Windows Phone 7 from a Digital Forensics' Perspective

Thomas Schaefer, Hans Höfken, Marko Schuba

FH Aachen, University of Applied Sciences,
52066 Aachen, Germany
sch.thomas@gmail.com,{hoefken,schuba}@fh-aachen.de

Abstract. Windows Phone 7 is a new smartphone operating system with the potential to become one of the major smartphone platforms in the near future. Phones based on Windows Phone 7 are only available since a few months, so digital forensics of the new system is still in its infancy. This paper is a first look at Windows Phone 7 from a forensics' perspective. It explains the main characteristics of the platform, the problems that forensic investigators face, methods to circumvent those problems and a set of tools to get data from the phone. Data that can be acquired include the file system, the registry, and active tasks. Based on the file system, further information like SMSs, Emails and Facebook data can be extracted.

Keywords: mobile, smartphone, forensics, Windows Phone 7

1 Introduction

Smartphones have become increasingly popular during the last years. Almost 25 percent of the cell phones shipped during quarter four 2010 worldwide have been smartphones [1], [2]. Besides the "plain old telephony service" these phones offer the functionality of a small computer. They run a complete operating system with open API, allow users to install third party applications (so-called apps) and their connectivity capabilities enable them to be always online.

The market for smartphone operating systems is currently dominated by four players which account for approximately 94% of the systems: Android (33% market share), Symbian OS (31%), iOS (16%) and Blackberry OS (14%) [2]. In October 2010 Microsoft launched Windows Phone 7, a completely re-worked successor for their outdated operating system Windows Mobile. So far, the market share of this newly launched operating system is limited but this might change in the future for two reasons: Firstly, the computer operating system market is still dominated by Windows. Many users like to have a homogeneous computer environment, which is usually easier to administrate. Therefore, they might combine their Windows computer with a smartphone running a state-of-the-art Windows operating system. Secondly, Microsoft and Nokia recently announced a strategic partnership in the smartphone area [3]. Windows Phone 7 could play an important role in such a collaboration and could quickly gain market share compared to e.g. Android or iOS.

From a digital forensics' point of view, a large number of Windows Phone 7 smartphones in the market leads to an increasing number of such phones ending up on

the desks of investigators. As the operating system is new, additional forensic methodologies and tools are needed to analyze the phones.

This paper presents initial investigations of the possibilities to forensically analyze a Windows Phone 7 smartphone. Section 2 of the paper gives a brief overview on the new operating system and its characteristics. Section 3 describes the approach that was taken to access relevant data and the tools that were used to extract the data. In section 4 examples of the extracted data are shown including the location of this data on the phone. Section 5 summarizes the results and gives a short outlook on further work.

2 Overview Windows Phone 7

The Windows Phone operating system was developed by Microsoft to regain market share from competitor systems, in particular the iOS and Android platforms. Windows Phone 7 is based on the Windows CE 6 kernel. The following sections will briefly describe the new Windows Phone 7 operating system features, the marketplace and the security model, which all impact the forensic analysis of the phone.

2.1 General Features of Windows Phone 7

Windows Phone comes with a new user interface, which uses a multi-touch screen and an on-screen virtual keyboard. Instead of well known icons for apps, the system uses a slightly modified version, so-called “Tiles”. The design of such Tiles is dynamic and it can be updated online (showing e.g. the latest photo that your contact uploaded in a social network). Data from multiple sources (local or online) can be organized in so-called “Hubs”. The People Hub for example integrates contact data from social networks with contact data of other apps on the smartphone.

Standard apps on a Windows Phone 7 smartphone include

- a web browser (Internet Explorer Mobile)
- email clients (Outlook client that can also be used for Hotmail, Yahoo!Mail, or googlemail)
- multimedia players for music, video and pictures
- Office suite (providing interoperability with the desktop programs)

2.2 Third Party Apps

Similar to the other smartphone platforms, Windows Phone 7 allows for the installation of 3rd party apps (in the following: user apps). Together with music and videos such apps are offered online in the “Windows Phone Marketplace”. This marketplace is managed by Microsoft. In an approval process, submitted user apps are checked and then signed before they can be downloaded by users.

