

Google™



# Native Client: Accelerating Web Applications

Brad Chen, David Sehr, Nicholas Fullagar  
28 May 2009



# Why Native Code?

Close the gap between desktop and web apps...

- Performance
- Choice of programming language
- Leverage legacy code

... but do not sacrifice

- Portability
- Safety

# What we mean by “Performance”

Key performance features include

- POSIX-like thread support
- Straightforward access to vector instructions
- Hand-coded assembler

Substantially all the CPU performance  
of desktop applications

# What does it mean for the Web?

Desktop CPU performance will enable Web apps with:

- Safer multimedia codecs
- Real-time audio and video synthesis
- Real-time physics simulations
- Local audio/video analysis and recognition
- Multimedia editors
- Flexible, high-throughput cryptography
- Application-specific data compression
- ...

Together with O3D we will enable:

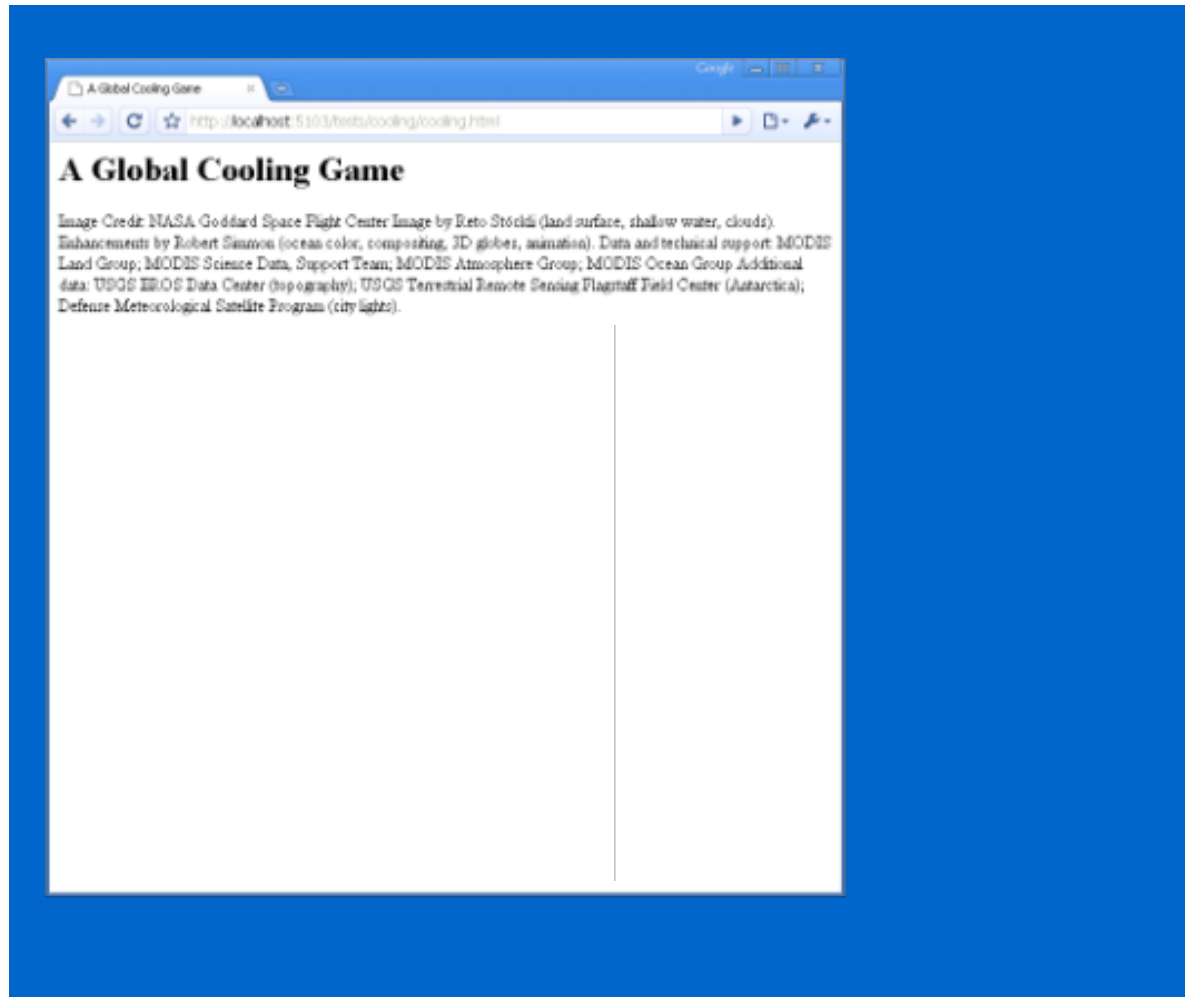
- High quality games
- CAD applications
- ...



