

May 2nd, 2012


Christopher Hale

Dr. Cihan Varol – Graduate Advisor

**A NEW VILLAIN:
INVESTIGATING STEGANOGRAPHY
IN SOURCE ENGINE BASED
VIDEO GAMES**




Table of Contents

- History behind platform
 - Impact of platform
 - Creating game levels with hidden data
 - Investigating these levels to recover information
 - Conclusion
 - Future Work
- 



The Source Engine

- Created by Valve
 - Two ex-Microsoft Employees started in 1996
 - Began with the release of Half Life in 1998
 - Originally a modified version of the Quake gaming engine
 - Known initially as \$Gldsrc
 - Modified further into Source engine
- 

The Source Engine – Cont'd

- One of the leading game engines in the world
- Released titles such as:
 - Half Life 1 & 2
 - Portal 1 & 2
 - Left 4 Dead 1 & 2
- Ongoing constant development

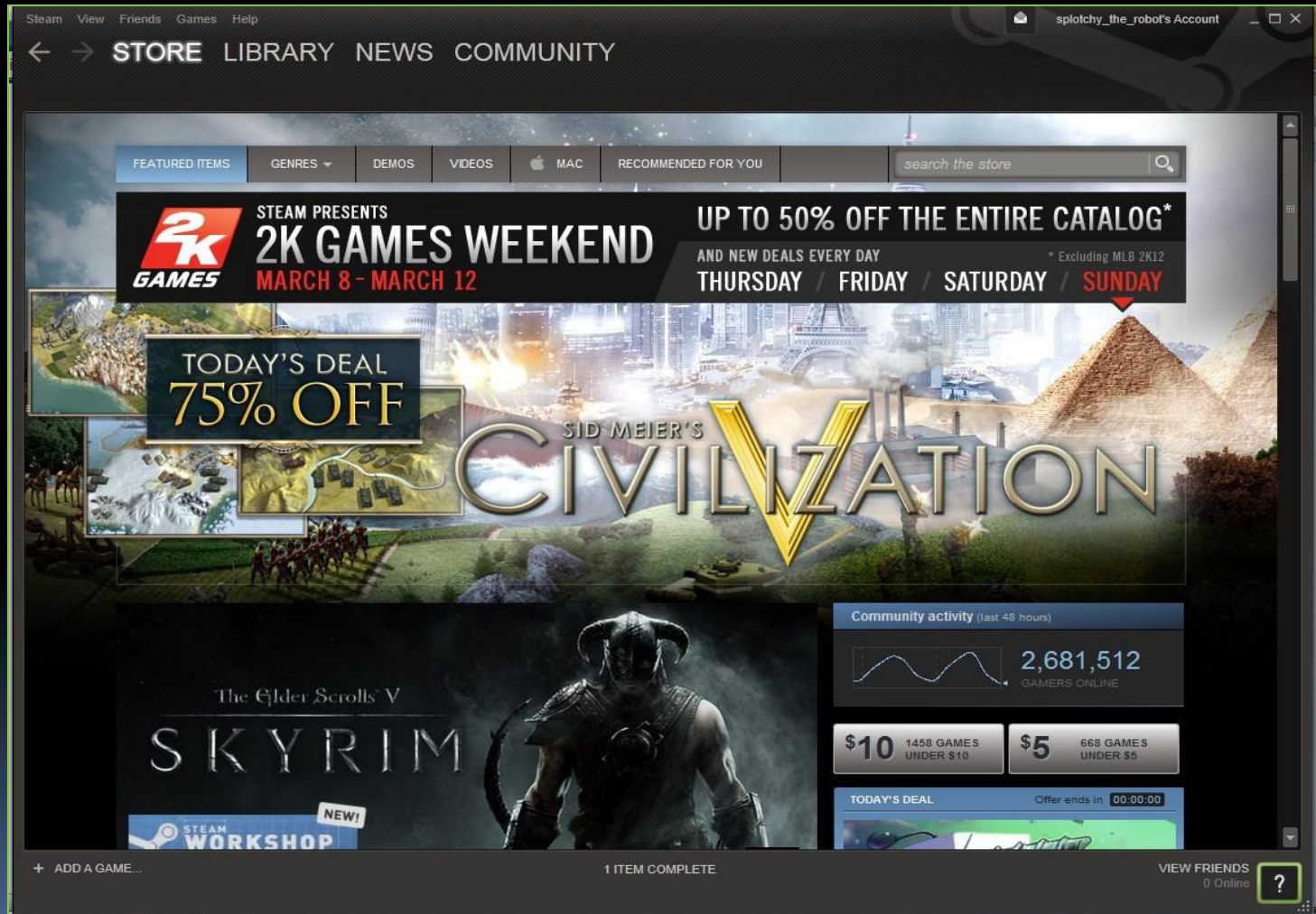
What is Steam?

