

Mobile Device Security and Ethical Hacking

# Mobile Application Penetration Testing

## Windows Phone 8

Wouter Veugelen

Copyright 2013, All Rights Reserved

# Mobile Application Security

- Background
  - Mobile operating systems
  - Microsoft operating systems
    - Windows 8, Windows RT, Windows Phone
- Windows Phone 8
  - Application Penetration Testing
    - XAP file format, sideloading, decompiling, configuring a web application proxy
  - Mobile Device Security Testing
    - Jailbreaking, File system analysis, network vulnerability assessment
- Future work
- Resources and further references

# Background

# Mobile operating systems

**Top Smartphone Operating Systems, Forecast Market Share and CAGR, 2012–2016**

Smartphone OS	2012 Market Share	2016 Market Share	CAGR 2012 - 2016 (%)
Android	68.3%	63.8%	16.3%
iOS	18.8%	19.1%	18.8%
BlackBerry OS	4.7%	4.1%	14.6%
Windows Phone	2.6%	11.4%	71.3%
Linux	2.0%	1.5%	10.5%
Others	3.6%	0.1%	-100.0%
<b>Total</b>	<b>100.0%</b>	<b>100.0%</b>	<b>18.3%</b>

Source: IDC Worldwide Mobile Phone Tracker, December 3, 2012

# Mobile operating systems

www.examiner.com/article/windows-phone-overtakes-blackberry-market-share

Interests Creative Games Automotive Gadgets & Tech Travel Video More

## Windows Phone overtakes BlackBerry in market share

MOBILE | FEBRUARY 6, 2013 | BY: R. CHASE RAZABDOUSKI | + [Subscribe](#)



10 33 0 0

Internet newsletter

**New pope**

**MORE CELEB**

**15 PHOTOS**

**SA**

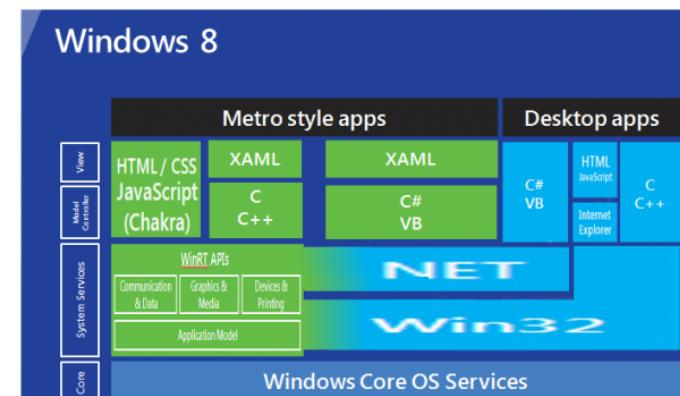
# Microsoft's current OS portfolio

- Windows 8
- Windows RT
- Windows Phone 8

	<b>Hardware Architecture</b>	<b>Applications Architecture</b>	<b>OS Kernel</b>
Windows 8	x86/x64	Win32/WinRT	Windows NT
Windows RT	ARM	WinRT	Windows NT
Windows Phone 7	ARM	Silverlight / XNA	Windows CE
Windows Phone 8	ARM	Windows Phone RT	Windows NT

# Windows 8

- x86/x64 CPU compatible hardware
- Win32 and WinRT application architecture
- Key OS security features:
  - ASLR (Address Space Layout Randomization)
  - DEP (Data Execution Prevention)
  - SMEP (Supervisor Mode Execution Protection)
  - Secure boot (UEF)
  - ELAM (Early Launch Anti-Malware)
  - Bitlocker
  - Application sandboxing
  - ...

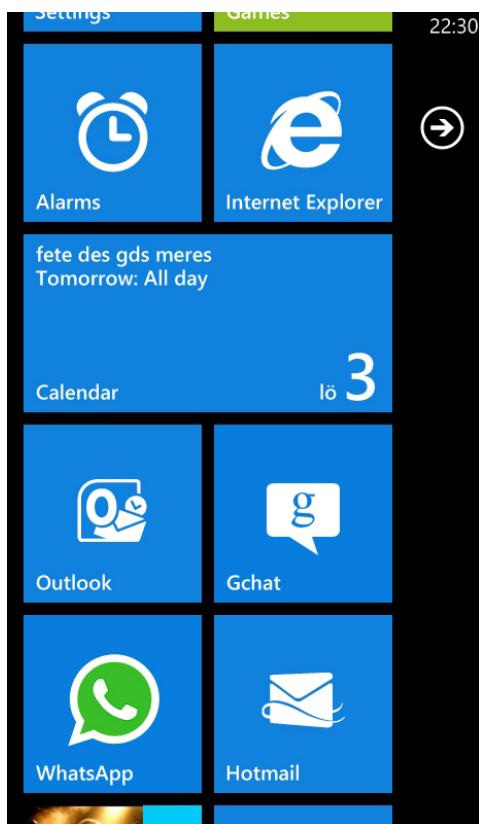


# Windows Phone



- 'Rebranded' Windows Mobile:
  - Up to v6.x: Windows Mobile
  - V7.x+: Windows Phone
- ARM hardware architecture (similar to iOS, Blackberry OS and Android)
- Windows Phone Runtime application architecture (not identical to WinRT)
- Windows Phone 7: Windows CE kernel
- Windows Phone 8: Windows NT kernel

# Windows Phone 7



- Windows CE kernel based
- First mobile MS OS with 'Metro' interface
- No device encryption
- Only Microsoft and Marketplace apps have digital signatures
- Apps require either a Silverlight or XNA runtime; Susceptible to reverse-engineering and manipulation
- Marketspace for Homebrew: DevStore8

# Windows Phone 8



- NT Kernel based
  - NTFS support
  - Device encryption (BitLocker)
  - Sandboxed apps
  - SafeBoot: Secure EUFI Boot (Unified Extensible Firmware Interface). UEFI = Successor to the legacy BIOS firmware interface
    - Makes it difficult for software without correct digital signature to be loaded on your Windows Phone
    - TPM 2.0 standard, requires unique keys to be burned into the chip during production
  - All Windows Phone 8 binaries must have digital signatures by Microsoft to run

# Windows Phone: Application Penetration Testing

# Prerequisites

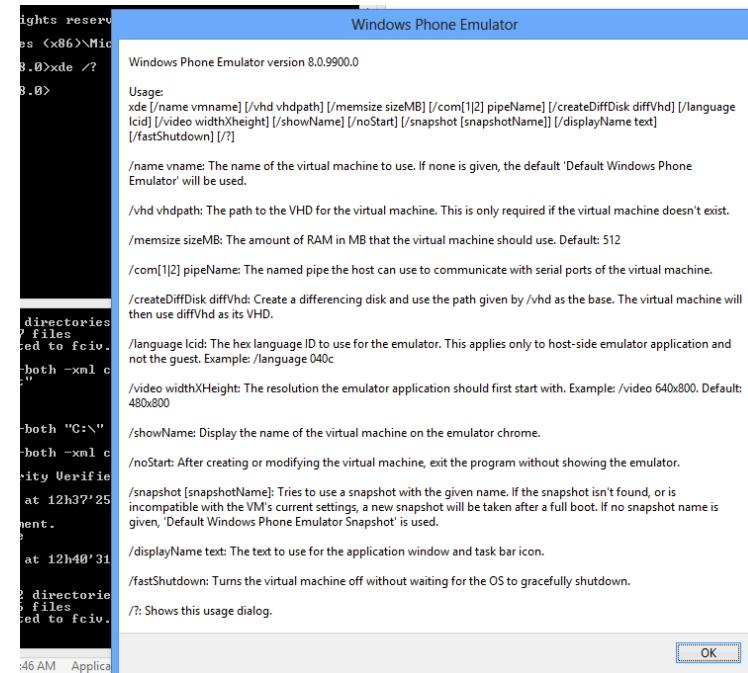
- When using a physical phone: unlocked phone is required
- Application logic and server side can be tested with an intercepting proxy (e.g. Burp) without unlocked phone, but local storage and local application configuration settings cannot.
- Unlocking phone:
  - Using a developer account and developer unlock: 99\$/year. Developer can install up to 10 sideloaded applications
  - Students: can install up to 3 sideloaded apps
  - Register a company trusted certificate for enterprise app stores: \$399 / year

# Prerequisites

- Windows Phone SDK install:  
<http://dev.windowsphone.com/>
- Emulator is installed as part of SDK. Emulator is installed at the following location:

C:\program files (x86)\  
Microsoft XDE\8.0\XDE.exe

- Visual Studio Express 2012 (free) or Visual Studio 2012



# Prerequisites

- Windows Phone Power Tools - <http://wptools.codeplex.com/>
- ILSpy - <http://ilspy.net/>
- Tangerine - <https://github.com/andreycha/tangerine>

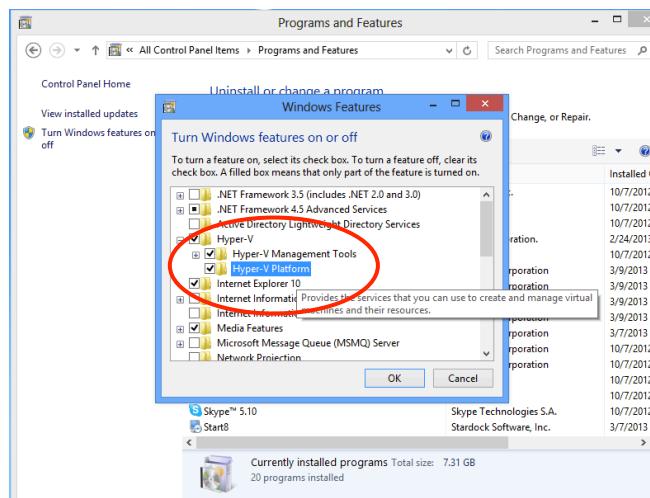
Commercial alternatives:

- XAML Spy - <http://xamlspy.com/>
- .NET Reflector - <http://www.reflector.net/>

# Prerequisites

- Windows Phone 8 emulators are Hyper-V virtual machines having their own IP address.
- When using an emulator for testing, system with ore i3, i5 or i7 or equivalent AMD processor supporting newer hardware virtualization features is required.

