# IT-Forensik im Wandel - Die Aufweichung des Paradigmas der Unveränderbarkeit am Beispiel von Smartphones mit dem Windows Phone Betriebssystem

Björn Roos · Harald Baier

Center for Advanced Security Research Darmstadt (CASED), Mornewegstr. 32, 64293 Darmstadt, Germany
Hochschule Darmstadt, Haardtring 100, 64293 Darmstadt, Germany
{bjoern.roos | harald.baier}@h-da.de

## Zusammenfassung

Wie bei allen forensischen Untersuchungen gilt auch bei IT-forensischen Ermittlungen das Paradigma der „Unveränderthеit der Daten“. Eine Veränderung des zugrundeliegenden Speichermediums kann zu einer Minderung des Beweiswertes oder sogar zu einem Beweisverwertungsverbot führen. Daraus hat sich die Vorgehensweise in der IT-Forensik abgeleitet, nach einer lesenden Datenakquise nur auf den Kopien der beweiserheblichen Daten zu arbeiten und mittels Prüfsumme zu belegen, dass die Kopie 1:1 mit dem Original übereinstimmt. IT-forensische Untersuchungen von mobilen Endgeräten können aber typischerweise nur vorgenommen werden, wenn der Datenträger verändert wird. Analysen von erfahrenen Computerforensikern an Geräten mit dem Windows Phone 7 Betriebssystem haben gezeigt, dass momentan eine softwarebasierte Datenakquise nur mit einer Veränderung des Datenspeichers erfolgen kann.
Die vorliegende Publikation leistet einen Beitrag zu der immer wichtiger werdenden Frage, wie mit einem veränderten Datenspeicher, der unter Verwendung bestimmter Techniken zur forensischen Untersuchung mobiler Datenträger auftreten kann, prozessrechtlich umgegangen werden soll. Aufgrund der technischen Gegebenheiten müssen für solche Ermittlungen die Prinzipien für forensische Untersuchungen aufgeweicht werden, um beweisrelevante Daten zu erhalten. Um dennoch dem Prozessrecht gerecht zu werden, schlagen wir bestimmte feste Regeln vor, bei deren Beachtung von einer Unverändertheit der beweiserheblichen Daten ausgegangen werden kann, obwohl Teile des Datenträgers verändert wurden. Wir zeigen die Gültigkeit dieser Regeln am Fallbeispiel eines synthetischen Ermittlungsverfahrens zum Besitz kinderpornographischen Materials.

## 1 Einleitung

IT-forensische Untersuchungen an mobilen Endgeräten, wie Smartphones, sind mit herkömmlichen IT-forensischen Untersuchungen an Desktop-PCs nicht zu vergleichen. Eine Post-Mortem-Analyse des internen Speichers kann, wenn überhaupt, nur selten erfolgen. Bei IT-forensischen Untersuchungen gilt das Gebot der „Unveränderthеit der Daten“. Eine Veränderung des Speichers kann unter Umständen zu einer Minderung des Beweiswertes oder sogar zu einem Beweisverwertungsverbot führen [Knop09]. Der Einsatz als Beweismittel in einem juristischen

N. N · N. N (Hrsg.) · D•A•CH Security 2012 · syssec (2012) 1-13.

Verfahren ist nicht immer ein direktes Ziel einer Ermittlung. Da sich die Beweisrelevanz typischerweise im Laufe oder nach den Ermittlungen ergibt, muss jedes Indiz, das belastbar und nutzbar sein soll, zwingend „lege artis“, also nach den Regeln der Kunst (rechts- und technikgerecht) erhoben worden sein. Beweise dürfen unter keinen Umständen alterniert werden. Dies führt somit zum gängigen Paradigma der IT-Forensik, nur an den Kopien der beweiserheblichen Daten zu arbeiten und mittels Prüfsumme zu belegen, dass die Kopie 1:1 mit dem Original übereinstimmt [Beck12].

IT-forensische Untersuchungen von mobilen Endgeräten können oftmals nur vorgenommen werden, wenn der Speicher verändert wird, da spezielle Software- oder Hardware-Tools verwendet und auf das Gerät installiert werden. Hierzu existieren unterschiedliche Techniken, die jeweils ihre Vor- und Nachteile haben. Nach [BJKKR] gibt es drei Verfahren für die Sicherung des internen Flash Speichers [PBOZ97]. Die Live Analyse mithilfe von installierten Applikationen gehört dort allerdings nicht dazu, obwohl diese bei vielen Geräten oftmals die am wenigsten riskante und verwendbare Analysemethode ist. Eine Sicherung des internen Speichers mithilfe des Betriebssystems, wie von Distefano in [ME2008] propagiert, ist aufgrund des Sicherheitskonzeptes des Windows Phone Betriebssystems im Moment nicht möglich. Die Forensiker verwenden deshalb, wenn es keine andere Möglichkeit als die riskante Chipextraktion gibt, die Live Analyse, um die Untersuchung durchzuführen. Die Live Analyse führt aber dazu, dass der interne Speicher im Laufe der Untersuchung verändert wird. Alleine das Einschalten des Gerätes bewirkt eine Veränderung des internen Datenspeichers.

Die zentrale Frage ist nun, wie mit einer Veränderung des internen Speichers bei der forensischen Untersuchung prozessrechtlich umgegangen wird, da dies gegen den Grundsatz der Unveränderheit von Beweismitteln verstößt und vor Gericht zu einem Beweisverwertungsverbot führen kann. Was ist erlaubt? Was nicht? Auf diese Fragen gibt der vorliegende Artikel Antworten.

Im Artikel [Ro2011] werden Regeln für zulässige Veränderungen am Beweismaterial im Rahmen einer Fallstudie für eine kontrollierte Veränderung an einem Notebook vorgestellt und auf alle forensischen Untersuchungen übertragen. Wir stellen allgemeine Regeln für ein Vorgehen an Smartphones vor, die trotz parzieller Veränderung des Datenspeichers des Gerätes die Unveränderheit der beweiserheblichen Daten gewährleisten. Die Veränderung darf daher nur irrelevante Dateien außerhalb der Nutzerdaten betreffen. Unserem Regelwerk liegt auch wie bei [Ro2011] die Idee zugrunde, dass aufgrund der technischen Gegebenheiten für solche Ermittlungen die Prinzipien für forensische Untersuchungen aufgeweicht werden müssen, um beweisrelevante Daten zu erhalten. Allerdings führt die differenzierte Sichtweise auf Smartphones zu einem abweichenden Regelwerk.