- PC based gaming solution
- Store
- Game Management
- Statistic Aggregation
- Patch Aggregation
- Social network

- Currently in Development – Steamworks API




The Steam Interface



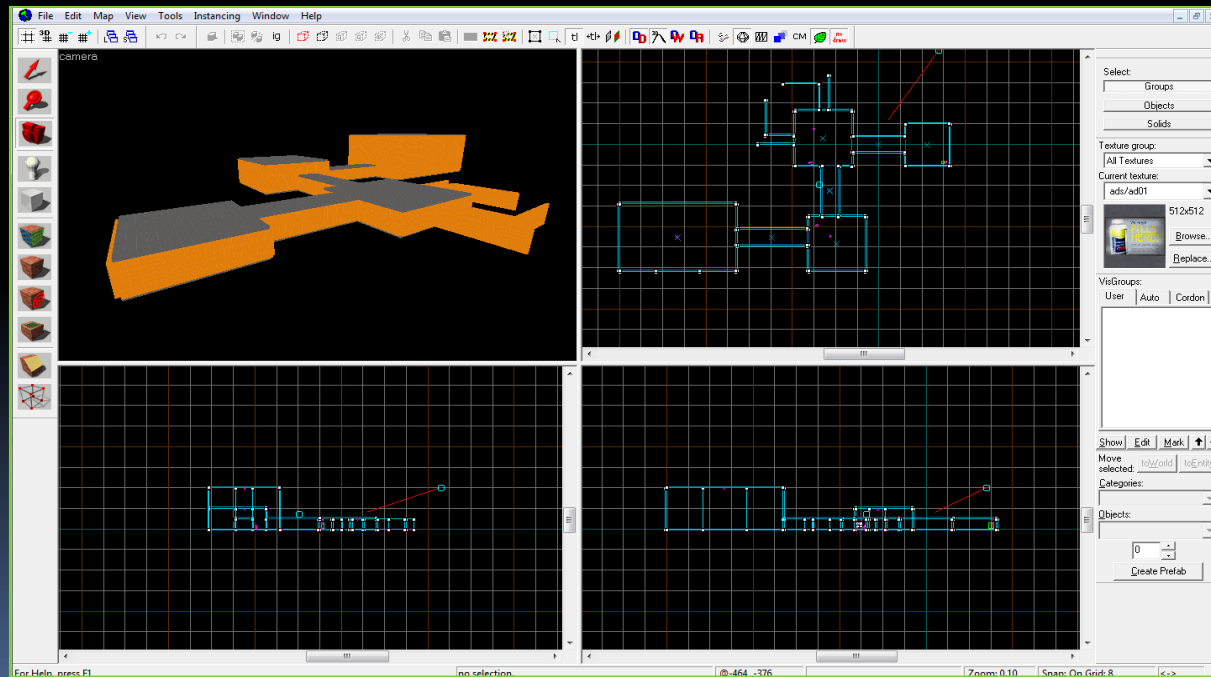


Steam Usage

- 1523 games available
 - 40 million active user accounts
 - 5 million concurrent players on January 2, 2012
 - 70% of the digital distribution market in 2009
 - Continual growth
- 


Hammer

- Official level (map) creation tool
- Used on all Source games
- Free with Source games