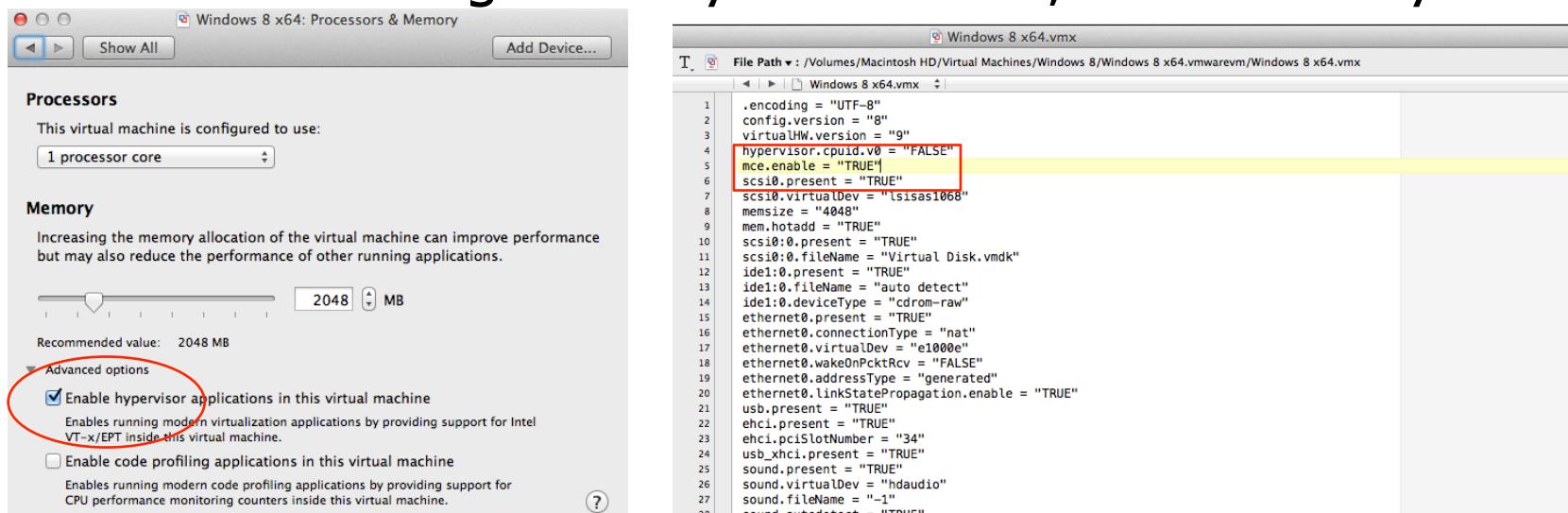
Check that Hyper-V is enabled in Windows:



# Prerequisites

When using vmware:

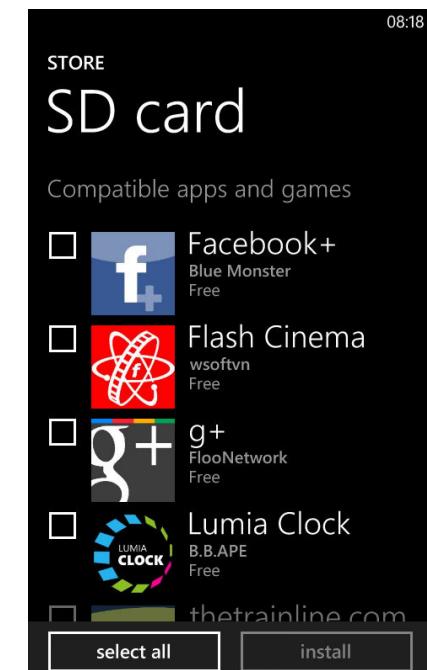
- enable the VT-x/EPT hypervisor option
- Add the following line to your vmx file, if not already there



Also make sure your hypervisor settings in your BIOS are enabled.

# Sideload apps

- Sideload: installing applications on your device without using the official Marketplace directly
- Windows Phone 8 only allows apps downloaded through the Windows Phone Store by default
- XAP applications can be download from the store or provided by the developer and sideloaded via MicroSD storage card
- Limitation:
  - Only apps signed with trusted certificates will run (on unlocked phones)
  - Phone will validate that the app on the storage card is the latest release



# Windows Phone: XAP files

- ZIP file formatted packages (similar to Android APK)
  - AppManifest.xaml file: defines the assemblies that get deployed in the client application. Updated when compiling your application
  - DLLs required
- MIME type: application/x-silverlight-app

Name	Type	Compressed size
AppManifest	Windows Markup File	1 KB
SilverlightApplication2.dll	Application Extension	4 KB
System.Windows.Controls	XML Document	25 KB
System.Windows.Controls.dll	Application Extension	71 KB
System.Windows.Controls.Extended	XML Document	11 KB
System.Windows.Controls.Extended.dll	Application Extension	56 KB

# Windows Phone: XAP files

- XAP Files from app store: PlayReady DRM encrypted

PlayReady DRM header:

```
<WRMHEADER xmlns="http://schemas.microsoft.com/DRM/2007/03/PlayReadyHeader"
version="4.0.0.0">

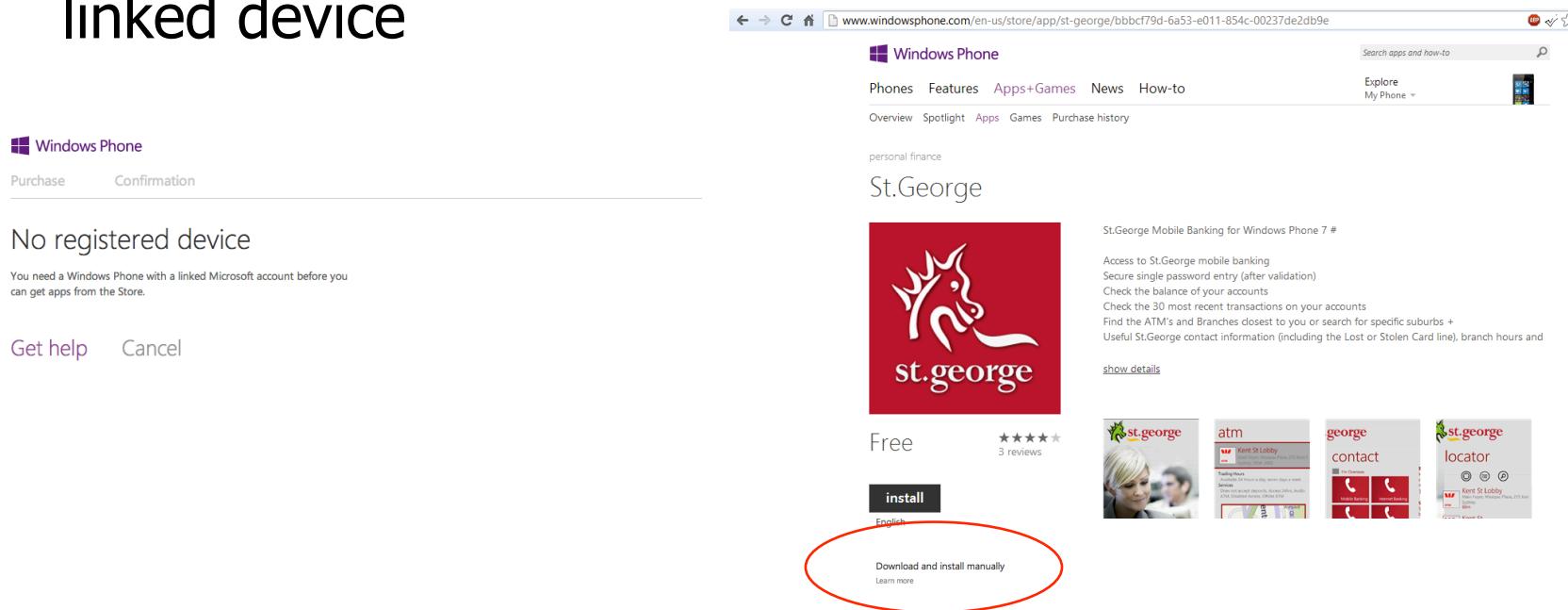
<DATA><PROTECTINFO><KEYLEN>16</KEYLEN><ALGID>AESCTR</ALGID></
PROTECTINFO><KID>w3i0edJP7EOqQ6aQzdAoSQ==</KID><LA_URL>http://microsoft.com/</
LA_URL><CUSTOMATTRIBUTES xmlns=" "><S>9FcV5qmfIsMc+X2MVmX3Hw==</S><KGV>0</
KGV></CUSTOMATTRIBUTES><CHECKSUM>Hu3+fizBvKU=</CHECKSUM></DATA>
```

</WRMHEADER>

- DRM is added by the marketplace in real time, based on the LiveID cookie value
- Encrypted XAP files do not run in emulator!

