

Chromium tip for beginners

Who are we?



Jeongeun Kim

(je_julie.kim@samsung.com, @chromium.org)

- Chromium Committer
- Working on WebAccessibility



Miyoung Shin

(myid.shin@samsung.com, @chromium.org)

- Chromium Committer
- Working on Input & Layout

Chromium

Activity

30 Day Summary

Apr 26 2015 — May 26 2015

- 11410 [Commits](#)
- 909 [Contributors](#)
- including [152 new contributors](#)

12 Month Summary

May 26 2014 — May 26 2015

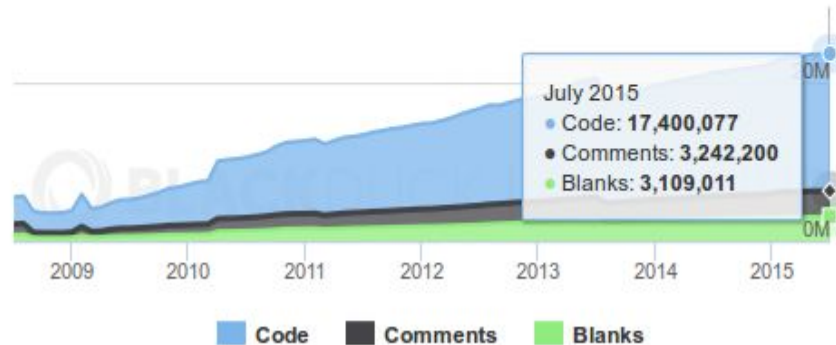
- 61454 [Commits](#)
- Down -89775 (59%) from previous 12 months
- 2457 [Contributors](#)
- Up + 1161 (89%) from previous 12 months

Languages



C++	57%	C	12%
JavaScript	9%	26 Other	22%

Lines of Code



A lot of things

- design documents :
<https://www.chromium.org/developers/design-documents>
- mailing groups : chromium-dev, blink-dev, input-dev, security-dev, ax-dev....
- new features are on going
- refactoring consistently codes

Through this session



Getting Start

- Choose one of machine :

Linux, Android, ChromeOS, cast, OSX, iOS, Windows,...

강사 권장 : Linux, 64 bit, 뽕뽕한 H/W

- Depot Tool (Linux/Mac 기준)

`$ git clone https://chromium.googlesource.com/chromium/tools/depot\_tools.git`

Add path in ~/.bashrc or ~/.zshrc

`$ export PATH=$PATH:/path/to/depot_tools`

- Getting code (it's a coffee time)

`$ fetch chromium` # Basic checkout for desktop Chromium

`$ fetch andorid` # Crhomium checkout for Android Platform

- For Linux (only once)