Tools Within Hammer

- Hammer is a set of tools to create, develop, and publish Source maps
 - Main game creation interface
 - Game logic
 - Tools to compile map data into playable levels
- 

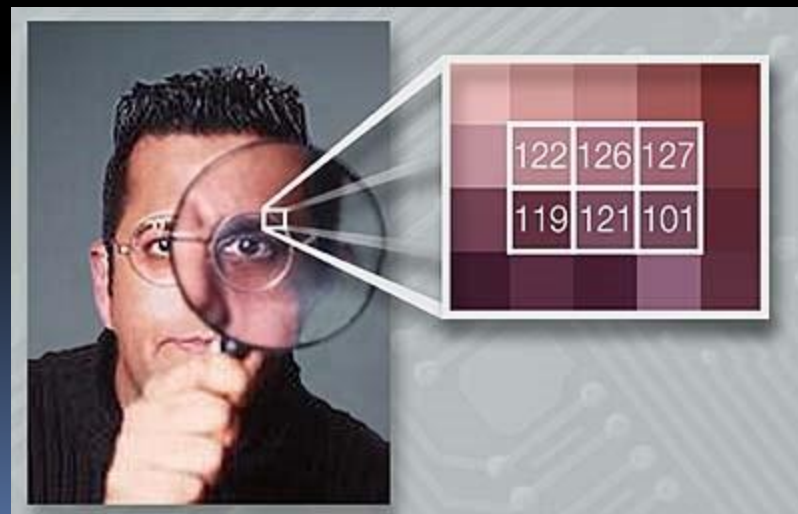


Exploiting the Source Engine

- Main focus of this project
 - Use video game files to hide data
 - Text Messages
 - Images
 - Steganography
- 

What is Steganography?

- Hiding Data Within Data
- Security Through Obscurity
- Only Sender/Receiver Recognize Data
- Advantages Over Encryption






Why Video Games?

- Size – Plenty of room to hide data
- Common – Video game installations are not out of place on computer systems
- Dynamic – Video game files are intended to change repeatedly
- Untraceable Information – Data hidden in these files cannot be viewed on a dead system
- Open Source Files - Source specific

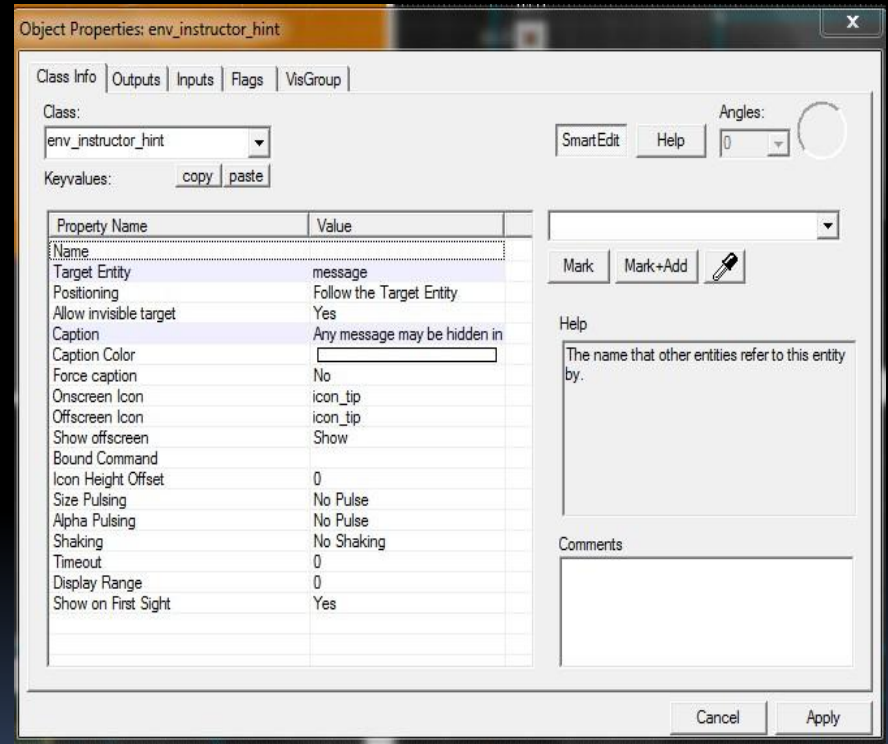


Embedding Text With Brushes

- Brushes are main level geometry
 - Brushes can be manipulated to form words and messages
 - Most basic data hiding technique
 - Easy to accomplish
 - Tedious to execute
 - Impossible to detect on disk
- 

