | Snapshot 0 |
| | | | Snapshot 1 |



ChatGPT 3.5 ▾

HE

You

In the information we obtained through this experiment there are no time stamps. Based on the information provided, can you present a likely course of events that correspond with "start WhatsApp, click on camera, take a picture, click tick and stop without sending it to anyone. Repeat for exp run."

ChatGPT:

Based on the experiment's actions and the observed file system changes, here's a reconstructed sequence of events that corresponds to the described activities within the WhatsApp application:

1. WhatsApp Launch and Camera Access:

- **Application Logs Updated:** The modification of WhatsApp's log files, such as `whatsapp-2023-05-26-15-23-21-522-WhatsApp-163-launch.log`, likely indicates the app's launch.
- **System and Cache Files Modified:** Changes in system logs (`general.log`, `lockdown.log`) and cache files (`cache.sqlite`, `cache.sqlite-shm`, `cache.sqlite-wal`) could correspond to the initial app startup and camera access, reflecting the app's internal state updates and preparation for camera use.

2. Taking a Picture:

- **Creation of Image Files:** The creation of JPEG files, e.g., `5E859D7-4914-4997-AC19-4E2439C114D3.jpg` and `8E4209F7-EF4F-49D9-84A8-524C8F880F30.jpg`, represents the pictures taken during the experiment. These files' presence in the `.Library/Camera/` directory confirms that the camera was used to capture images.
- **Temporary Files Created:** The creation of temporary files, such as `45578AA2-CF26-4C89-AF05-94D9CF1BF00D.mmep-img`, could be related to the processing or temporary storage of image data before deciding on the next action (e.g., sending or deletion).

3. Stopping without Sending:

- **Deletion of Images:** The deletion of images, like `FDACA796-4F3D-4F91-BC68-3454F4656238.jpg` and `B8E8D8EB-D8F3-447D-EDED-9D42A8454F3F.jpg`, likely corresponds to the action of not sending the taken pictures and possibly removing them from the temporary storage.
- **Cache and Database Updates:** Modifications to cache files and databases (`cache_encrypted.db-wal`, `cache_encrypted.db-shm`, `Cache.sqlite-shm`) might reflect the app's state update after discarding the images, including any changes in the media cache or message drafts.

4. Repeating the Experiment:

- **Subsequent Image Files Created and Deleted:** The repetition of creating and then deleting image files indicates the experiment's repeat actions, capturing new images followed by not sending and deleting them.
- **Continuous Log and Cache Updates:** Ongoing modifications in log and cache files, along with the creation of new temporary files (`A435665F-E22E-43ED-BA93-7D5A464CE20E-export.jpg`), suggest multiple cycles of the described activities, each leaving a similar digital footprint.

The absence of timestamps limits precise timing, but the sequence and nature of file changes provide a clear narrative of app usage patterns: launching WhatsApp, using the camera to take pictures, opting not to send the images, and removing evidence

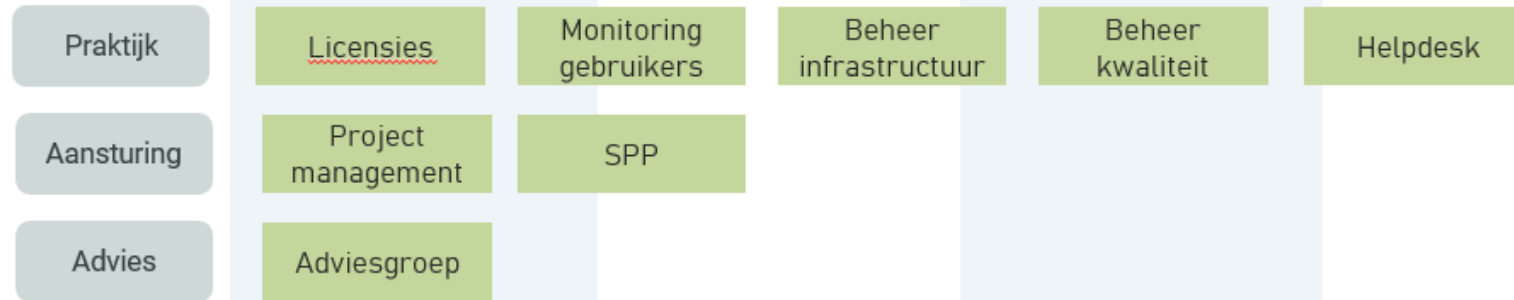


ROADMAP

COMMUNITY



BEHEER



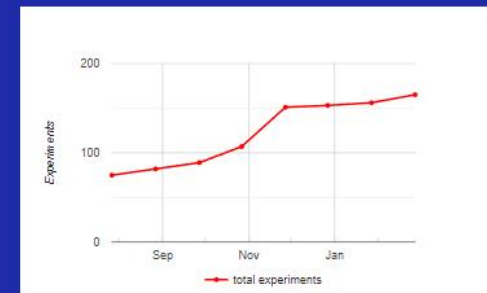
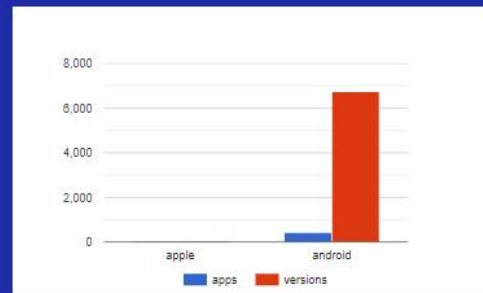


Aardwolf

Application Analysis Results Directory With Open-source Library Foundation

An EU project

Which files change when you interact with a mobile phone app? And vice versa: given certain files, which apps could have been involved in modifying them? Aardwolf is a platform that enables forensic researchers to conduct and share experiments that find quick answers to these questions. In addition Aardwolf provides you with any app version you need for your experiment.





Netherlands Forensic Institute
Ministry of Justice and Security

Vragen?

Aardwolf support

aardwolf@nfi.nl