Ablation Tutorial

Augmenting Static Analysis

Paul Mehta

paul@paulmehta.com | pmehta@Cylance.com

What is Ablation?

- Ablation is a tool that extracts information from processes as they execute.

- It was designed to simplify the process of reverse engineering

Setup (summary)

- Download the Pintool Compiler Kit and unzip Abation.zip to \source\tools\
- Build release versions of
  - Ablation.dll
  - AblationClient.exe
  - PinTest.exe (if you want a simple test app)
- Copy the release builds to \ia32\bin\
- Run a sample test
  - pin.exe -t Ablation.dll -module pintest -output . -- PinTest.exe

Setup

- Visual Studio 2013
  - If you’re using 2012/2010, make sure you get the right VC++ runtime, and Pintool Compiler Kit
- Install Visual C++ 2013 Redistributable (x86)
  - https://www.microsoft.com/en-us/download/details.aspx?id=40784
- Download the Pintool kit (Rev. 71313 Feb 03, 2015 vc12)
  - https://software.intel.com/en-us/articles/pintool-downloads
  - http://software.intel.com/sites/landingpage/pintool/downloads/pin-2.14-71313-msvc12-windows.zip

Setup

- Extract the Pintool compiler kit, and copy the Ablation source folder to
  - *\pin-2.14-71313-msvc12-windows\source\tools\*
  - Create a Win32 release build
    - Copy *\pin-2.14-71313-msvc12-windows\source\tools\Ablation\Release\Ablation.dll* to *\pin-2.14-71313-msvc12-windows\ia32\bin\Ablation.dll*

- Create a release build of *AblationClient*
  - Copy *AblationClient.exe* to *\pin-2.14-71313-msvc12-windows\ia32\bin\AblationClient.exe*

Setup

- Use Windows 7
  - Pintool won’t work on Win10
- If you’re running Ablation in a VM, give it plenty of memory
  - I’m using 4gb
- Copy the folder *\pin-2.14-71313-msvc12-windows\ia32\bin*\ to the VM

Setup

- For a simple test app, build PinTest.exe
- Run
  - pin.exe -t Ablation.dll -module pintest -output . -- PinTest.exe

Using Ablation

- Launch
  - pin.exe -t Ablation.dll -module [modulename] -- application.exe
- Attach
  - pin.exe -pid [pid] -t Ablation.dll -module [modulename]
- Display help
  - Pin.exe -t Ablation.dll -h -- application.exe

Examples:

```
pin.exe -t Ablation.dll -module LibGLESv2 -verbose -- "c:\Program Files (x86)\Mozilla Firefox\firefox.exe" | AblationClientLite.exe LibGLESv2.ablation.py
pin.exe -pid 1234 -t Ablation.dll -module vgx
```

Ablation.dll command-line switches

Command-Line Switch	Default Value	Description
-module	[default]	Specify the module to instrument (without file extension). Ex. -module kernel32
-output	[default console]	Specify a file name for output. If not specified, console is used.
-verbose	[default false]	Includes additional output as comments.
-no_resolve_virtual_calls	[default false]	Don't resolve indirect calls.
-no_trace	[default false]	Don't trace basic blocks.
-append	[default false]	Do not include script header (appending to existing).
-trace_color	[default 0x7BF0D3]	The initial color (light green) for control flow tracing.
-defer_output	[default false]	Defer output till process exit. Otherwise, live output from live process.
-no_console	[default false]	Do not output to console.
-no_symbols	[default false]	Do not Load Symbols.
-symbol_path	[default]	List of paths separated with semicolons that is searched for symbols.
-h	[default 0]	Print help message (print help message)
-help	[default 0]	Print help message (print help message)

Examples

- pin.exe -t Ablation.dll -module pintest -output pintest.ablation.py -- PinTest.exe
- pin -pid 7660 -t Ablation.dll -module Flash32_20_0_0_228 –output .
- pin.exe -t Ablation.dll -module pintest -- PinTest.exe | AblationClient.exe pintest.ablation.py --show-delay
- pin.exe -t Ablation.dll -module LibGLESv2 -- "c:\Program Files (x86)\Mozilla Firefox\firefox.exe" https://www.shadertoy.com/ | AblationClient.exe
- pin.exe -t Ablation.dll -module pintest –verbose -- PinTest.exe | AblationClient.exe pintest.ablation.py --no-gui

AblationClient.exe command-line switches

Command-Line Switch	Default Value	Description
-a	[default false]	Append to existing log file.
-append	[default false]	Append to existing log file.
-show_delay	[default false]	Display elapsed time between messages more than 5 seconds apart.
-no_gui	[default false]	Do not display the GUI interface (used to change colors, etc.).
-filter	[default false]	Filter the output of unexpected script content.

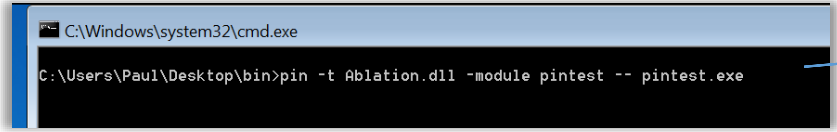
The AblationClient source is a bit rough, so don't expect much from it ;)