`$ cd src && ./build/install-build-deps.sh`

- Repo sync & Run hooks

`$ gclient sync` or `$gclient runhooks`

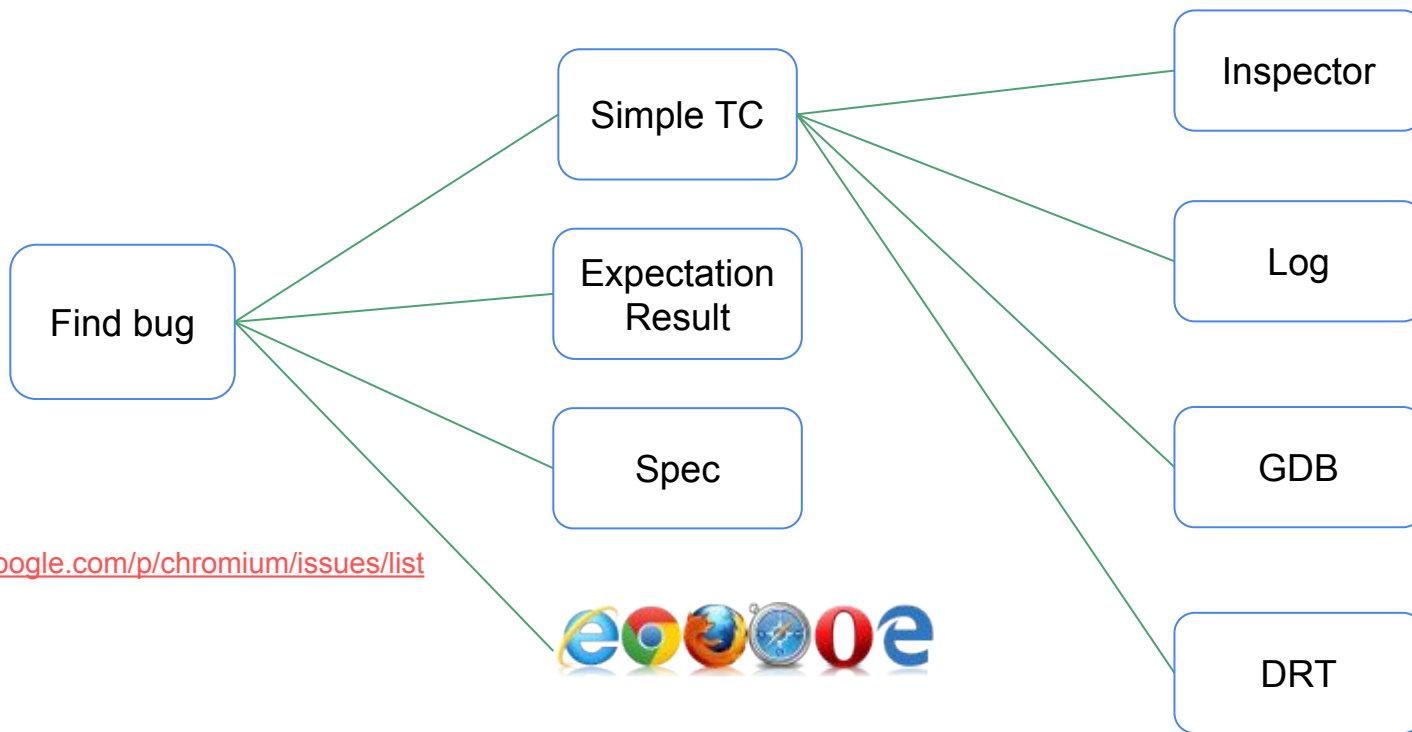
- Build

`$ ninja -C out/Debug chrome`

- Run

`$ ./out/Debug/chrome`

Maybe we will



<https://code.google.com/p/chromium/issues/list>

예제 1 - hover issue

described an issue like

Steps to reproduce the problem:

1. Clone the github repo and open the chrome-iframe-hover/iframe-hover.html file.
2. Hover on the item in the iframe (Yellow background. Turns red when hovered)
3. Move the mouse **SLOWLY** to the overlapped element further up the page (Contains the content "MENU")

What is the expected behavior?

Expect the iframe to lose hover, but it doesn't. Moving the mouse quickly seems not to create the issue.

What went wrong?

Hover is not lost from the iframe. Querying it with JS also reports the it still has hover. e.g. `$('*:hover')` returns the element when the mouse is no longer in the iframe.

Sample TC :

<https://github.com/tgandrews/bug-hunting/tree/master/chrome-iframe-hover>

Inspector 활용

yellow -> red 는 hover 속성에 의해 발생

```
div {  
  display: block;  
  height: 100px;  
  width: 100%;  
  background-color: yellow;  
}  
div:hover {  
  background-color: red;  
}
```

hover 속성은 ? node 가 이동되면 hover 속성은 clear 되어야 함.

