FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Windows Phone 7

aus forensischer Sicht

Thomas Schaefer

IT Forensik
FH Aachen

Inhalt

- Einleitung
- Windows Phone 7
- Dateisystem
- Analyse (live)
- Fazit

Einleitung

- Neues Smartphone Betriebssystem
  - Release: Oktober 2010

- Ziel: Möglichkeiten einer Analyse:
  - Logisch: SMS / MMS, CallLogs, Audio/Video etc.
  - Dateisystem: Dateien, Apps etc.

Windows Phone 7

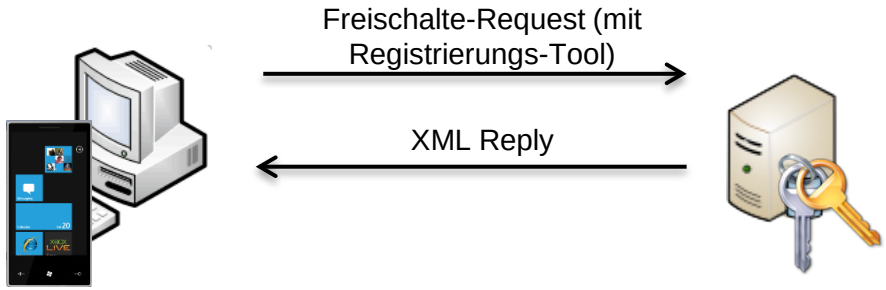
- Neues Smartphone Betriebssystem
  - Release: Oktober 2010

- Neuerungen unter anderem:
  - Hardware
  - Marketplace Anbindung
  - Entwicklung

Windows Phone 7

- Freischalte-Prozess (normal)
  1. Einrichtung von Entwicklerkonten
  2. GeoTrust Verifikation
  3. Freischaltung des physischen Gerätes
  4. Deploy möglich

Windows Phone 7



Entwickler-Workstation mit Phone

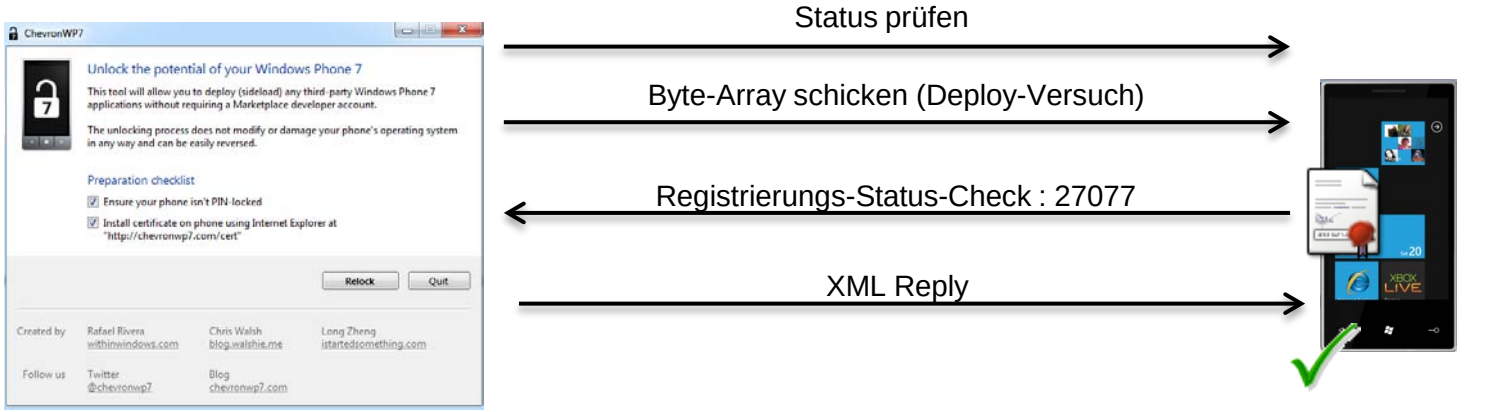
Microsoft Registrierungs-Server

Freischalte-Prozess (normal)

Windows Phone 7

- Freischalte-Prozess (ChevronWP7)
  - Bildet Registration Tool nach (Reflector)
  - Modifiziert den Prozess
  - Verteilt „gefälschtes“ Reply-XML

Windows Phone 7



ChevronWP7
Laufender Check des Ports 27077

Windows Phone 7

Freischalte-Prozess (ChevronWP7)

