

Source and Executable

Mike Lai, mikelai@microsoft.com
Microsoft Corp

```
main()
{
    cout <<
    "Hello World\n";

    return 0;
}
```

HelloWorld.cpp

Human readable
C++ source code
file



```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68
69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F
74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20
6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00
48 B6 98 3C 0C D7 F6 6F 0C D7 F6 6F 0C D7 F6 6F
84 B0 F3 6E 14 D7 F6 6F 84 B0 F2 6E 07 D7 F6 6F
84 B0 F5 6E 0E D7 F6 6F 84 B0 F7 6E 09 D7 F6 6F
69 B1 F7 6E 08 D7 F6 6F 0C D7 F7 6F 5E D7 F6 6F
0D BA F3 6E 0E D7 F6 6F 0D BA 09 6F 0D D7 F6 6F
0D BA F4 6E 0D D7 F6 6F 52 69 63 68 0C D7 F6 6F
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

HelloWorld.exe

Machine readable
(binary) executable
file

Customer Question: Was the executable running in my machine really built from the same source code files that I or your 3rd party evaluators / auditors have reviewed / analyzed ?

Microsoft Response: Would you feel more comfortable if there are additional artifacts to resolve the Customer Question?

Is that really the source code for this software?

- ❑ A generic issue of software -- including Open Source Software
 - ❖ <https://blogs.kde.org/2013/06/19/really-source-code-software>
 - ❖ <https://blog.torproject.org/blog/deterministic-builds-part-one-cyberwar-and-global-compromise>
 - ❖ <https://wiki.debian.org/ReproducibleBuilds>
 - ❖ <https://reproducible-builds.org/>
 - ❖ Video: <https://www.sfscon.it/talks/you-think-youre-not-a-target-a-tale-of-three-developers/>
 - ❖ Video: Hardware implants in the supply-chain
https://media.ccc.de/v/35c3-9597-modchips_of_the_state#t=106

The source / executable correspondence question is asked more often than we think

equivalence can be demonstrated at scale. The NCSC has advised the Oversight Board that the priority should be to rectify these underlying flaws as part of Huawei's transformation plan. Unless and until this is done it is not possible to be confident that the source code examined by HCSEC is precisely that used to build the binaries running in the UK networks.