Die Gültigkeit dieser Regeln werden am Fallbeispiel eines synthetischen Ermittlungsverfahrens zum Besitz kinderpornographischen Materials gezeigt. Dazu wird ein Smartphone mit dem Windows Phone 7 Betriebssystem verwendet, um exemplarisch die Anwendbarkeit unserer Regeln zu zeigen.

Die aktuellen Arbeiten von Schuba, Höfken und Schäfer ([SHS11], [Hakin9]) an Geräten mit dem Windows Phone 7 haben gezeigt, dass momentan softwarebasierte Untersuchungen nur mit einer Veränderung des Datenspeichers erfolgen können. Daher eignet sich ein solches Smartphone gut als Proof of Concept der Regeln.

Die Problematik auf einem gesperrten Gerät eine forensische Untersuchung durchzuführen, ist nicht Ziel dieses Dokumentes. Es wird deshalb nicht weiter darauf eingegangen.

In Kapitel 2 wird das Windows Phone Betriebssystem und das verwendete Gerät vorgestellt. Im anschließenden Kapitel 3 wird die Vorgehensweise erläutert, wie eine Datenakquise auf einem Smartphone mit dem Windows Phone 7 Betriebssystem durchgeführt werden kann. Die durch den Jailbreak und durch die Analyse auftretenden Veränderungen am Speicher werden dabei aufgezeigt. Im Kapitel 4 werden die Regeln zur minimal-invasiven forensischen Ermittlung vorgestellt und deren Anwendbarkeit anhand einer beispielhaften forensischen Untersuchung unter Annahme des Straftatbestandes *Besitz kinderpornographischen Materials* diskutiert. Dieser Beitrag schließt mit einer Zusammenfassung und einem Ausblick in Kapitel 5.

# 2 Das Windows Phone 7 Betriebssystem

Das Windows Phone 7 OS ist vom Hersteller Microsoft ein für Mobiltelefone entwickeltes Betriebssystem. Es wird seit dem 21. Oktober 2010 in Deutschland auf Smartphones vertrieben. Das Betriebssystem ist für eine Bedienung mit Fingern und Multi Touch entwickelt worden und basiert auf der Benutzeroberfläche des Zune HD.

## 2.1 Aufbau

Das Windows Phone 7 Betriebssystem basiert auf dem Windows Embedded CE 6.0 Kernel und kann in Hardware- und Softwarekomponenten unterteilt werden. Microsoft gibt die Hardware Komponenten der Smartphones vor, welche von den Hersteller erfüllen werden müssen. Die Software Komponenten können in einem Kernel Mode und einem User Mode Bereich aufgeteilt werden [Corp]:

- Kernel Mode: Bereich mit Kernel, Board Support Package (BSP), Grafiken und Rendering Technologien, Netzwerk, Dateisystem und Telefonupdate.
- User Mode: Bereich mit Service Host, User Mode, Treiber Host, Shell, Telefon Dialer, Applikation Layer und Windows Phone Applikations Plattform.

### 2.1.1 Speicher Modell und Management

Das Windows Phone 7 OS ist ein 32 Bit Betriebssystem, das einen 4 GB virtuellen Adressraum verwendet. 2 GB Speicher sind für den Kernel vorgesehen. Dieser beinhaltet auch das Dateisystem und den Kernel Mode Geräte Treiber Manager. Die verbleibenden 2 GB sind für den derzeit ausgeführten Prozess. Der Prozess Code, User-Mode DLLs und im Speicher abgelegten Dateien sind diesem virtuellen Applikations-Adressraum zugeordnet [Corp].

### 2.1.2 Wichtige Verzeichnisse und Speicherstruktur von Apps

Für Forensiker sind vor allem die Ordner: Application Data, Applications, My Documents und Windows interessant. Im Ordner "Application Data" sind die vorinstallierten Applikationen, wie Outlock, Internet Explorer, Maps usw. gespeichert. Der Ordner "Applications" beinhaltet Anwendungen, die vom Benutzer installiert werden. Der Ordner "My Documents" enthält unter anderem verschiedene Office Dokumente, Musik, Bilder und Videos. Im "Windows" Ordner werden die Dateien für das Betriebssystem gespeichert. Der Ordner "IsolatedStore" besitzt jede Applikation und stellt den isolierten Speicherbereich der Anwendung dar. Bei der Installation von Anwendungen können Umgebungsvariablen in der Registry des Gerätes gespeichert werden. Die WP7 Registry ist eine Datenbank analog zu den Windows Betriebssystemen auf Desktop PCs [SHS11].

## 2.2 Sicherheitskonzept

Das Windows Phone 7 Sicherheitsmodel basiert auf dem Prinzip der Isolation und der geringsten Vergabe von Rechten. Es verwendet das sogenannte „Kammer“ Konzept. Jede Kammer stellt eine Sicherheitsgrenze und durch Konfiguration eine Isolationsgrenze dar, innerhalb derer ein Prozess läuft. Jede Kammer wird umgesetzt und mithilfe eines Systems aus Richtlinien definiert. Die Sicherheitsrichtlinien einer Kammer definieren auf welche Betriebssystem-Funktionen die Prozesse dieser Kammer zugreifen können [Corp]. Das Sicherheitsmodell verwendet vier Typen von Kammern. Drei dieser Kammern verwenden feste Berechtigungssätze. Beim vierten Kammertyp sind die Berechtigungen variabel. Applikationen, die diesen Kammertyp verwenden, haben Leistungsanforderungen, die während der Installation und zur Laufzeit berücksichtigt werden [Corp].