Windows Phone 7

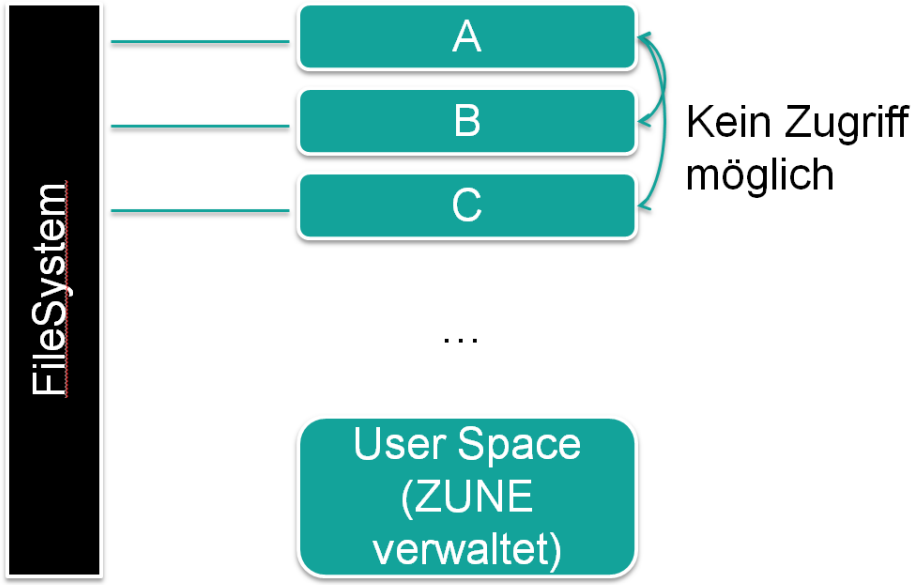

```
<ResponseOfRegisteredDeviceStatus xmlns="Microsoft.WindowsMobile.Service.Ma
rketplace" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">

<ResponseCode>0x00000000</ResponseCode>
<ResponseMessage i:nil="true"/>
<Entity xmlns:a="http://schemas.datacontract.org/2004/07/Microsoft.WindowsM
obile.Service.Marketplace.BLLDevPortal.Entities">
    <a:DaysLeft>365</a:DaysLeft>
    <a:AppsAllowed>10</a:AppsAllowed>
</Entity>
```

Reply-XML

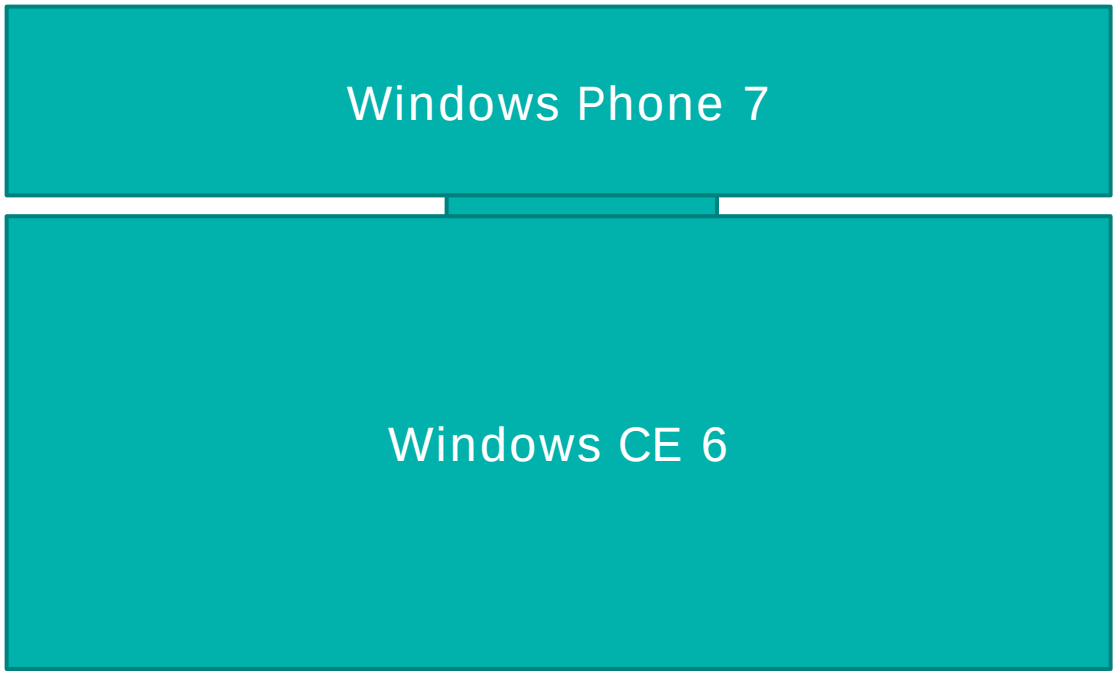
Windows Phone 7 Dateisystem

- Dateisystem **nicht** zugänglich!
- IsolatedStorage Prinzip:
  - Anwendungen dürfen **nur** auf ihren **eigenen** IsolatedStorage zugreifen



Windows Phone 7 Dateisystem

- „Unterbau“ ist Windows CE 6!