Debugging Point !! cursor 를 slow 로 움직일 때 hover 속성이 clear 되지 못했을 가능성

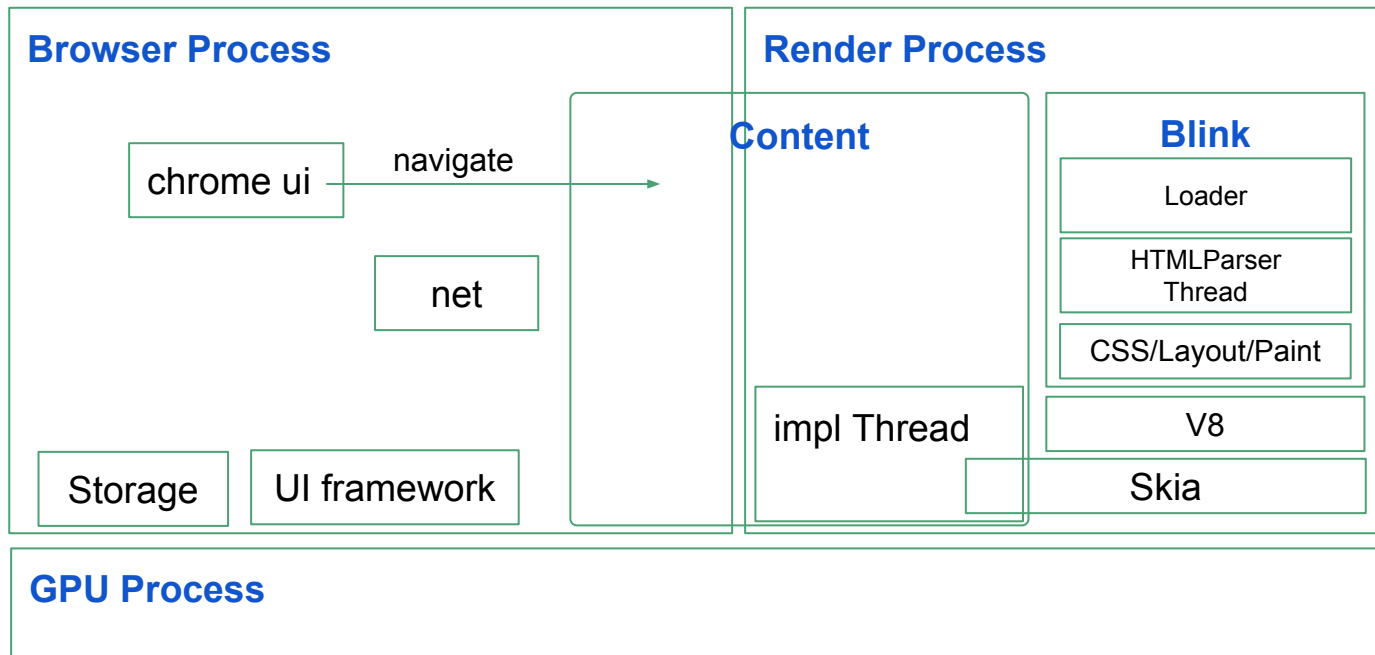
잠깐 여기서! 디렉토리 구조를 알아보자

src

- | - base : generic utility like string, message
- | - breakpad : crash report
- | - build : Build-related configuration
- | - cc : graphic compositor
- | - chrome : chrome browser UI and functionality as history/bookmark
- | - **content** : Interface layer between chrome and WebKit(Blink) for a multi-process sandboxed browser
 - | - browser : I/O and communication with the child processes
 - | - gpu : Code for the GPU process
 - | - **renderer** : talks to browser for I/O.
- | - extension : chrome extension
- | - gpu : work on gpu process, implement gl command
- | - ipc : IPC among Processes
- | - net : network libralies
- | - skia : 2d graphic Engine
- | - third_party : A bunch of external libraries
 - | - **WebKit** : Rendering engine
- | - ui : UI framework
- | - v8 : javascript engine

<https://www.chromium.org/developers/how-tos/getting-around-the-chrome-source-code>

Simple Block



Primary Debugging Points

- Loading
 - FrameLoader.cpp (blink)
 - url_request.cc (net)
- Input : keyboard, mouse, touch(gesture)
 - EventHandler.cpp
- Layout
 - FrameView.cpp: layout()
- Paint
 - CompositingLayerMapping.cpp: paintContents()
- Compositor
 - thread_proxy.cc: SetDeferCommits() (main thread -> impl thread)
 - layer_tree_host_impl.cc: BeginCommit(), CommitComplete() (impl thread)
- V8 Binding : script to generate idl files, non-generated files
 - third_party/WebKit/Source/bindings

GDB - RenderProcess

```
$ out/Debug/content_shell --no-sandbox --renderer-startup-dialog test.html
```

```
[10506:10506:0904/174115:2537132352130:ERROR:child_process.cc(131)] Renderer (10506) paused  
waiting for debugger to attach. Send SIGUSR1 to unpause.
```

```
$ gdb -p 10506
```

```
$ (gdb) b blink::LayoutView::layout
```

```
$ (gdb) c
```

```
$ kill -s SIGUSR1 10506
```