Kammertypen [Corp]:

- Trusted Computing Base (TCB): Dieser Kammertyp besitzt die umfassendste Rechte. Sie erlaubt Prozessen uneingeschränkten Zugriff auf die meisten Ressourcen des Windows Phone 7 Betriebssystems. Die TCB Kammer kann Sicherheitsrichtlinien verändern und das Sicherheitsmodell durchsetzen. Der Kernel und die Kernel-Mode Treiber laufen in diesem Kammertyp. Je weniger Software den TCP Typ verwendet, umso weniger Angriffsfläche bietet das Betriebssystem.
- Elevated Rights Chamber (ERC): Die Prozesse können auf alle Ressourcen außer der Sicherheitsrichtlinie zugreifen. Der ERC Kammertyp wird für Service und User-Mode Treiber verwendet, die die Funktionalität für die Nutzung durch andere Telefonanwendungen liefern.
- Standard Rights Chamber (SRC): Dies ist die Standard Kammer für vorinstallierte Anwendungen. Alle Anwendungen, die keine geräteweite Dienste anbieten laufen in dieser Kammer.
- Least Privileged Chamber (LPC). Die Standard Kammer für alle Nicht-Microsoft Anwendungen, die über den Marktplatz Hub verfügbar sind. Die LPC Kammern werden durch die „Capabilities“ konfiguriert.

### 2.2.1 Capabilities

Eine Capability ist eine Ressource im Windows Phone 7 Betriebssystem für die hinsichtlich Privatsphäre, Sicherheit, Kosten oder Business, Bedenken bestehen. Solche Ressourcen sind zum Beispiel die Lokation mittels GPS, Kamera, Mikrophone, Netzwerk und Sensoren. Standardmäßig ist in der LPC Kammer ein minimaler Satz von Zugriffsrechten definiert. Allerdings ist dieser Kammertyp dynamisch und kann unter Verwendung von Capabilities erweitert werden. Die Capabilities werden während der Installation der Anwendung bewilligt. Die dazugehörigen Privilegien können nicht während der Laufzeit erhöht werden [Corp].

### 2.2.2 Sandbox

Alle Anwendungen im Windows Phone 7 Betriebssystem laufen in ihrer eigenen isolierten Kammer. Diese werden durch die deklarierten Capabilities definiert, die die Anwendung benötigt. Grundsätzlich wird jeder Anwendung ein Basis-Berechtigungssatz gewährt. Hierzu gehört auch der Zugang zu einer isolierten Speicherdatei. Es gibt im Gegensatz zur Cloud Umgebung, keine Kommunikationskanäle zwischen den Anwendungen auf dem Telefon. Jede

Anwendung ist isoliert von der anderen. Auf dem verwendeten Speicher oder die gespeicherten Daten können fremde Anwendungen nicht zugreifen [Corp].

# 3 Datenakquise

Die forensische Untersuchung des internen Speichers eines Smartphones ist nicht mit der herkömmlichen Untersuchung eines Desktop PCs vergleichbar. Der interne Speicher von Mobiltelefone ist fest installiert. Aus diesem Grund gibt es unterschiedliche Methoden, um dennoch eine forensische Analyse durchzuführen. Der Ausbau des Flash Speichers und die anschließende Analyse liefert zwar die meisten Ergebnisse allerdings birgt diese Methode auch die Gefahr, dass der Speicher zerstört wird, da dieser heraus gelötet werden muss. Das Auslesen des Flash Speichers mittels JTAG Prüfpunkte ist eine weitere Methode. Leider ist diese Methode nur bedingt einsetzbar, da viele Geräte keine JTAG Prüfpunkte besitzen oder nicht gefunden werden können. Die dritte Methode ist eine softwarebasierte Methode. Hierzu wird entweder eine Applikation auf das zu untersuchende Gerät installiert oder das Gerät wird in den Bootstrap Modus versetzt und eine Flash Loader Software in den RAM geschrieben. Diese Software besitzt einen Low Level Zugriff auf den Flash Speicher [SK10]. Die Bootstrap Methode ist aber nicht auf allen Geräten möglich, so dass auf Root Tools zurückgegriffen wird, um eine 1:1 Kopie zu erstellen oder um eine Live Analyse durchzuführen. Allerdings ist eine 1:1 Kopie des internen Speichers abhängig vom Betriebssystem und kann nicht auf allen Geräten durchgeführt werden. Dies führt zwangsläufig zu einer Live Analyse. Alle Methoden sind stark abhängig von den Geräten und installierten Betriebssystemen und haben ihre Vor- und Nachteile. Im Weiteren wird auf die softwarebasierte Live Analyse Methode eingegangen, welche eine installierte Applikation auf dem Gerät verwendet und ein Jailbreak des Gerätes voraussetzt. Im Moment existieren keine kommerzielle- und open-source Software für forensische Untersuchungen an Geräten mit dem Windows Phone 7 Betriebssystem.
Applikationen, die nicht im Microsoft Marktplace angeboten werden, können normalerweise nicht auf ein Smartphone mit dem Windows Phone 7 OS installiert werden. Anwendungen zur forensischen Untersuchungen sind im Markplace nicht vorhanden und müssen unter Umgehung des Marktplaces auf das Gerät gebracht werden. Um dies zu bewerkstelligen muss die Sperre von Microsoft umgangen werden (Jailbreak). Hierzu existieren unterschiedliche Methoden, die ihre Vor- und Nachteile haben und auf die im Folgenden näher eingegangen wird. Eine beispielhafte forensische Analyse erfolgt zu einem späteren Zeitpunkt anhand von aufgestellten Regeln für einen minimalen invasiven Eingriff.

## 3.1 Windows Phone 7 Unlock-Typen und Methoden

Für das Windows Phone 7 OS existieren unterschiedliche Unlocks. Abhängig vom Gerät und der OS Version gewähren sie unterschiedliche Rechte am Gerät. Nicht jede Unlock Variante ist auf allen Geräten und OS Versionen einsetzbar.