Embedding Text with Overlays

- In-Game messages
- Physical locations
- Implemented with Entities
- Env_instructor_hint
- Info_target
- Relatively easy to implement and use
- Detectable on disk by investigator



Embedding Images with Textures

- Developer jargon for images
- Image handling by Source - VTF
- Size considerations
- File format
- Metadata file
- VTFEdit

Embedding Images with Textures



- Once images are converted, they can be added to the map
- Face Edit tool



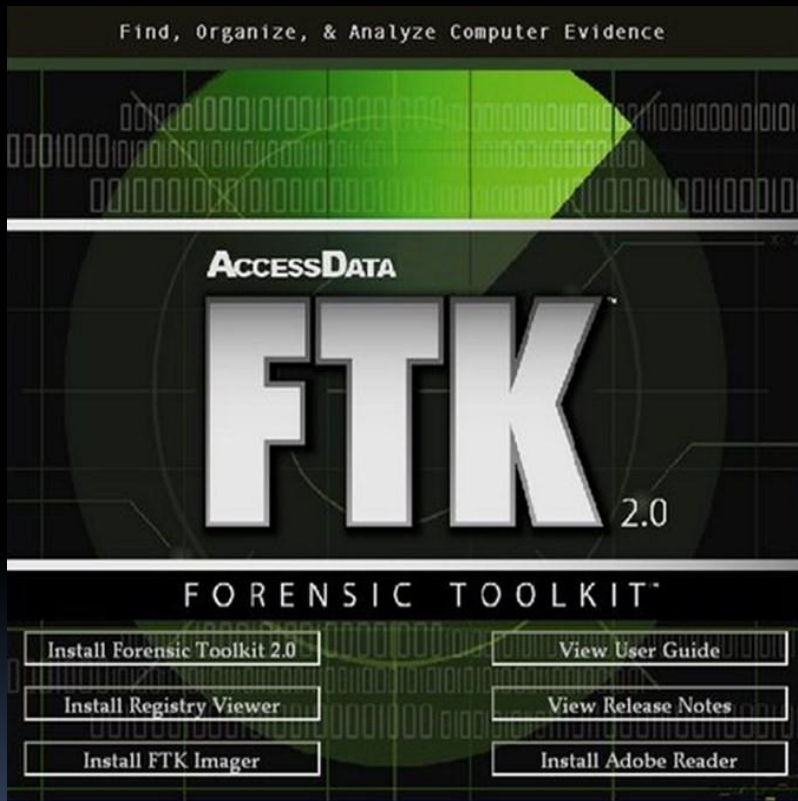
Map Distribution

- VPK File
- VPK File Contents
 - Level Data
 - Textures
 - Assets
- VPK Tool
- Distribution
- Installation

Demonstration!




Investigating Source Games



- Source games can be used to hide data
- Investigators must have a way to recover this data
- Forensic Toolkit (FTK) used for investigation