GDB - RenderProcess

```
myid@myid-400B4C-400B5C-200B4C-200B5C: ~/Dev/blinkproj/src
```

```
Inferior 1 [process 3746] will be killed.
```

```
Quit anyway? (y or n) y
```

```
myid@myid-400B4C-400B5C-200B4C-200B5C:~/Dev/blinkproj/src$ gdb -tui -ex=r --args out/Debug/content_shell --no-sandbox --renderer-startup-dialog ~/www/soscon2015.html
```

```
myid@myid-400B4C-400B5C-200B4C-200B5C:~/Dev/blinkproj/src$ out/Debug/content_shell --no-sandbox
[3963:3963:1018/151737:5191757043:ERROR:browser_main_loop.cc(204)] Running without the SUID sandbox! See https://code.google.com/p/chromium/wiki/LinuxSUIDSandboxDevelopment for more information on developing with the sandbox on.
[3963:3963:1018/151737:5191814768:ERROR:proxy_service.cc(1510)] ProxyConfigService for Chromium should be created in profile_io_data.cc::CreateProxyConfigService and this should be used only for examples.
[3981:3981:1018/151738:5192054218:ERROR:child_process.cc(131)] Renderer (3981) paused waiting for debugger to attach. Send SIGUSR1 to unpause.
```

```
^C
```

```
myid@myid-400B4C-400B5C-200B4C-200B5C:~/Dev/blinkproj/src$ out/Debug/content_shell --no-sandbox --renderer-startup-dialog ~/www/soscon2015.html
```

```
[4063:4063:1018/152646:5740564614:ERROR:browser_main_loop.cc(204)] Running without the SUID sandbox! See https://code.google.com/p/chromium/wiki/LinuxSUIDSandboxDevelopment for more information on developing with the sandbox on.
[4063:4063:1018/152646:5740671557:ERROR:proxy_service.cc(1510)] ProxyConfigService for Chromium should be created in profile_io_data.cc::CreateProxyConfigService and this should be used only for examples.
[4081:4081:1018/152646:5740846671:ERROR:child_process.cc(131)] Renderer (4081) paused waiting for debugger to attach. Send SIGUSR1 to unpause.
```

```
myid@myid-400B4C-400B5C-200B4C-200B5C:~/Dev/blinkproj/src$ kill -s SIGUSR1 4081
```

```
myid@myid-400B4C-400B5C-200B4C-200B5C: ~
```

```
myid@myid-400B4C-400B5C-200B4C-200B5C:~$ kill -s SIGUSR1 4081
```

```
myid@myid-400B4C-400B5C-200B4C-200B5C: ~
```

```
myid@myid-400B4C-400B5C-200B4C-200B5C:~$ sudo gdb -p 4081
```

```
GNU gdb (Ubuntu 7.7.1-0ubuntu5~14.04.2) 7.7.1
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word".
Attaching to process 4081
Reading symbols from /home/myid/Dev/blinkproj/src/out/Debug/content_shell...done.
Reading symbols from /home/myid/Dev/blinkproj/src/out/Debug/lib/libui_base.so...done.
Loaded symbols for /home/myid/Dev/blinkproj/src/out/Debug/lib/libui_base.so
Reading symbols from /home/myid/Dev/blinkproj/src/out/Debug/lib/libgl_in_process.so...done.
Loaded symbols for /home/myid/Dev/blinkproj/src/out/Debug/lib/libgl_in_process.so
Reading symbols from /home/myid/Dev/blinkproj/src/out/Debug/lib/libstorage_common.so...done.
```

GDB - BrowserProcess

```
$ gdb -tui -ex=r --args out/Debug/content_shell --disable-seccomp-sandbox test.html
```