### 3.1.1 Developer Unlock /Chevron WP7 Unlock

Mit Hilfe dieses Unlock Typs ist es möglich mittels Sideloading, über die Entwicklungsumgebung, Applikationen außerhalb des Marketplace vom Desktop des angeschlossenen PCs auf das Gerät zu installieren. Selbsterstellte Homebrew Applikationen können so auf dem Gerät deployed werden. Das Gerät wird hierbei in den Developer Modus versetzt. Außer in der Registry werden am Betriebssystem keine weiteren Modifikationen vorgenommen. Der Unlock

kann jederzeit wieder rückgängig gemacht werden. Ein legaler Developer Unlock kostet $99 pro Jahr. Eine kostengünstigere Variante für einen Developer Unlock ist mit dem ChevronWP7 Tool möglich. Sie kostet einmalig $9 und die Verwendung ist von Mircosoft legitimiert. Hierzu hat Microsoft dem ChevronWP7 Team Tokens zur Verfügung gestellt. Für jedes Gerät wird ein eigener Token benötigt. Allerdings sind im Moment alle vergriffen. Dieser Unlock Typ funktioniert auf allen Geräten und OS Versionen [XDADa].

### 3.1.2 Interop Unlock

Seit Windows Phone 7 Mango besteht eine sogenannte Interop Sperre. Sie verhindert das nativer Code aus einer .NET-Anwendung aufgerufen wird, um z.B. Zugriff auf die Systemtreiber zu erlangen. Der Interop Unlock ist ein erweiterter Unlock eines Developer Unlocks. Mit dessen Hilfe ist es möglich unsignierte Applikationen zu installieren, um z.B. auf die Registry des Gerätes zuzugreifen. Die Vorgehensweise für diesen Unlock ist trivial. In der Registry wird, wenn nicht vorhanden der Eintrag *MaxUnsignedApp* angelegt. Der Wert des Eintrages wird normalerweise durch den Typ des Developer Unlocks bestimmt. Bei einem AppHub Account ist dieser Wert auf 10 und bei einem Studenten Account auf 3 gesetzt. Bei dem Interop Unlock wird dieser Wert auf 300 oder mehr gesetzt, was unrealistisch für einen normalen Developer Account ist. Es ist aber denkbar, dass dieser Wert nur für Microsoft Mitarbeiter und OEM Developer eingestellt werden kann. Es existieren unterschiedliche Varianten um den Interop Unlock durchzuführen. Aber alle haben gemeinsam das Ziel den *MaxUnsignedApp* Wert hochzusetzen [XDADa].
Es existiert eine Variante die einen Developer Unlock voraussetzt oder eine Variante auf die nun näher eingegangen wird, die keinen Developer Unlock benötigt. Dieser Interop Unlock wurde von Jaxbox aus dem Windows Phone Hacker Team entwickelt. Dieser Unlock verwendet eine Schwachstelle in der Microsoft ZipView Applikation und in der Geräte Provisioning Funktionalität. Durch die ZipView Applikation ist es möglich Dateien in übergeordnete Verzeichnisse zu entpacken. Normalerweise speichert ZipView die Daten im Verzeichnis Data "*\Volatile\Zipview\<random id >*". Wird nun der Verzeichniseintrag "*../../../../provxml*" in der ZIP Datei vorgenommen, so können Dateien in das Verzeichnis \provxml gespeichert werden. Normalerweise unterbindet das Sandbox Sicherheitsmodel das Speichern von Dateien durch weniger privilegierte Applikationen [XDADb].

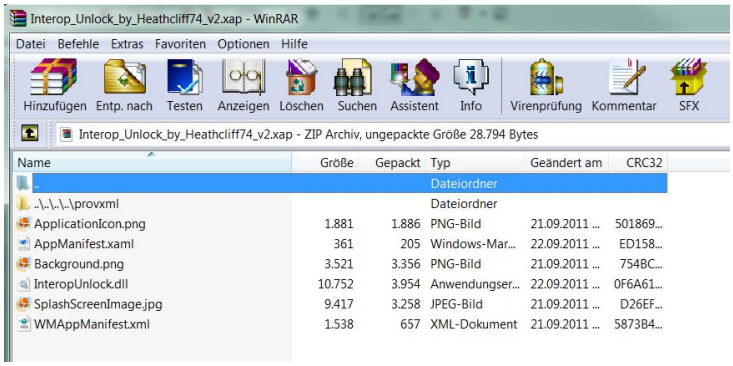


**Abb. 1:** Dateien des Interop Unlocks von Heathcliff74.

Im Verzeichnis "*\provxml*" werden Provisioning XML Dateien gespeichert. Sie werden verwendet um das Mobile Gerät einzurichten. Die ausführbare Datei *RapiConfig.exe* ist ein Desktop Konfigurationstool. Es erlaubt die Ausführung von Provisioning XML Dateien, die im Verzeichnis "*\provxml*" gespeichert sind. Allerdings besitzt die Least Privileged Chamber

```
<?xml version="1.0"?>
- <wap-provisioningdoc>
  - <characteristic type="Registry">
    - <characteristic type="HKLM\Comm\Security\LVMod">
        <parm datatype="integer" value="1" name="DeveloperUnlockState"/>
      </characteristic>
    - <characteristic type="HKLM\Software\Microsoft\DeviceReg">
        <parm datatype="string" value="" name="PortalUrlProd"/>
        <parm datatype="string" value="" name="PortalUrlInt"/>
      </characteristic>
    - <characteristic type="HKLM\Software\Microsoft\DeviceReg\Install">
        <parm datatype="integer" value="2147483647" name="MaxUnsignedApp"/>
      </characteristic>
    </characteristic>
</wap-provisioningdoc>
```

**Abb. 2:** Provisioning XML Datei, um den MaxUnsignedApp Eintrag zu verändern

(LPC) nicht die Rechte binäre Dateien auszuführen. Um dies zu erreichen ist es notwendig ein ungesichertes Geräte IOCTL Interface zu verwenden, um die *RapiConfig.exe* auszuführen. Bei Samsung Geräten wird hierzu z.B. der GPRS Treiber verwendet. Im GPRS Manager wird ein weiterer Verzeichniseintrag zur Verfügung gestellt, der die *RapiConfig.exe* Datei mit den entsprechenden Konfigurationsdaten ausführt.

