10.20378/irb-58426

Forensic determination of movement and usage profiles using smartphone apps

Onur Güngör

Hamburg Police, onur.guengoer@polizei.hamburg.de

Wilfried Honekamp

IACS, Hochschule Stralsund, wilfried.honekamp@hochschule-stralsund.de

Abstract:

Mobile phones are becoming increasingly important for forensic investigations. Users generate a lot of data by playing mobile games. We tried to replicate the 2016 research that forensically extracted usage and location data from the Pokémon GO app's storage. In an experiment, the actions taken with the app were manually logged and compared with the data obtained from the logical and physical imaging of two cell phones. We found that while there is less information stored, usage and location data is still available for investigators to establish profiles.

JEL Classification: K39, O33

Keywords: Computer Forensics, Mobile Phones, Movement Profiles, Usage Profiles, Pokémon GO.

1 Introduction

The cell phone gave up its common character as a pure mobile telecommunication device with the introduction of the Apple iPhone in 2007. The smartphone is one of the most important innovations in modern society. The range of countless functions of modern smartphones makes the original idea of the device for making mobile phone calls obsolete. The Google Play Store from Android or the AppStore from Apple offer an unmanageable number of applications (apps) that give users the opportunity to equip their smartphone with functions and gadgets as they wish. The smartphone has developed into the perfect companion of the modern age and is increasingly becoming the focus of everyday life. This technological progress, from the clamshell cell phone with a single-color display and illuminated buttons to the supercomputer in your pocket, harbours not only its advantages but also potential dangers (Huber 2019).

Daily use and enrichment of personal data make the smartphone an image of its user. Messages, photos and videos, but also the history of visited websites and saved login data on various social platforms, can display sensitive content on the smartphone. For many, the loss of such a device is no longer just a financial misery - the personal data it contains is by far more valuable. The European General Data Protection Regulation (GDPR), which came into force on May 25, 2018 (Intersoft Consulting 2020), arose from the basic idea that digital data is also a commodity in need of protection, especially in connection with data processing systems. It regulates the processing of personal data and thus symbolises the sensitivity of data and its increasing importance for modern society. This increase in the importance of the smartphone for society inevitably also influences its importance in the investigation context. The ubiquitous presence of smartphones often makes them the subject of criminal matters (Ludewig 2019).

Mobile forensics represents a small sub-area of digital forensics and deals, among other things, with the backup and evaluation of data on smartphones. In addition to messages, photos and documents, processes running in the background can play an important role in the investigation. Apps often use the functions and sensors of the smartphone, for example to serve as a navigation system or fitness tracker while jogging and generate data. Few users are aware of how their data is handled, how the data processing takes place, and which data is affected by it differs from app to app (Federrath 2015). Thus, the question arises as to which forensic findings can be drawn from apps on a smartphone.

This question is to be examined in more detail in this contribution with a view to the place and time of use of the smartphone using the example of the Pokémon GO app.

Pokémon GO sparked worldwide hype after its release in July 2016. With the innovative game principle, it got millions of people to hunt for Pokémon with their smartphones (Schwartz 2016). The example Pokémon GO is suitable for this investigation on the one hand due to its popularity and on the other hand from a forensic point of view. In addition to data that provide information about the use of the app, GPS data may also be found during the evaluation, which is also a forensically relevant source of information.

2 Background

In contrast to computer forensics, mobile forensics represents a relatively new area of forensic evaluation. For a better understanding a basic introduction to mobile forensics and a detailed description of the Pokémon GO with a view to the legal and investigation context is given.

2.1 Pokémon GO

In 2016, Niantic published the smartphone game Pokémon GO (Niantic 2020) in collaboration with Google, Nintendo and The Pokémon Company. New to Pokémon GO is the innovative augmented reality (AR) game principle in conjunction with GPS localisation. Shortly after its release, it became one of the most downloaded apps. In the first month, Pokémon GO was downloaded approx. 55 million times (Comscore 2016), in the second month approx. 180 million times (Kratzer 2017), and in the third month 550 million times (Wagner-Greene et al. 2017). When installed, the app requires numerous authorisations for Android devices, which are shown in Table 1.