3rd party developers have two official options to test their apps [4]. The first one is to deploy and test the user app in an emulator environment, which is distributed as part of Microsoft's application development framework. The second option is to go through a registration process, publish the user app in Microsoft's App Hub and then test the unsigned app on a registered physical device. An overview on the application development lifecycle process is depicted in Figure 2.

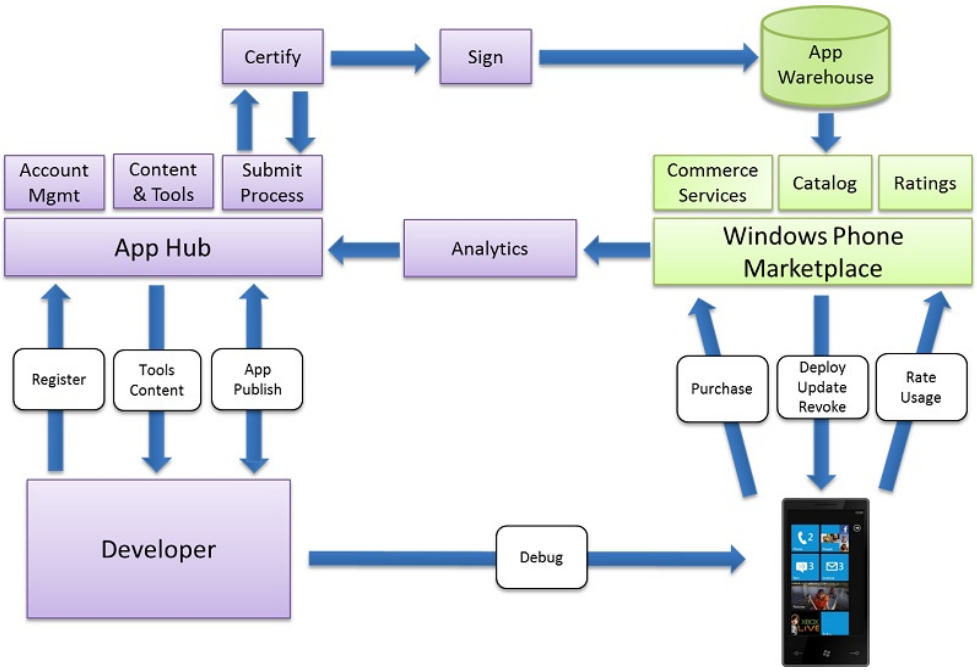


Fig. 2. Application development lifecycle [5]

2.3 Windows Phone 7 Security Model

The Windows Phone 7 security model uses the principle of least privilege, which is implemented in the form of chambers [6]. The chambers basically define the set of privileges that is given to a certain process. There are four different chambers in Windows Phone 7 security model which are illustrated in figure 3.

User apps run in the least privileged chamber, i.e. they have very limited rights. If user apps want to persistently keep application data, they can store it in an isolated area [7]. Each user app creates and manages its own isolated storage. Access to the isolated storage for other user apps is prohibited. A few storage areas of the phone can be accessed from more than one user app, for example the media libraries, which store multimedia files like videos or photos. The only other way to share data between user apps is to store the data externally and access them via web services. Figure 4 illustrates the concept of isolated storage for three different user apps A, B, and C.