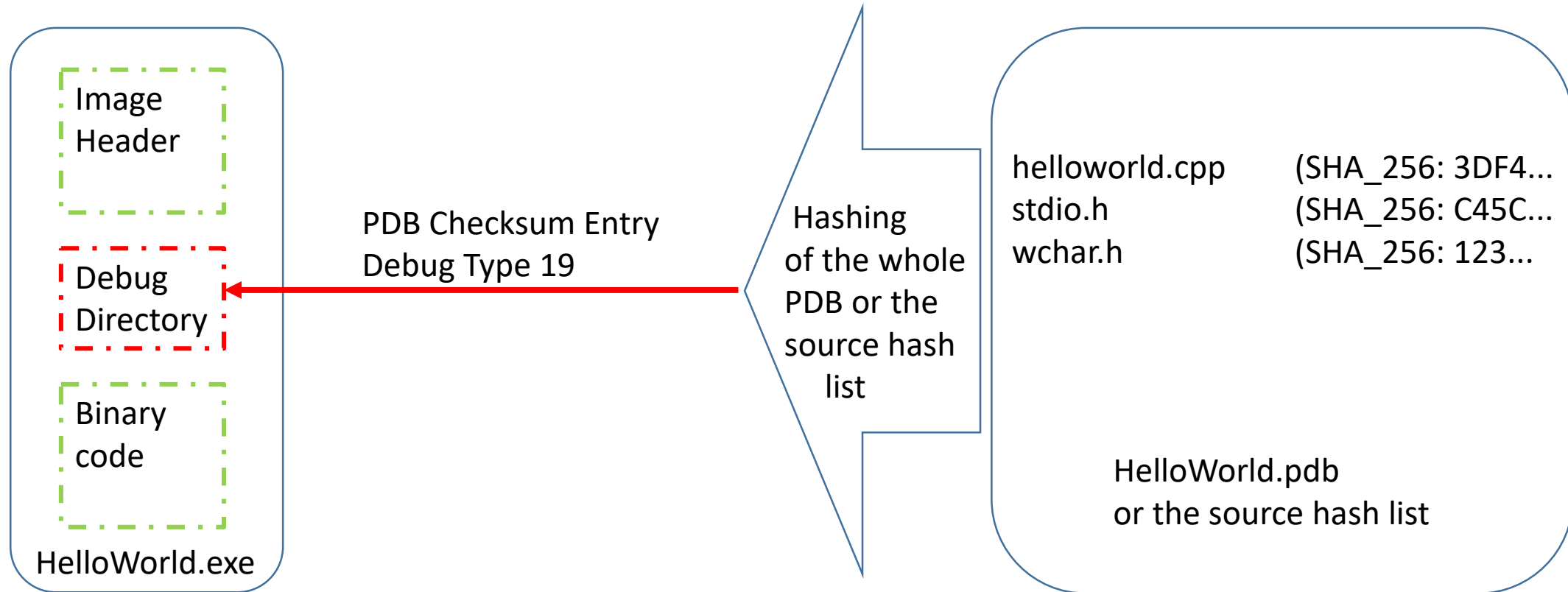
Our approach

Based on the artifacts being generated by compiler/linker toolchains

Compiler Generated Artifacts

- Compiler reads source code files
- Compiler outputs a pair of files:
 1. Executable (exe, dll, sys, etc) containing the machine instructions
 2. Program Database (PDB) storing the debugging information
- Compiler computes strong hash values of source files
- Compiler stores the hash values and the path names of source files in the PDB
- U computes the strong hash of the PDB or list of src hash values
- U stores the PDB or src hash list hash in a dir of the executable
- See <https://msdn.microsoft.com/en-us/magazine/mt795185>

Artifact Interrelationship (following ECMA-335)



On top of a stronger binding between the exe and PDB pair, your digital signing of the exe enables the integrity and authenticity of the PDB (which includes the source file hashes) as well as the exe (which contains the actual compiled binary code)

Confirm that a source file was used during the compilation of an executable

- You compute the hash value of the source file in question (certutil -hashfile from system32)
- You discover the PDB file pairing with the executable in question (symchk from MSDN)
- You verify that the hash value that you just computed matches the hash value with the same source file name in the PDB that you just discovered
- See KB 3195907 (<http://bit.ly/2gNthQk>)
- Exactly what WinDbg does before using the source file

Still not convinced ?

Customer request: I want to recompile your sources to reproduce the executable files myself and to compare the reproduced with the original, as in the case of OSS

Microsoft Response: Please stop by one of our Transparency Centers

See <https://www.microsoft.com/en-us/securityengineering/gsp> for details

Not as easy as one thought (1) – hex compare