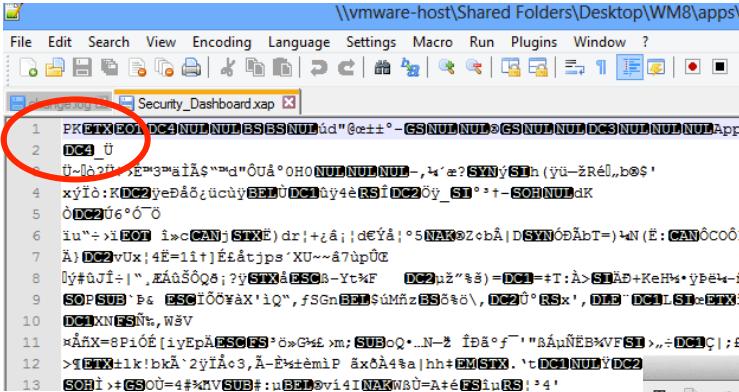
# Windows Phone: XAP files

- XAP application binaries can be downloaded from Windows Phone Store from a computer
- Windows Live account required with Windows Mobile linked device



# Windows Phone: XAP files

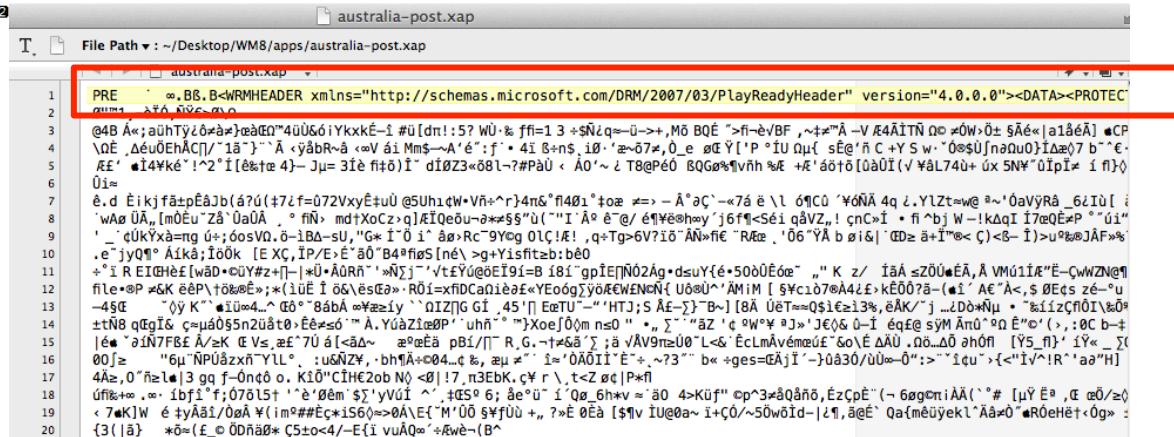
- How to recognise difference?



```
\\vmware-host\Shared Folders\Desktop\WM8\apps\Security_Dashboard.xap
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
Security_Dashboard.xap [3]
1 PKETXEO DC4 NUL NUL E8BSNULúd"@@@! - GS NUL NUL @ GS NUL NUL DC3 NUL NUL NUL App
2 DC4 _Ü
3 Ü~@2ft>E=3@áíš"m@"ÔU@ÓHO NUL NUL NUL - ,@?SYN@Gh (jü-žR@,b@S
4 xýf@:KDC2y@áé@úcúyB@U@DC1uy@e@RS@DC2@öy_@S@, + -S@N@U@dK
5 öDC2Ú6°ö
6 iu"=x@OT i@cCANj@STX@ dr;+@a;@d@Y@!@5NAK@Z@b@|@SYN@D@B@=)@N (E:CAN@CO@i
7 A) DC2@v@X@;4@=1@t]@é@t@ps@XU@~@7@p@U@C
8 D@#üJ@!|@,E@S@ö@;?@STX@ES@-Yt@F DC2@u@%@=DC1@=+T:@>SI@P+KeH@+j@p@e@-h
9 S@P@S@B@ E@S@j@ö@W@x@i@Q@,f@G@B@S@M@z@B@ö@,DC2@j@RS@ , D@B@ DC1@S@-E@T@X@i
10 DC1@X@N@S@N@,W@V
11 x@R@x@=8@P@Ó@i@y@P@E@S@F@G@P@f@m@;S@B@Q@..N@-@ I@D@f@-@ "B@U@N@B@V@F@S@>..@DC1@C@;E
12 >@T@X@+l@k@b@k@.2@y@A@3@,A-@E@t@em@P@ a@x@A@4@a@h@+E@T@X@.t@DC1@N@U@Y@DC2@C@;E
13 S@H@, +@S@O@U@+@#4@M@V@S@B@:u@E@P@v@i@N@K@W@U@A@+@E@F@i@U@RS@, +@4@
```

Not encrypted: PK (ZIP) header

Encrypted: PlayDRM header

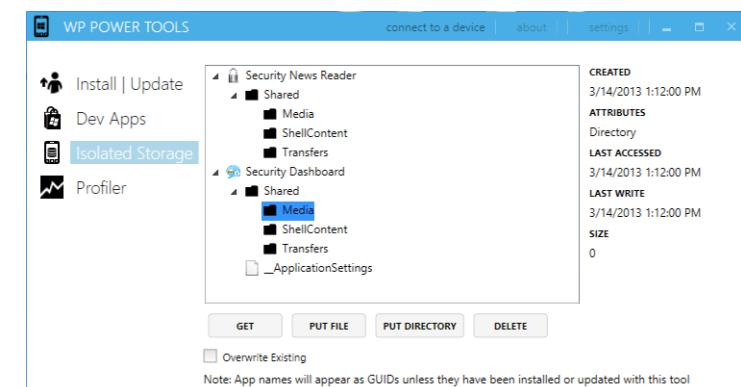
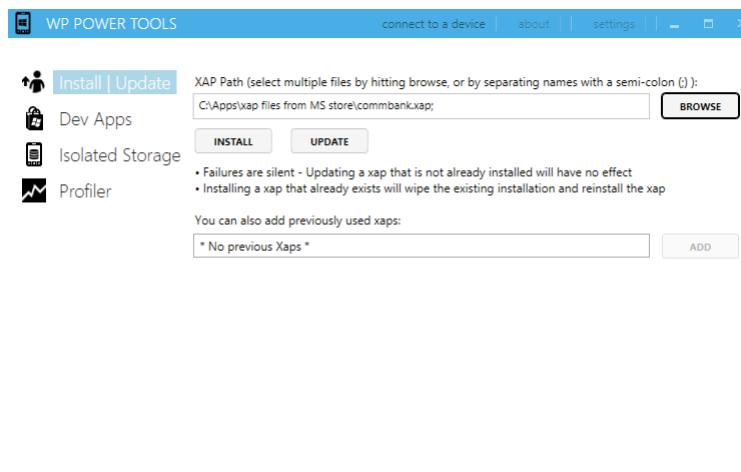


```
australia-post.xap
File Path: ~/Desktop/WM8/apps/australia-post.xap
PRE @ B8 B<DRMH@DRMHEADER xmlns="http://schemas.microsoft.com/DRM/2007/03/PlayReadyHeader" version="4.0.0.0"><DATA><PROTEC
1 @#4B Á@;au@T@z@p@a@;@é@Q@4@U@Ó@Y@K@K@-@ #@U@dn@!5@? W@·@f@=1@ 3@+S@N@q@-@->@,M@ B@Q@>@f@-@v@B@F@, @#z@-@V@R@A@T@N@Q@ @@W@·@S@A@<@a@l@é@Á@>@C@P@A@E@_@á@U@, @d@e@ñ@A@C@/@l@á@>@ Á@<@y@b@r@-@<@V@á@M@n@-@A@'@é@;f@·@4@i@-@n@, i@·@-@-@7@x@, @_@e@Y@!@P@>@U@n@{s@é@'@n@C@+@S@w@·@0@s@U@n@o@U@}>@a@7@b@-@€@·@F@·@!@4@K@!@2@f@{@t@t@4@-@J@u@=3@i@f@o@!@í@ d@i@Z@3@-@8@l@-@#@P@u@<@A@~@t@8@P@e@0@ B@Q@G@P@v@h@ %@E@+@á@t@o@[@ú@U@(@v@l@7@4@u@ ú@x@N@Y@í@p@í@x@í@ f@}>@U@í@
```

# Windows Phone Power Tools

Great tool that can be used to:

- Deploy XAP files
- Inspect device storage on a physical device or on an emulator