Examples

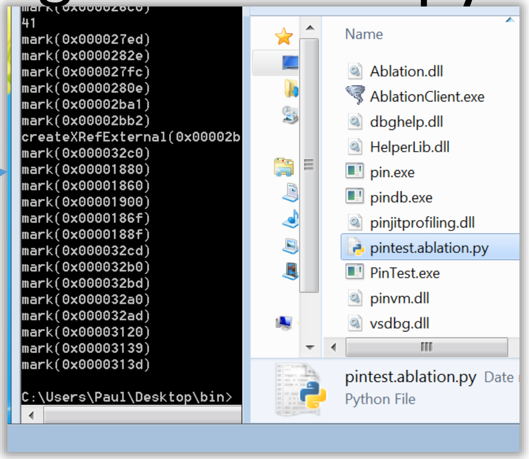
- pin.exe -t Ablation.dll -module pintest -output . -- PinTest.exe
- pin.exe -t Ablation.dll -module pintest -- PinTest.exe | AblationClient.exe pintest.ablation.py --show-delay
- pin.exe -t Ablation.dll -module pintest -verbose -- PinTest.exe | AblationClient.exe pintest.ablation.py --no-gui
- pin.exe -t Ablation.dll -module d3dcompiler_47 -- "c:\Program Files (x86)\Mozilla Firefox\firefox.exe" https://www.khronos.org/registry/webgl/sdk/tests/conformance/programs/ | AblationClient.exe d3dcompiler_47.ablation.py

Running the import script

- When ablation is complete, it will have generated a python script file
  - Probably named *module.ablation.py*

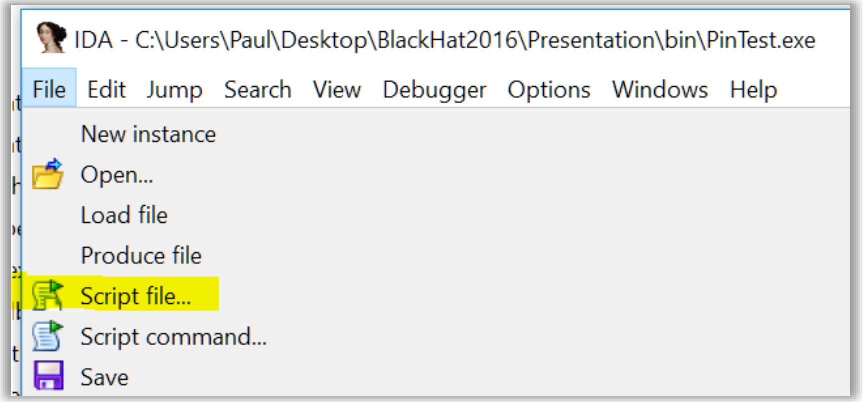


```
C:\Users\Paul\Desktop\bin>pin -t Ablation.dll -module pintest -- pintest.exe
```



```
mark(0x000028c0)
41
mark(0x000027ed)
mark(0x0000282e)
mark(0x000027fc)
mark(0x0000280e)
mark(0x00002ba1)
mark(0x00002bb2)
createXRefExternal(0x00002b
mark(0x000032c0)
mark(0x00001880)
mark(0x00001860)
mark(0x00001900)
mark(0x0000186f)
mark(0x0000188f)
mark(0x000032cd)
mark(0x000032b0)
mark(0x000032bd)
mark(0x000032a0)
mark(0x000032ad)
mark(0x00003120)
mark(0x00003139)
mark(0x0000313d)

C:\Users\Paul\Desktop\bin>
```

- Copy the script file to a location that IDA can access
  - Disassemble the module
  - Run the generated script file
- All the information will be imported