Dieser Interop-Unlock funktioniert im Moment nur auf Samsung Geräten, auf dem nicht das KK2 Update eingespielt wurde. Im Prinzip funktioniert dieser Unlock auch auf Geräten anderer Hersteller, jedoch blockieren Nokia, HTC Registry Einträge in Provisioning Dateien. Smartphones vom Hersteller LG sind eine Ausnahme, denn diese können mit dem von Haus aus installierten Registry Editor gejailbreakted werden.

### 3.1.3 Full Unlock und Full Root Access

Ein voller Unlock ermöglicht es „Nativ Executables“ auszuführen. Alle Applikationen sind Silverlight Applikationen, die in einer Sandbox laufen. Sie werden als DLL kompiliert und laufen in der TaskHost.exe mit den geringst möglichen Privilegien. Im Moment existieren keine veröffentlichten „Full Unlocks“. Es wird aber an ROMs mit „Full Unlocks“ gearbeitet. Für eine forensische Untersuchung ist aber ein flashen mit einem ROM keine Alternative [XDADa].

Ein „Full Root Access“ für alle Smartphones mit dem Windows Phone 7 OS existiert im Moment nur für das HTC HD2 Smartphone. Er ermöglicht Applikationen die Restriktionen des Policy Systems zu umgehen, in dem das Policy System einfach abgeschaltet wird. Allerdings muss auch hier das Gerät mit einem neuen ROM geflasht werden [XDADa].

## 3.2 Forensische Software

Auf dem Markt existieren zahlreiche kommerzielle Produkte für forensische Untersuchungen, wie z.B. Paraben Device Seizure, Oxygen Forensic Suite, EnCase, MobilEdit usw. Allerdings kann kein Tool softwarebasierte forensische Untersuchungen an Geräten mit dem Windows Phone 7 Betriebssystem vornehmen.

Es existieren auch keine spezielle Open Source Software für forensische Untersuchungen. Allerdings gibt es Software, wie Touchxperience, mit deren Hilfe sehr gute Untersuchungsergebnisse erzielt werden können. Der Zugriff auf das System ist hierbei aufgrund von fehlenden Rechte eingeschränkt. Ein voller Zugriff auf das System ist nicht möglich und es wird ein Interop Jailbreak bzw. Unlock benötigt.

# 4 Regeln zur minimal invasiven Ermittlung

Im Kapitel 3 wurde aufgezeigt, dass die forensische Untersuchung von mobilen Geräten zum Teil eine andere Vorgehensweise erfordert, als bei Desktop PCs. Oftmals ist eine Untersuchung nur mittels einer Live Analyse möglich. Aus diesem Grund muss das Paradigma der Unveränderthеit des zu untersuchenden Speichers aufgeweicht werden. Hierzu werden Regeln vorgestellt, die die neuen Anforderungen an Hardware und an Betriebssysteme berücksichtigen.

## 4.1 Regeln

Die Einhaltung von Regeln bei der forensischen Untersuchung ist ein Muss für jeden Forensiker. Umso wichtiger ist es bei der Veränderung von Beweismitteln, das diese eingehalten werden, da eine Verletzung sonst zu einem Beweisverwertungsverbot führen könnte. Die folgenden Regeln konnten aufgrund der Untersuchungsergebnisse und den neuen Anforderungen ermittelt werden:

- **Die Veränderung muss gerechtfertigt sein.**
  Eine Veränderung des Speichers sollte wenn möglich vermieden werden. Falls eine andere Untersuchungsmethode ebenso gute Untersuchungsergebnisse erzielt und der Speicher der Gefahr der Zerstörung dabei nicht ausgesetzt wird, dann sollte diese verwendet werden. Es besteht die Gefahr eines Beweisverwertungsverbotes oder der Beweisminderung, wenn eine Untersuchungsmethode eingesetzt wird, die den Speicher verändert, obwohl es eine andere gibt, die gleich gute Ergebnisse liefert und den Speicher nicht verändert. Eine Rechtfertigung für das Handeln dürfte in diesem Fall schwierig sein.
- **Die Veränderung des Speichers sollte so minimal wie möglich sein.**
  Für die forensische Analyse können unterschiedliche Untersuchungsmethoden und Tools bestehen. Es sollte deshalb immer die Variante gewählt werden, die den Speicher am geringsten verändert. Als Beispiel könnte hier der Einsatz von Jailbreak Tools angeführt werden. Es können Varianten existieren, bei denen Dateien auf dem Gerät gespeichert werden müssen und welche die einen schon installierten Registry Editor verwenden, um die nötigen Einstellungen durchzuführen. Des Weiteren könnten zu einem späteren Zeitpunkt neue Möglichkeiten bestehen den Speicher besser zu untersuchen. So könnte ein übermäßiges überschreiben des Speichers zu einer Vernichtung an Beweise führen. Diese Gefahr besteht in jedem Fall. Allerdings sollte das Risiko so gering wie möglich gehalten werden.
- **Die Veränderung muss genauestens protokolliert sein.**
  Bei jeder forensischen Untersuchung muss die Analyse genauestens protokolliert werden. Bei der Veränderung des Speichers durch die Untersuchung muss dies noch genauer vollzogen werden. Nur so kann dem Gericht verdeutlicht werden, was bei der Untersuchung gemacht wurde, welche Daten verändert wurden und vor allem, dass keine Beweise verfälscht oder absichtlich gelöscht wurden. Eine nicht protokollierte Veränderung könnte sonst als Versuch der Täuschung gewertet werden. Auch ohne Absicht könnte dies zu einem Beweisverwertungsverbot führen, da angenommen werden könnte, dass weitere nicht protokollierte Veränderungen vorgenommen wurden. Umso wichtiger ist es deshalb zu wissen, welche Veränderungen durchgeführt wurden [Kirc03]. Der Einsatz von selbst entwickelten Tools wäre ein guter Schritt in die richtige Richtung.
- **Die Veränderung darf keine Auswirkungen auf die Beweise haben.**
  Eine forensische Analyse, die Beweise löscht oder verfälscht führt zu einem Beweisver-

wertungsverbot. Es ist deshalb sicher zu stellen, das die eingesetzten Methoden keinerlei Auswirkungen auf die Beweise haben. Durch eine lückenlose Protokollierung und der Einsatz von selbstgeschriebenen Tools kann dies bewerkstelligt werden.