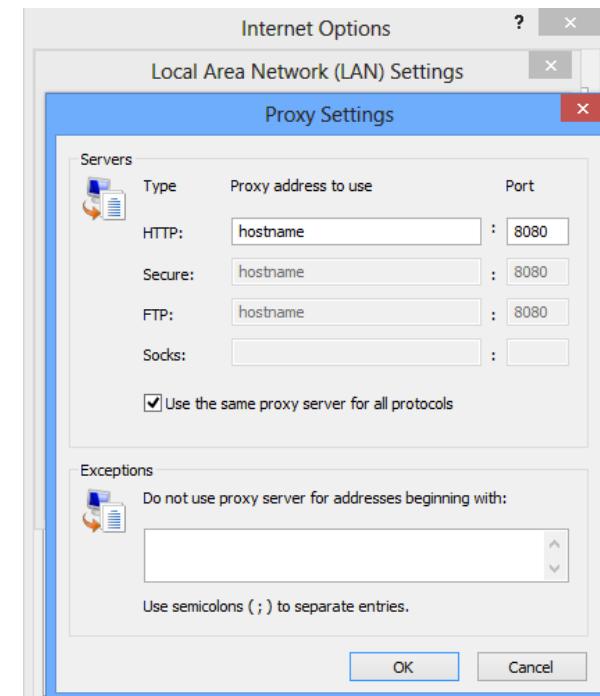


# Setting up your proxy server

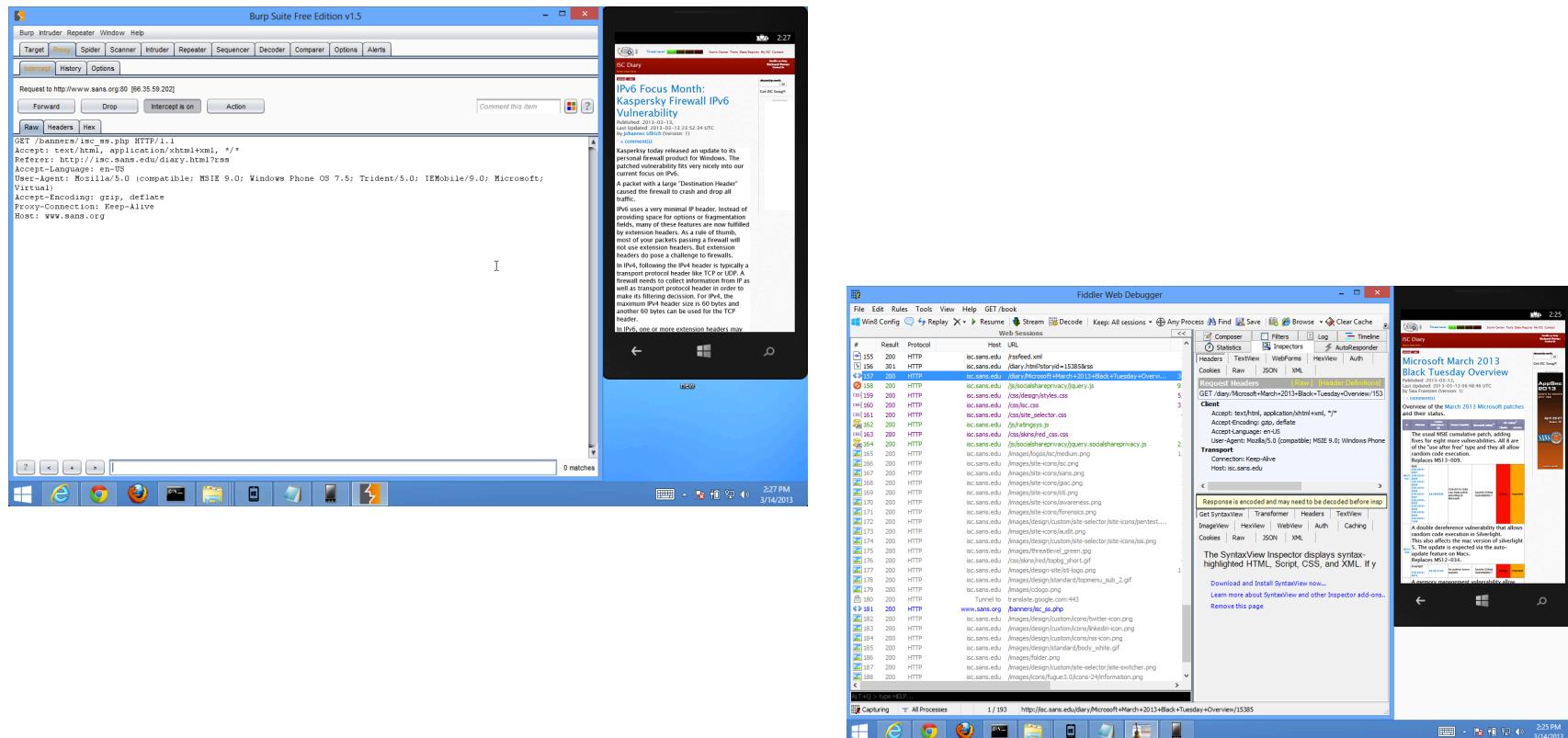
- Windows Phone 8 emulators are Hyper-V virtual machines having their own IP address.
- Network traffic needs to route from the Hyper-V virtual machines through the Hyper-V host (i.e. our test machine)
- As a result, we need to:
  - Make sure your proxy software is configured to **not** only listen on the local interface
  - Configure your IE proxy settings to proxy through your **HOSTNAME**, not 127.0.0.1 or LOCALHOST!

# Setting up your proxy server

- Change the proxy settings in Internet Explorer to your system HOSTNAME
- Restart your emulator (Each time you change your proxy settings you will need to restart the emulator)



# Demo



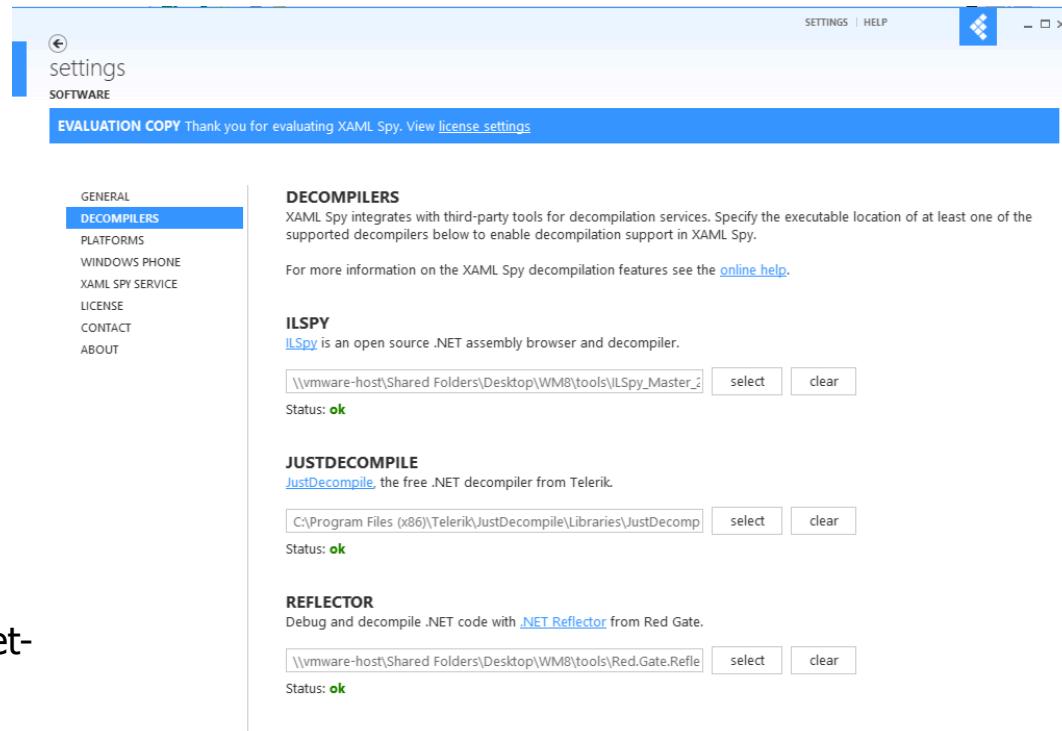
# Decompiling applications: XAML Spy

XAML Spy (\$79, free trial). Prerequisites are 1 of the following:

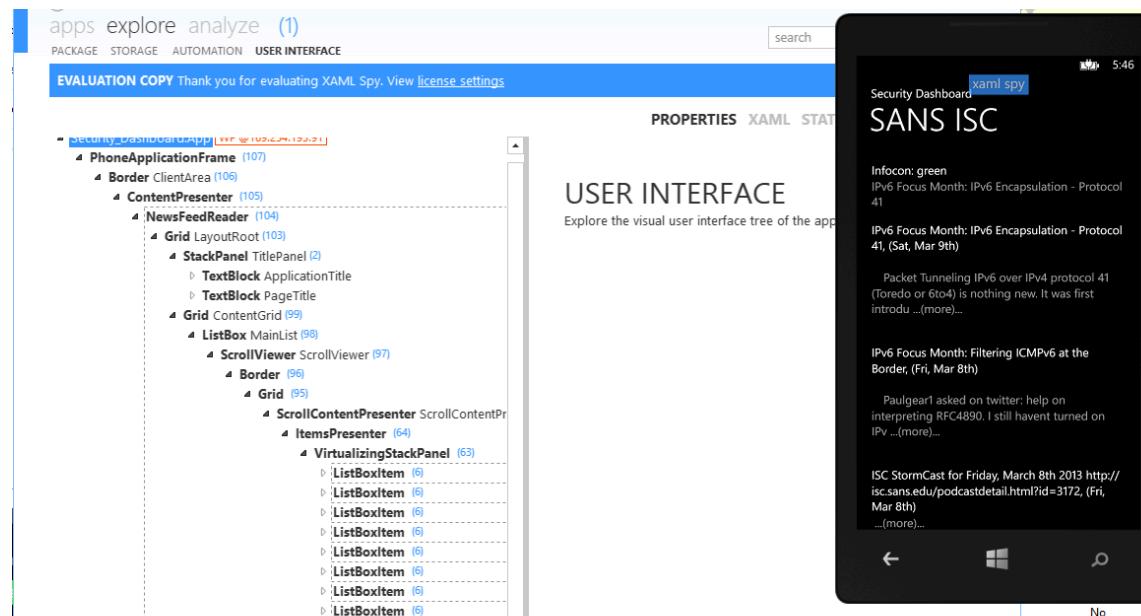
- ILSPY
- JustDecompile
- Reflector

- ILSPY (free): <http://ilspy.net/>
- JustDecompile (free):  
<http://www.telerik.com/products/decompiler.aspx>
- Reflector (\$95, free trial)  
<http://www.red-gate.com/products/dotnet-development/reflector/>