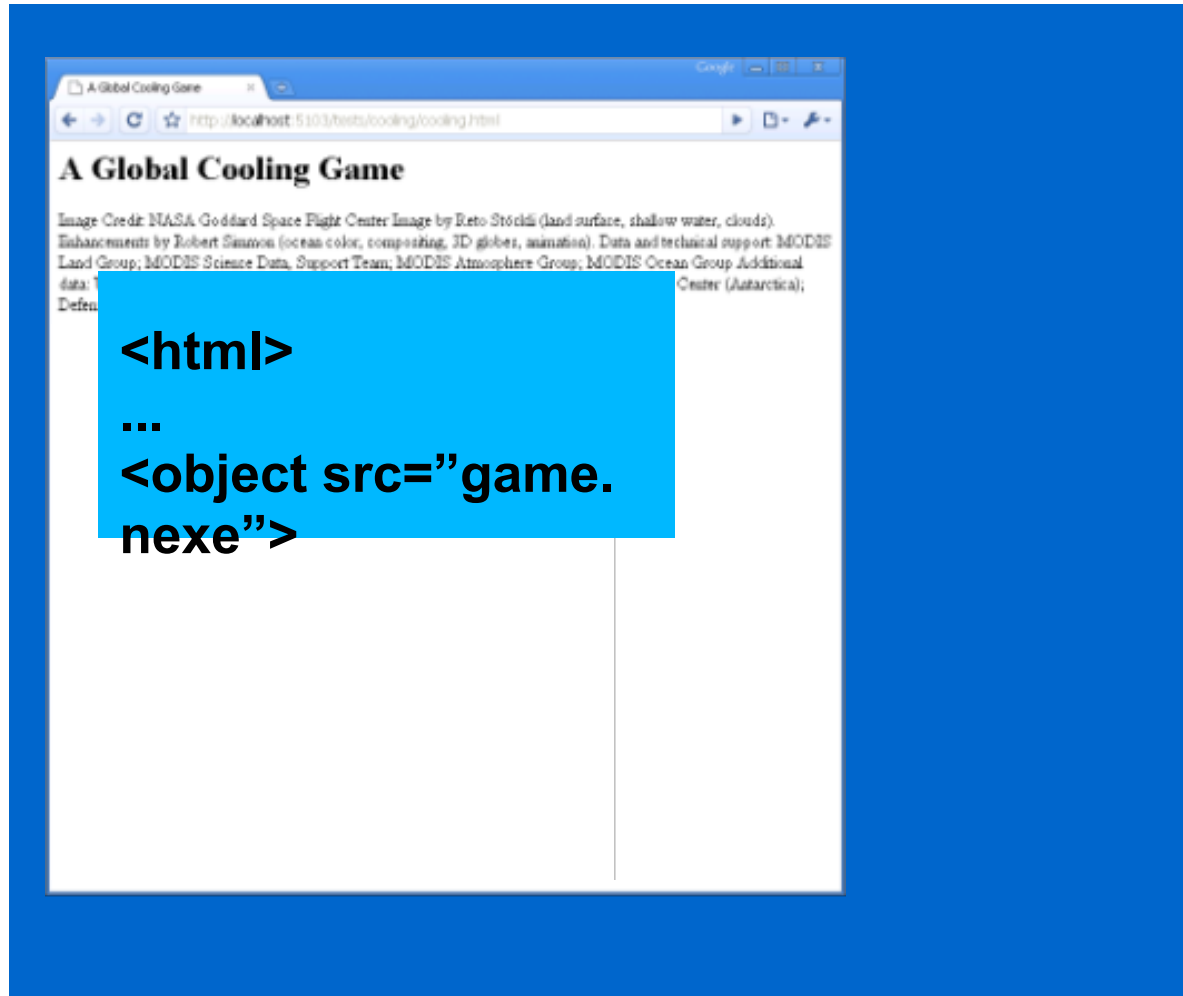
# The Life of a NaCl-Enabled Web App



# The Life of a NaCl-Enabled Web App

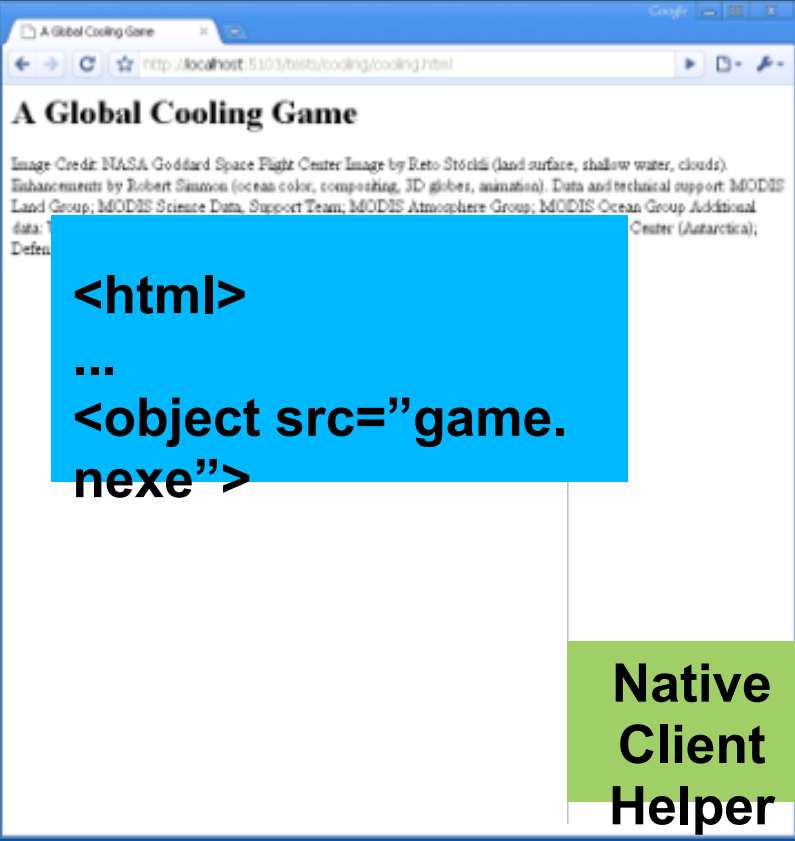


# The Life of a NaCl-Enabled Web App





# The Life of a NaCl-Enabled Web App

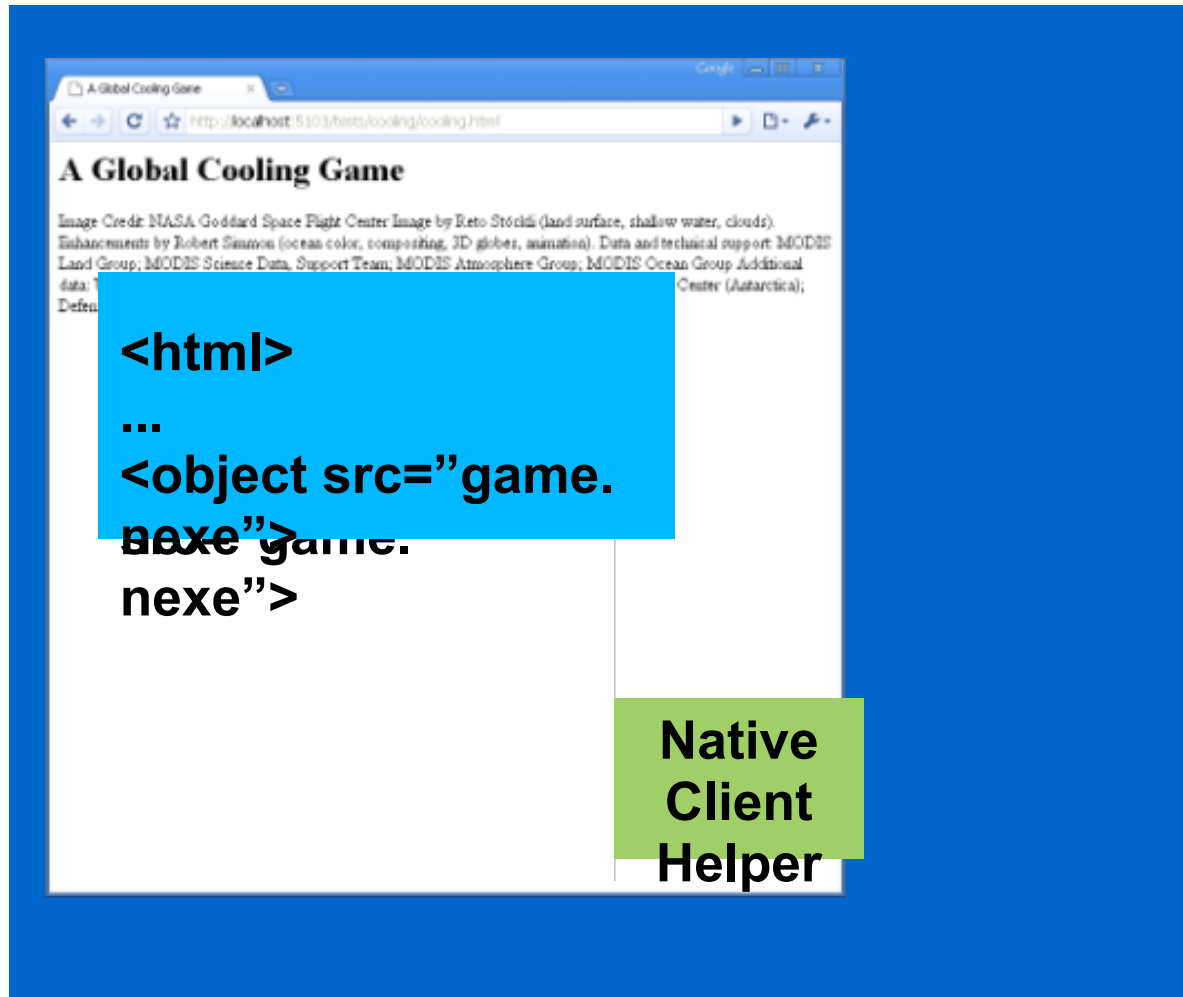


The screenshot shows a web browser window titled "A Global Cooling Game" with the URL "http://localhost:5103/tests/loading/loading.html". The page content includes a title and a paragraph of text. Two code snippets are overlaid on the page: a blue box containing HTML tags and a green box containing the text "Native Client Helper".

```
<html>  
...  
<object src="game.nexe">
```

Native Client Helper

# The Life of a NaCl-Enabled Web App



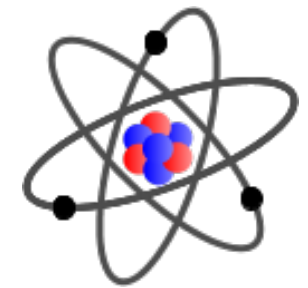
A screenshot of a web browser window titled "A Global Cooling Game". The address bar shows "http://localhost:5103/tests/loading/loading.html". The page content includes a title "A Global Cooling Game" and a paragraph of text: "Image Credit: NASA Goddard Space Flight Center Image by Reto Stöckli (land surface, shallow water, clouds). Enhancements by Robert