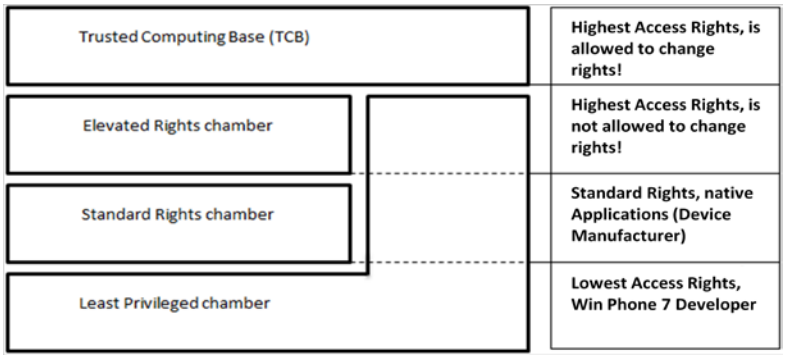


Fig. 3. Chambers of the Windows Phone 7 security model

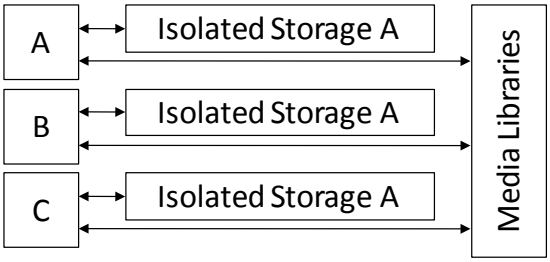


Fig. 4. Isolated storage for different user apps

The execution environment of user apps is restricted as well. Every user app runs in a sandbox and is not allowed to directly access other applications memory or operating systems internals. For certain system features user controlled access to shared resources is possible via a set of built-in API methods. After a mandatory user authorization, a user app can for instance save a contact's phone number or place a phone call.

Apps of device manufacturers (so called native apps) operate in the Standard Rights Chamber and therefore have an extended set of rights compared to user apps. Of particular interest with respect to isolated storage is the fact that native apps have access to the Windows CE 6 kernel (and thus the isolated storage), while user apps have not (see figure 5).

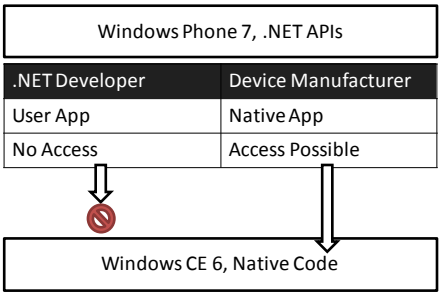


Fig. 5. Windows CE 6 kernel access for user and native apps

3 Data Acquisition Methodology

A typical approach to read data from a smartphone in a forensic investigation is to install a small app on the device which then extracts data and sends it to a connected computer. Even though this results in a small change of the evidence, it is sometimes the only way to get hold of certain information at all. As long as the changes to the device are controlled and well documented, such a procedure can still be considered forensically sound.

Access to large parts of the storage area of a Windows Phone 7 device requires the installation of an app with privileges of the “Standard Rights Chamber” (or higher). As will be seen in the following sections, such an app can easily be created by importing manufacturer DLLs into user apps and thus allowing user app access to methods which otherwise would be restricted to native apps. Moreover, a few helper tools will be presented, which are needed to get the apps onto the phone and the data back to the computer.

3.1 Native Methods in User Apps

To import and execute native code in a user app [8] the DLL “Windows.Phone.interopService” is used, which is part of an application from Samsung (Network Profile). This DLL provides the method "RegisterComDLL", which is able to import native manufacturer DLLs. If the “Windows.Phone.interopService” DLL is included in a .NET user app, it is possible to execute native code within this app and to get access to the entire file system of the phone, isolated storage included (cf. figure 6).

Once the app is ready it needs to be installed on the phone. To deploy an app on Windows Phone 7, the phone and the developer must be registered and unlocked by Microsoft. Only then the delivery over the Windows Mobile Marketplace is possible. One way to circumvent this cumbersome process is to use ChevronWP7, a small tool which allows bypassing of the marketplace procedure (Jailbreak) [9].

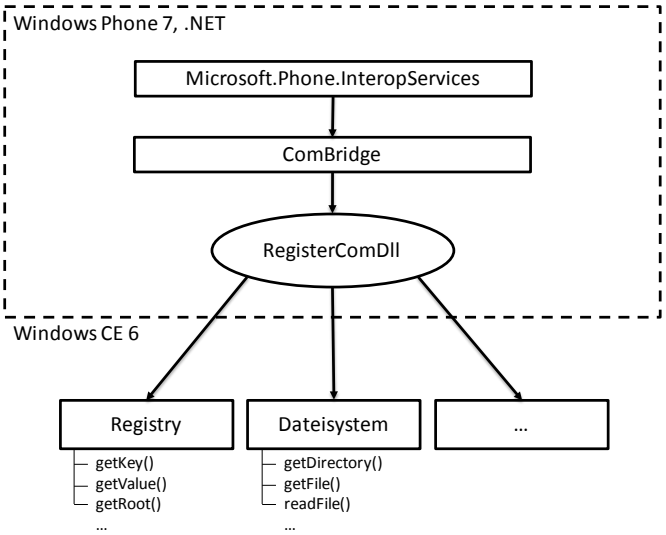


Fig. 6. Enabling native code execution in user apps

3.2 Apps to Extract Data

Two apps, which import the DLLs as described above, have been used to get access to the data on a Windows Phone 7. The app "TouchXperience" [10] has been designed within a developer community project. The other app is an own development and is called "Una". In order to be able to connect to their server both TouchXperience and Una require the Microsoft Zune Software [11] to run on the computer.