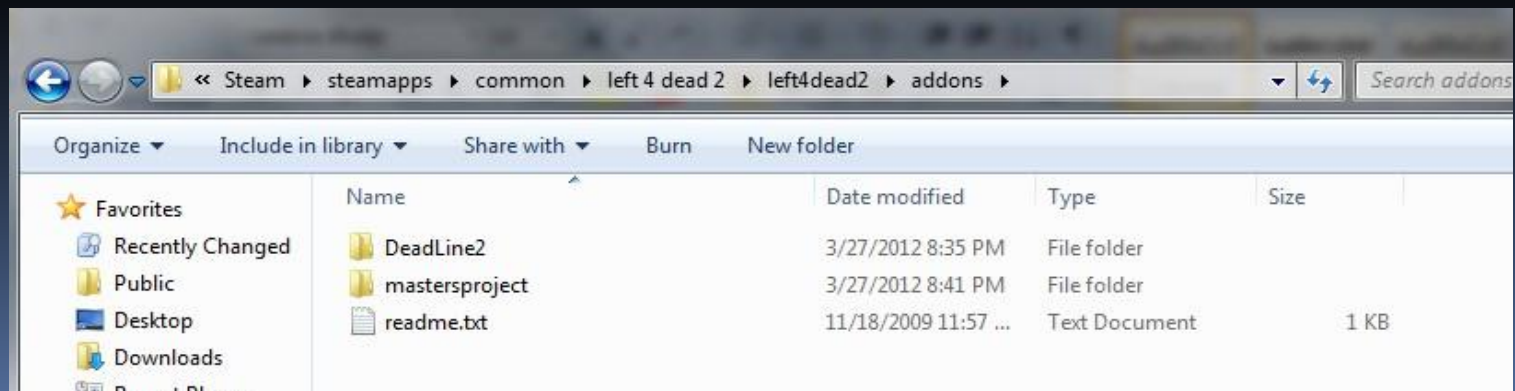


Issues Facing Investigators

- Multitude of game files
 - Size of game file installations
 - No native support in investigative software
 - Reliance on non-forensic level tools
 - Viability in court
- 

The First Step: Finding Game Files

- The first step in the investigative process is to identify and locate game files
- Two main approaches
- Game directory structure
 - Steam\steamapps\common*gamename*\addons
- File header
 - 0x55aa 1234




Finding Game Files – cont'd

- Once a VPK has been found, it must be decompressed and unpacked
- GCFScape Tool
- Allows users to view and extract files from a VPK
- Used by an investigator to work with data



Investigating Data Hidden with Brushes

- Impossible to do
 - Cannot be detected in disk
 - Only visible when game is played
- 

Investigating Data Hidden with Overlays

- Data hidden in overlays can be recovered on disk
- VPK file must be decompressed
- Data resides in *mapname.bsp* file
- Stored in “entity lumps”
- Search for keywords
- “hint_caption” followed by message
- "hint_caption" "Malicious information here!"

Entity Lump

```
{  
    "world_maxs" "480 480 480"  
    "world_mins" "-480-480 -224"  
    "maxpropscreenwidth" "-1"  
    "skyname" "sky_wasteland02"  
    "classname" "worldspawn"  
}  
  
{  
    "origin" "-413.793 -384 -192"  
    "angles" "0 0 0"  
    "classname" "info_player_start"  
}
```