Simon (ocean color, compositing, 3D globe, animation). Data and technical support: MODIS Land Group; MODIS Science Data, Support Team; MODIS Atmosphere Group; MODIS Ocean Group Additional data: Center (Antarctica); Defn".

Overlaid on the screenshot is a blue box containing the following HTML code:

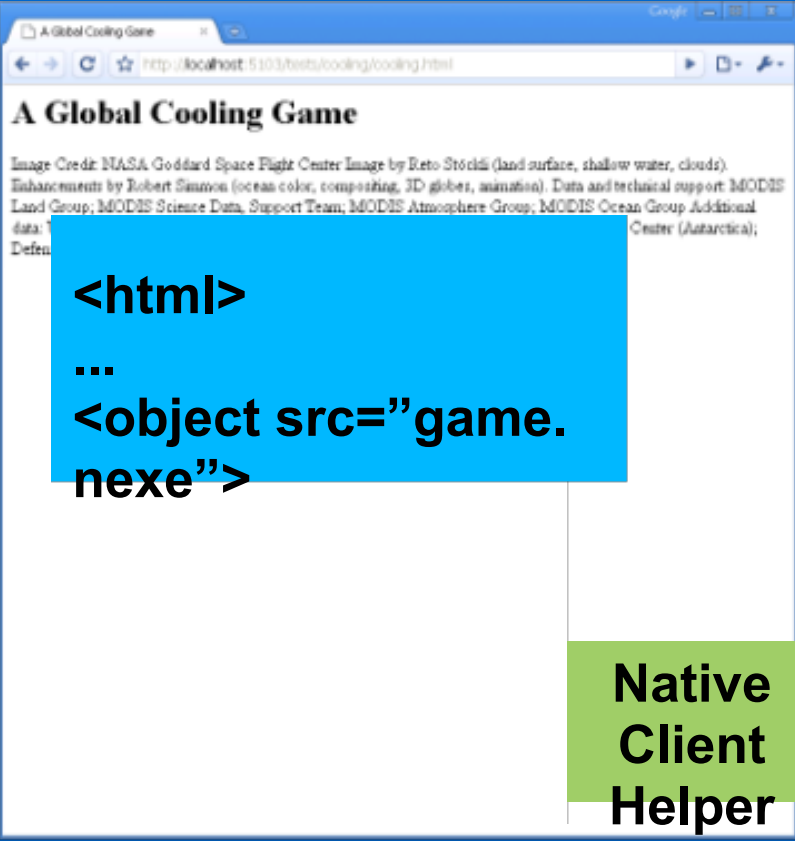
```
<html>  
...  
<object src="game.  
vaxe">game.  
nexe">
```

Below the code box is a green box containing the text:

Native Client Helper



# The Life of a NaCl-Enabled Web App



A screenshot of a web browser window titled "A Global Cooling Game". The address bar shows "http://localhost:5103/tests/loading/loading.html". The page content includes a title "A Global Cooling Game" and a paragraph of text: "Image Credit: NASA Goddard Space Flight Center Image by Reto Stöckli (land surface, shallow water, clouds). Enhancements by Robert Simon (ocean color, compositing, 3D globe, animation). Data and technical support: MODIS Land Group; MODIS Science Data, Support Team; MODIS Atmosphere Group; MODIS Ocean Group. Additional data: [redacted] Center (Antarctica); Defini".