TouchXperience

The app TouchXperience is delivered in combination with the Windows Mobile Device Manager (hereinafter referred to as WPDM, a management software for Windows Phone 7). The two programs form a client server architecture: while the client app (TouchXperience) extracts data such as the file system from the mobile device, WPDM receives the data and converts them into a human readable graphical format.

In addition to many functions such as application management, media management and synchronization of files and folders, the File Explorer is especially interesting for forensics. It provides read-, write- and executable access to almost all the files from Windows Phone 7. Depending on the manufacturer of the Windows Phone 7 device, the results delivered by TouchXperience differ slightly (different DLLs used). The TouchXperience File Explorer provides the basis for many of the forensic tests of section 4.

Una

Una has been developed at Aachen University of Applied Sciences. It is a client server application that is able to read data from the mobile that currently cannot be extracted by TouchXperience: general device information (manufacturer id, device id etc.), running processes (process name, process id), and registry (general Windows keys and manufacturer specific keys). Figure 7 shows a screenshot of the Una client app running on the mobile device.

Fig. 7. Una app interface on the mobile device

The Una server uses a Windows Communication Foundation (WCF) service [12], [13] for asynchronous communication with the client app. The communication flow is depicted in figure 8.

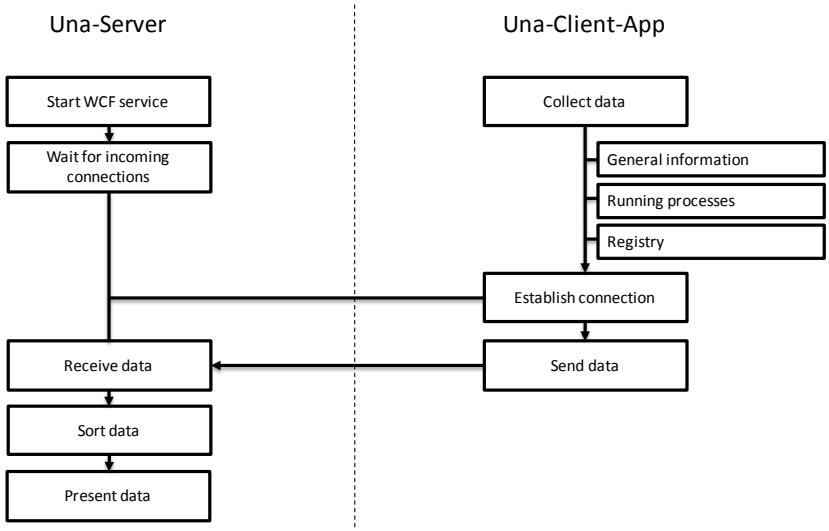


Fig. 8. Program and communication flow of the Una application

4 System and Application Data Acquisition

The acquisition methodology described in the previous section can be used to acquire two main types of data on a Windows Phone 7 smartphone. *System data* is the set of data required by the smartphone to work properly. The data can only be accessed and modified via the operating system. *Application data* is the data created and maintained by the different apps on the phone.

Table 1 lists the different types of system and application data that have been successfully acquired on a HTC Trophy 7 smartphone.

Table 1. Acquired system and application data.

Data	Data Type	Acquisition and Analysis
File System	System	WPDM/TouchXperience
Registry	System	Una
Active Tasks	System	Una
Device Information	System	.NET 4, Una
SMS	Application	WPDM/TouchXperience, Hex-Editor, Perl-Parse-Script
Email	Application	WPDM/TouchXperience, Hex-Editor
Contacts	Application	WPDM/TouchXperience
Call Logs	Application	.NET 4, WPDM/TouchXperience, Hex-Editor
GSM / Wi-Fi	Application	WPDM/TouchXperience, Hex-Editor
Maps	Application	WPDM/TouchXperience, Hex-Editor
Internet Explorer	Application	WPDM/TouchXperience, Hex-Editor
Private Documents	Application	WPDM/TouchXperience, Hex-Editor
Notes	Application	WPDM/TouchXperience, Hex-Editor
Pictures / Videos	Application	WPDM/TouchXperience, Hex-Editor
Facebook	Application	WPDM/TouchXperience, Hex-Editor

The following sections describe the majority of the listed data in more detail.