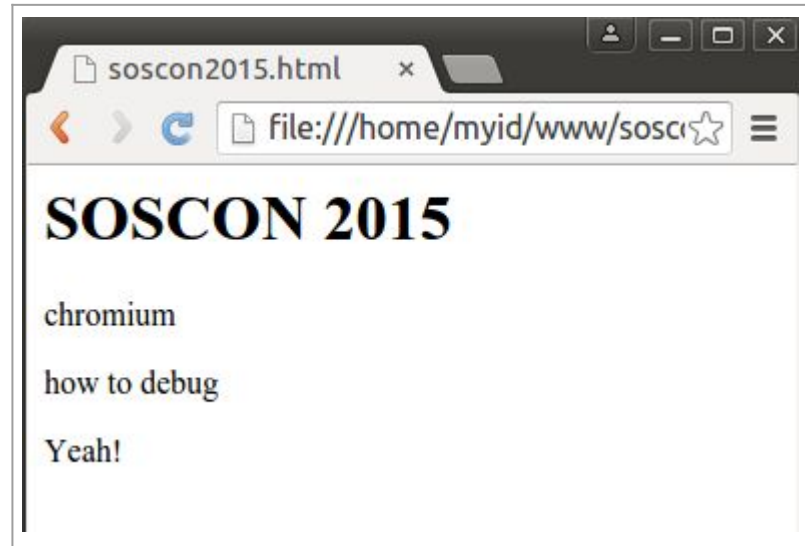
```
browser/renderer_host/render_view_host_impl.cc
1134     }
1135
1136     void RenderViewHostImpl::OnStartDragging(
1137         const DropData& drop_data,
1138         WebDragOperationsMask drag_operations_mask,
1139         const SkBitmap& bitmap,
1140         const gfx::Vector2d& bitmap_offset_in_dip,
1141         const DragEventSourceInfo& event_info) {
B+ 1142     RenderViewHostDelegateView* view = delegate_>GetDelegateView();
> 1143     if (!view)
1144         return;
1145
1146     DropData filtered_data(drop_data);
1147     RenderProcessHost* process = GetProcess();
dl-debug.c:74: No such file or directory.
dl-debug.c:74: No such file In: content::RenderViewHostImpl::OnStartDragging 1143

Breakpoint 1, content::RenderViewHostImpl::OnStartDragging (this=0x5e774a7d360, drop_data=...,
    drag_operations_mask=blink::WebDragOperationEvery, bitmap=..., bitmap_offset_in_dip=..., event_info=...)
    at ../../content/browser/renderer_host/render_view_host_impl.cc:1142
(gdb) n
```

https://chromium.googlesource.com/chromium/src/+master/docs/linux_debugging.md#Basic-browser-process-debugging

Simple Page

```
<html>
  <h1>SOSCON 2015</h1>
  <div>
    chromium
    <p>how to debug</p>
    Yeah!
  </div>
</html>
```



Blink tree - DOM tree

(gdb) print this->showTreeForThis()

```
BODY      0xb11a64141a8
  H1       0xb11a6414010
    #text  0xb11a6420160 "SOSCON 2015"
  #text    0xb11a64201d0 "\n "
* DIV     0xb11a6414098
  #text    0xb11a64200f0 "\n  chromium\n  "
  P        0xb11a6414120
    #text  0xb11a6420010 "how to debug"
    #text  0xb11a6420240 "\n  Yeah!\n  "
  #text    0xb11a6420080 "\n\n"
```

Blink tree - Layout tree

(gdb) print this->showLayoutTreeForThis()

```
LayoutView 0x296826e04010    #document    0xb11a6404010
  LayoutBlockFlow 0x296826e1c010    HTML    0xb11a64142b8
    LayoutBlockFlow 0x296826e1c110    BODY    0xb11a64141a8
      LayoutBlockFlow 0x296826e1c310    H1    0xb11a6414010
        LayoutText 0x296826e201f0    #text    0xb11a6420160 "SOSCON 2015"
      LayoutBlockFlow 0x296826e1c610    DIV    0xb11a6414098
        LayoutBlockFlow (anonymous) 0x296826e1c410
*      LayoutText 0x296826e20150    #text    0xb11a64200f0 "\n    chromium\n    "
      LayoutBlockFlow 0x296826e1c510    P    0xb11a6414120
        LayoutText 0x296826e200b0    #text    0xb11a6420010 "how to debug"
      LayoutBlockFlow (anonymous) 0x296826e1c210
        LayoutText 0x296826e20010    #text    0xb11a6420240 "\n    Yeah!\n    "
```

Blink tree - dump Layout Tree

```
$ out/Debug/content_shell --run-layout-test soscon2015.html
```

```
Content-Type: text/plain
layer at (0,0) size 800x600
  LayoutView at (0,0) size 800x600
layer at (0,0) size 800x600
  LayoutBlockFlow {HTML} at (0,0) size 800x600
    LayoutBlockFlow {BODY} at (8,8) size 784x584
      LayoutBlockFlow {H1} at (0,0) size 784x37
        LayoutText {#text} at (0,0) size 204x37
          text run at (0,0) width 204: "SOSCON 2015"
      LayoutBlockFlow {DIV} at (0,58.44) size 784x86
        LayoutBlockFlow (anonymous) at (0,0) size 784x18
          LayoutText {#text} at (0,0) size 66x18
            text run at (0,0) width 66: "chromium"
        LayoutBlockFlow {P} at (0,34) size 784x18
          LayoutText {#text} at (0,0) size 88x18
            text run at (0,0) width 88: "how to debug"
        LayoutBlockFlow (anonymous) at (0,68) size 784x18
          LayoutText {#text} at (0,0) size 40x18
            text run at (0,0) width 40: "Yeah!"
```