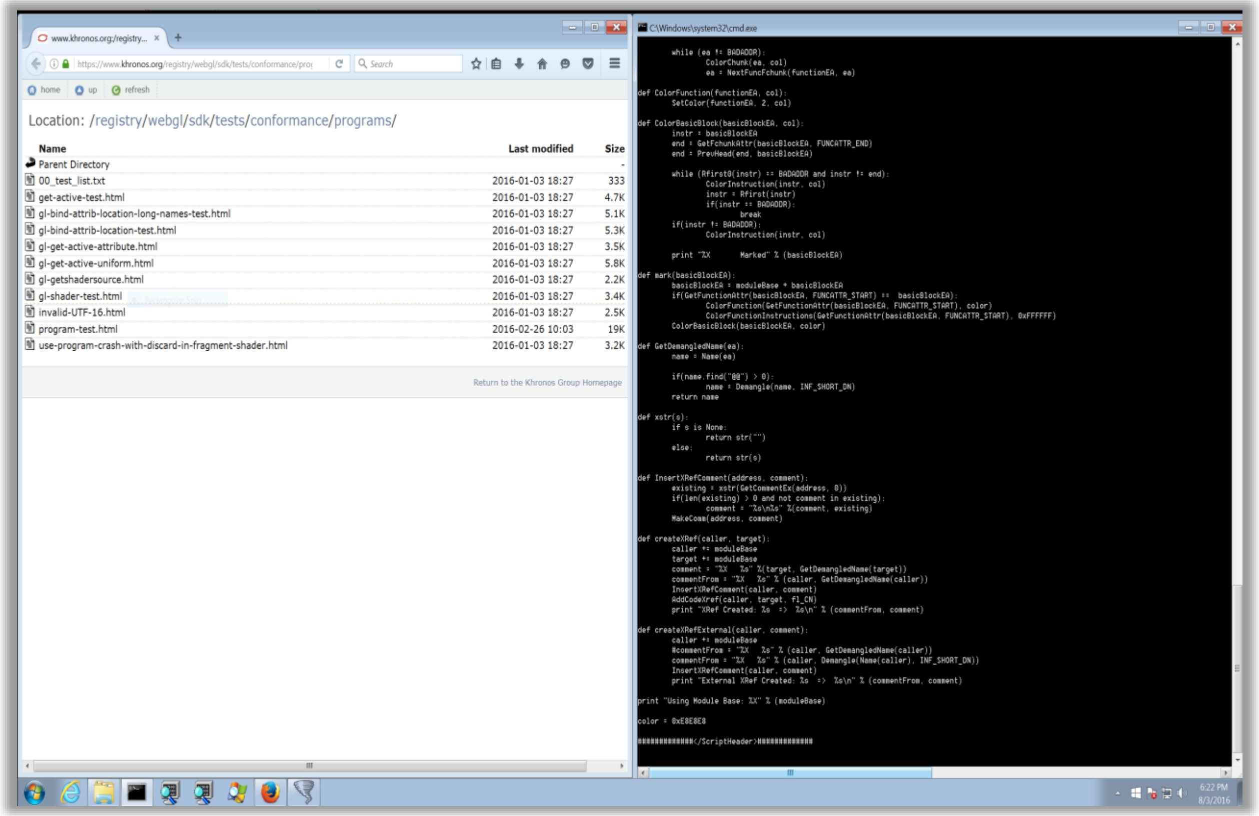
Diff Tutorial

Run Ablation the following arguments

- pin.exe -t Ablation.dll -module d3dcompiler_47 -trace_color 0xCCCCCC -- "c:\Program Files (x86)\Mozilla Firefox\firefox.exe" https://www.khronos.org/registry/webgl/sdk/tests/conformance/programs/ | AblationClient.exe d3dcompiler_47.ablation.py

What the arguments mean:

- pin.exe -t Ablation.dll -module d3dcompiler_47
  - Ablation is targeting d3dcompiler_47
- -trace_color 0xCCCCCC
  - We want the first set of BBl's (Basic Blocks) to be shaded grey
  - The default is light-green 0x7BF0D3
- Everything following ("--") is the command line for the application
- The output is then piped to AblationClient.exe which will be used to change the basic block trace shading.



www.khronos.org/registry...
https://www.khronos.org/registry/webgl/sdk/tests/conformance/pro
Search
home
up
refresh
C:\Windows\system32\cmd.exe

Location: /registry/webgl/sdk/tests/conformance/programs/

Name	Last modified	Size
Parent Directory		-
00_test_list.txt	2016-01-03 18:27	333
get-active-test.html	2016-01-03 18:27	4.7K
gl-bind-attrib-location-long-names-test.html	2016-01-03 18:27	5.1K
gl-bind-attrib-location-test.html	2016-01-03 18:27	5.3K
gl-get-active-attribute.html	2016-01-03 18:27	3.5K
gl-get-active-uniform.html	2016-01-03 18:27	5.8K
gl-getshadersource.html	2016-01-03 18:27	2.2K
gl-shader-test.html	2016-01-03 18:27	3.4K
invalid-UTF-16.html	2016-01-03 18:27	2.5K
program-test.html	2016-02-26 10:03	19K
use-program-crash-with-discard-in-fragment-shader.html	2016-01-03 18:27	3.2K

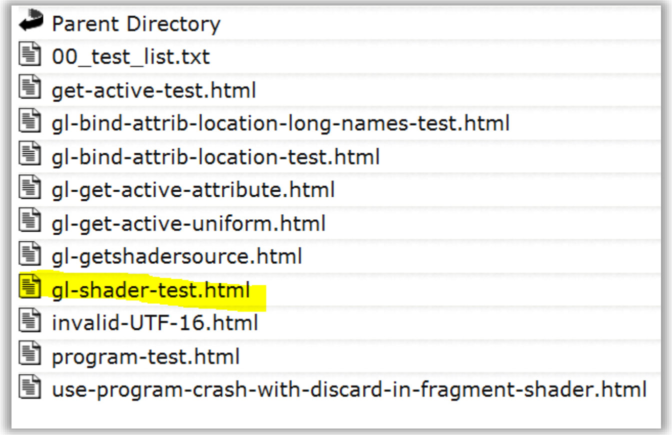
Return to the Khronos Group Homepage

```
        while (ea != BADADDR):
                ColorChunk(ea, col)
                ea = NextFuncFchunk(functionEA, ea)

def ColorFunction(functionEA, col):
        SetColor(functionEA, 2, col)

def ColorBasicBlock(basicBlockEA, col):
        instr = basicBlockEA
        end = GetFchunkAttr(basicBlockEA, FUNCATTR_END)
        end = PrevHead(end, basicBlockEA)

        while (Rfirst0(instr) == BADADDR and instr != end):
                ColorInstruction(instr, col)
                instr = Rfirst(instr)
                if(instr == BADADDR):
                        break
        if(instr != BADADDR):
                ColorInstruction(instr, col)

        print "%X       Marked" % (basicBlockEA)

def mark(basicBlockEA):
        basicBlockEA = moduleBase + basicBlockEA
        if(GetFunctionAttr(basicBlockEA, FUNCATTR_START) ==  basicBlockEA):
                ColorFunction(GetFunctionAttr(basicBlockEA, FUNCATTR_START), color)
                ColorFunctionInstructions(GetFunctionAttr(basicBlockEA, FUNCATTR_START), 0xFFFFFF)
        ColorBasicBlock(basicBlockEA, color)

def GetDemangledName(ea):
        name = Name(ea)

        if(name.find("@@") > 0):
                name = Demangle(name, INF_SHORT_DN)
        return name

def xstr(s):
        if s is None:
                return str("")
        else:
                return str(s)

def InsertXRefComment(address, comment):
        existing = xstr(GetCommentEx(address, 0))
        if(len(existing) > 0 and not comment in existing):
                comment = "%s\n%s" %(comment, existing)
        MakeComm(address, comment)

def createXRef(caller, target):
        caller += moduleBase
        target += moduleBase
        comment = "%X   %s" %(target, GetDemangledName(target))
        commentFrom = "%X   %s" % (caller, GetDemangledName(caller))
        InsertXRefComment(caller, comment)
        AddCodeXref(caller, target, fl_CN)
        print "XRef Created: %s  =>  %s\n" % (commentFrom, comment)

def createXRefExternal(caller, comment):
        caller += moduleBase
        #commentFrom = "%X   %s" % (caller, GetDemangledName(caller))
        commentFrom = "%X   %s" % (caller, Demangle(Name(caller), INF_SHORT_DN))
        InsertXRefComment(caller, comment)
        print "External XRef Created: %s  =>  %s\n" % (commentFrom, comment)

print "Using Module Base: %X" % (moduleBase)

color = 0xE8E8E8

############</ScriptHeader>############
```