4.1 File System

The Windows Phone 7 file system can be compared to normal desktop file systems as they come with Windows XP, Windows Vista or Windows 7. It is structured with the usual directories and files, which can be reached from the file system root directory. Using a Unified Storage System, the complexity of several partitions on different internal and external storage devices is hidden and only a single directory tree structure is visible.

Important folders from a forensic investigator's perspective are "Application Data", "Applications", "My Documents", and "Windows", which are all located in the root directory.

- The "Application Data" folder contains data of preinstalled apps on the phone, including Outlook, Maps and Internet Explorer.

- Apps, which are deployed by the user, are located in the folder “Applications”. Note that these folders also contain the isolated storage for the different apps.
- “My Documents” holds different Office documents, e.g. Word, Excel or PowerPoint. The folder also includes configuration files and multimedia files like music or videos.
- The “Windows” folder contains files of the Windows Phone 7 operating system.

4.2 Registry

The Windows Registry, a database in which the operating system and applications can store environment variables, is available on Windows Phone 7 as well. In order to extract the data and store them on the a forensic workstation, the tool Una is used. Figure 9 shows an example of an extracted registry on a workstation.

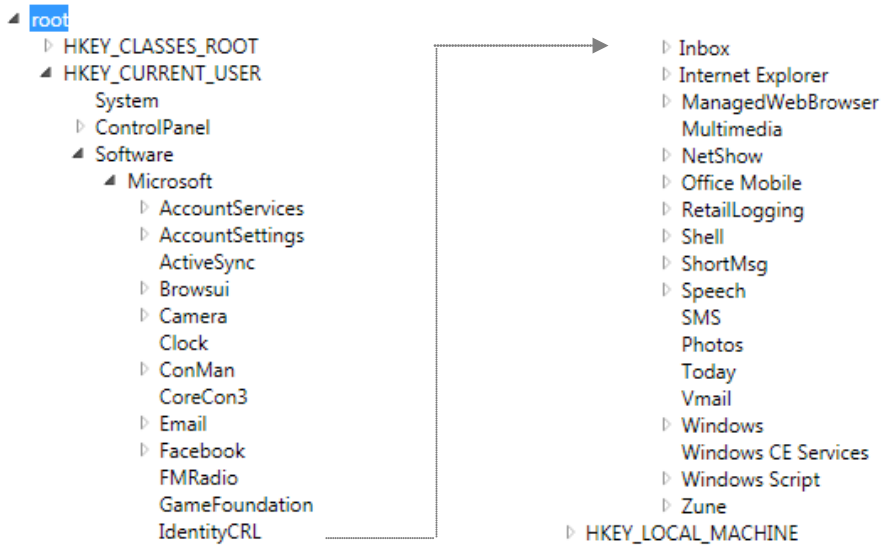


Fig. 9. Screenshot of the registry extraction with Una

As can be seen from the screenshot, the registry looks very much like a normal Windows desktop registry. It contains comprehensive information, e.g. on the applications the user has installed. This information can be further analyzed using normal registry analysis methods.

4.3 Active Tasks

The active tasks are the running processes on a Windows Phone 7 system. From an investigator's point of view, those tasks are interesting, because unknown active tasks might indicate that malware is running on the system.

The acquisition of the data related to active tasks is also achieved via the tool Una. Through different implemented methods, the Una client is able to access the running processes, extract information about them and to send this information to an application running on the forensic workstation. Here, the data is shown under the category "Volatile data" including for example process names, process ids and kernel times (start and end time of the last multitasking time slot). The end times refer to processes which are still running but are currently in the background (simulated multitasking).

Figure 10 shows a snapshot of the active tasks taken on a Windows Phone 7 smartphone using Una.