Overlaid on the screenshot is a blue box containing the following HTML code:

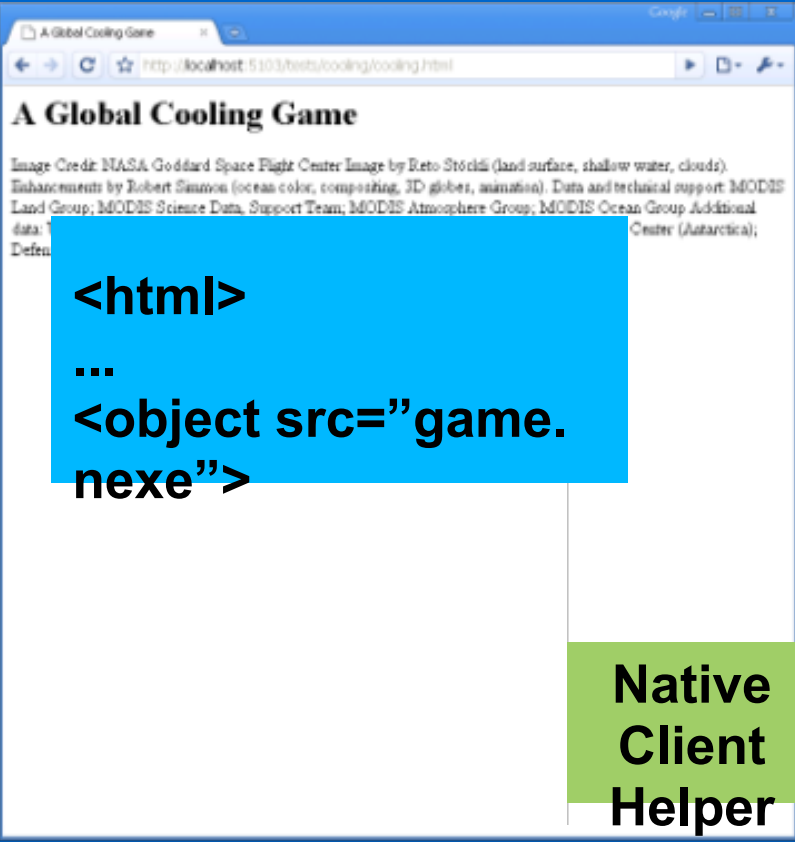
```
<html>  
...  
<object src="game.nexe">
```

Below the code box is a green box containing the text:

Native Client Helper



# The Life of a NaCl-Enabled Web App

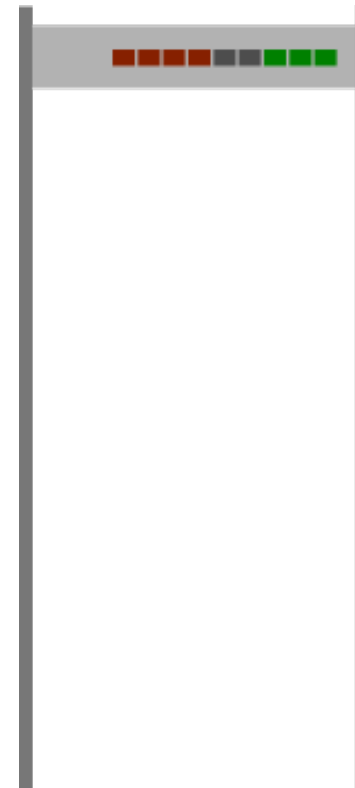


A screenshot of a web browser window titled "A Global Cooling Game". The address bar shows "http://localhost:5103/tests/loading/loading.html". The page content includes the title "A Global Cooling Game" and a paragraph of text: "Image Credit: NASA Goddard Space Flight Center Image by Reto Stöckli (land surface, shallow water, clouds). Enhancements by Robert Simon (ocean color, compositing, 3D globe, animation). Data and technical support: MODIS Land Group; MODIS Science Data, Support Team; MODIS Atmosphere Group; MODIS Ocean Group Additional data: Center (Antarctica); Defn".

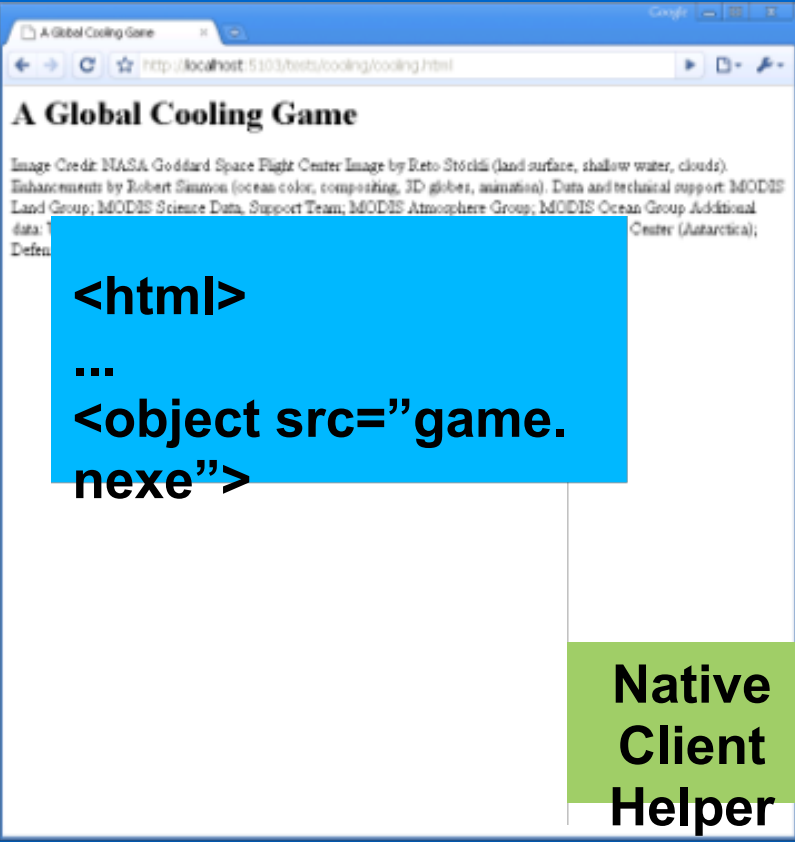
Overlaid on the screenshot is a blue box containing the following HTML code:

```
<html>  
...  
<object src="game.nexe">
```

Below the code box, a green box contains the text "Native Client Helper".



# The Life of a NaCl-Enabled Web App



A screenshot of a web browser window titled "A Global Cooling Game". The address bar shows "http://localhost:5103/tests/loading/loading.html". The page content includes a title "A Global Cooling Game" and a paragraph of text: "Image Credit: NASA Goddard Space Flight Center Image by Reto Stöckli (land surface, shallow water, clouds). Enhancements by Robert Simon (ocean color, compositing, 3D globe, animation). Data and technical support: MODIS Land Group; MODIS Science Data, Support Team; MODIS Atmosphere Group; MODIS Ocean Group Additional data: ... Center (Antarctica); Defn".