6:22 PM
8/3/2016

Diff Tutorial

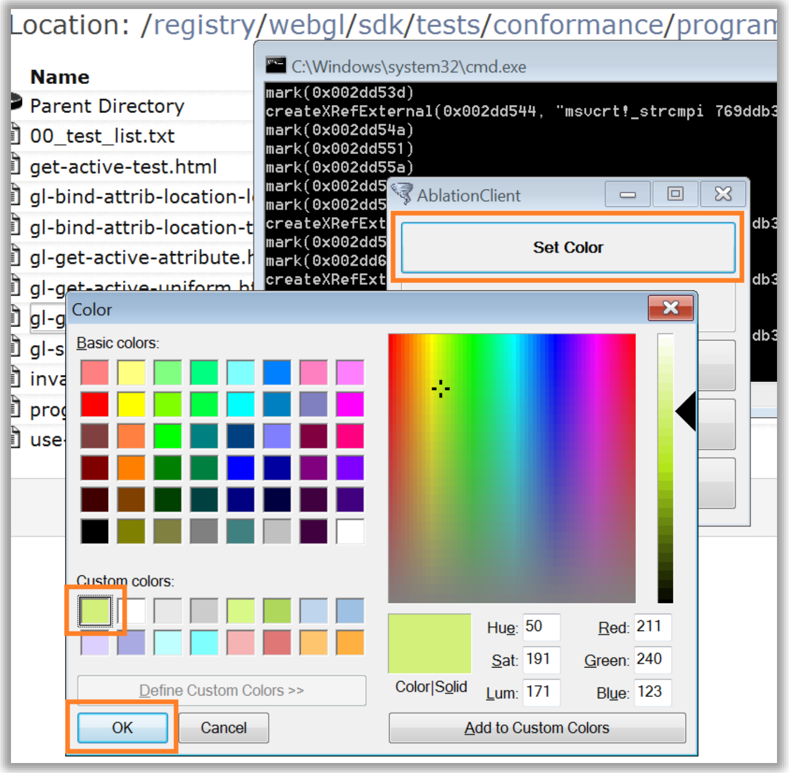
- Once Firefox finishes loading, load a sample
  - When it is finished processing, return to the sample index before continuing



Parent Directory
00_test_list.txt
get-active-test.html
gl-bind-attrib-location-long-names-test.html
gl-bind-attrib-location-test.html
gl-get-active-attribute.html
gl-get-active-uniform.html
gl-getshadersource.html
gl-shader-test.html
invalid-UTF-16.html
program-test.html
use-program-crash-with-discard-in-fragment-shader.html

Diff Tutorial

- Press the “Set Color” box, and select a different color to change the trace shading.



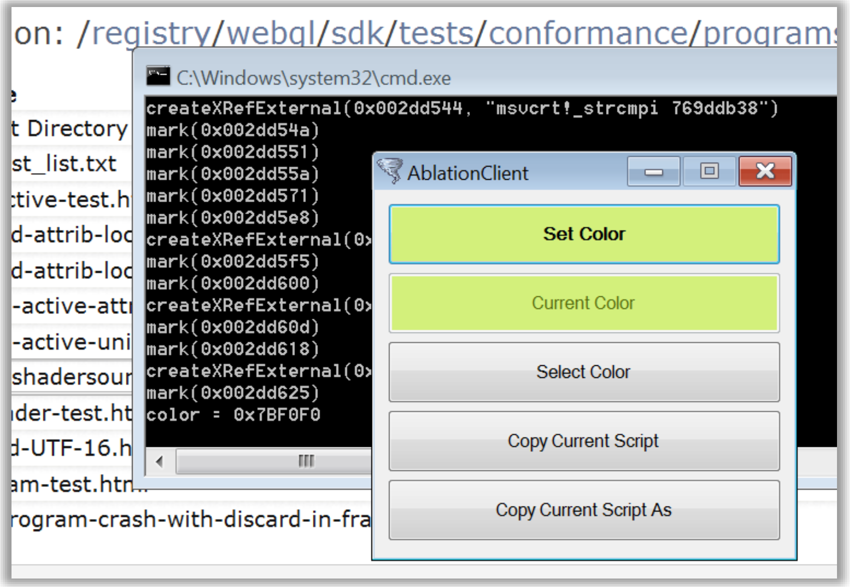
Location: /registry/webgl/sdk/tests/conformance/program

C:\Windows\system32\cmd.exe

```
mark(0x002dd53d)
createXRefExternal(0x002dd544, "msvcrt!_strcmpi 769ddb3
mark(0x002dd54a)
mark(0x002dd551)
mark(0x002dd55a)
mark(0x002dd5
mark(0x002dd5
createXRefExt
mark(0x002dd5
mark(0x002dd6
createXRefExt
```