In Pokémon GO, players are asked to move around the real world with their smartphones or tablets. They control an avatar on the virtual map, which is calculated using the smartphone's GPS module and displayed on the map. The map is a simplified and adapted version of Google Maps. In addition to the avatar, nearby Pokéstops and arenas are also displayed on the map. Users can interact with the Pokéstops and gather there with other players or fight against each other in the arenas. Pokéstops represent collection points and form an interface between the virtual and real world. As the players move around, random algorithms will show them Pokémon that are in their vicinity on their display. The player can then interact with the Pokémon and catch them. The "Adventure Sync" feature allows the player to count kilometres run even if the app is not or was not actively open. In order to be able to use this feature, the player must authorise access to the data on the smartphone (Medicus 2019).

Camera	Take pictures and videos
Contacts	Find accounts on the device
Location	- Access exact location (GPS and network based) - Access the approximate location (network based)
Storage	- Edit or delete SD card content - Read SD card content
Miscel-laneous	- Access Bluetooth settings - Control the vibration alarm - Google Play billing service - Run at startup - Access all networks - Get network connections - Deactivate hibernation - Play Install Referrer API - Call up WLAN connections - Perform pairing with Bluetooth devices - Get internet data - Activity detection

Table 1: App authorisation for Pokémon GO version 0.169.0 (Google Play Store)

2.2 Previous research

The primary research goal of this work is to determine when and where Pokémon GO has been used. Sablatura and Karabiyik already carried out an extensive forensic evaluation using the example of Pokémon GO in 2017. Their research shows that within the directories of Pokémon GO various forensically useful data can be found. On the one hand, they were able to use their developed open-source Pokémon GO: Forensic Analysis Tool to extract and display geodata. The determination and storage of spatial data is a non-standardised procedure. Therefore, depending on the operating system, device and app, it can vary whether, how and in which directory this data is saved (Sablatura/Karabiyik 2017). The format of geodata can also differ: it can be text-based or by determining the longitude and latitude (Maus/Höfken/Schuba 2011).

On the other hand, in addition to geodata, other forensically relevant data such as logs and user data could be found. Protocols or log files determine, among other things, the start and end times of so-called sessions. The times at which data is created or modified are indexed using Unix timestamps. Data that has such a time stamp provide information about the possible time when Pokémon GO was used. The user data contained information about the smartphone used, the username respectively avatar name of the player and the email address used (Sablatura/Karabiyik 2017, p. 5f.).

Murphy (2016) also dealt with the forensic evaluation of Pokémon GO on mobile devices and she was also able to find various files with Unix timestamps that determine the active use of the application. In addition, she analysed so-called breadcrumbs in the directory *com.crittercism* on Android devices. Breadcrumbs are log files specifically created by the app. The contents of these log files are: malfunctions in the app, Pokémon encounters, captured Pokémon and other internal incidents. Murphy's analysis showed that there are two pieces of interesting information within these breadcrumbs: encounter ID and cell ID. It is assumed that the encounter ID are 64-bit long representations of Pokémon properties such as type, strength, etc. The cell ID, on the other hand, when converted into hexadecimal code, re-present reference points on the world map in a Hilbert curve that correspond to the user's locations.

3 Methods

For this evaluation, Pokémon GO was installed and executed on two Android smartphones. A manual data record was created for the game sessions on a Sony Xperia Z5C, which logs all actions on the smartphone and within the app over a period of 15 days. The manual data record is used to verify the time of the entries and data within the app and, if possible, also to assign the content. No manual data record was created for the Motorola G2, which has root access. It primarily serves to answer the question of whether a forensic evaluation of a smartphone with root access leads to more or different findings than without.

The Oxygen Forensic Detective tool performs and compares the two basic backup methods, logical (without root access) and physical (with root access) backup. The data gained this way is then compared with the manual data set in order to check the temporal authenticity of the data. The aim is to find data in the Pokémon GO directories from which the time and place of use of the smartphone can be derived. By comparing them with the manual data set, the results should be assessed from an investigation point of view. In addition, the question arises as to whether the points in time of the data actually represent the course of reality or not. The experiment is intended to show whether there is a correlation between the times and places in the data from the smartphone and journalised data. For the second experiment, an An-

droid smartphone with root access is to be evaluated. This should enable a comparison of logical and physical security and determine whether or what added value a root access provides. In order to generate evaluable data, Pokémon GO has been tested to the full extent of its functions for 15 days. Various customisations of the app and Android settings (GPS module accuracy, energy-saving mode) were made to find out whether this influences the data storage. In order to get access to Pokémon GO at all, a Google account had to be created as part of the data collection. Without a Google account, it is not possible to log in to the Google Play Store and the app could not be downloaded. The Google account created for this was also used to register with Pokémon GO and to create an avatar. A Facebook profile was also created and linked to the Google account within the Pokémon GO app. This is to find out whether the access data from the Google account and those of the Facebook profile can be read out during the forensic evaluation.

