FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Live Response für Windows 8

Alpaslan Aktas
Lehrgebiet Datennetze

IT Forensik
FH Aachen

Gliederung

- Warum Live Response für Windows?
- Vorgehensweise
- Neuerungen in Windows 8
- bisherige Ergebnisse

Warum Live Response für Windows?

- Live Response wichtig
  - aufschlussreiche Informationen gehen verloren
  - wegen Verschlüsselung von Daten
- Windows 8 neu und wichtig
  - Consumer Preview (Beta) am 29. Februar 2012 erschienen

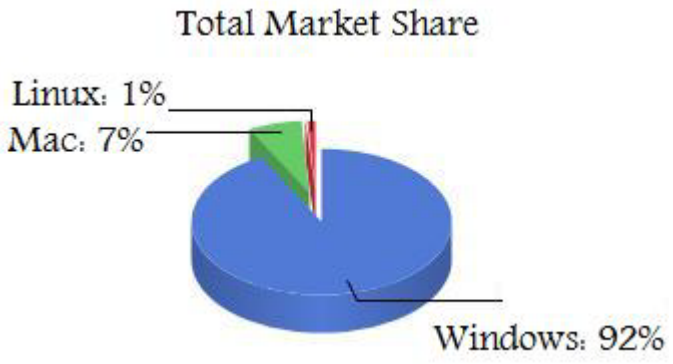
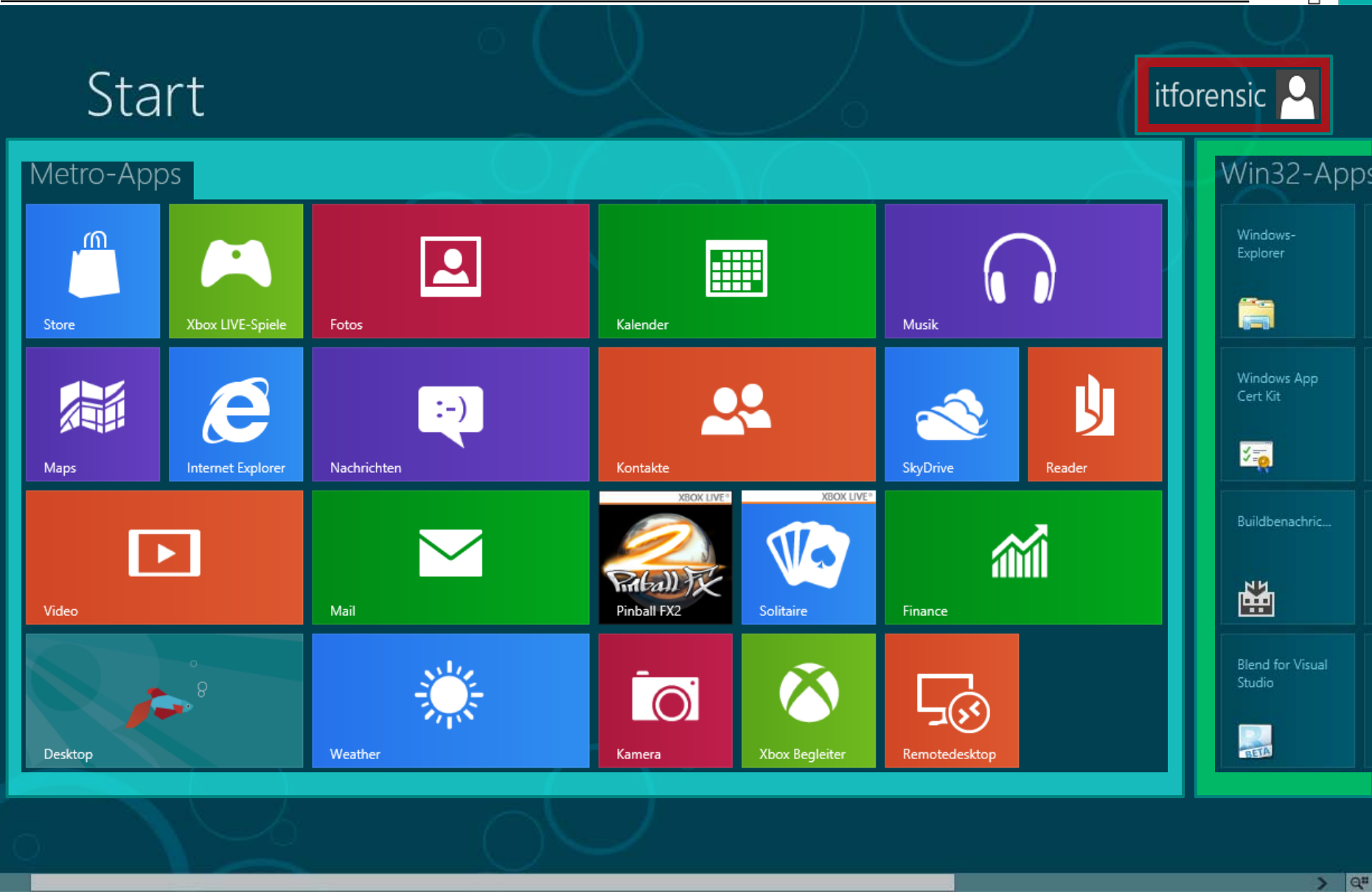