## 4.2 Fallbeispiel: Beweissuche für Kinderpornographie

Im nachfolgenden generierten Beispiel wird gezeigt, wie anhand der aufgestellten Regeln eine forensische Untersuchung durchgeführt werden kann, die vor Gericht verwertbare Beweise liefert. Die Untersuchung erfolgt an einem LG Optimus 7 mit Windows Phone 7.5 und der Software Touchxperience.
Simuliert wird ein Austausch von kinderpornographischen Inhalten. Zur Verdeckung wurde versucht entsprechendes belastendes Material vom Gerät zu löschen. Die forensische Untersuchung umfasst in unserem Beispiel nur die Analyse des SMS Verkehrs und die Suche nach belastenden multimedialen Inhalten.

- **Anwendung der 1. Regel: Die Veränderung muss gerechtfertigt sein.**
  Vor der Untersuchung muss geklärt werden, wie das Gerät untersucht werden kann. Es ist zu klären, ob es eine Methode gibt, die den Speicher am geringsten oder gar nicht verändert. Der Ausbau des Speichers sollte hierbei immer zuletzt gewählt werden, da der Speicher unter Umständen irreparabel beschädigt werden kann. Für das LG Optimus 7 sind bisher keine JTAG Prüfpunkte bekannt und es existiert auch keine Bootstrap Methode. Es ist allerdings über einen Jailbreak und einer Untersuchungssoftware möglich das Gerät mittels einer Live Analyse eingeschränkt zu untersuchen. In diesem Fall existiert keine andere Möglichkeit für eine forensische Untersuchung.
- **Anwendung der 2. Regel: Die Veränderung des Speichers sollte so minimal wie möglich sein.**
  Um die forensische Untersuchung durchführen zu können, muss das Gerät "gejailbreakt" werden und es muss eine Applikation, die eine Untersuchung erlaubt auf das Gerät installiert werden. LG Geräte können über den vorinstallierten Registry Editor "gejailbreakt" werden. Eine Aufspielung von Dateien, wie es bei anderen Geräten unter Umständen notwendig ist, ist hier nicht erforderlich. Des weiteren sollten zur Untersuchung, wenn möglich selbst geschriebene Applikationen oder Anwendungen verwendet werden, bei denen die Veränderung des Speichers genau nachvollzogen werden kann und aufgeblähte Software nicht unnötig Daten überschreibt. In diesem Fall wurde die Applikation "Touchxperience" in der Version 2.3 verwendet. Diese wird durch die Software "Windows Phone Device Manager", welche auf einer forensischen Workstation installiert ist, automatisch beim Start der Software als Applikation auf dem Smartphone deployed.
- **Anwendung der 3. Regel: Die Veränderung muss genauestens protokolliert sein.**
  Alle Maßnahmen und Veränderungen müssen für forensische Untersuchungen genauestens protokolliert werden. Hierzu gehören die Änderungen in der Registry für den Jailbreak und der Applikation, die installierten Daten der Applikation und die durch die Untersuchung erstellten Kopien von Dateien auf dem Flashspeicher (s.u.). Der Jailbreak an LG Sartphones erfordert nur die Änderungen von Einträgen in der Registry mithilfe des installierten Editors. Die Änderungen sind aus Abbildung 2 ersichtlich. Die Applikation TouchXperience wird durch die Software Windows Phone Device Manager auf dem Gerät automatisch deployed. Sie installiert sich im Ordner "*\Applications\Install\44435744-8A09-42AA-BE3D-80A4BB68001C\Install*". Die zugehörigen Daten werden im Ordner "*\Applications\Data\44435744-8A09-42AA-BE3D-80A4BB68001C\Data*" gespei-

chert. Änderungen der Registry durch die Applikation konnten nicht protokolliert werden. Eine Anfrage an den Hersteller blieb bis heute unbeantwortet. Ein Vergleich des SHA256-Hashwertes der Registry Dateien *system.hv*, *user.hv* und *default.vol* im Verzeichnis \Windows\Regsitry zeigte vor und nach der Installation von TouchXperience keine Veränderung. Ein Änderung der Registry durch TouchXperience kann somit ausgeschlossen werden.

- **Anwendung der 4. Regel: Die Veränderung darf keine Auswirkungen auf die Beweise haben.**
  Damit die forensische Untersuchung vor Gericht ihre Beweiskraft entfalten kann, dürfen durch die Analyse keine Beweise, gelöscht oder verfälscht werden. Anhand der folgenden beispielhaften forensische Untersuchung, wird verdeutlicht, das eine mit Sorgfalt durchgeführte Untersuchung keine Beweise löscht oder verfälscht. Eine genaue Protokollierung ist hierbei eine Voraussetzung.

  1. **Suche nach Bilder**
     Auf dem Gerät werden Bilder normalerweise im Verzeichnis "*\My Documents\Zune \Content\0300\00*" gespeichert. In diesem Verzeichnis befinden sich allerdings keine verdächtigen Bilder. Es ist aber keine Gewähr dafür, das sich nicht an anderen Stellen im Dateisystem Bilder befinden könnten. Diese könnten vom Benutzer gelöscht oder durch ein "gejailbreaktes" Gerät an einer anderen Stelle versteckt worden sein. Des Weiteren können sich Bilder auch als Anhang an einer SMS / eMail oder außerhalb des Gerätes z.B. in der Cloud befinden.
  2. **Analyse der SMS Daten**
     Die SMS Daten werden in dem File *store.vol* gespeichert. Diese befindet sich im Verzeichnis "*\Application Data\Microsoft\Outlook\Stores\DeviceStore*". Die Datei ist eine EDB Datenbank und wird vom System verwendet, sodass sie nicht auf die Workstation kopiert werden kann. Eine Umbenennung legt eine Kopie an. Es zeigt sich, dass Beweise hierbei weder gelöscht noch verändert werden. Die erstellte Datei kann anschließend kopiert werden.