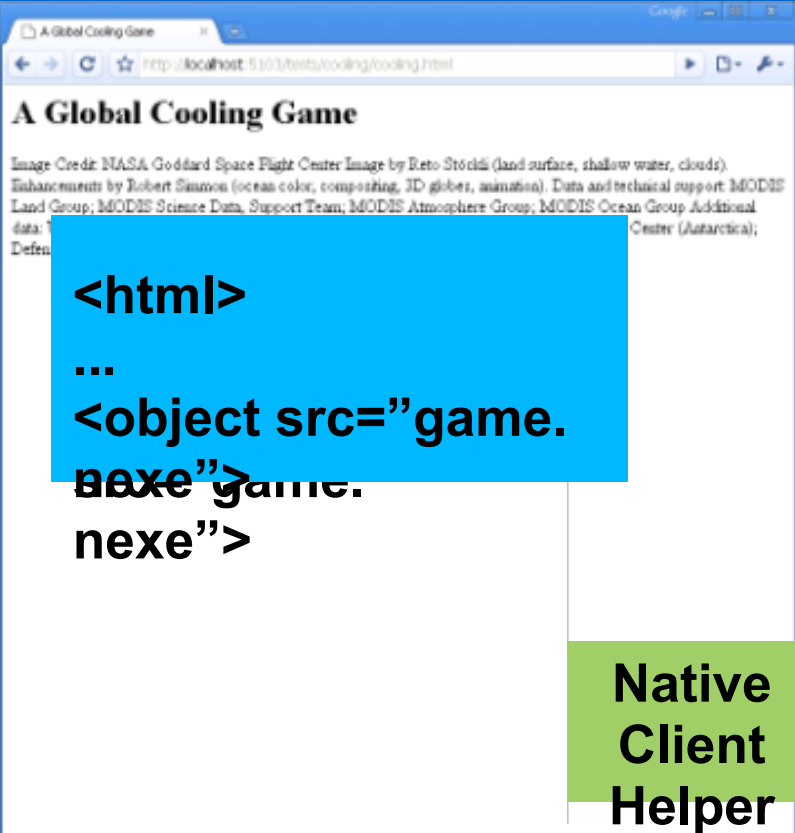
Overlaid on the screenshot is a blue box containing the following HTML code:

```
<html>  
...  
<object src="game.nexe">
```

Below the code box is a green box with the text "Native Client Helper".



# The Life of a NaCl-Enabled Web App

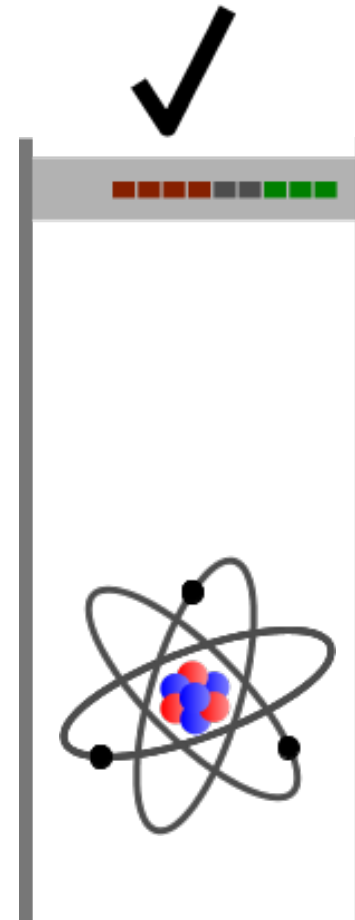


A screenshot of a web browser window titled "A Global Cooling Game". The address bar shows "http://localhost:5103/tests/loading/loading.html". The page content includes a title "A Global Cooling Game" and a paragraph of text: "Image Credit: NASA Goddard Space Flight Center Image by Reto Stöckli (land surface, shallow water, clouds). Enhancements by Robert Simon (ocean color, compositing, 3D globe, animation). Data and technical support: MODIS Land Group; MODIS Science Data, Support Team; MODIS Atmosphere Group; MODIS Ocean Group. Additional data: ... Center (Antarctica); Defn".

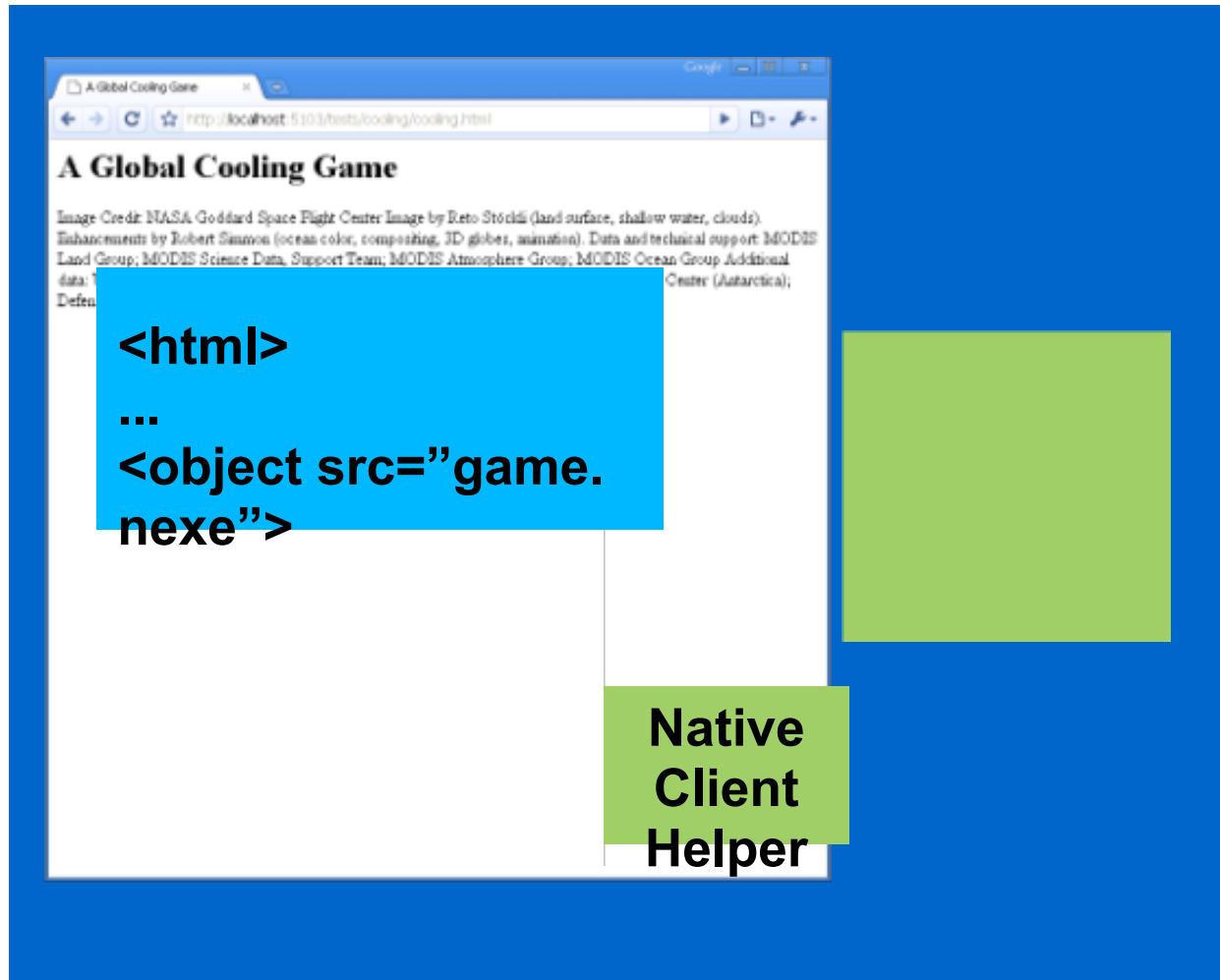
Overlaid on the screenshot is a blue box containing the following HTML code:

```
<html>  
...  
<object src="game.  
next">game.  
next">
```