Investigating Data Hidden with Overlays – cont'd

The screenshot displays the AccessData Forensic Toolkit (AD1) interface. The main window shows the 'File Content' view for a file named 'simplemap1.bsp'. The interface includes a menu bar (File, Edit, View, Evidence, Filter, Tools, Manage, Help), a filter dropdown set to '-unfiltered-', and a toolbar with icons for Explore, Overview, Email, Graphics, Bookmarks, Live Search, Index Search, and Volatile. The 'Evidence Items' pane on the left shows a tree structure with folders for 'maps', 'materials', and 'missions', and files for 'mastersproject [AD1]' and 'mastersproject.vpk [AD1]'. The 'File Content' pane displays a hex-to-text conversion of the file's data. The text is as follows:


```
00c310 30 22 0A 22 68 69 6E 74-5F 70 75 6C 73 65 6F 70 0".hint_pulseop
00c320 74 69 6F 6E 22 20 22 30-22 0A 22 68 69 6E 74 5F tion" "0".hint_
00c330 6E 6F 6F 66 66 73 63 72-65 65 6E 22 20 22 30 22 nooffscreen" "0"
00c340 0A 22 68 69 6E 74 5F 69-63 6F 6E 5F 6F 6E 73 63 ."hint_icon_onsc
00c350 72 65 65 6E 22 20 22 69-63 6F 6E 5F 74 69 70 22 reen" "icon_tip"
00c360 0A 22 68 69 6E 74 5F 69-63 6F 6E 5F 6F 66 66 73 ."hint_icon_offs
00c370 65 74 22 20 22 30 22 0A-22 68 69 6E 74 5F 69 63 et" "0".hint_ic
00c380 6F 6E 5F 6F 66 66 73 63-72 65 65 6E 22 20 22 69 on_offscreen" "i
00c390 63 6F 6E 5F 74 69 70 22-0A 22 68 69 6E 74 5F 66 con_tip".hint_f
00c3a0 6F 72 63 65 63 61 70 74-69 6F 6E 22 20 22 30 22 orcaption" "0"
00c3b0 0A 22 68 69 6E 74 5F 63-6F 6C 6F 72 22 20 22 32 ."hint_color" "2
00c3c0 35 35 20 32 35 35 20 32-35 35 22 0A 22 68 69 6E 55 255 255".hin
00c3d0 74 5F 63 61 70 74 69 6F-6E 22 20 22 41 6E 79 20 t_caption" "Any
00c3e0 6D 65 73 73 61 67 65 20-6D 61 79 20 62 65 20 68 message may be h
00c3f0 69 64 64 65 6E 20 69 6E-20 67 61 6D 65 20 61 73 idden in game as
00c400 20 74 65 78 74 21 22 0A-22 68 69 6E 74 5F 61 75 text!".hint_au
00c410 74 6F 5F 73 74 61 72 74-22 20 22 31 22 0A 22 68 to_start" "1".h
00c420 69 6E 74 5F 61 6C 70 68-61 6F 70 74 69 6F 6E 22 int_alphaoption"
00c430 20 22 30 22 0A 22 68 69-6E 74 5F 61 6C 6C 6F 77 "0".hint_allow
00c440 5F 6E 6F 64 72 61 77 5F-74 61 72 67 65 74 22 20 _nodraw_target"
00c450 22 31 22 0A 22 63 6C 61-73 73 6E 61 6D 65 22 20 "1".classname"
00c460 22 65 6E 76 5F 69 6E 73-74 72 75 63 74 6F 72 5F "env_instructor_
00c470 68 69 6E 74 22 0A 22 68-61 6D 6D 65 72 69 64 22 hint".hammerid
```

Below the text, the status bar indicates 'Sel start = 50125, len = 13'. At the bottom of the main window, the file path 'mastersproject [AD1]/maps/simplemap1.bsp' is shown, along with 'Ready' and 'Explore Tab Filter: [None]'. The 'File List' pane at the bottom shows a table of files:

File List	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256
<input type="checkbox"/>	simplemap1.bsp		1003	bsp	mastersproject [AD1]/m...	Unknown	n/a	1872 KB	6FA65...	3CA99...	0E2F33...
<input type="checkbox"/>	simplemap1.nav		1004	nav	mastersproject [AD1]/m...	Unknown	n/a	41.54 KB	D7C15...	A9891...	56CBE...




Investigating Data Hidden with Textures

- Identification
 - File System structure
 - Header
 - 0X5654 4600 0700 – VTF \0
 - Once identified, textures can be investigated
 - VTFEdit may be used
- 




Conclusion

- Data privacy is a right of every individual
 - Sometimes this right can be abused
 - Data can be hidden in Source game files
 - Investigators have ways to recover this data, albeit rudimentary
 - The widespread impact of data hidden in this way drives demand for solutions on both sides
- 



Future Work

- New methods of data hiding
 - New methods of data recovery
 - Development of investigative tools
 - Support for Source files in FTK and others
 - Forensic verification
 - Expansion to other game engines
 - Expansion to other platforms
- 

References

- [1] M. Fossi and T. Mack, *"Symantec Internet Security Threat Report: Trends for 2010,"* Symantec Corp., Mountain View, CA, Tech. Rep. 21182883, Apr. 2011
- [2] Entertainment Software Association, (2011). *Essential Facts about the Computer And Video Game Industry* [Online]. Available: http://www.theesa.com/facts/pdfs/ESA_EF_2011.pdf.
- [3] Entertainment Software Association, (2011). *Industry Facts: Economic Data* [Online]. Available: <http://www.theesa.com/facts/econdata.asp>.
- [4] Valve Corporation, (2010). *Welcome to Valve* [Online]. Available: <http://www.valvesoftware.com/company/index.html>.
- [5] T. Bayer, (2010). *14 years of Quake Engine: The Famous Games with id Technology* [Online]. Available: <http://www.pcgameshardware.com/aid,687947/14-years-of-Quake-Engine-The-famous-games-with-id-Technology/News/>
- [6] M. Thomsen, (2009). *Ode to Source: A History of Valve's Tireless Game Engine* [Online]. Available: <http://pc.ign.com/articles/102/1027317p1.html>.