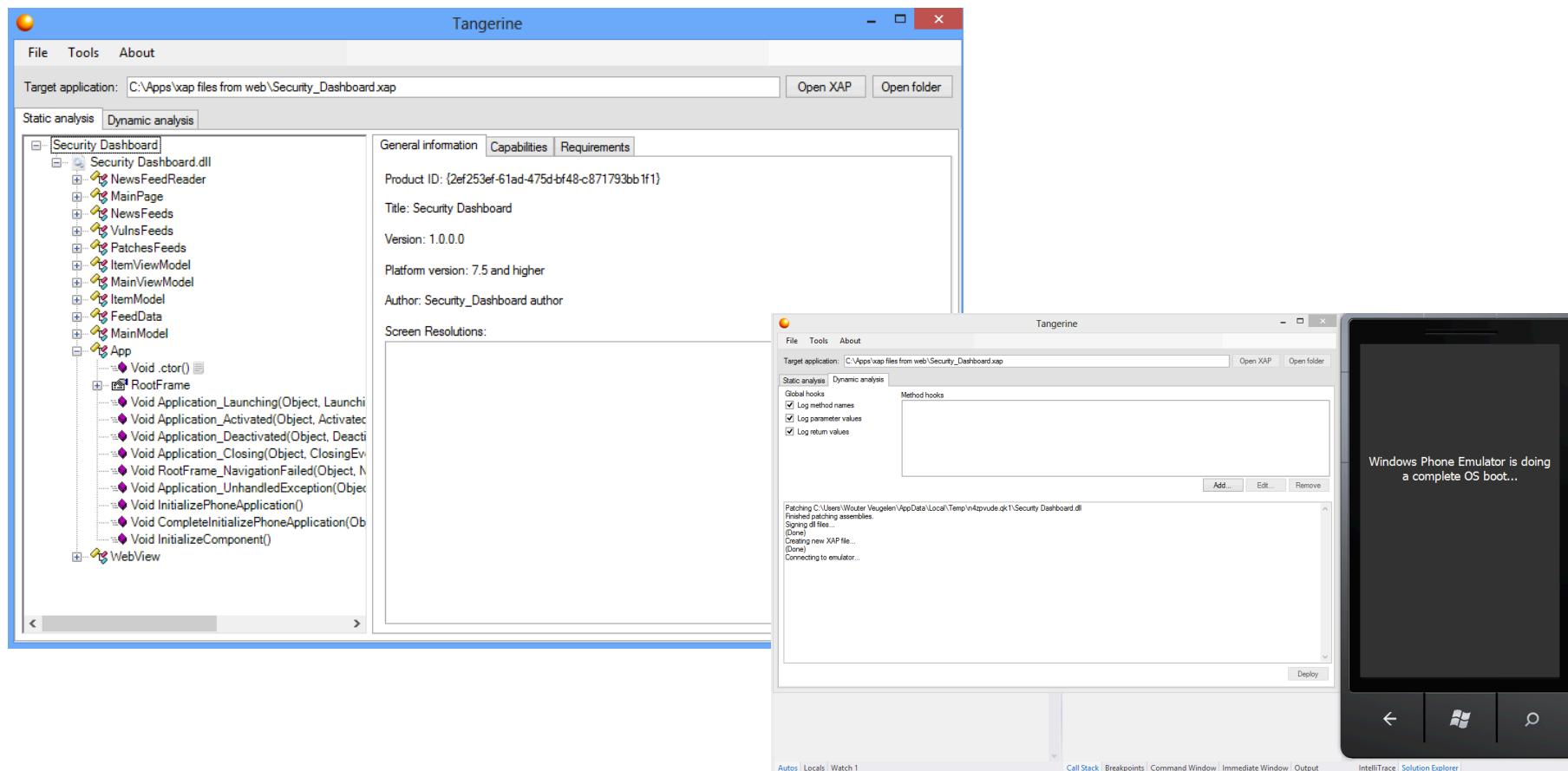


# Decompile XAP files: XAML Spy (Commercial)



Limitations: only works for non DRM protected XAP files (i.e. apps **not** from Microsoft store)

# Decompile XAP files: Tangerine (Free)



# Windows Phone: Mobile Device Security Testing



# Windows Phone 8



www.wpcentral.com/microsoft-beefing-security-windows-phone-8

Windows Phone Central

Forums News Reviews Help & How To Devices Apps Games Contests Developers Editorials Search...

SHOP ONLINE | Cases Chargers Batteries Bluetooth & More New accessories FREE SHIPPING on orders over \$50

## Microsoft's beefing up security with Windows Phone 8 may make custom ROMs a thing of the past

By George Ponder, Monday, Sep 3, 2012 at 7:43 pm

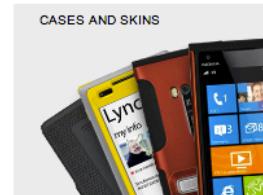
**NEWS** **FEATURED** **DEVELOPERS**



**Tip Us On News!**

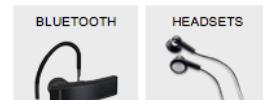
**SHOP ACCESSORIES**

BROWSE ALL ACCESSORIES

**CASES AND SKINS** 

**CHARGERS** 

**CRADLES** 

**BLUETOOTH** 

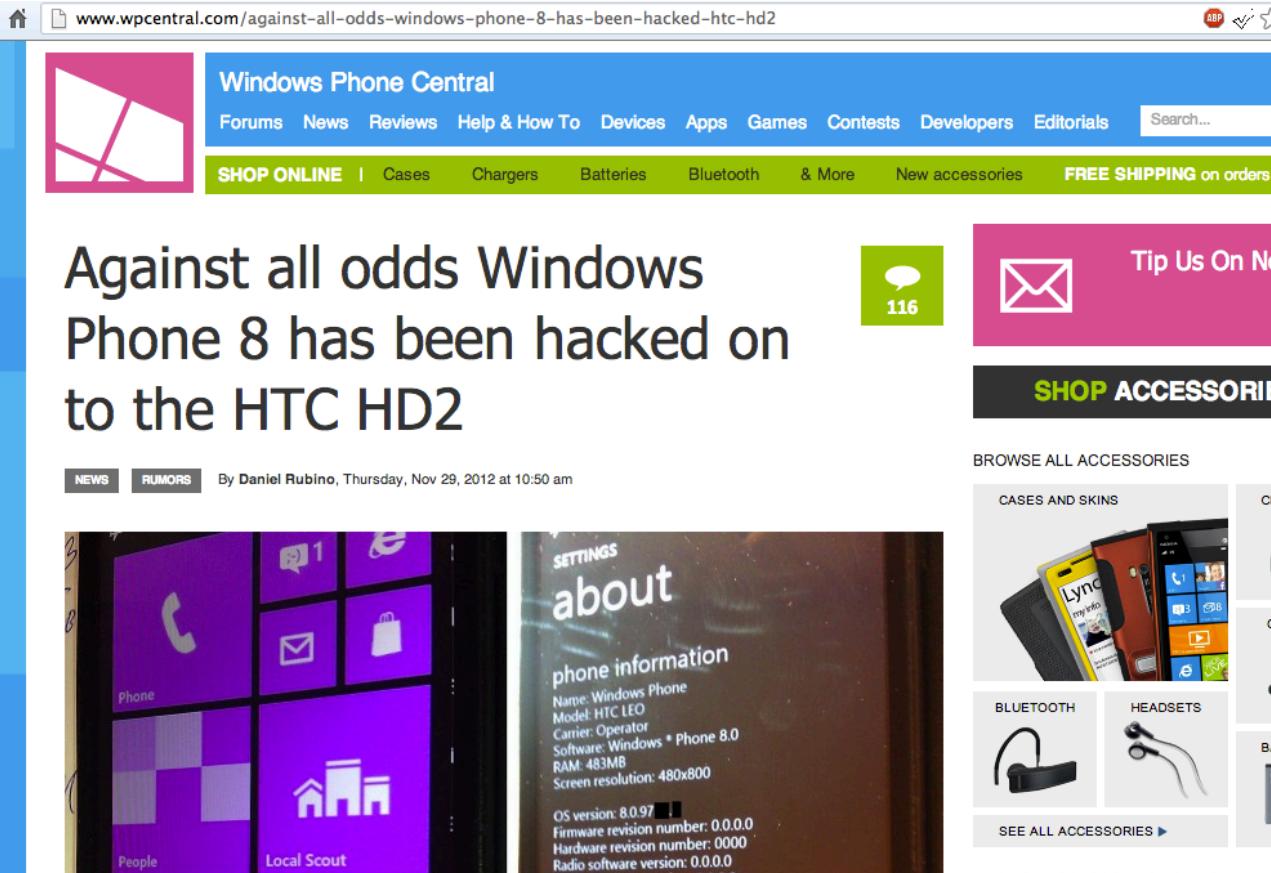
**HEADSETS** 

**BATTERIES** 

SEE ALL ACCESSORIES ►

BROWSE ACCESSORIES FOR YOUR PHONE

# Windows Phone 8



The screenshot shows a news article on the Windows Phone Central website. The title is "Against all odds Windows Phone 8 has been hacked on to the HTC HD2". The article is categorized as "NEWS" and "RUMORS". It was written by Daniel Rubino on Thursday, Nov 29, 2012 at 10:50 am. The article includes two images: one showing the Windows Phone 8 home screen and another showing the "about" screen with device details. The website has a blue header with the logo and navigation links: Forums, News, Reviews, Help & How To, Devices, Apps, Games, Contests, Developers, Editorials, and a search bar. A green banner at the top of the main content area says "SHOP ONLINE" and lists categories: Cases, Chargers, Batteries, Bluetooth, & More, New accessories, and "FREE SHIPPING on orders over \$50". On the right side, there are social media links for "Tip Us On Next" (116 messages) and "SHOP ACCESSORIES". Below that is a "BROWSE ALL ACCESSORIES" section with categories: CASES AND SKINS, BLUETOOTH, HEADSETS, and a "SEE ALL ACCESSORIES" button. There is also a "BROWSE ACCESSORIES FOR YOUR PHONE" section.

# Jailbreaking

- Windows Phone 8 is a closed operating system.
- During a mobile device security test we need to conduct activities such as inspecting the file system, data storage, memory, and transfer files which is all prevented out of the box.
- It is possible to test the application with a web application proxy without jailbreaking

# Jailbreaking methods?

- Escalate privileges:
  - Drive by Download IE 10 exploit
  - Exploit trusted OEM app on phone
- Enable support for running untrusted code
  - SecureBoot bypass: Secure the boot process prevents the loading of drivers or OS loaders that are not signed with an acceptable digital signature
  - Disable application code signing
  - Add private Enterprise App Store certificate
- ...

# Drive by Download

- pwn2own March 2012
  - Internet Explorer 10: owned
  - Windows RT + IE10: owned

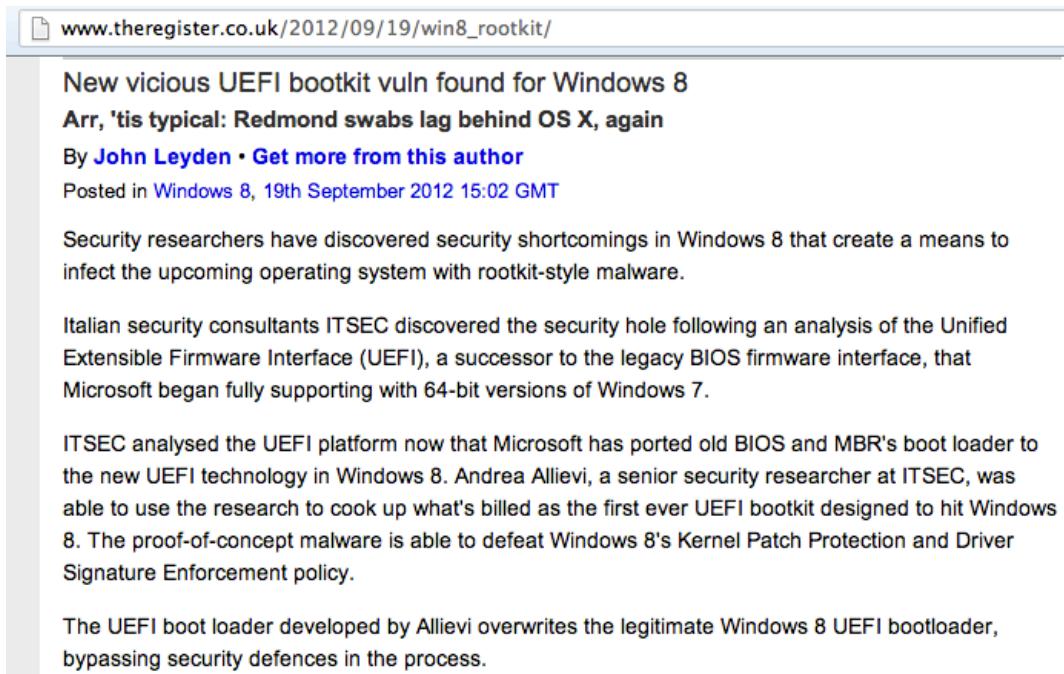


Windows Phone 8  
uses....