After the data collection phase, both devices were subjected to a forensic evaluation using the Oxygen Forensic Detective evaluation tool. The evaluation was carried out on a Lenovo ThinkPad L380 host system. A Virtual Machine (VM) with Windows 10 was set up for the evaluation. The smartphones were connected to the host system with a USB cable and passed on to the VM. On the one hand, the Pokémon GO directories were extracted without software through simple access to the internal memory of the devices and, on the other hand, they were extracted and evaluated using forensic software. In addition to Windows 10, a second virtualisation was set up with the Linux derivative Santoku. Santoku is a non-proprietary open-source operating system specially developed for mobile forensics, malware and security for the evaluation and presentation of extracted data (Santoku 2020).

For the Sony Z5C, a backup via Android Debug Bridge (ADB) was created by Oxygen. The backup corresponds to a logical backup and represents a copy of all allocated directories and files. The backup was then imported in the Oxygen software and analysed. The creation of a physical backup was not possible due to the non-existent root access. It turns out that Oxygen uses an exploit to attempt to create a temporary root and then perform a physical backup. However, this exploit only works with smartphones with Android OS version older than 7.0. All newer versions have already fixed this security gap, so the exploit can no longer be executed. If physical security is still desired, the root access must either be established on the device or the smartphone must be installed with an Android version older than 7.0. After the backup has been created and evaluated, it is compared with the manually created data set. The aim is to find temporal matches between the log files of the Pokémon GO app and the manually logged actions. With the Motorola G2, a physical backup could be created due to root access. Both a logical and a physical backup were created. Thus, the Pokémon GO directory from the logical backup can be compared directly

with that from the physical backup. The aim is to assess as to whether a quantitative or qualitative difference in the forensically obtained data volume can be determined with regard to the research question.

4 Results

The directory *Android/com.nianticlabs.pokemongo*, which was simply extracted from the phone memory of the Sony Z5C, has a total size of 175 MB and has two subdirectories *cache* and *files*. There are 437 items in the *cache/UnityShaderCache* subdirectory. With the exception of a readable file name version, all other 436 elements are shown as hash-like values. The size of the files varies between 1 KB and 29 KB. None of the files can be displayed legibly. However, when looking at the manual data set, it is noticeable that 225 elements with the time stamp on September 2nd, 2019 at 7:33 p.m., 113 elements at 7:38 p.m., 10 elements at 7:40 p.m. and 29 elements between 8:10 p.m. and 8:36 pm have been created. The manual data set shows that the Pokémon GO app was started for the first time on the Android device at 7:33 p.m. The creation of the avatar began at 7:38 p.m., the creation was completed at 7:40 p.m. and the application closed at 7:41 p.m. At 8:08 p.m. the Pokémon GO app ran again and at 8:11 p.m. the first Pokémon was caught. These parallels between the two data sets indicate the use of the app at the specified times.

The *files/bundles* subdirectory is 132 MB in size and contains 626 elements. The size of the files varies between 5 KB and 2,843 KB. As in the *UnityShaderCache* directory, the file names are similar to hash values and they cannot be displayed legibly either. The time stamps range from 09/02/2019 to 09/18/2019. This corresponds to the period in which the smartphone was actually used to play Pokémon GO. The time stamps match those of the manual protocol with the exception of minimal deviations. The comparison of Pokémon GO and the manual data set of different days suggests that Pokémon GO made entries when Pokémon were caught. The first file of September 12th, 2019 was created in the *bundles* directory at 7:54 p.m. and the last file at 8:18 p.m. The manual data record shows on September 12th, 2019 at 7:54 p.m. that the first Pokémon and at 8:17 p.m. the last Pokémon of the game session were caught. The smartphone was turned on at 7:52 p.m. that day and turned off at 8:27 p.m. This pattern can be derived from a comparison of the two data sets on each game day.