Below the code box is a green box with the text "Native Client Helper".



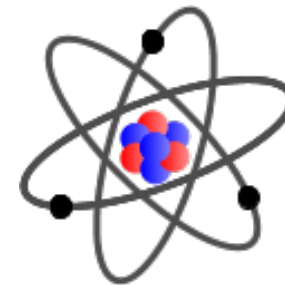
# The Life of a NaCl-Enabled Web App



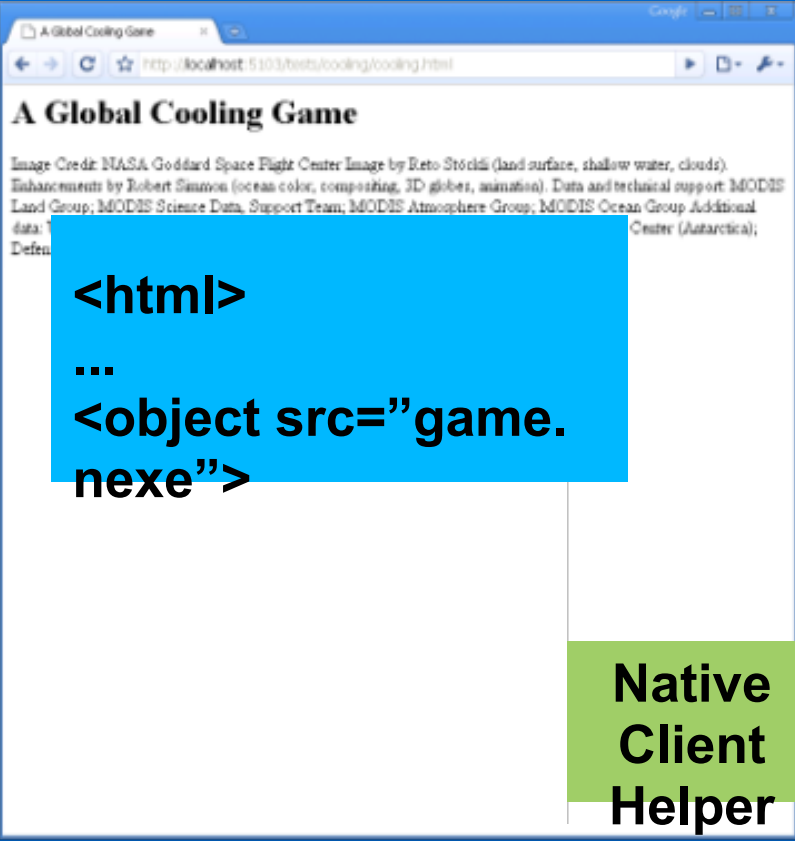
The screenshot shows a web browser window titled "A Global Cooling Game" with the URL "http://localhost:5103/tests/loading/loading.html". The page content includes a title and a paragraph of text. Overlaid on the page are two code snippets in blue boxes and a green box labeled "Native Client Helper".

```
<html>  
...  
<object src="game.nexe">
```

Native Client Helper



# The Life of a NaCl-Enabled Web App



The screenshot shows a web browser window with the title "A Global Cooling Game" and the URL "http://localhost:5103/tests/loading/loading.html". The page content includes a title, a paragraph of text with image credits, and a code block. The code block contains the following HTML code:

```
<html>  
...  
<object src="game.nexe">
```

To the right of the code block is a diagram of an atom with a central nucleus of red and blue spheres and three black electrons orbiting in elliptical paths. Below the code block is a green box with the text "Native Client Helper".



# The Life of a NaCl-Enabled Web App

The screenshot shows a web browser window with the address bar displaying `http://localhost:5103/tests/loading/loading.html`. The page title is "A Global Cooling Game". Below the title, there is a paragraph of text: "Image Credit: NASA Goddard Space Flight Center Image by Reto Stöckli (land surface, shallow water, clouds). Enhancements by Robert Simon (ocean color, compositing, 3D globe, animation). Data and technical support: MODIS Land Group; MODIS Science Data, Support Team; MODIS Atmosphere Group; MODIS Ocean Group Additional data: Center (Antarctica); Defn".