References cont'd.

- [7] A. Capriole and J. Phillips, (2008). *The History of Valve* [Online]. Available: <http://planethalflife.gamespy.com/View.php?view=Articles.Detail&id=121>.
-
- [8] Warf!y, (2011). *About the Steamless CS Project* [Online]. Available: <http://v5.steamlessproject.nl/index.php?page=about>.
-
- [9] Valve Corporation, (2010). *Games* [Online]. Available: http://store.steampowered.com/search/#category1=998&advanced=0&sort_order=ASC&page=1.
-
- [10] K. Mudgal, (2012). *Valve Releases PR; Steam Userbase Doubles in 2011, Big Picture Mode Coming Soon* [Online]. Available: <http://gamingbolt.com/valve-releases-pr-steam-userbase-doubles-in-2011-big-picture-mode-coming-soon>.
-
- [11] T. Senior, (2012). *Steam Hits Five Million Concurrent Players* [Online]. Available: <http://www.pcgamer.com/2012/01/03/steam-hits-five-million-concurrent-players/>.
-
- [12] K. Graft, (2009). *Stardock Reveals Impulse, Steam Market Share Estimates* [Online]. Available: http://www.gamasutra.com/php-bin/news_index.php?story=26158.

References cont'd.

- [13] *Hammer Editor Version History* (2010) [Online]. Available: https://developer.valvesoftware.com/wiki/Hammer_Editor_version_history.
-
- [14] *Mapping Overview* (2010) [Online]. Available: https://developer.valvesoftware.com/wiki/Introduction_to_Editing.
-
- [15] *VMF Documentation* (2012) [Online]. Available: https://developer.valvesoftware.com/wiki/VMF_documentation.
-
- [16] *Hammer Game Configurations* (2011) [Online]. Available: https://developer.valvesoftware.com/wiki/Game_Configurations.
-
- [17] *VBSP* (2011) [Online]. Available: <https://developer.valvesoftware.com/wiki/Vbsp>.
-
- [18] *VVIS* (2011) [Online]. Available: <https://developer.valvesoftware.com/wiki/Vvis>.
-
- [19] *VRAD* (2012) [Online]. Available: <https://developer.valvesoftware.com/wiki/Vrad>.
-
- [20] *Env_Instructor_Hint* (2011) [Online]. Available: https://developer.valvesoftware.com/wiki/Env_instructor_hint

References cont'd.

- [20] *Env_Instructor_Hint* (2011) [Online]. Available: https://developer.valvesoftware.com/wiki/Env_instructor_hint.
-
- [21] *Info_target* (2012) [Online]. Available: https://developer.valvesoftware.com/wiki/Info_target.
-
- [22] *Valve Texture Format* (2011) [Online]. Available: https://developer.valvesoftware.com/wiki/Valve_Texture_Format.
-
- [23] *VTFEdit* (2011) [Online]. Available: <https://developer.valvesoftware.com/wiki/VTFEdit>.
-
- [24] *Material* (2011) [Online]. Available: <https://developer.valvesoftware.com/wiki/Material>.
-
- [25] *VPK File Format* (2011) [Online]. Available: https://developer.valvesoftware.com/wiki/VPK_File_Format.
-
- [26] *VPK* (2011) [Online]. Available: <https://developer.valvesoftware.com/wiki/VPK>.
-
- [27] R. Gregg, (2006). *AboutGCFscape* [Online]. Available: <http://nemesis.thewavelength.net/index.php?p=25>.
-

Questions?