The *files/DiskCache* subdirectory is 18.7 MB in size and contains 143 further subdirectories with a total of 212 files. 211 file names are stored with hash value-like names. Although the files are not recognised as images by the operating system, they can be opened and displayed with an image processing program. Most of the images are of visited Pokéstops and arenas. On September 7th, 2019 at 12:18 pm, the Pokéstop "Screamthing With A Crown" is recorded in the manual log. The file created at the same time from the *DiskCache* directory matches the entry from the manual data

record. During the evaluation it was noticed that Pokéstops and arenas, regardless of how often they were interacted with, were only created once as an image file the first time they have been visited.

4.1 ADB Backup

The ADB backup was evaluated using the Oxygen tool. The backup created for the Sony Z5C was implemented in the Oxygen mask and then evaluated. The directory *com.nianticlabs.pokemongo* from the ADB backup has a size of 173 MB. In addition, the structure also differs. The file *_hs_db_helpshift_users* has a tab *user_table* in the database structure. The name of the avatar and the e-mail address used by the user are stored in it. The information can also be displayed as plain text with a text editor. The directory *f* is not forensically relevant except for the subdirectory *com.crittercism*. The subdirectory *com.crittercism* contains the breadcrumbs directory mentioned by Murphy (2016). The directory is 42.7 KB in size and contains 250 items. The files can be displayed in text format and, in addition to a time stamp in the format "YYYY-MM-DDThh:mm:ss.000Z", contain further information about the recorded event such as “Pokemon encounters and captures, encounter and adding of wild Pokemon”, Wi-Fi changes, application errors, cell IDs, cell removings, RPC, etc.

All elements in the *breadcrumbs* directory contain a timestamp from the last game day 2019-09-18 between 05:45:43.084Z and 05:53:24.096Z. This shows a difference of two hours to the manual protocol. The logged events in the period in the breadcrumbs directory (250 elements) are quantitatively much more extensive than the events from the manual log (17 entries). However, apart from the above information about the logged events, no further data could be obtained. The conversion of the cell ID into GPS coordinates could not be reproduced. The directory r contains cookies with no definable content and a directory named *hs_code_cache* with a file helpshift*_dexDir.classes2.dex*. It is a Java file. This file was not examined further as it is not relevant to the evaluation. The *sp* directory contains files in XML file format. The file *app-boy.storage.device_cache.v3.04f* contains information such as the Android operating system version 25, the model of the device used E5823, the screen resolution used 720x1184, the location de_De as well as the time zone Europe/Berlin. The file *com.facebook.AccessTokenManager.SharedPrefernces* contains the user's first and last name, provided a link to the Facebook profile had been established.

4.2 Comparison of ADB backup and physical backup

The root access on the Motorola G2 made it possible to create a physical backup in addition to the ADB backup. The data from the different security procedures were then compared and compared with one another. The directory structure of the directory *com.nianticlabs.pokemongo* (size: 51.2 MB) of the ADB backup has already

been explained in detail from the above evaluation of the Sony Z5C. This is almost identical with the Motorola G2, with the difference that the subdirectory *f/com.crittercism/breadcrumbs* was not existent. Items similar to content that match those in the directory *breadcrumbs* could not be found. *Shared_prefs* corresponds to the directory *sp* in the ADB backup. The file *appboy.storage.device_cache.v37a* with information about the device used can also be found here, for example. Although the login was made with the same user account as on the Sony Z5C, no Facebook profile data can be found on the Motorola G2. The file *com.facebook.Access TokenManager.SharedPreferences* exists but is without content. It was also noticed that the files starting with *com.crittercism* are missing in the directory.

If you compare the data records of the ADB Backup and the physical backup of the *com.nianticlabs.pokemongo* directory, one comes to the conclusion that, despite the root access, no forensic added value can be determined. The forensically relevant information given within the Pokémon GO directory is almost identical for the ADB backup and the physical backup. With the logical backup (ADB backup) a total of 3,597 files from the Motorola G2 can be accessed. With the physical backup, a total of 14,083 files were available.