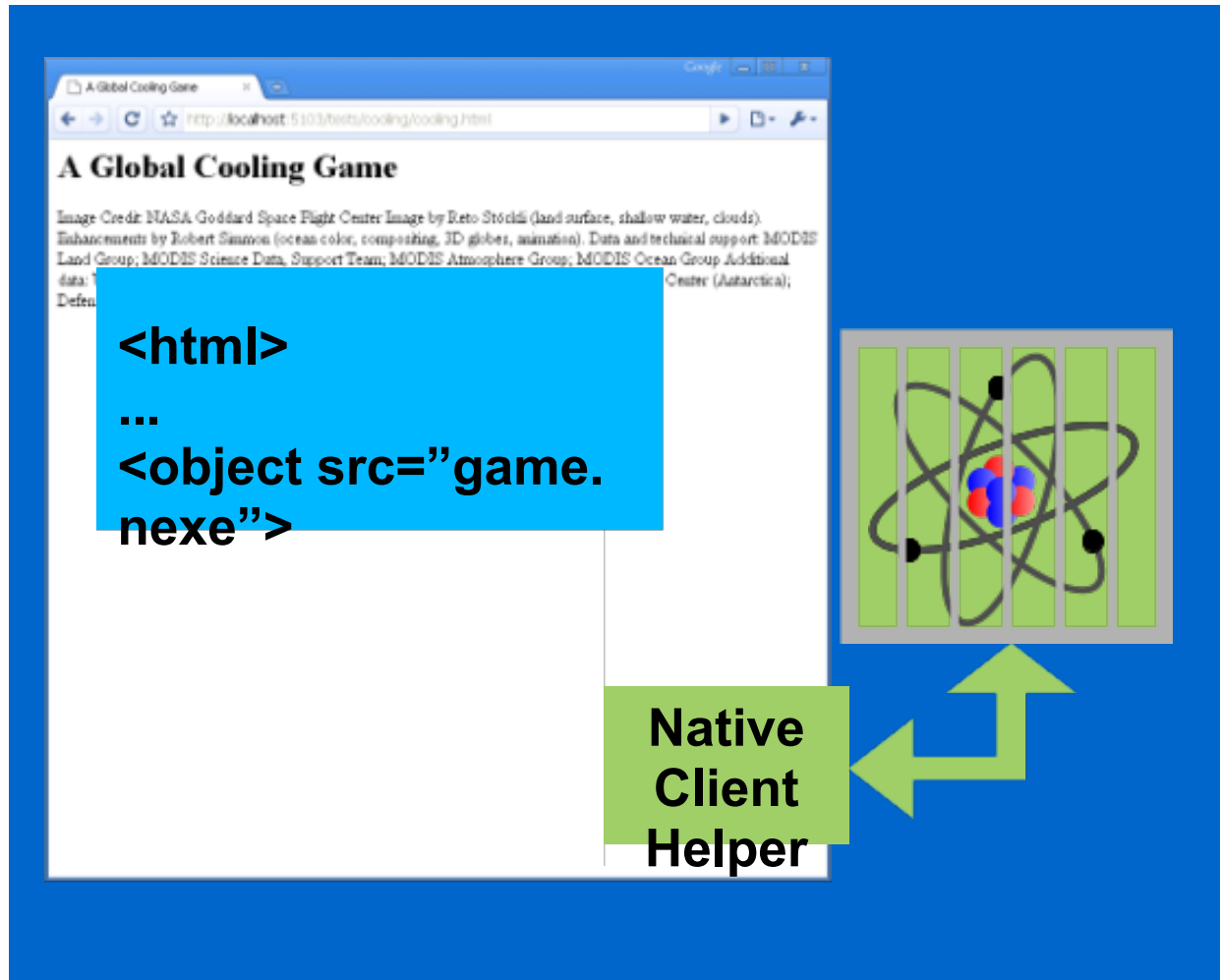
Overlaid on the screenshot are two callout boxes:

- A blue box containing the following HTML code:

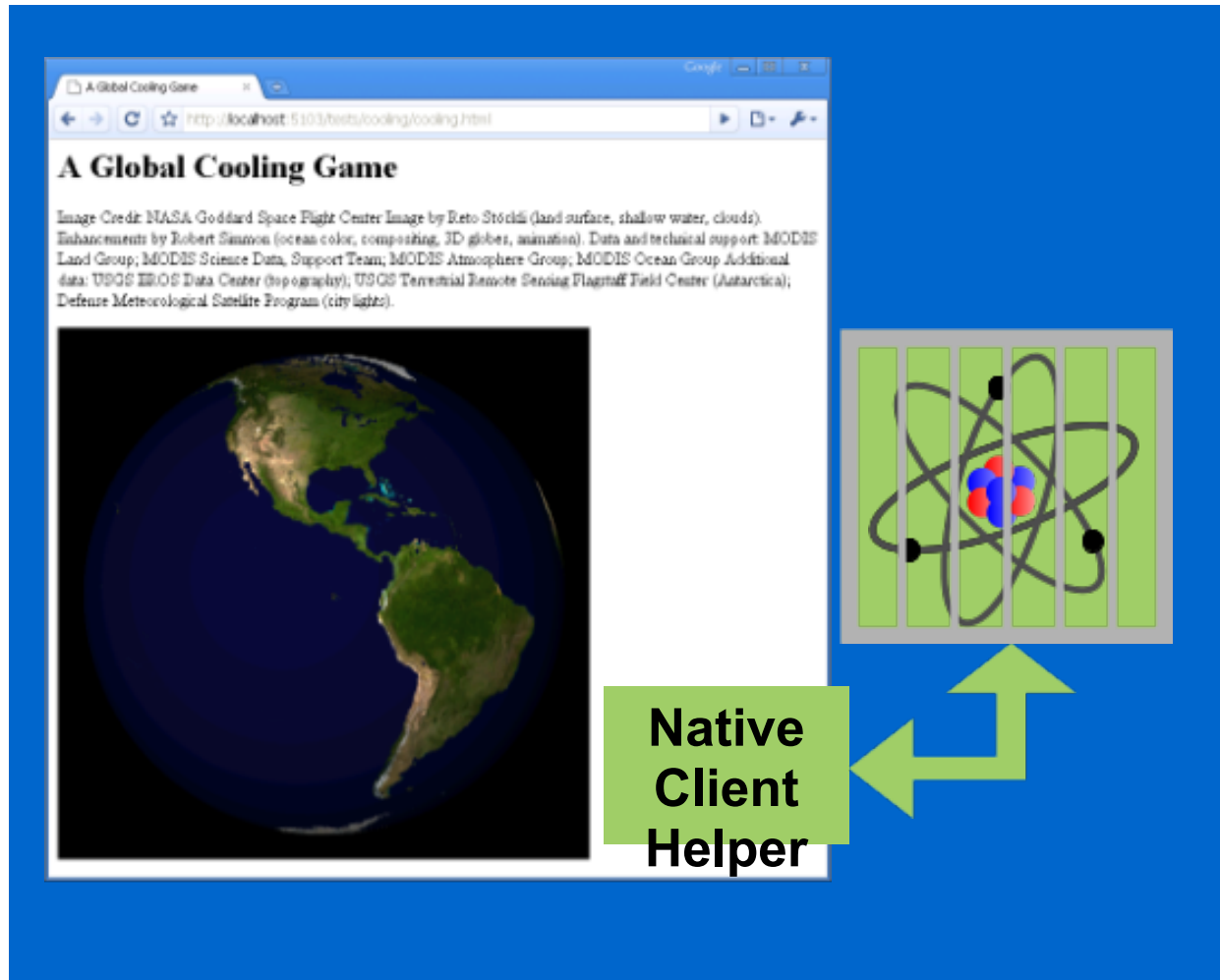
```
<html>
...
<object src="game.
nexe">
```
- A green box containing the text "Native Client Helper".