File		
NK.EXE	servicesd.exe	udevice.exe
udevice.exe	udevice.exe	udevice.exe
udevice.exe	dw.exe	Compositor.exe
servicesd.exe	SirepServerAppDev.exe	dmsrv.exe
udevice.exe	servicesd.exe	servicesd.exe
udevice.exe	DeviceReg.exe	servicesd.exe
servicesd.exe	servicesd.exe	cprog.exe
servicesd.exe	ssupdate.exe	XDrmRemoteServ.exe
servicesd.exe	telshell.exe	TaskHost.exe

Fig. 10. Active tasks extracted with Una

4.4 Device Information

The third category of data that can be acquired from a Windows Phone 7 using Una is information about the device itself. This information can be read directly using the method „DeviceExtendedProperties.TryGetValue(String, object)" of the .NET API library „Microsoft.Phone.Info". As a result, the investigator gets data about the device manufacturer, name, id, memory and firmware version. Figure 11 gives an example of the device information extracted from an HTC 7 Trophy.

Manufactor	DeviceName	DeviceUniqueId	DeviceTotalMemory	DeviceFirmwareVersion
HTC	7 Trophy	System.Byte[]	497635328	2250.09.10903.162

Fig. 11. Device information – example results

4.5 Geodata - GSM and Wi-Fi

As many other smartphone platforms, Windows Phone 7 is able to offer location based services. Before apps can access geodata to provide such services, the user has to give her consent.

The Windows Phone 7 directory structure contains a folder “Location” with two subdirectories “GSM” and “WIFI”. The folders contain files with extensions “.bcn” and “.tile”. It is assumed that those files contain information about GSM cell ids and Wi-Fi hotspot locations. However, decoding of such files has not been successful so far.

4.6 SMS

Windows Phone 7 stores all incoming and outgoing short messages (SMSs) in the file „store.vol“ that can be found in the directory „\Application Data\Microsoft\Outlook\Stores\DeviceStore“. The file cannot be copied directly, which is most likely due to the fact that this file is constantly in use. However, when the file is renamed, Windows Phone 7 automatically creates a copy of the file which can be analyzed using a normal text editor. Figure 12 shows the renamed and copied file “store.vol.txt” and its content.

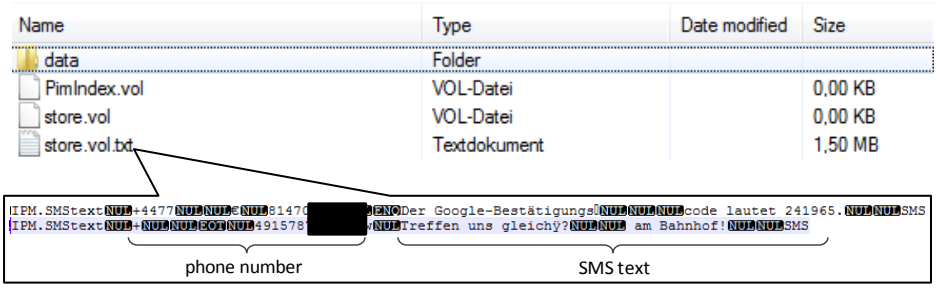


Fig. 12. SMSs extracted from the file “store.vol.txt”: “Google Confirmation Code” and “Meeting at the train station”

For all incoming and outgoing SMSs both the sender’s phone number and the message content can be found in the text file. While this was still done manually in the context of this paper, automatic processing can be easily implemented.

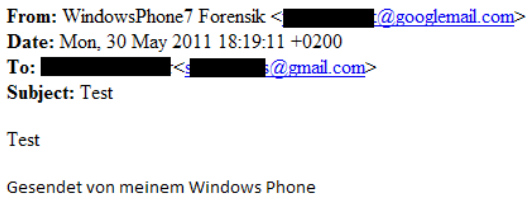
4.7 Emails

The standard email client on Windows Phone 7 devices is Outlook, which allows users to synchronize with various email services, for example googlemail. All Outlook data (including pictures of the contacts that emails are sent to) is stored in the

directory „\Application Data\Microsoft\Outlook\Stores\DeviceStore\data". The folder contains a set of numbered directories, each of them holding different content.

Folder "3" stores pictures of the user's contacts (email receivers) in files with extension ".dat". File carving shows that such files actually contain jpeg images and after renaming an example file with the extension ".jpg", the picture becomes visible.

Folder "4" contains emails, which are in the case of googlemail stored as html files. Figure 13 shows an example of a test email.