4.3 Comparison of the data sets

To illustrate the forensic value of the times when and places where smartphone apps were used, the data record from the ADB backup is explicitly compared with that of the manual log. The acquired data is exported to an Excel sheet with Oxygen. Only the Folders Sheets Images and Other files are important for the comparison of the data records. Images contains the entire image files and Other files contains all other non-assignable files such as breadcrumbs. In the Excel sheet Modified (UTC) indicates the time at which the file was created by the application or the device. The time difference of two hours between the two data sets is due to the logging in CET (manual data set) and UTC (Pokémon GO). Size shows the size of the file in KB. Full path indicates the relative path of the file and Hash (SHA-1) represents the hash value of the file. The entries from 09/12/2019 agree with those of the manual protocol, apart from minor deviations. The consistency of the Pokémon GO data sets and the manual log is becoming increasingly evident.

In order to determine a possible correlation between the settings made and the quantitative data, the records collected on September 5th, 7th and 17th were analysed and compared to each other. The entries in the manual data record result from opening and closing the Pokémon GO app and the number of actions on the different days. The internal data record describes the simple access to the directory *com.niantcilabs.pokemongo*. The numbers describe the sum of the elements in the subdirectories *UnityShader-Cache*, *bundles* and *DiskCache* on the different days. The

entries Other files and Images in the ADB backup were taken from the Excel sheet. The above protocols were selected according to their different setting parameters: Stamina mode On/Off, Location mode High accuracy/GPS only, and Adventure Sync On/Off. The tables show that, despite various setting parameters, no direct connection to the quantitative data volume can be established. The data on Thursday and Saturday were collected with the same setting parameters and also have the same number of manual entries, with a slight deviation of 5 actions. It can be seen that the Pokémon GO app shows twice as many entries on Thursday than on Saturday. It is noticeable that the app made 48 entries on Saturday and 42 entries on Tuesday, although 41 fewer actions were carried out on Tuesday. Furthermore, when comparing the tables, it can be seen that a forensic evaluation via ADB backup is not necessary to determine when the smartphone was used: the simple evaluation of the directory *com.nianticlabs.pokemongo* provides both quantitative and qualitatively the same amount of relevant data emerges.

The Adventure Sync feature was activated on September 17th, 2019. Pokémon GO was terminated at 5:17 p.m. according to manual protocol. However, the phone remained on until 6:20 p.m. The last entry from Pokémon GO was made at 5:14 pm that day. On September 6th, 2019 Pokémon GO was opened at 11:57 a.m., closed at 12:42 p.m. and the phone switched off at 12:56 p.m. - that means Adventure Sync was active for about 14 minutes. Pokémon GO reopened later in the day at 5:19 p.m. On September 6th, 2019, the Pokémon GO directory shows that entries were made between 11:59 a.m. and 12:39 p.m. and between 5:20 p.m. and 5:30 p.m. - i. e. only if the application was actively opened and used has been.

Recently it was not possible to extract geodata, either from various files or from the metadata of the images in the DiskCache directory. However, the image files contain a time stamp. This indicates the time at which the image was created or generated by the app. If the picture shows a Pokéstop or an arena, then it can be assumed, that the phone, and thus the phone's user at that time, had been at this location. If it cannot be clearly identified by geospatial data, it is possible to locate the depicted location on the image by doing an Internet search. A short internet research can reveal the exact location of the shown Pokéstop or arena. Combining the two pieces of information reveals, that the smartphone user was on September 17th, 2019 at 5:09 pm at the Goblinstadt location in Wandsbek, Hamburg. This information can also be verified by the manual protocol dated September 17th, 2019.

5 Discussion

The above results from the evaluation of the Sony Z5C show that the data was created in the Pokémon GO directory when the smartphone and the app were actively in use. The data from the directory *com.nianticlabs.pokemongo* is provided with a time

stamp from which the use of the app can be derived. The time stamps are available both for the data from the directory *com.nianticlabs.pokemongo/files/bundles* and for the images in the subdirectory *DiskCache*. In addition to images from within the game, the images also show Pokéstops and arenas that have been visited. This motion picture can provide information about when and where the user was at a certain time. The PokéStops and arenas visited from the data on the smartphone show temporal coincidences with the actual movement image. This was shown by the comparison of the data sets. This finding largely coincides with the previous investigations into Pokémon GO.