Hue: 50 Sat: 191 Lum: 171

Red: 211 Green: 240 Blue: 123



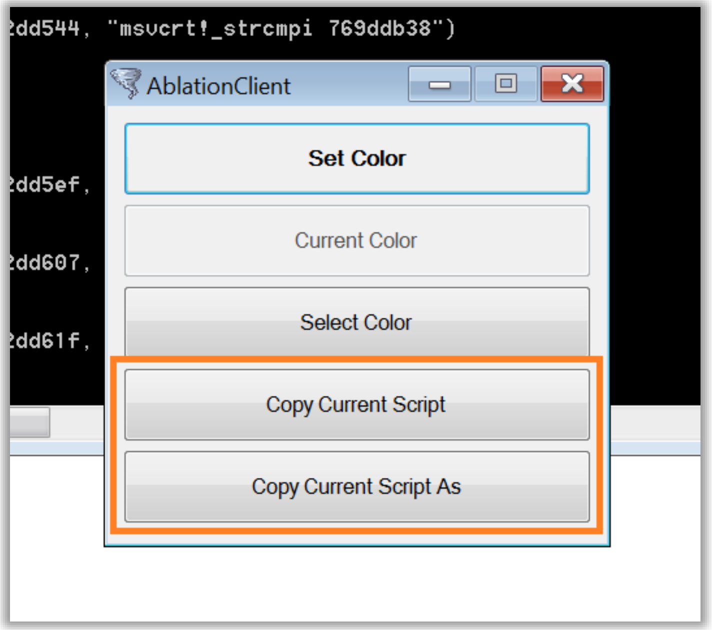
on: /registry/webgl/sdk/tests/conformance/programs

C:\Windows\system32\cmd.exe

```
createXRefExternal(0x002dd544, "msvcrt!_strcmpi 769ddb38")
mark(0x002dd54a)
mark(0x002dd551)
mark(0x002dd55a)
mark(0x002dd571)
mark(0x002dd5e8)
createXRefExternal(0x
mark(0x002dd5f5)
mark(0x002dd600)
createXRefExternal(0x
mark(0x002dd60d)
mark(0x002dd618)
createXRefExternal(0x
mark(0x002dd625)
color = 0x7BF0F0
```

Diff Tutorial

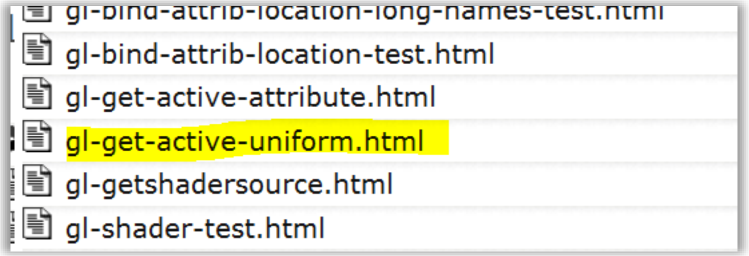
- You can use “Copy Current Script” to save a copy the current state at any time, or “Copy Current Script As” to specify the filename.



```
dd544, "msvcrt!_strcmpi 769ddb38")
dd5ef,
dd607,
dd61f,
```