Abb.1: netmarketshare.com, Stand: 04.04.2012

Vorgehensweise

- Testen von Tools für Windows7
- Programmieren von neuen Tools
  - Aufgrund von Neuerungen in Windows 8
- Programmieren einer Benutzeroberfläche
  - Benutzer wird durch Live Response geführt
  - Ausgabe eines Reports

Neuerungen in Windows 8



Neuerungen in Windows 8

- Windows On ARM
  - Einstieg ins Tablet-Segment
  - Keine Unterstützung für Desktopapplikationen
- alte GUI wegen Kompatibilitätsgründen verfügbar
  - Alte Win32-Programme laufen hierauf weiterhin
- „Metro“ auf Touchscreen ausgelegte neue GUI
  - Alte GUI nur über diese startbar
  - Metro-Apps bekommen eine neue Laufzeitumgebung Windows Runtime (WinRT)

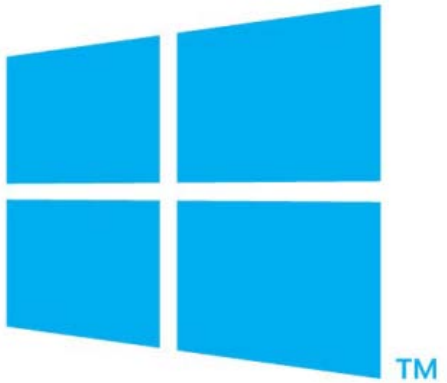
GUI: Graphical User Interface (Grafische Benutzeroberfläche)

Neuerungen in Windows 8

- Neues Dateisystem „ReFS“ (ResilientFS)
  - wichtig für die Post Mortem-Analyse
- „Refresh“-Funktion sichert benutzerspezifische Daten und setzt Windows zurück
- „Windows to Go“ (Windows auf USB)
  - Windows für mobilen Einsatz
  - installierte Software und Daten jederzeit dabei
- Cloud-Anbindung (SkyDrive)
  - Anmeldung bei Microsoft Windows Live nötig
  - alle Konfigurationen und Daten sind online verfügbar

bisherige Ergebnisse

- für die Tests verwendete Windowsversion
  - Microsoft Windows 8 Consumer Preview (Beta) von 29. Februar 2012
- Vergleich mit früheren Betriebssystemen
  - Microsoft Windows Vista Home Premium
  - Microsoft Windows 7 Professional



bisherige Ergebnisse

Windows Forensik Toolchest*

- Toolsammlung für vorherige Windows Betriebssysteme
- Tools deren Hash-Wert nicht mit dem Hash in der Konfigurationsdatei übereinstimmen werden trotzdem gestartet
- alte GUI: vorhandene Tools laufen ohne Probleme
  - Ausnahme: pclip.exe – sollte Daten aus der Zwischenablage ausgeben
- neue GUI: keine Kompatibilität wegen WinRT

*Quelle: http://www.foolmoon.net/security/wft/

bisherige Ergebnisse

Windows Sysinternals

PsTools*

- pslist – listet alle laufenden Prozesse
  - Problem: Apps werden nur als WWAHost.exe aufgelistet
- alle anderen laufen ohne Probleme
  - psloggedon – listet alle angemeldeten Benutzer
  - psloglist – Abbilden von Ereignisprotokollen
  - psservice – Anzeigen und Steuern von Diensten
  - psinfo – listet Informationen über ein System

*Quelle: http://technet.microsoft.com/de-de/sysinternals/bb896649

bisherige Ergebnisse

- Nächster Schritt:
  - Testen von weiteren Tools
  - Überprüfen und Dokumentieren von Änderungen am System durch die Tools
- Verschlüsselung - ein riesiges Problem
  - RAM-Analyse für Extraktion des BitLocker-Schlüssels
  - RAM Imaging nicht mehr mit allen Tools möglich
    - dd und mdd ohne Funktion
    - winen von Guidance Software ohne Probleme

Guidance Software | EnCase

FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Vielen Dank für Ihre Aufmerksamkeit

Haben Sie noch Fragen?

IT Forensik
FH Aachen