Already at the beginning of the evaluation it was noticed that the current directory structure of Pokémon GO differs from the previous research. As a result, it was only possible to a limited extent to reproduce, verify or refute the results of previous work. Above all, it was not possible to extract geospatial data from the directory com.nianticlabs.pokemongo, to accurately map the motion of the user playing Pokémon GO in latitude and longitude. Reproducing Murphy's method of converting the cell ID into hexadecimal code and implementing them in an s2 library was unsuccessful. In addition to Murphy, Sablatura and Karabiyik were also able to extract geodata from Pokémon GO. They managed to read the geodata of the last location of the last game session in the upsight.db file. The upsight.db file was in the directory *upsight.model.location* (Sablatura/Karabiyik 2017). Such a directory could not be found either in the ADB backup of the Sony Z5C or in the physical backup of the Motorola G2. The different directory structure, especially in connection with upsight files, is also evident in the analysis by Murphy and The Security Sleuth. The Security Sleuth (2016) carried out the analysis on an Android device in August of the same year and determined a directory structure of *a*, *db*, *ef*, *f*, *sp*. In the present work, however, directory a and its contents were completely missing. The directory a contained the file *base.apk*. The apk file format stands for “Android Package” and designates installation files.

The evaluation by Wingfield (2016), which was also carried out in August of the same year, produced a completely different directory structure and thus positioned itself apart from the previous and the present work. The differing results of the present work on the above-mentioned investigations can possibly be explained by the fact that the investigations by Murphy, The Security Sleuth and Wingfield were all carried out in August 2016, i. e. only one month after the publication of the app. It is not uncommon for innumerable changes to be made to the app with the release, as problems and challenges often arise in practice that had not previously arisen during development. More than three years of game practice, new smartphones and new An-

droid versions lie between the previous investigations and the present work. Deviating directory structures and missing geodata can therefore be a product of the ongoing development of the app and can lead to different results again in the future.

User data such as e-mail address or first and last name of the linked Facebook account were also found in other files and directories in the current work, as well as in previous evaluations. Wingfield located the e-mail address registered with the account in the file *com.nianticlabs.pokemongo.PREFS*. The file was in the directory *shared_prefs* (Wingfield 2016). In this evaluation, however, the file had no forensically relevant content. The Security Sleuth localised user data such as avatar name and data on the end device such as the screen resolution in the directory sp (The Security Sleuth 2016), but also in other, partly non-existent files of this evaluation. This fact suggests that the different directory structures and contents are due to Pokémon GO updates and previous game versions.

Another aspect of this investigation was to gain more knowledge through the most detailed manual data set possible than just by determining when the app was used. The authors assume that by logging all actions carried out and their descriptions, a regularity of the file names or their contents could be recognised. The idea was to be able to assign actions such as "Pokémon / Pokéball - Wiesor / 1, caught" to the entries in Pokémon GO. However, contrary to expectations, the evaluation showed that neither the file names nor their content reveals such regularity. If you compare this with the manual data record, the files cannot be assigned to any property or action despite the supposed sequence. The assignment of the actions to the corresponding entries based on the file names and contents must therefore be rejected.

6 Conclusions

The topic of mobile forensics depicts a very complex area in terms of content, which in this article could only be examined in relation to an app. The results show that data could be found from various subdirectories of the Pokémon GO directory that indicate when the smartphone was used through entries and images of places visited. The ADB backup did not provide any further information to answer the research question compared to the simple evaluation of the Pokémon GO directory from the phone memory. The comparison of ADB backup and physical backup did not provide any further information with regard to the forensic determination of the use of the smartphone by Pokémon GO. Thus, the additional effort to be carried out, which is associated with a root and a physical backup of the smartphone memory, is not worth striving for with a view to the research question. The results of this work differ from previous work in the point that the forensically relevant content and data were to be found in other files and sometimes in other directories. Contrary to expectations and

some previous work, geospatial data could not be found. The localisation of the user's locations using geodata from Pokémon GO could not be reproduced or reconstructed.

Pokémon GO has received tons of updates and changes since it was released in July 2016. In order to meet the demands of the users, updates and innovations for Pokémon GO will also be introduced in the future. So, the question arises as to how long current analyses and evaluations of such apps and the associated forensic findings actually remain up-to-date. For this research work it can at least be stated that, apart from the geodata, the results from 2016/2017 can be transferred to 2020. It has been shown, however, that the storage locations of forensically relevant information and contents can vary from version to version and therefore it is not possible to determine the exact storage locations.