Diff Tutorial

- Now browse to a different sample
  - I’m using

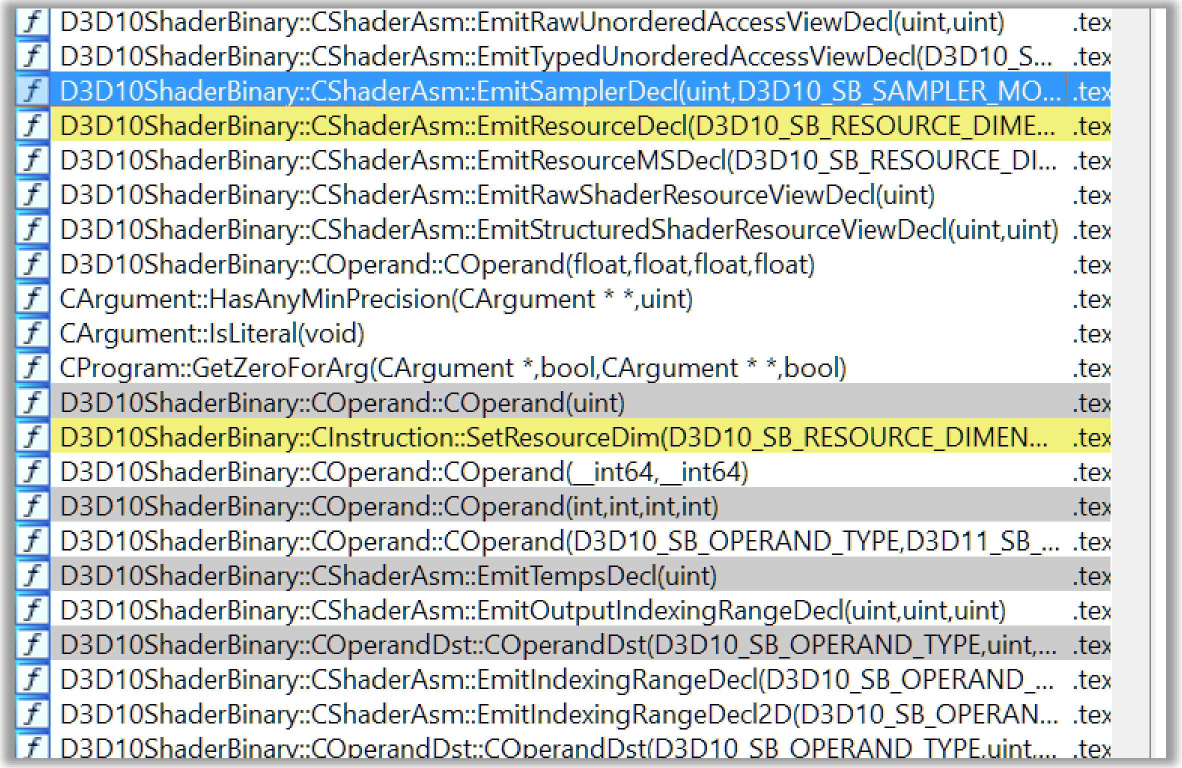


gl-bind-attrib-location-long-names-test.html
gl-bind-attrib-location-test.html
gl-get-active-attribute.html
gl-get-active-uniform.html
gl-getshadersource.html
gl-shader-test.html

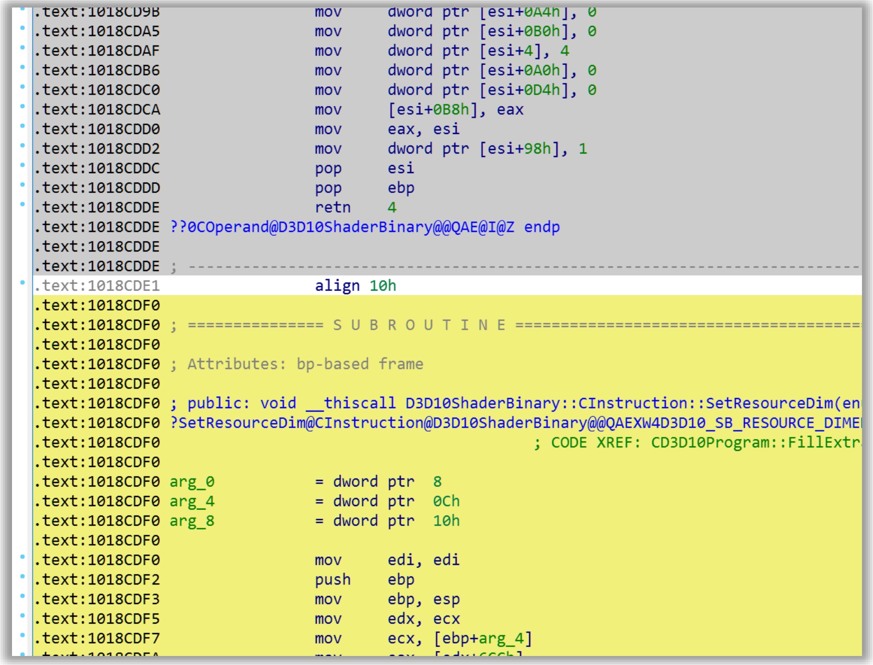
- Once it’s finished processing, close Firefox, and the AblationClient window.
- If running in a vm, copy the script file generated (d3dcompiler_47.ablation.py) to your host machine
- Disassemble D3DCompiler_47.dll with IDA, let it finish the auto-analysis, and then run the script to import the data.

Diff Tutorial

- The results:



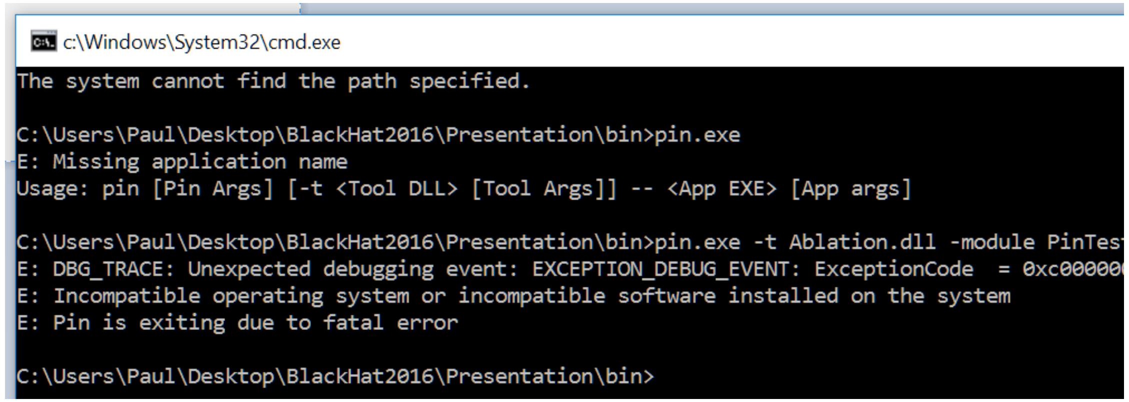
```
D3D10ShaderBinary::CShaderAsm::EmitRawUnorderedAccessViewDecl(uint,uint)         .tex
D3D10ShaderBinary::CShaderAsm::EmitTypedUnorderedAccessViewDecl(D3D10_S...       .tex
D3D10ShaderBinary::CShaderAsm::EmitSamplerDecl(uint,D3D10_SB_SAMPLER_MO...       .tex
D3D10ShaderBinary::CShaderAsm::EmitResourceDecl(D3D10_SB_RESOURCE_DIME...        .tex
D3D10ShaderBinary::CShaderAsm::EmitResourceMSDecl(D3D10_SB_RESOURCE_DI...        .tex
D3D10ShaderBinary::CShaderAsm::EmitRawShaderResourceViewDecl(uint)              .tex
D3D10ShaderBinary::CShaderAsm::EmitStructuredShaderResourceViewDecl(uint,uint)  .tex
D3D10ShaderBinary::COperand::COperand(float,float,float,float)                  .tex
CArgument::HasAnyMinPrecision(CArgument * *,uint)                               .tex
CArgument::IsLiteral(void)                                                      .tex
CProgram::GetZeroForArg(CArgument *,bool,CArgument * *,bool)                    .tex
D3D10ShaderBinary::COperand::COperand(uint)                                     .tex
D3D10ShaderBinary::CInstruction::SetResourceDim(D3D10_SB_RESOURCE_DIMEN...       .tex
D3D10ShaderBinary::COperand::COperand(__int64,__int64)                          .tex
D3D10ShaderBinary::COperand::COperand(int,int,int,int)                          .tex
D3D10ShaderBinary::COperand::COperand(D3D10_SB_OPERAND_TYPE,D3D11_SB_...        .tex
D3D10ShaderBinary::CShaderAsm::EmitTempsDecl(uint)                              .tex
D3D10ShaderBinary::CShaderAsm::EmitOutputIndexingRangeDecl(uint,uint,uint)      .tex
D3D10ShaderBinary::COperandDst::COperandDst(D3D10_SB_OPERAND_TYPE,uint,...       .tex
D3D10ShaderBinary::CShaderAsm::EmitIndexingRangeDecl(D3D10_SB_OPERAND_...        .tex
D3D10ShaderBinary::CShaderAsm::EmitIndexingRangeDecl2D(D3D10_SB_OPERAN...        .tex
D3D10ShaderBinary::COperandDst::COperandDst(D3D10_SB_OPERAND_TYPE,uint,...       .tex
```



```
.text:1018CD9B                 mov     dword ptr [esi+0A4h], 0
.text:1018CDA5                 mov     dword ptr [esi+0B0h], 0
.text:1018CDAF                 mov     dword ptr [esi+4], 4
.text:1018CDB6                 mov     dword ptr [esi+0A0h], 0
.text:1018CDC0                 mov     dword ptr [esi+0D4h], 0
.text:1018CDCA                 mov     [esi+0B8h], eax
.text:1018CDD0                 mov     eax, esi
.text:1018CDD2                 mov     dword ptr [esi+98h], 1
.text:1018CDDC                 pop     esi
.text:1018CDDD                 pop     ebp
.text:1018CDDE                 retn    4
.text:1018CDDE ??0COperand@D3D10ShaderBinary@@QAE@I@Z endp
.text:1018CDDE
.text:1018CDDE ; ---------------------------------------------------------------------------
.text:1018CDE1                 align 10h
.text:1018CDF0
.text:1018CDF0 ; =============== S U B R O U T I N E =======================================
.text:1018CDF0
.text:1018CDF0 ; Attributes: bp-based frame
.text:1018CDF0
.text:1018CDF0 ; public: void __thiscall D3D10ShaderBinary::CInstruction::SetResourceDim(en
.text:1018CDF0 ?SetResourceDim@CInstruction@D3D10ShaderBinary@@QAEXW4D3D10_SB_RESOURCE_DIME
.text:1018CDF0                                         ; CODE XREF: CD3D10Program::FillExtr
.text:1018CDF0
.text:1018CDF0 arg_0           = dword ptr  8
.text:1018CDF0 arg_4           = dword ptr  0Ch
.text:1018CDF0 arg_8           = dword ptr  10h
.text:1018CDF0
.text:1018CDF0                 mov     edi, edi
.text:1018CDF2                 push    ebp
.text:1018CDF3                 mov     ebp, esp
.text:1018CDF5                 mov     edx, ecx
.text:1018CDF7                 mov     ecx, [ebp+arg_4]
```

Troubleshooting

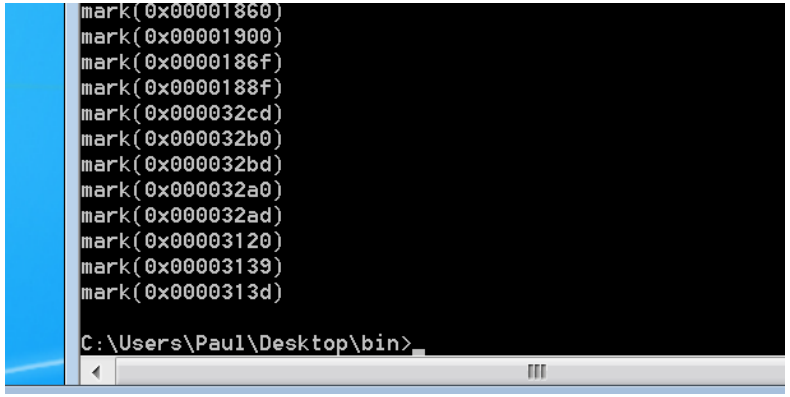
- PinTool doesn’t work on Windows 10, use Windows 7



c:\Windows\System32\cmd.exe

```
The system cannot find the path specified.

C:\Users\Paul\Desktop\BlackHat2016\Presentation\bin>pin.exe
E: Missing application name
Usage: pin [Pin Args] [-t <Tool DLL> [Tool Args]] -- <App EXE> [App args]

C:\Users\Paul\Desktop\BlackHat2016\Presentation\bin>pin.exe -t Ablation.dll -module PinTes
E: DBG_TRACE: Unexpected debugging event: EXCEPTION_DEBUG_EVENT: ExceptionCode  = 0xc00000
E: Incompatible operating system or incompatible software installed on the system
E: Pin is exiting due to fatal error

C:\Users\Paul\Desktop\BlackHat2016\Presentation\bin>
```