To the right of the code boxes is a stylized illustration of an atom with a central nucleus of red and blue spheres and three black electron orbits, all contained within a grey frame with vertical green bars.

# The Life of a NaCl-Enabled Web App



# The Life of a NaCl-Enabled Web App



The image shows a screenshot of a web browser window titled "A Global Cooling Game". The address bar shows the URL "http://localhost:5103/tests/cooling/cooling.html". Below the title, there is a paragraph of text: "Image Credit: NASA Goddard Space Flight Center Image by Reto Stöckli (land surface, shallow water, clouds). Enhancements by Robert Simon (ocean color, compositing, 3D globe, animation). Data and technical support: MODIS Land Group; MODIS Science Data, Support Team; MODIS Atmosphere Group; MODIS Ocean Group Additional data: USGS EOS Data Center (topography); USGS Terrestrial Remote Sensing Flagstaff Field Center (Antarctica); Defense Meteorological Satellite Program (city lights)." Below the text is a 3D rendering of the Earth showing landmasses and oceans. To the right of the globe is a diagram of a Native Client Helper, which is a stylized atomic symbol with a central nucleus of red and blue spheres and three black electron orbits. The diagram is enclosed in a grey frame with vertical bars, and a green arrow points from it to a green box labeled "Native Client Helper".



# Native Client Security



# Native Client Security

Our goal: make native code at least as safe as JavaScript.

Steps we've taken include:

- Multiple internal security reviews
- Open sourced our system; encouraged critical public review
- Published a peer reviewed technical paper in the *IEEE Symposium on Security and Privacy*
  - See <http://oakland09.cs.virginia.edu>
- Held an Security Contest

# Native Client Security Contest

- 25 February to 5 May 2009
- Over 400 teams and 600 individuals participated
- 22 valid issues submitted
- Profile of valid issues:
  - Inner sandbox (1 + 1 prior to contest)
  - Outer sandbox (not yet enabled)
  - Binary module loader
  - Trampoline interfaces (1 – direction flag)
  - IMC communications interface
  - NPAPI interface (3 – including same origin issues)
  - System calls (1 – unmap / map)
  - Browser integration (8)

# Example Security Contest Issues

#50: `data16` prefix with two-byte control flow instructions

- We had assumed `data16` only applied to data arithmetic, and was safe with all two-byte instructions
- Problem: `data16` also impacts some address calculations
- Solution: disallow `data16` for most two-byte instructions
- Solution: protect bottom 64KB of the address space

#51: stack-smashing attack via `eflags` direction flag

- `eflags` state was preserved across trusted runtime calls
- Problem: Some Windows APIs use `rep movs` without checking flag direction

- Solution: use `cld` to clear flags during trusted runtime calls



# **NaCl Today and Tomorrow**





# Native Client Research Release

## Today

- NPAPI plugin
- x86-32 only
- Raster graphics
- Mirrored public SVN

# Native Client Developer Release...

## Today

- NPAPI plugin
- x86-32 only
- Raster graphics
- Mirrored public SVN

## *The Future*

- ***Built into browser***
  - ***Web Workers***
  - ***Revised NPAPI***
- ***x86-32, x86-64, ARM***
- ***O3D integration***
- ***Develop off public SVN***

# Preview: Native Web Workers

## Web Workers: Simple threading model for the browser

- No shared data, no DOM access
- `postMessage`, `XMLHttpRequest`, `openDatabase`
- See specification at <http://whatwg.org/ww>

## Goals of Native Web Workers:

- Support workers in C, C++, Ruby, ...
- Maintain the simplicity of the Web Worker model
- Support 'low frequency' applications



# Demo: Native Web Workers



# Preview: Revised NPAPI

- Plugin use today is very limited
  - Well known security issues
  - Pop-up boxes asking unreasonable questions
  - API is under-specified
  - Web portability falls apart
- Creating a brighter future for plugins
  - Address known misfeatures of NPAPI, ActiveX
  - Avoid limitations of Web Workers
    - High frequency applications
    - Real-time applications
    - Synchronous DOM access



# An H.264 Video Player



# Porting a H.264 transcoder from Linux

- Based on a Google internal H.264 decoder
- Original test code decoded H.264 into raw frames
- 20-line change to create simple video player
- 230-lines to add audio and frame-rate control

Porting a Linux application to Native Client can be very simple.

# g264\_unittest.c

```
int main(int argc, char *argv[]) {
...
#ifdef __native_client__
int r = nacl_multimedia_init(NACL_SUBSYSTEM_VIDEO);
if (-1 == r) {
printf("Multimedia system failed to initialize! errno: %d\n", errno);
exit(-1);
}
r = nacl_video_init(NACL_VIDEO_FORMAT_RGB, image_width, image_height);
if (-1 == r) {
printf("Video subsystem failed to initialize! errno; %d\n", errno);
exit(-1);
}
write_file_ptr = NULL;
#else
write_file_ptr = fopen("output.yuv", "wb");
#endif
...
}
```



# g264\_unittest.c

```
...
#ifdef __native_client__
YV12toRGB24_generic(img->luma_sample, img->luma_width,
img->chroma_sample[0], img->chroma_sample[1],
img->chroma_width, RGB24_out,
img->luma_width, img->luma_height,
img->luma_width);

r = nacl_video_update(RGB24_out);
if (-1 == r) {
printf("nacl_video_update() returned %d\n", errno);
}
#else
fwrite(img->luma_sample, frame_size, 1, write_file_ptr);
fwrite(img->chroma_sample[0], frame_size>>2, 1, write_file_ptr);
fwrite(img->chroma_sample[1], frame_size>>2, 1, write_file_ptr);
#endif
...
```



# Demo: H.264 Video Decoder





# Demo: Native Client Darkroom



# Contribute

Please visit us at <http://code.google.com/p/nativeclient>

- Write new apps
- Port existing C/C++ libraries
- Help us test

# Questions?

**On the web:** <http://code.google.com/p/nativeclient>

## **Today at Google IO:**

Client Fireside Chat: 1pm

Native Client Office Hours: 3pm

## **Related projects:**

Chromium: <http://dev.chromium.org>

O3D: <http://code.google.com/p/o3d>

Google™