From: WindowsPhone7 Forensik <[redacted]@googlemail.com>
Date: Mon, 30 May 2011 18:19:11 +0200
To: [redacted]<[redacted]@gmail.com>
Subject: Test

Test

Gesendet von meinem Windows Phone

Fig. 13. Test email found in the Outlook folders of a Windows Phone 7 smartphone

4.8 Facebook

Facebook users can install a Facebook app on their Windows Phone 7 smartphone. The app creates a number of folders in the file system including the folders "Cache", "History" and "IsolatedStore". These folders contain general settings of the Facebook app and subfolders like "Images" and "DataCache.%userid%" (in which "%userid%" is replaced with the user's id). The last folder contains all the user's Facebook application data in clear text.

The folders can be very interesting for investigators as they store a lot of information. In order to limit the length of the paper, only two examples are shown with figures.

- File "%userid%.settings" contains the user's profile name and a link to the user's profile and her profile picture.
- Every picture, which the user viewed via the Facebook app, is stored in the folder "Images" of the directory "IsolatedStore". This includes pictures of the user's friends. In order to view the images, the extension of the files has to be changed to ".jpg". See figure 14 for an example.
- The "DataCache.%userid%" holds information about the user's home page (including her last location if that was enabled), incoming and outgoing messages, and a list of the user's friends (including their birthday, their id and a link to their profile picture). For an example outgoing message, see figure 15.

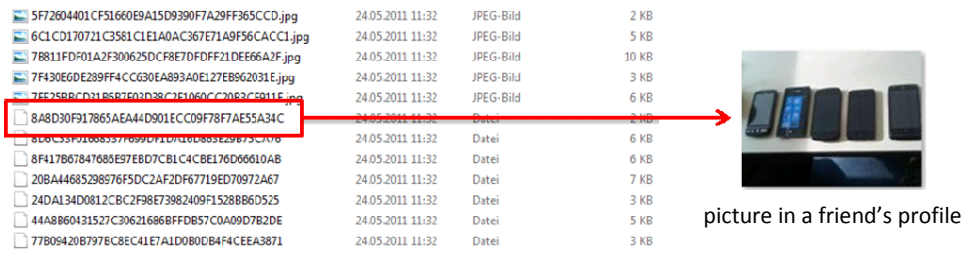


Fig. 14. Picture in a friend's profile, which was viewed by the user

```
0x20: 01 30 00 00 00 00 45 48 61 6C 6C 6F 2C 0A 0A 68   .0....EHallo,..h
0x30: 65 75 74 65 20 41 62 65 6E 64 20 74 72 65 66 66   eute Abend treff
0x40: 65 6E 20 77 69 72 20 75 6E 73 21 20 0A 0A 31 39   en wir uns! ..19
0x50: 20 55 68 72 20 69 6E 20 41 61 63 68 65 6E 0A 0A    Uhr in Aachen..
0x60: 47 72 75 C3 9F 0A 54 68 6F 6D 61 73 0F 31 30 30   GruÃ.[redacted]100
0x70: 30 30 31 34 36 35 39 35 38 30 31 33 0E 28 6B 65   001465958013.(ke
```

Fig. 15. Outgoing message sent via Facebook app: "Meeting at 7 pm in Aachen"

4.9 Internet Explorer

The standard web browser on Windows Phone 7 platforms is Internet Explorer. From an investigator's point of view, visited web sites might be of interest. All relevant data can be found in the file "TabsStorage.bin" of the directory "Application Data\ Microsoft\Internet Explorer". An extract of this file is shown in figure 16.

```
0x01040: 24 00 00 00 68 00 74 00 74 00 70 00 3A 00 2F 00   $...h.t.t.p.:./.
0x01050: 2F 00 6D 00 2E 00 74 00 65 00 73 00 74 00 2E 00   /.m...t.e.s.t...
0x01060: 64 00 65 00 2F 00 00 00 6F 00 6D 00 2F 00 77 00   d.e./...o.m./.w.
0x01070: 65 00 6C 00 63 00 6F 00 6D 00 65 00 2F 00 00 00   e.l.c.o.m.e./...
0x01080: 02 00 00 00 00 00 74 00 74 00 70 00 3A 00 2F 00   ......t.t.p.:./.
0x01090: 2F 00 6D 00 2E 00 74 00 65 00 73 00 74 00 2E 00   /.m...t.e.s.t...
0x010A0: 64 00 65 00 2F 00 00 00 00 00 00 00 00 00 00 00   d.e./...........
```

Fig. 16. Visited link of Internet Explorer

4.10 Maps

"Maps" is a Microsoft app on Windows Phone 7 to determine the user's location and to calculate routes. Maps' application data is stored in directory "Application Data\ Maps". The hex content of the file "MapsSetData.dat" shows the last location of the device in clear text (see figure 17). Interesting to note is the fact that the location is given as an address and not as longitude and latitude GPS coordinates. Tests showed that the given address is quite accurate with a deviation of two houses only.