Win 10

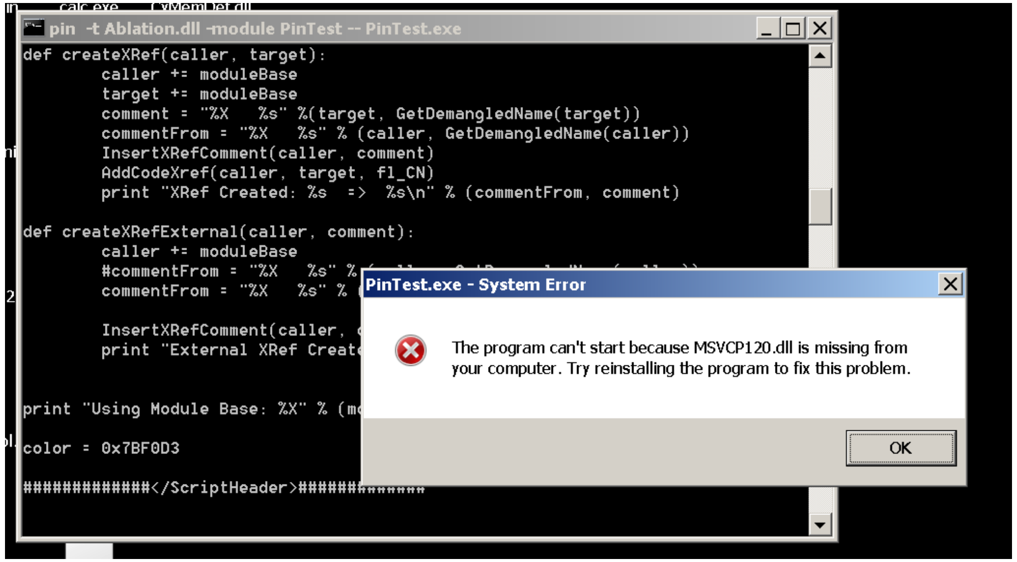


```
mark(0x00001860)
mark(0x00001900)
mark(0x0000186f)
mark(0x0000188f)
mark(0x000032cd)
mark(0x000032b0)
mark(0x000032bd)
mark(0x000032a0)
mark(0x000032ad)
mark(0x00003120)
mark(0x00003139)
mark(0x0000313d)

C:\Users\Paul\Desktop\bin>
```

Win 7

Troubleshooting

- Missing MSVCP120.dll?



pin -t Ablation.dll -module PinTest -- PinTest.exe

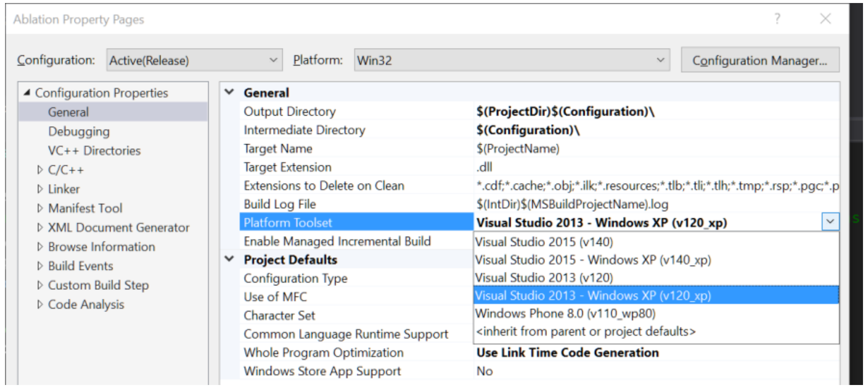
```
def createXRef(caller, target):
        caller += moduleBase
        target += moduleBase
        comment = "%X   %s" %(target, GetDemangledName(target))
        commentFrom = "%X   %s" % (caller, GetDemangledName(caller))
        InsertXRefComment(caller, comment)
        AddCodeXref(caller, target, fl_CN)
        print "XRef Created: %s  =>  %s\n" % (commentFrom, comment)

def createXRefExternal(caller, comment):
        caller += moduleBase
        #commentFrom = "%X   %s" %
        commentFrom = "%X   %s" %

        InsertXRefComment(caller,
        print "External XRef Creat


print "Using Module Base: %X" % (mo

color = 0x7BF0D3

#############</ScriptHeader>#############
```

PinTest.exe - System Error

The program can't start because MSVCP120.dll is missing from your computer. Try reinstalling the program to fix this problem.

- Install Visual C++ 2013 Redistributable (x86)
  - https://www.microsoft.com/en-us/download/details.aspx?id=40784

- Or build Ablation for a different toolset



Ablation Property Pages

Configuration: Active(Release) Platform: Win32

General
Output Directory: $(ProjectDir)$(Configuration)\
Intermediate Directory: $(Configuration)\
Target Name: $(ProjectName)
Target Extension: .dll
Extensions to Delete on Clean: *.cdf;*.cache;*.obj;*.ilk;*.resources;*.tlb;*.tli;*.tlh;*.tmp;*.rsp;*.pgc;*.p
Build Log File: $(IntDir)$(MSBuildProjectName).log
Platform Toolset: Visual Studio 2013 - Windows XP (v120_xp)
Enable Managed Incremental Build

Project Defaults
Configuration Type
Use of MFC
Character Set
Common Language Runtime Support
Whole Program Optimization: Use Link Time Code Generation
Windows Store App Support: No

Visual Studio 2015 (v140)
Visual Studio 2015 - Windows XP (v140_xp)
Visual Studio 2013 (v120)
Visual Studio 2013 - Windows XP (v120_xp)
Windows Phone 8.0 (v110_wp80)
<inherit from parent or project defaults>