Print Backtrace

non-component build vs component build

```
+#include <base/debug/stack_trace.h>
namespace blink {

namespace {
@@ -162,6 +163,9 @@ void LayoutObject::operator delete(void* ptr)

LayoutObject* LayoutObject::createObject(Element* element, const ComputedStyle& style)
{
+   base::debug::StackTrace st;
+   st.Print();

--- a/third_party/WebKit/Source/core/layout/LayoutObject.cpp
+++ b/third_party/WebKit/Source/core/layout/LayoutObject.cpp
@@ -162,6 +162,8 @@ void LayoutObject::operator delete(void* ptr)

LayoutObject* LayoutObject::createObject(Element* element, const ComputedStyle&
{
+   BACKTRACE();
+
   ASSERT(isAllowedToModifyLayoutTreeStructure(element->document()));
```

Backtrace

```
#0 0x0000006df25e base::debug::StackTrace::StackTrace()
#1 0x0000037d93c2 blink::LayoutObject::createObject()
#2 0x000002c59ead blink::Element::createLayoutObject()
#3 0x000002c82d64 blink::LayoutTreeBuilderForElement::createLayoutObject()
#4 0x000002c656df blink::LayoutTreeBuilderForElement::createLayoutObjectIfNeeded()
#5 0x000002c5a739 blink::Element::attach()
#6 0x000002c9e2ba blink::Node::reattach()
#7 0x000002c5baf6 blink::Element::recalcOwnStyle()
#8 0x000002c5b5c3 blink::Element::recalcStyle()
#9 0x000002c175aa blink::Document::updateStyle()
#10 0x000002c16f63 blink::Document::updateLayoutTree()
#11 0x000002370517 blink::Document::updateLayoutTreeIfNeeded()
#12 0x00000331ca06 blink::FrameView::performPreLayoutTasks()
#13 0x00000331dd2d blink::FrameView::layout()
#14 0x00000232b687 blink::WebViewImpl::resizeViewWhileAnchored()
#15 0x00000232b8d5 blink::WebViewImpl::resize()
#16 0x000004fd08b1 content::RenderWidget::Resize()
#17 0x000004fd6547 content::RenderWidget::OnResize()
#18 0x000004fb79ea content::RenderViewImpl::OnResize()
#19 0x000004faa022 content::RenderViewImpl::Initialize()
#20 0x000004faca01 content::RenderViewImpl::Create()
#21 0x000004f9b256 content::RenderThreadImpl::OnCreateNewView()
```

Chromium Command Line Options

content/public/common/content_switches.cc

```
// Causes the browser process to crash on startup.
const char kBrowserCrashTest[] = "crash-test";

// Path to the exe to run for the renderer and plugin subprocesses.
const char kBrowserSubprocessPath[] = "browser-subprocess-path";

// Dumps extra logging about plugin loading to the log file.
const char kDebugPluginLoading[] = "debug-plugin-loading";

// Sets the tile size used by composited layers.
const char kDefaultTileWidth[] = "default-tile-width";
const char kDefaultTileHeight[] = "default-tile-height";
```

\$ out/Debug/content_shell --no-sand-box

<http://peter.sh/examples/?/chromium-switches.html>

Chromium Log

```
$ out/Debug/content_shell --enable-logging --v=1
```

```
[3716:3732:1022/001755:3525091541:VERBOSE1:resource_loader.cc(360)] OnReadCompleted: "https://www.google.co.kr/exte
rn_chrome/72e1b64e6f93a412.js?bav=on.2,or." bytes_read = 11338
[3716:3732:1022/001755:3525091621:VERBOSE1:resource_loader.cc(360)] OnReadCompleted: "https://www.google.co.kr/exte
rn_chrome/72e1b64e6f93a412.js?bav=on.2,or." bytes_read = 0
[3716:3732:1022/001755:3525091643:VERBOSE1:resource_loader.cc(637)] ResponseCompleted: https://www.google.co.kr/ext
ern_chrome/72e1b64e6f93a412.js?bav=on.2,or.
```