IE10!

# SecureBoot bypass: Windows 8

Successful attack on Windows 8 (September 2012)



The screenshot shows a news article from The Register. The URL in the address bar is [www.theregister.co.uk/2012/09/19/win8\\_rootkit/](http://www.theregister.co.uk/2012/09/19/win8_rootkit/). The article title is "New vicious UEFI bootkit vuln found for Windows 8". It includes the subtitle "Arr, 'tis typical: Redmond swabs lag behind OS X, again", author information "By John Leyden • Get more from this author", and a timestamp "Posted in Windows 8, 19th September 2012 15:02 GMT". The main content discusses a security hole in the UEFI platform discovered by ITSEC, which Microsoft began supporting in Windows 7. It details how the malware overwrites the Windows 8 UEFI bootloader to bypass security defenses.

New vicious UEFI bootkit vuln found for Windows 8

Arr, 'tis typical: Redmond swabs lag behind OS X, again

By John Leyden • Get more from this author

Posted in Windows 8, 19th September 2012 15:02 GMT

Security researchers have discovered security shortcomings in Windows 8 that create a means to infect the upcoming operating system with rootkit-style malware.

Italian security consultants ITSEC discovered the security hole following an analysis of the Unified Extensible Firmware Interface (UEFI), a successor to the legacy BIOS firmware interface, that Microsoft began fully supporting with 64-bit versions of Windows 7.

ITSEC analysed the UEFI platform now that Microsoft has ported old BIOS and MBR's boot loader to the new UEFI technology in Windows 8. Andrea Allievi, a senior security researcher at ITSEC, was able to use the research to cook up what's billed as the first ever UEFI bootkit designed to hit Windows 8. The proof-of-concept malware is able to defeat Windows 8's Kernel Patch Protection and Driver Signature Enforcement policy.

The UEFI boot loader developed by Allievi overwrites the legitimate Windows 8 UEFI bootloader, bypassing security defences in the process.

<http://www.saferbytes.it/2012/09/18/uefi-technology-say-hello-to-the-windows-8-bootkit/>

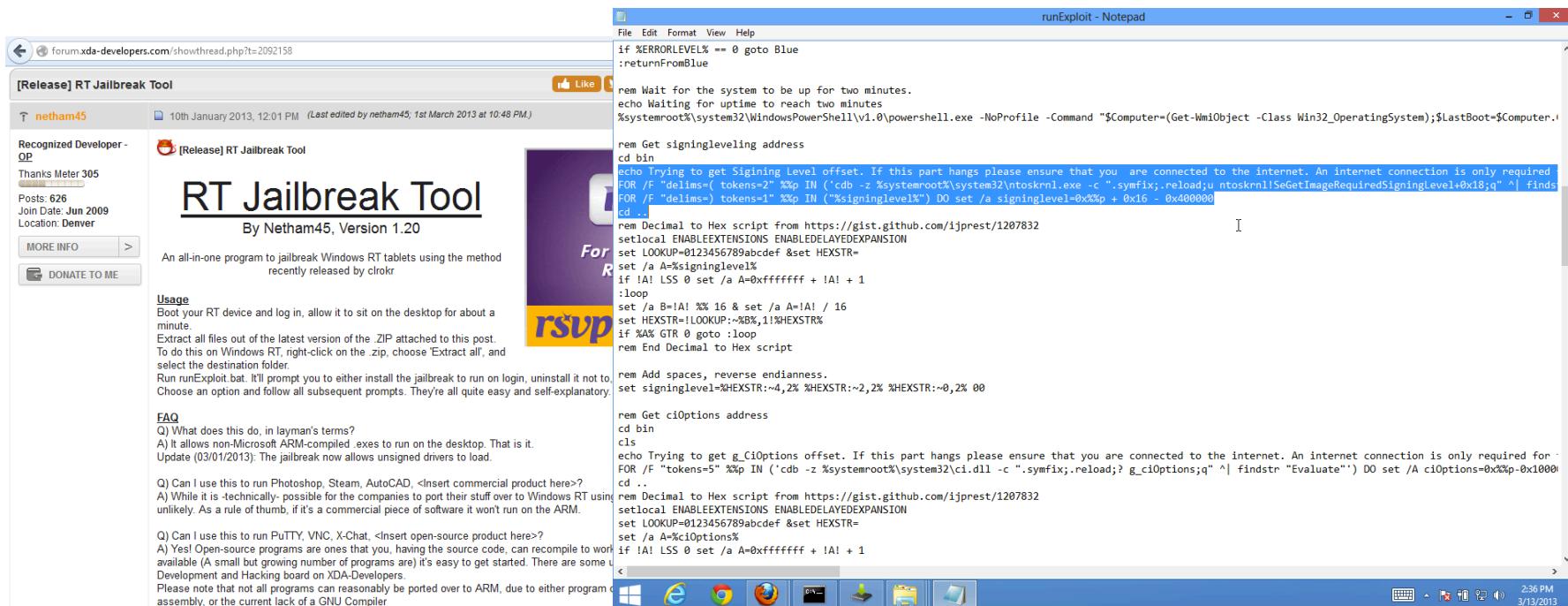
# Disable application code signing

- Vulnerability in the Windows kernel that has existed for a long time — since before Microsoft ported Windows from x86 to ARM
- Windows kernel on your computer is configured to only execute files that meet a certain level of authentication:
  - Unsigned (0), Authenticode (4), Microsoft (8), and Windows (12).
- Windows 8: default value is Unsigned
- Windows RT: default, hard-coded setting is Microsoft (8); i.e. only apps signed by Microsoft, or parts of Windows itself, can be executed.”

# Disable application code signing: Windows RT

... and successfully replicated on Windows RT

- Proof of concept: January 2013
- Jailbreak script released: February 2013



The image shows a screenshot of a forum post on XDA Developers and a Notepad window on Windows RT.

**Forum Post (Left):**

- Post by **netham45** on 10th January 2013, 12:01 PM (Last edited by netham45, 1st March 2013 at 10:48 PM).
- Subject: [Release] RT Jailbreak Tool
- Developer: netham45 (OP)
- Thanks Meter: 305
- Posts: 626
- Join Date: Jun 2009
- Location: Denver
- More Info
- Donate to Me

**Post Content:**

**RT Jailbreak Tool**  
By Netham45, Version 1.20

An all-in-one program to jailbreak Windows RT tablets using the method recently released by cirok

**Usage:**  
Boot your RT device and log in, allow it to sit on the desktop for about a minute.  
Extract all files out of the latest version of the ZIP attached to this post. To do this on Windows RT, right-click on the .zip, choose 'Extract all', and select the destination folder.  
Run runExploit.bat! It'll prompt you to either install the jailbreak to run on login, uninstall it not to, Choose an option and follow all subsequent prompts. They're all quite easy and self-explanatory.

**FAQ:**

Q) What does this do, in layman's terms?  
A) It allows non-Microsoft ARM-compiled .exes to run on the desktop. That is it.  
Update (03/01/2013): The jailbreak now allows unsigned drivers to load.

Q) Can I use this to run Photoshop, Steam, AutoCAD, <Insert commercial product here>?  
A) While it is technically possible for the companies to port their stuff over to Windows RT using unlikely. As a rule of thumb, if it's a commercial piece of software it won't run on the ARM.

Q) Can I use this to run PuTTY, VNC, X-Chat, <Insert open-source product here>?  
A) Yes! Open-source programs are ones that you, having the source code, can recompile to work available (A small but growing number of programs are) it's easy to get started. There are some Development and Hacking board on XDA-Developers.  
Please note that not all programs can reasonably be ported over to ARM, due to either program assembly, or the current lack of a GNU Compiler

**Notepad Window (Right):**

File Edit Format View Help runExploit - Notepad

```
if %ERRORLEVEL% == 0 goto Blue
:returnFromBlue

rem Wait for the system to be up for two minutes.
echo Waiting for uptime to reach two minutes
%systemroot%\system32\WindowsPowerShell\v1.0\powershell.exe -NoProfile -Command "$Computer=(Get-WmiObject -Class Win32_OperatingSystem);$LastBoot=$Computer.I

rem Get signingleveling address
cd bin
echo Trying to get SigningLevel offset. If this part hangs please ensure that you are connected to the internet. An internet connection is only required
FOR /F "tokens=2" %%p IN ('cd\ -z %systemroot%\system32\ntoskrnl.exe -c ".symfix";.reload;u ntoskrnl!SeGetImageRequiredSigningLevel+0x18;q" ^| finds
FOR /F "tokens=1" %%p IN ("%signinglevel%") DO set /a signingLevel=0x%%p + 0x16 - 0x400000
cd ..

rem Decimal to Hex script from https://gist.github.com/ijprest/1207832
setlocal ENABLEEXTENSIONS ENABLEDELAYEDEXPANSION
set LOOKUP=0123456789abcdef &set HEXSTR=
set /A=signinglevel%
if !A! LSS 0 set /a A=0xffffffff + !A! + 1
:loop
set /B=!A! % 16 & set /a A=!A! / 16
set HEXSTR=!LOOKUP:~%A%,1%HEXSTR%
if %%A%% GTR 0 goto :loop
rem End Decimal to Hex script

rem Add spaces, reverse endianness.
set signinglevel=%HEXSTR:~4,2% %HEXSTR:~2,2% %HEXSTR:~0,2% 00

rem Get ciOptions address
cd bin
cls
echo Trying to get g_ciOptions offset. If this part hangs please ensure that you are connected to the internet. An internet connection is only required for
FOR /F "tokens=5" %%p IN ('cd\ -z %systemroot%\system32\ci.dll -c ".symfix;.reload;? g_ciOptions;q" ^| findstr "Evaluate"') DO set /A ciOptions=0x%%p-0x1000
cd ..
rem Decimal to Hex script from https://gist.github.com/ijprest/1207832
setlocal ENABLEEXTENSIONS ENABLEDELAYEDEXPANSION
set LOOKUP=0123456789abcdef &set HEXSTR=
set /A=ciOptions%
if !A! LSS 0 set /a A=0xffffffff + !A! + 1
```