For the criminal police context, the results of this work are meaningful insofar as the time stamps of the data and images represent a reliable source of information due to the comparison with the manual data set. The comparison of the results of simple backup, ADB backup and physical backup showed that all three backup methods lead to the same result. An important finding for the practice with regard to securing the smartphone is that the Pokémon GO app only changed and modified directories and data if the app was actually actively open in the foreground. No data was found to demonstrate that the Adventure Sync modified Pokémon GO even though the app was not actively in use. This means that there is reason to believe that the integrity of the data within the Pokémon GO directory will be preserved when the app is not used in the foreground.

The question arises whether the results of this work could also be achieved on an Apple device. Smartphones are constantly changing due to technological progress. This dynamic regularly presents mobile forensics with new challenges and hurdles. In order not to lose the scientific and practical connection, research in the field of mobile and digital forensics will also be necessary in the future.

7 References

Comscore (2016): Pokémon GO Captures 55 Million Mobile Users in July. Ranking 13th Among All Apps. Accessed at 03.05.2021, from https://www.comscore.com/ita/Public-Relations/Blog/Pokemon-GO-Captures-55-Million-Mobile-Users-in-July-Ranking-13th-Among-All-Apps.

Federrath, H. (2015): Mein Smartphone weiß mehr als ich - Beobachtung und Sammlung von Nutzeraktivitäten. In: Weiterdenken - Heinrich-Böll-Stiftung Sachsen (ed.), Digitale Schwellen – Privatheit und Freiheit in der digitalen Welt, Sachsen.

Huber, E. (2019): Cybercrime – Eine Einführung. Springer VS, Wiesbaden.

Intersoft Consulting (2020): Datenschutz-Grundverordnung. Accessed at 02.05.2021, from https://dsgvo-gesetz.de.

Kratzer, T. (2017): Das Phänomen Pokémon Go. Bachelor Thesis. University of Applied Sciences Mittweida.

Ludewig, S. (2019): Die Sicherstellung und Auswertung des Smartphones – Kriminalpolitischer Anpassungsbedarf? In: Kriminalpolitische Zeitschrift, 05.

Maus, S.; Höfken, H.; Schuba, M. (2011): Forensic Analysis of Geodata in Android Smartphones. Cyberforensics 2011, Glasgow.

Medicus, M. (2019): Pokémon GO Abenteuer-Sync aktivieren: Liste aller Belohnungen. PC Magazin. Accessed at 02.05.2021, from https://www.pc-magazin.de/ratgeber/pokemon-go-abenteuer-sync-aktivieren-belohnungen-liste-3200079.html.

Murphy, C. (2016): A Sneak Peek at Pokemon Go Application Forensics. SANS. Accessed at 02.05.2021, from https://www.sans.org/blog/a-sneak-peek-at-pokemon-go-application-forensics.

Niantic (2021): The Niantic Story. Accessed at 02.05.2021, from https://nianticlabs.com/en/about/.

Sablatura, J.; Karabiyik, U. (2017): Pokémon GO Forensics: An Android Application Analysis. In: Information, 8 (3), 71.

Santoku (2020): Welcome - Santoku Linux. Accessed at 03.05.2020, from https://santoku-linux.com.

Schwartz, J. (2016): How does Pokémon GO Compare to Other Apps? SimilarWeb. Accessed at 02.05.2021, from https://www.similarweb.com/corp/blog/pokemon-go-compared.

The Security Sleuth (2016): Call me Ash Ketchum: Open Source Forensics with Pokemon Go. Accessed at 02.05.2021, from https://www.security-sleuth.com/sleuth-blog/2016/8/13/call-me-ash-ketchum-open-source-forensics-with-pokemon-go.

Wagner-Greene, V. R.; Wotring, A. J.; Castor, T.; Kruger, J.; Dake, J. A. (2017): Pokémon GO: Healthy or Harmful. In: AJPH Perspectives, 107 (1).

Wingfield, L. (2016): Pokemon Go: An Introductory Forensic Study. Intraforensics. Accessed at 02.05.2021, from https://www.intaforensics.com/2016/08/05/pokemon-go-an-introductory-forensic-study.