content/browser/loader/resource_loader.cc

```
358 void ResourceLoader::OnReadCompleted(net::URLRequest* unused, int bytes_read) {
359     DCHECK_EQ(request.get(), unused);
360     DVLOG(1) << "OnReadCompleted: \"" << request->url().spec() << "\"
361     | | | | << " bytes_read = " << bytes_read;
362
363     // bytes_read == -1 always implies an error.
364     if (bytes_read == -1 || !request->status().is_success()) {
365         ResponseCompleted();
366         return;
367     }
```

Blink Log

```
$ out/Debug/content_shell --blink-platform-log-channels=ResourceLoading
```

```
ResourceFetcher::requestResource 'https://www.google.com/', charset '', priority=-1, forPreload=0, type=MainResource
Loading Resource for 'https://www.google.com/'.
MemoryCache::add Added 'https://www.google.com/', resource 0x35c198c10010
Evicting resource 0x35c198c10010 for 'https://www.google.com/' from cache
ResourceFetcher::requestResource 'https://www.google.co.kr/images/nav_logo231.png', charset '', priority=-1, forPreload=1, type=Image
```

third_party/WebKit/Source/core/fetch/ResourceFetcher.cpp

```
334     bool isStaticData = request.resourceRequest().url().protocolIsData() || substituteData.isVa
335     if (isStaticData)
336         preCacheData(request, factory, substituteData);
337
338     KURL url = request.resourceRequest().url();
339     TRACE_EVENT1("blink", "ResourceFetcher::requestResource", "url", urlForTraceEvent(url));
340
341     WTF_LOG(ResourceLoading, "ResourceFetcher::requestResource '%s', charset '%s', priority=%d,
```

Blink Log - WTFLogChannel

BackForward/Editing/Events/Frames/FTP/History/IconDatabase...

third_party/WebKit/Source/platform/Logging.cpp

```
WTFLogChannel* getChannelFromName(const String& channelName)
{
    if (!(channelName.length() >= 2))
        return 0;

    if (equalIgnoringCase(channelName, String("BackForward")))
        return &LogBackForward;

    if (equalIgnoringCase(channelName, String("Editing")))
        return &LogEditing;

    if (equalIgnoringCase(channelName, String("Events")))
        return &LogEvents;

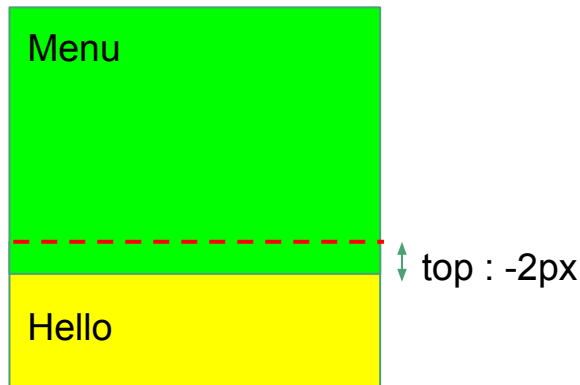
    if (equalIgnoringCase(channelName, String("Frames")))
        return &LogFrames;
```

Hover 그 문제는?

```
<body>
  <div id="menu">MENU</div>
  <iframe id="content" style="width:100%; height:300px;" src=
    "./iframe-content.html">
  </iframe>
</body>
```

```
#document
  <!DOCTYPE html>
  <html>
    <head>
```

```
#content {
  border: 1px solid black;
  width: 100%;
  height: 300px;
  position: relative;
  top: -2px;
  z-index: 1;
}
```



디버깅을 통해 알아낸 내용

- 일반적인 동작 : **iframe** 간 **mouse** 가 이동이 발생할 때, **last frame** 의 **hover** 속성을 **clear** 시킴
- 원인 : **last frame** 에서 **mouse leave** 를 **mouse move** 로 처리되어 **last frame(Hello)** 이 **main frame(Menu)**로 변경되나 **hover** 를 **clear** 시키지 못함
- 수정 : **frame mouse leave** 이벤트로 변경
- 이후, 수많은 잠재 이슈들 발현!!!! 아직도 커뮤니티는 ongoing..

감사합니다