     Die *store.vol* Datei umfasst auch gelöschte SMS. Diese können mit einem beliebigen Editor ausgelesen werden.

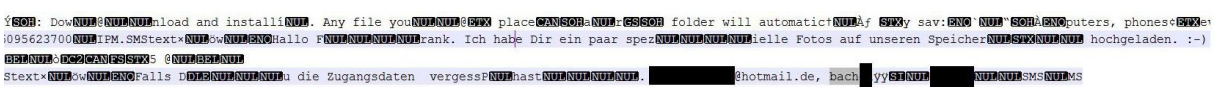


**Abb. 3:** Anzeige zweier gelöschte SMS mit Zugangsdaten zu einem Online Account

Aus den SMS ist ersichtlich, das der Verdächtige mit einer Person namens Frank in Kontakt steht. Dieser hat ihm Bilder auf einem Online Speicher zur Verfügung gestellt und in einer weiteren SMS noch einmal die Zugangsdaten bereitgestellt. Neben dem Text ist auch die Telefonnummer zu ermitteln. Für welchen Dienst der Benutzername und das Passwort den Zugang ermöglicht, ist in diesem Zusammenhang noch nicht ersichtlich. Eine Analyse der installierten Applikationen könnte allerdings ein Hinweis geben. Die vom Benutzer installierten Applikationen werden im Verzeichnis "*\Applications\Install*" installiert.

3. **Analyse einer Cloud Applikation**
   Es zeigt sich das der Verdächtige eine Skydrive Applikation installiert hat.

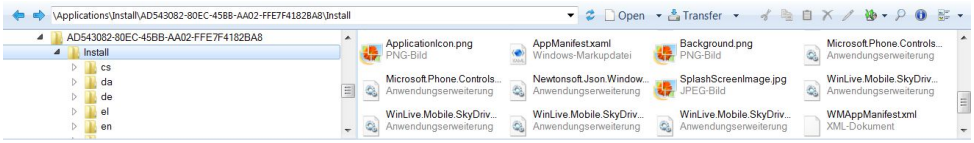


**Abb. 4:** Installierte Skydrive Applikation

Heruntergeladene Bilder aus dem Cloud Speicher werden normalerweise im allgemeinen Bilderverzeichnis gespeichert. Es zeigte sich aber, dass in diesem Verzeichnis keine belastendes Material zu finden war. Allerdings speichert Skydrive die online betrachtenden Bilder temporär im Verzeichnis "$\backslash Applications \backslash Data \backslash \{SkydriveApplikation\} \backslash Data \backslash IsolatedStore \backslash FileCache$"

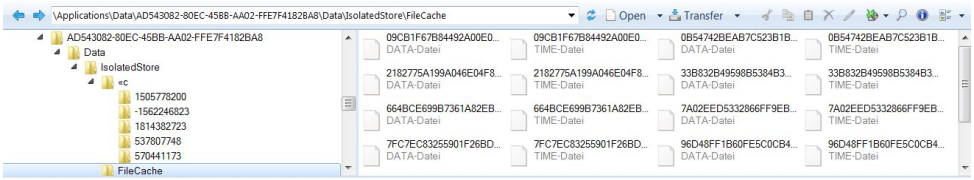


**Abb. 5:** Temporär gepspeicherte Bilder der Skydrive Applikation

Die Bilddaten werden in DATA Dateien gespeichert. Diese sind mit jeder beliebigen Bildbetrachtungs-Software zu öffnen. Die TIME Dateien enthalten die Uhrzeit und das Datum des Betrachtungszeitpunktes.

Mithilfe der via SMS übermittelten Zugangsdaten, konnte auf einen Skydrive Account zugegriffen werden. Dort befanden sich weitere zahlreiche Inhalte mit kinderpornographischen Inhalten.

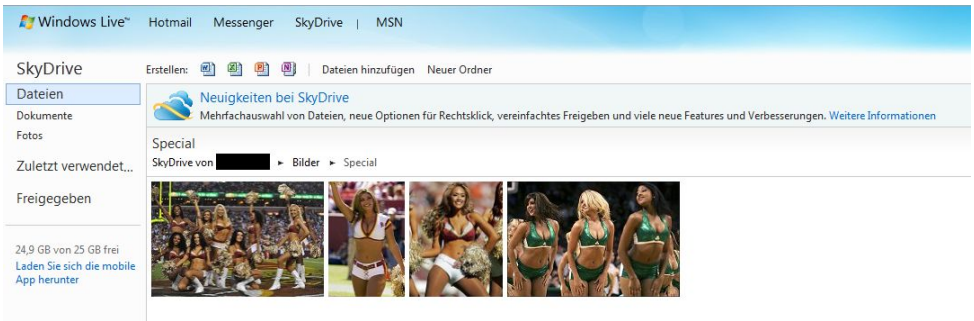


**Abb. 6:** Gespeicherte Bilder in der Cloud

- **Zusammenfassung der Analyse**
  Aufgrund der beispielhaft durchgeführten forensischen Untersuchung konnte belastbares Material gefunden werden, die ohne den Jailbreak und des Verwendens der Applikation Touchxperience nicht gefunden werden konnten. Neben den Änderungen an der Registry (Änderungen und Hinzufügen von Variablen durch den Jailbreak und der Touchxperience Applikation), dem Belegen eines kleinen Teil des Speichers durch die Touchxperience

Applikation und der Kopie des SMS Datenbank wurde der Flash Speicher nur minimal durch die Untersuchung verändert. Vor allem konnte detailliert aufgezeigt werden, welche Veränderungen durchgeführt worden sind und weiter, dass diese keine Auswirkungen auf das belastbare Material im Speicher hatten. Die Analyse ist nicht abschließend und stellt nur einen kleinen Teil der zu untersuchenden Daten bereit.