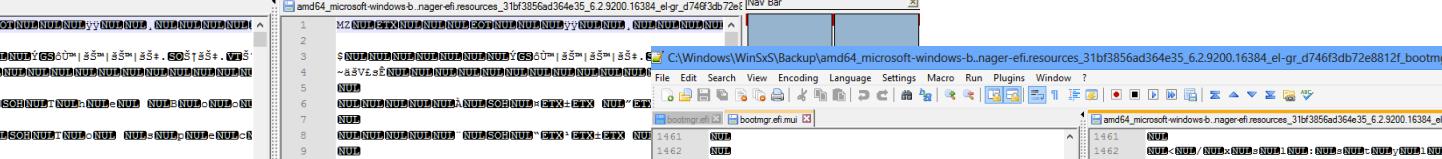
2:36 PM 3/13/2013

# SecureBoot bypass: Windows Phone

- How about replicating the Windows RT jailbreak on Windows Phone?
- This has not been done yet

# SecureBoot bypass: Windows Phone

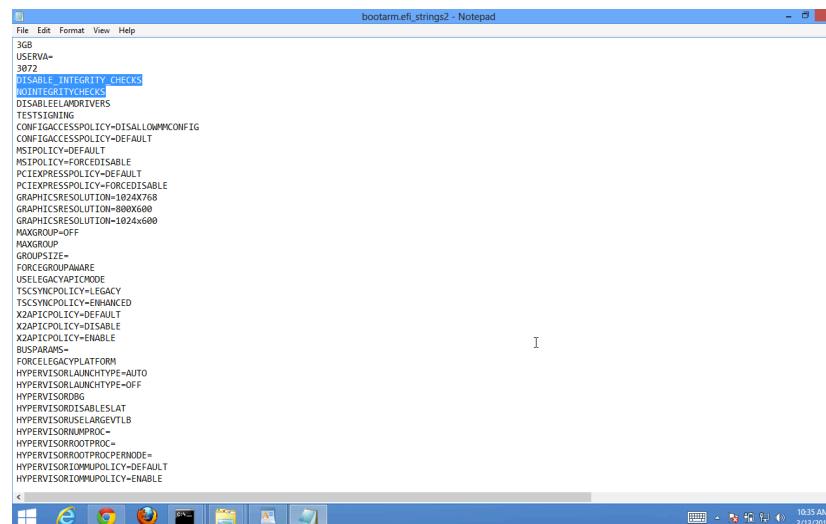
- Quick analysis performed: bootloaders look very, very similar (Windows 8 vs. Windows Phone 8)



The image shows a multi-pane hex editor interface with several windows open, each displaying a portion of the `bootmgr.efi.mui` file. The panes show the raw hex data and its corresponding ASCII representation. Various sections of the file are highlighted in different colors (e.g., green, yellow, red) to indicate different components or sections of the firmware. The interface includes standard file operations like 'File', 'Edit', 'Search', and 'Run'.

# SecureBoot bypass: Windows Phone

- Looking at the Windows Phone 8 bootloader with strings.exe, the same configuration parameters that were exploited in the WinRT jailbreak can be found



The screenshot shows a Windows Phone 8 Notepad window with the title "bootarm.efi\_strings2 - Notepad". The content of the window is a list of configuration parameters, many of which are preceded by a question mark, indicating they are optional or dynamically generated. The parameters include:

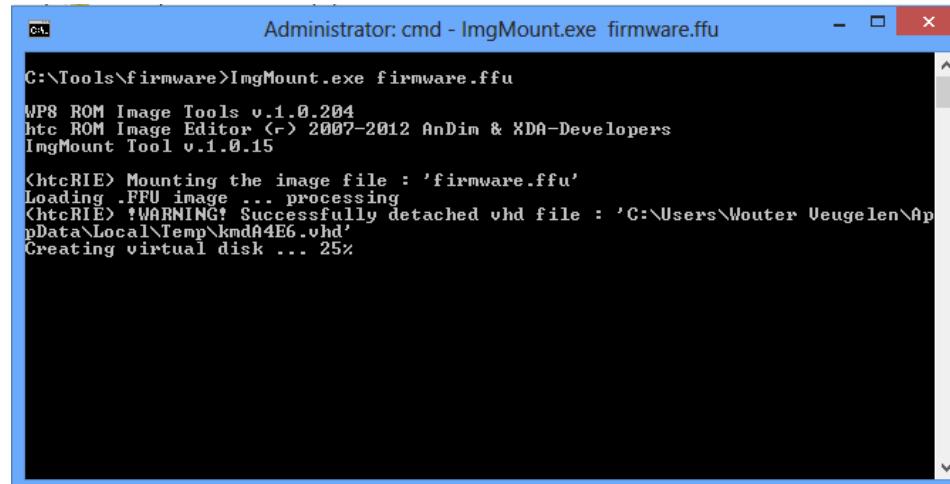
- ?DISABLE\_INTEGRITY\_CHECKS
- ?!INTEGRITYCHECKS
- ?DISABLEELAMDDRIVERS
- ?TESTSIGNER
- ?COMPILEXPRESSPOLICY=>DISALLOWMMCONFIG
- ?CONFIGACCESSPOLICY=>DEFAULT
- ?MSIPOLICY=>DEFAULT
- ?MSIPOLICY=FORCEDISABLE
- ?PCIEEXPRESSPOLICY=>DEFAULT
- ?PCIEEXPRESSPOLICY=FORCEDISABLE
- ?GRAPHICRESOLUTION=1024x768
- ?GRAPHICRESOLUTION=800x600
- ?GRAPHICRESOLUTION=1024x600
- ?MAXGROUP=OFF
- ?MAXGROUP
- ?GROUPSIZE=
- ?FORCELEGACYPAWME
- ?USELEGACYAPTEKME
- ?TSCSYNCPOLICY=LEGACY
- ?TSCSYNCPOLICY=>ENHANCED
- ?X2APICPOLICY=>DEFAULT
- ?X2APICPOLICY=DISABLE
- ?X2APICPOLICY=>ENABLE
- ?BUSPOWER
- ?FORCELEGACYPLATFORM
- ?HYPERVISORLAUNCHTYPE=AUTO
- ?HYPERVISORLAUNCHTYPE=OFF
- ?HYPERVISORDB
- ?HYPERVISORLATENCY=LEGLAT
- ?HYPERVISORLARGEVTLB
- ?HYPERVISORNUMPROCS=
- ?HYPERVISORROOTPROC=>
- ?HYPERVISORROOTPROC=PERNODE=
- ?HYPERVISORIOMMU\_POLICY=>DEFAULT
- ?HYPERVISORIOMMU\_POLICY=ENABLE

# File system analysis

- No file system access without jailbreak :(
- How can we gain an understanding of the Windows Phone 8 file system architecture and configuration?
  - Analyse Windows Phone 8 firmware files

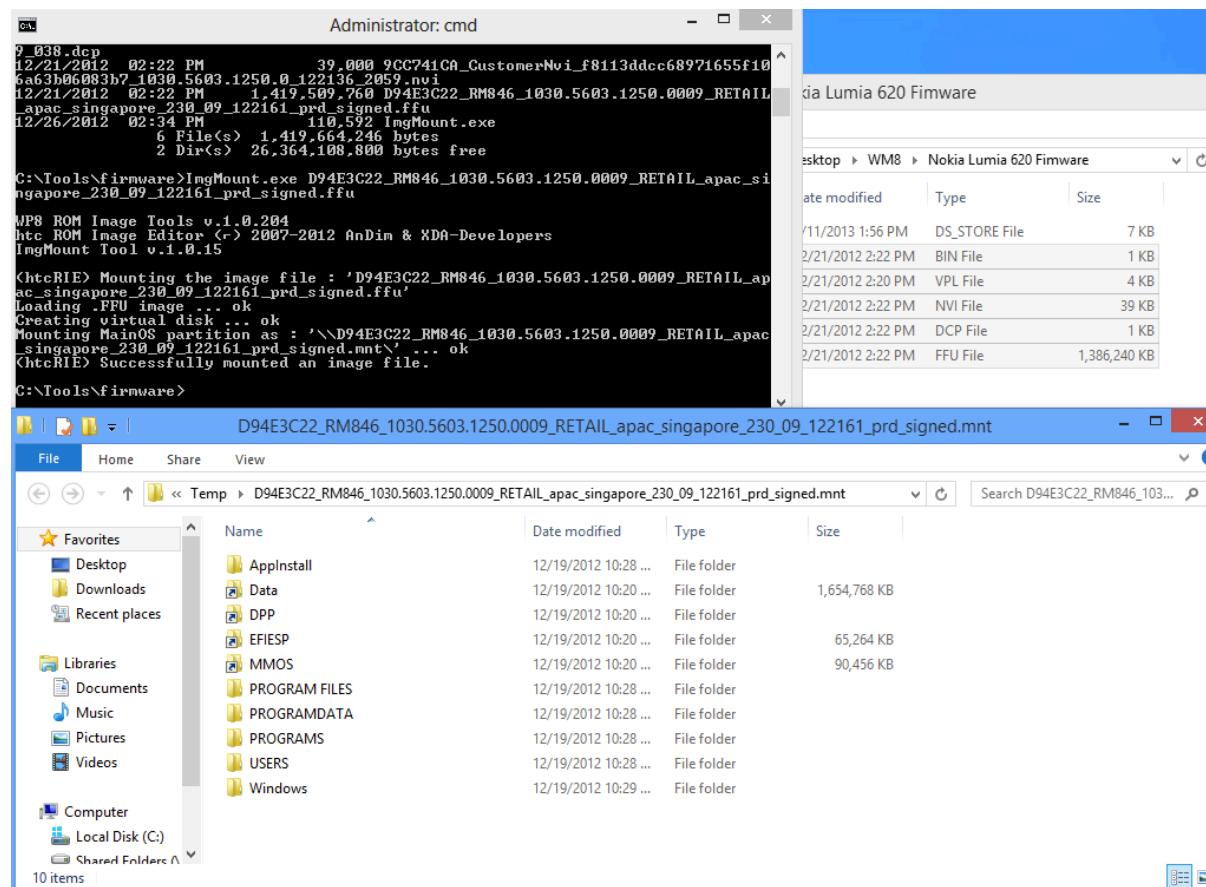
# File system analysis

- Windows Phone is a closed OS: It is not possible to browse the file system on a Windows Phone device.