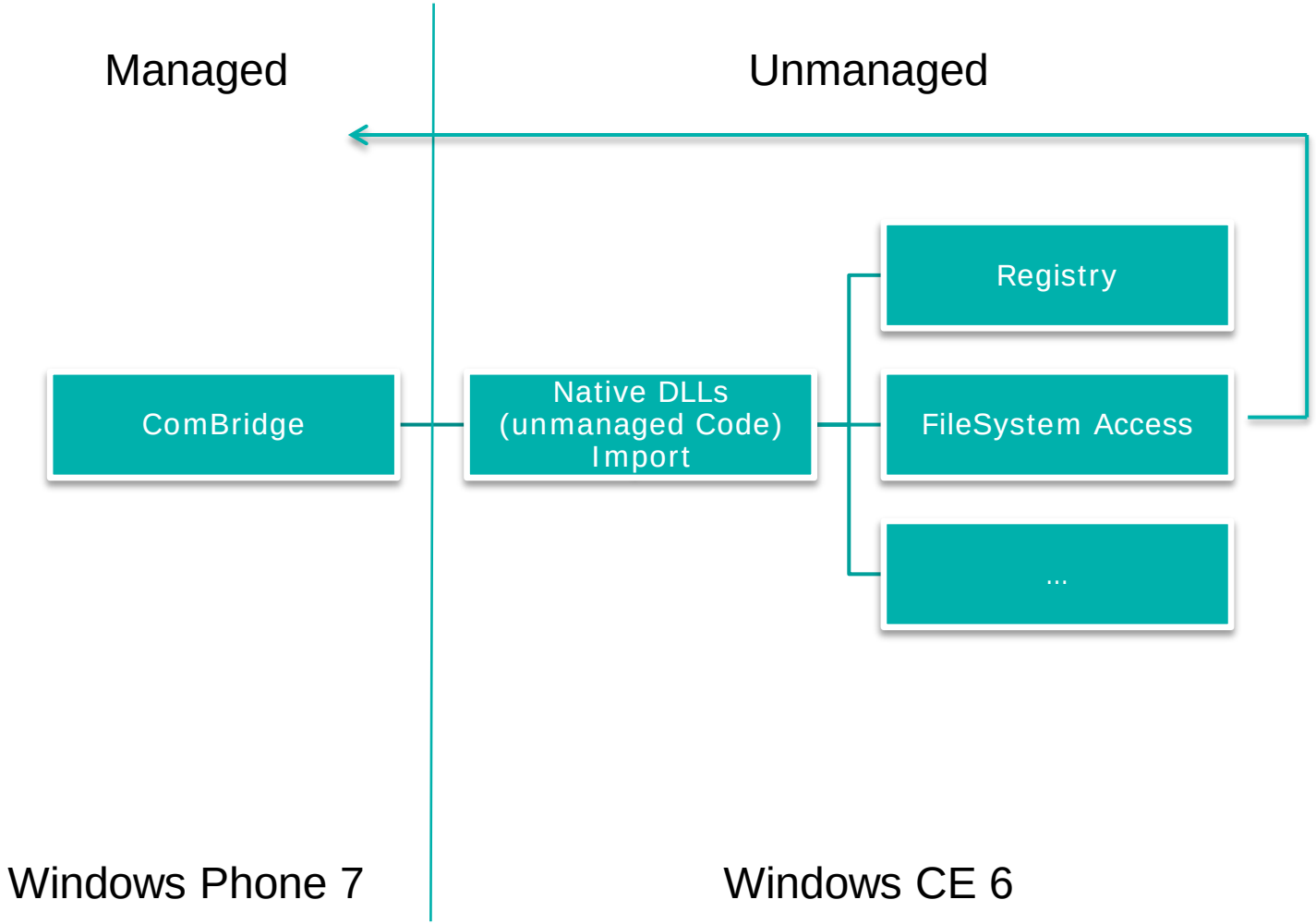


Windows Phone 7 Dateisystem

- „Tunnel“ zu Unterbau über DLL:
  - Microsoft.Phone.InteropServices.dll
  - Klasse ComBridge
  - Herkunft: WireShark Sniff

- Es ist möglich COM Elemente zu importieren und zu benutzen (Windows CE DLLs)

Managed vs. Unmanaged Code



Analyse (live)

- Auf dieser Basis sind folgende Auswertungen (bisher) erfolgreich:
  - System

Daten	Tool
Registry	Una, PhoneApp
Aktive Tasks	Una, PhoneApp
Telefon Informationen	Una, PhoneApp
Datei-System	WPDM
...	

Analyse (live)

- Auf dieser Basis sind folgende Auswertungen (bisher) erfolgreich:
  - Anwendungsdaten

Daten	Anwendungen
Nachrichten (SMS / Email / Facebook)	WPDM, TouchXperience, HexEditor, Perl-Skript
Dokumente	WPDM
CallHistory	WPDM, Hex-Editor
Facebook	WPDM, Hex-Editor (und andere…)
…	

Fazit

- Vieles ist schon jetzt möglich
- Auswertungs-Anwendungen **werden** mächtiger
- Grundlage für eine Forensic-Suite ist gegeben

Fazit

Ende