Fig. 17. Last location of the device stored in clear text

5 Summary

A new smartphone platform is always a challenge for forensic investigators and Windows Phone 7 is no exception. The main problem preventing investigators to access data on Windows Phone 7 devices is the limited access rights of normal user apps, in particular the isolated storage. However, this obstacle can be circumvented by methods already available in the internet community, e.g. through the use of native DLLs and simplified app installation methods. When these mechanisms are combined, a small set of tools can be installed on the device that allow for the acquisition of the file system and other system data. Once this data is available, it can be further analyzed. As a result, a large amount of interesting data can be obtained from a Windows Phone 7 phone, for instance emails of the user, SMSs, Facebook contacts or web pages visited with Internet Explorer.

The results presented in this paper are initial results. One of the next steps planned with Windows Phone 7 is to automate the analysis of the extracted files in order to make investigations more efficient. Also it needs to be tested, if the mechanisms work on Windows Phone 7 platforms of different vendors (the results were achieved on a HTC Trophy 7).

References

1. Zeman, E., “Top 5 Handset Makers Of 2010 Ranked”, InformationWeek, http://www.informationweek.com/news/mobility/smart_phones/showArticle.jhtml?articleID=229200009 (2011, accessed on 28 February 2011)
2. Canalys research release, “Google’s Android becomes the world’s leading smart phone platform”, http://www.canalys.com/pr/2011/r2011013.html (2011, accessed on 28 February 2011)
3. Microsoft press release, “Nokia and Microsoft Announce Plans for a Broad Strategic Partnership to Build a New Global Mobile Ecosystem”, http://www.microsoft.com /presspass/press/2011/feb11/02-11partnership.mspx (2011, accessed on28 February 2011)
4. Microsoft App Hub, “how it works – create”, http://create.msdn.com/en-US/home /about/how_it_works_create (2011, accessed on 28 February 2011)
5. Microsoft MSDN Library, “Application Platform Overview for Windows Phone”, http://msdn.microsoft.com/de-de/library/ff402531.aspx (2011, accessed on 28 February 2011)
6. Microsoft, “Windows Phone 7 security model”, http://download.microsoft.com/download/9 /3/5/93565816-AD4E-4448-B49B-457D07ABB991/ Windows%20Phone%207%20Security%20Model_FINAL_122010.pdf (2010, accessed on 31 May 2011)
7. Microsoft MSDN Library, “Isolated Storage Overview for Windows Phone”, http://msdn.microsoft.com/en-us/library/ff402541%28v=vs.92%29.aspx (2011, accessed on 28 February 2011)
8. Thomas Hounsell, “Avoiding Reflection: Adding the InteropServices library to the WP7 SDK”, http://thounsell.co.uk/2010/11/avoiding-reflection-adding-the-interopservices-library-to-the-wp7-sdk/ (2010, accessed on 16 May 2011)
9. Rafael Rivera, Chris Walsh, Long Zheng, „Pursuing the future of homebrew on Windows Phone 7“, http://www.chevronwp7.com/post/2057541126/pursuing-the-future-ofhomebrew-on-windows-phone-7, (2010, accessed on 31 May 2011)
10. TouchXperience – Project Website, http://www.touchxperience.com/ (accessed on 31 May 2011)
11. Microsoft, „Getting to know the Zune software“, http://www.microsoft.com/ windowsphone/en-ww/howto/wp7/music/get-to-know-the-zune-software.aspx (accessed on 3 May 2011)
12. Chris Peiris, Dennis Mulder „Hosting and Consuming WCF Services“, http://msdn.microsoft.com/en-us/library/bb332338.aspx, (2007, accessed on 31 May 2011)
13. Microsoft, „What is Windows Communication Foundation?“, http://msdn. microsoft.com/en-ww/library/ms731082.aspx, (accessed on 31 May 2011)