- Software required: ImgMount.exe  
<http://forum.xda-developers.com/showthread.php?p=36014289>

# File system analysis



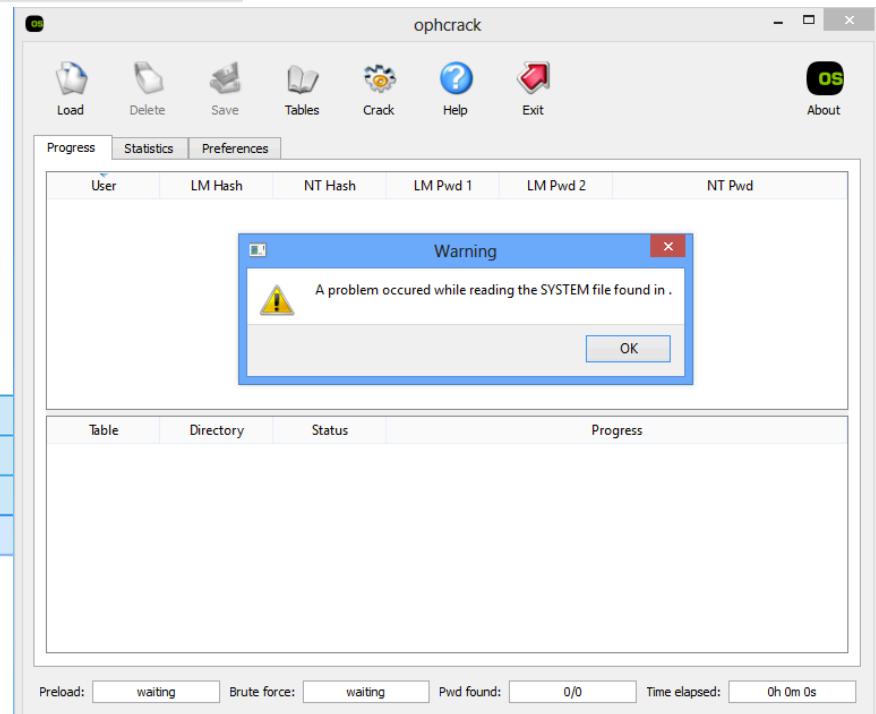
# SAM files

## SAM files

er Veugelen > AppData > Local > Temp > firmware.mnt > Windows > System32 > config

Name	Date modified	Type
MOUNTMGR	12/19/2012 10:30 ...	File folder
REGBACK	12/19/2012 10:28 ...	File folder
SYSTEMPROFILE	12/19/2012 10:28 ...	File folder
unmodified	12/19/2012 10:27 ...	File folder
DEFAULT	12/19/2012 10:28 ...	File
DRIVERS	12/19/2012 10:28 ...	File
FP	9/1/2012 6:00 PM	File
ProvisionStore	12/19/2012 10:28 ...	File
SAM	12/19/2012 10:28 ...	File
SECURITY	12/19/2012 10:28 ...	File
SOFTWARE	12/19/2012 10:28 ...	File
SYSTEM	12/19/2012 10:30 ...	File

Bad luck...



The screenshot shows the ophcrack tool interface. A 'Warning' dialog box is centered in the foreground, stating: 'A problem occurred while reading the SYSTEM file found in.' with an 'OK' button. The main window has tabs for 'User', 'LM Hash', 'NT Hash', 'LM Pwd 1', 'LM Pwd 2', and 'NT Pwd'. Below the tabs is a progress bar and a status bar at the bottom with the text: 'Preload: waiting', 'Brute force: waiting', 'Pwd found: 0/0', 'Time elapsed: 0h 0m 0s'.

# Certificates

## Applications – signing CA's

Microsoft Root Certificate Authority 2010

28 CC 3A 25 BF BA 44 AC 44 9A 9B 58 6B 43 39 AA

Microsoft Corporation Third Party Marketplace Root

33 95 9C 19 50 48 71 91 42 38 DF 73 D3 B4 9A 3D

Microsoft Windows Phone Production PCA 2012

33 00 00 00 00 0b fc f9 8e 58 4c 15 50 bf 00 00 00 00 00 00 0b

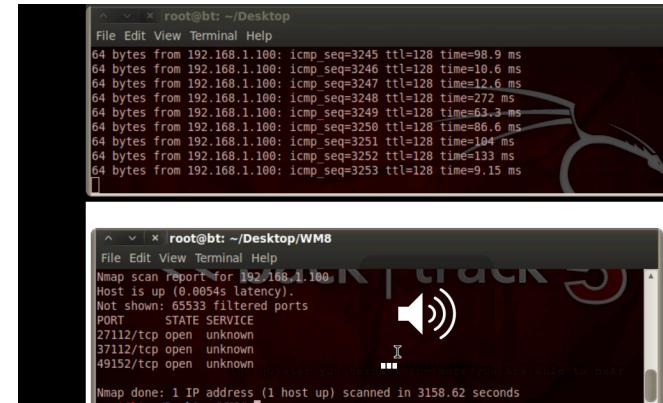
Microsoft Time-Stamp PCA 2010

261 09 81 2a 00 00 00 00 00 00 02

# Portscan results - TCP

- Open ports:
  - 27112/tcp open unknown
  - 37112/tcp open unknown
  - 49152/tcp open unknown
- Port 27112 fingerprint:

```
SF-Port27112-TCP:V=6.01%I=7%D=1/23%Time=50FFD97B%P=x86_64-unknown-linux-gn
SF:u%r(%GetRequest%,70,"HTTP/1\.1\x20404\x20File\x20Not\x20Found\r\nContent-
SF:Length:\x200\r\nServer:\x20NWP-HTTPAPI/2\.0\r\nDate:\x20Sat,\x2009\x20M
SF:ar\x202013\x2002:46:31\x20GMT\r\n\r\n")%r(HTTPOptions,70,"HTTP/1\.1\x20
SF:404\x20File\x20Not\x20Found\r\nContent-Length:\x200\r\nServer:\x20NWP-H
SF:TPAPI/2\.0\r\nDate:\x20Sat,\x2009\x20Mar\x202013\x2002:46:31\x20GMT\r\
SF:n\r\n")%r(%RTSPRequest%,70,"HTTP/1\.1\x20404\x20File\x20Not\x20Found\r\nC
SF:ontent-Length:\x200\r\nServer:\x20NWP-HTTPAPI/2\.0\r\nDate:\x20Sat,\x20
SF:09\x20Mar\x202013\x2002:46:31\x20GMT\r\n\r\n")%r(%FourOhFourRequest%,70,"
SF:HTTP/1\.1\x20404\x20File\x20Not\x20Found\r\nContent-Length:\x200\r\nSer
SF:ver:\x20NWP-HTTPAPI/2\.0\r\nDate:\x20Sat,\x2009\x20Mar\x202013\x2002:46
SF::31\x20GMT\r\n\r\n")%r(%SIPOptions%,70,"HTTP/1\.1\x20404\x20File\x20Not\x
SF:20Found\r\nContent-Length:\x200\r\nServer:\x20NWP-HTTPAPI/2\.0\r\nDate:
SF:\x20Sat,\x2009\x20Mar\x202013\x2002:46:31\x20GMT\r\n\r\n");
```



```
root@bt: ~/Desktop
File Edit View Terminal Help
64 bytes from 192.168.1.100: icmp seq=3245 ttl=128 time=98.9 ms
64 bytes from 192.168.1.100: icmp seq=3246 ttl=128 time=10.6 ms
64 bytes from 192.168.1.100: icmp seq=3247 ttl=128 time=12.6 ms
64 bytes from 192.168.1.100: icmp seq=3248 ttl=128 time=272 ms
64 bytes from 192.168.1.100: icmp seq=3249 ttl=128 time=63.3 ms
64 bytes from 192.168.1.100: icmp seq=3250 ttl=128 time=86.6 ms
64 bytes from 192.168.1.100: icmp seq=3251 ttl=128 time=104 ms
64 bytes from 192.168.1.100: icmp seq=3252 ttl=128 time=133 ms
64 bytes from 192.168.1.100: icmp seq=3253 ttl=128 time=9.15 ms

root@bt: ~/Desktop/WM8
File Edit View Terminal Help
Nmap scan Report for 192.168.1.100
Host is up (0.0054s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE
27112/tcp open  unknown
37112/tcp open  unknown
49152/tcp open  unknown
Nmap done: 1 IP address (1 host up) scanned in 3158.62 seconds
```

Microsoft  
Lync?

# Portscan results - UDP

```
root@bt: ~/Desktop/WM8
View Terminal Help
/Desktop/WM8# cat nmap_udp.txt
/Desktop/WM8# nmap -sU 192.168.1.100 -p 0-65535 --reason

Nmap 6.01 ( http://nmap.org ) at 2013-01-23 23:41 EST
  report for 192.168.1.100
  p, received reset (0.00013s latency).
  scanned ports on 192.168.1.100 are open|filtered because of 6

/Desktop/WM8#
```

# Future work

- Write Windows Phone 8 application that:
  - Hooks into a remote debugger
  - Search for the code signing parameters
  - Change the code signing parameters in memory (Similar to Windows RT jailbreak )
- Identify vulnerabilities trusted OEM app on phone
- Research manual unlocks of Windows Phone 8
  - Capture, analyse and replay device unlock communications ( IP over USB) between host and Windows Phone

# Resources and further references



- SANS SEC575 Mobile Device Security and Ethical Hacking
  - SANS Canberra 2013
  - Jul 1, 2013 - Jul 13, 2013
- XDA-developers – Windows Phone 8 Development and Hacking forum