# 5 Zusammenfassung und Ausblick

Die eingesetzten Techniken des Jailbreaks und Analysemethoden haben gezeigt, das bei einer forensischen Untersuchung keine beweisrelevanten Daten verändert werden. Die Veränderungen für den Jailbreak sind abhängig vom Gerät und Betriebssystem. Sie betreffen hauptsächlich die Registry und überschreiben je nach Unlock-Typ einen kleinen Teil des Flash Speichers. Das gleiche gilt auch für die Touchxperience Applikation. Alle Veränderungen konnten protokolliert und nachvollzogen werden. Ein Verbot für Beweise, die auf diese Weise gewonnen wurden ist deshalb nicht notwendig und wäre in Folge der obigen Ausführungen nicht nachvollziehbar. Dem hat auch das BSI Rechnung getragen, in dem es vorschreibt, dass bei Veränderungen an den Daten diese festgehalten und dokumentiert werde sollen. Im Rahmen der abschließenden Dokumentation soll dann die Verfälschung gerechtfertigt und der Verfälschungsgrad und dessen Bedeutung bewertet werden, was unter Umständen einen Einfluss auf die Beweiskrafttendenz hat [Info11].

Für forensische Untersuchungen an mobilen Endgeräten müssen und sollten deshalb die Prinzipien für forensische Untersuchungen aufgeweicht werden. Folgende Voraussetzungen sind für Untersuchungen an mobilen Endgeräten, die eine Veränderung des Beweismittels hervorrufen zwingend notwendig:

- Die Veränderung muss gerechtfertigt sein.
- Die Veränderung des Speichers sollte so minimal wie möglich sein.
- Die Veränderung muss genauestens protokolliert sein.
- Die Veränderung darf keine Auswirkungen auf die Beweise haben.

Im Artikel von [Ro2011] werden die Regeln für zulässige Veränderungen am Beweismaterial im Rahmen einer Fallstudie für eine kontrollierte Veränderung an einem Notebook vorgestellt und auf alle forensische Untersuchungen übertragen. Das führt aber zu der Problematik, dass durch die Verallgemeinerung nicht auf alle Besonderheiten in Bezug auf mobile Geräte eingegangen werden kann. Zum Beispiel sagt die dritte Regel nach Roth, dass Änderungen nur an den Kopien vorkommen dürfen. [Ro2011] setzt voraus, dass vom internen Speicher von Smartphones eine Kopie erstellt werden kann. Das dies aber nicht bei allen Geräten möglich ist, wurde von Schuba, Höfken und Schäfer [ScHS] an Smartphones mit dem Windows Phone Betriebssystem gezeigt. Des Weiteren geht Roth [Ro2011] auch nicht der Frage nach, ob die Veränderung überhaupt gerechtfertigt ist. Es können bessere Möglichkeiten bestehen, die den Speicher weniger oder gar nicht verändern. Diese Unterschiede sind auf die unterschiedlichen Sichtweisen zurückzuführen. Eine Verallgemeinerung auf alle forensischen Untersuchungen, würde nicht alle Besonderheiten der Hard- und Software berücksichtigen. Aus diesem Grund sollte eine differenzierte Sicht bei der Erstellung der Regeln angenommen werden.

# Literatur

[Beck12] H. Becker: Beweissicherung in IT-Systemen. URL: http://www.henrikbecker.de/index.php?id=Grundlagen&kat=01&part=10, (18.04.2012).

[Corp] Microsoft Corportaion: Architecture Guide for Windows Phone OS 7.0. URL: http://www.pocketpc.ch/windows-phone-7-entwicklung/93608-windows-phone-7-os-guides-leaked.html, (18.04.2012).

[Info11] BSI: Leitfaden It-Forensik. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Leitfaden_IT-Forensik_pdf.pdf?__blob=publicationFile, (18.04.2012).

[Kirc03] J. Kirchner: Forensische Analyse. URL: http://www.jenskirschner.com/pub/ forensik.pdf, (2003).

[Knop09] M. Knopp:: Rechtliche Perspektiven zur digitalen Beweisführung. GI Jahrestagung, Vol. 154GI, p. 1552-1566, (2009).

[Hakin9] H. Höfken, Marko Schuba, T. Schaefer: Smartphone Forensik. URL: Ihttp://www.schuba.fh-aachen.de/papers/12_Smartphone_Forensik_Hakin9.pdf, (2012).

[SHS11] T. Schaefer, H. Höfken, M. Schuba: Windows Phone 7 from a Digital Forensics Perspective. In: ICDF2C '11: Digital Forensics and Cyber Crime, Third International ICST Conference, Dublin, IRL (2011).

[SK10] S. Krause: Mobile Forensics. URL: http://www.all-about-security.de/security-artikel/endpoint-sicherheit/mobile-computing-und-pdas/artikel/11982-mobile-forensics, (18.04.2012).

[ME2008] G. Me: MIAT - Mobile Internal Acquisition Tool. URL: http://www.dfrws.org/2008/proceedings/p121-distefano_pres.pdf

[PBOZ97] P. Pavan, R. Bez, P. Olivo, E. Zanoni: Flash Memory Cells - An Overview, Proceedings of the IEEE, Vol. 85, No. 8, August 1997, pp. 1248-1271

[BJKKR] M. Breeuwsma, M. de Jongh, C. Klaver, R. van der Knijff and M. Roeloffs: Forensic Data Recovery from Flash Memory, Small Scale Digital Device Forensics Journal, Vol. 1, No. 1, June 2007, pp. 1-17

[Ro2011] C. Roth: Handy auf dem Seziertisch. URL: http://www.computer-beweissicherung.de/mforensic.pdf, (2011).

[XDADa] H. XDA Developer: WP7 Root Tools for MANGO, URL: http://forum.xda-developers.com/showthread.php?t=1265321, (2010).

[XDADb] J. XDA Developer: The WindowBreak Project, URL: http://forum.xda-developers.com/showthread.php?p=20619864, (2011).