```
00000080 48 B6 98 3C 0C D7 F6 6F HJ~<.x0o
00000088 0C D7 F6 6F 0C D7 F6 6F 84 B0 F3 6E 14 D7 F6 6F .x0o.x0o,,°ón.x0o
00000098 84 B0 F2 6E 07 D7 F6 6F 84 B0 F5 6E 0E D7 F6 6F ,,°ón.x0o,,°ón.x0o
000000A8 84 B0 F7 6E 09 D7 F6 6F 69 B1 F7 6E 08 D7 F6 6F ,,°+n.x0oi±+n.x0o
000000B8 0C D7 F7 6F 5E D7 F6 6F 0D BA F3 6E 0E D7 F6 6F .x+o^x0o.°ón.x0o
000000C8 0D BA 09 6F 0D D7 F6 6F 0D BA F4 6E 0D D7 F6 6F .e.o.x0o.°ón.x0o
000000D8 52 69 63 68 0C D7 F6 6F 00 00 00 00 00 00 00 Rich.x0o.....
000000E8 00 00 00 00 00 00 00 00 50 45 00 00 64 86 09 00 .....PE..dt.
000000F8 8F F6 3C 76 00 00 00 00 00 00 00 F0 00 22 00 .ö<v.....ð."
00000108 0B 02 0E 16 00 84 00 00 00 60 00 00 00 00 00 00 .....
00000118 0F 10 00 00 00 10 00 00 00 00 40 01 00 00 00 .....@....
00000128 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 .....
00000138 06 00 00 00 00 00 00 00 00 50 01 00 00 04 .....P....
00000146 00 00 00 00 00 00 03 00 60 81 00 00 10 00 00 00 .....
00000156 00 00 00 00 00 00 10 00 00 00 00 10 00 00 00 .....
00000166 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 .....
00000176 00 00 00 00 00 00 00 00 00 00 68 F4 00 00 00 .....hõ
00000183 00 64 00 00 00 00 30 01 00 3C 04 00 00 00 00 .....d...ø.<.
00000191 E0 00 00 64 05 00 00 00 00 00 00 00 00 00 .....ä..d.....
0000019F 00 00 40 01 00 58 00 00 60 B8 00 00 54 00 .....@.X...T.
000001AE 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000001BE 00 00 00 00 00 00 00 00 00 00 C0 B8 00 00 08 01 .....Ä....
000001CE 00 00 00 00 00 00 00 00 00 00 F0 00 00 68 04 .....ð.h.
000001DE 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000001EE 00 00 00 00 00 00 00 00 00 00 2E 74 65 78 74 00 .....text.
000001FE 00 00 A7 82 00 00 00 10 00 00 84 00 00 00 04 .....š,.....
0000020E 00 00 00 00 00 00 00 00 00 00 00 00 20 00 .....
0000021E 00 60 2E 72 64 61 74 61 00 00 DF 2C 00 00 00 A0 .....rdata.š,....
0000022E 00 00 00 2E 00 00 88 00 00 00 00 00 00 00 .....
0000023E 00 00 00 00 00 00 00 40 00 00 4E 64 61 74 61 00 .....@.@.data.
0000024E 00 00 F0 08 00 00 00 D0 00 00 02 00 00 00 B6 .....ð...ð.....Ĵ
0000025E 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 .....@
0000026E 00 C0 2E 70 64 61 74 61 00 00 14 07 00 00 00 E0 .....Ä.pdata.....
0000027E 00 00 00 08 00 00 00 B8 00 00 00 00 00 00 00 .....
0000028E 00 00 00 00 00 00 40 00 00 40 2E 69 64 61 74 61 .....@.@.idata
0000029E 00 00 DC 13 00 00 00 F0 00 00 00 14 00 00 00 C0 .....Û....ð.....Ä
000002AE 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 .....@
000002BE 00 40 2E 6D 73 76 63 6A 6D 63 76 01 00 00 00 10 .....@.msvcjmcv....
000002CE 01 00 00 02 00 00 00 D4 00 00 00 00 00 00 00 .....ð.....
00000080 69 BE 58 BE 2D DF 36 ED 2D DF 36 ED 2D DF 36 ED iXX-B6i-B6i-B6i
00000090 24 A7 A5 ED 27 DF 36 ED AC B4 33 EC 3C DF 36 ED $$$i'B6i~'3i<B6i
000000A0 AC B4 32 EC 27 DF 36 ED AC B4 35 EC 2F DF 36 ED ~'2i'B6i~'5i/B6i
000000B0 AC B4 37 EC 28 DF 36 ED 48 B9 37 EC 2F DF 36 ED ~'7i(B6iH^7i/B6i
000000C0 2D DF 37 ED 13 DF 36 ED 1B B3 3F EC 2C DF 36 ED -B7i.B6i.³?i,B6i
000000D0 1B B3 C9 ED 2C DF 36 ED 1B B3 34 EC 2C DF 36 ED .³éi,B6i.³4i,B6i
000000E0 52 69 63 68 2D DF 36 ED 00 00 00 Rich-B6i...
000000EB 00 00 00 00 00 50 45 00 00 64 86 06 00 .....PE..dt.
000000F8 67 05 26 5D 00 00 00 00 00 00 00 F0 00 22 00 g.&].....ð."
00000108 0B 02 0E 15 00 10 00 00 00 20 00 00 00 00 00 .....
00000118 34 15 00 00 00 10 00 00 00 00 40 01 00 00 00 4.....@....
00000128 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 .....
00000138 06 00 00 00 00 00 00 00 00 80 00 00 00 04 .....€.
00000146 00 00 00 00 00 00 03 00 60 81 00 00 10 00 00 00 .....
00000156 00 00 00 10 00 00 00 00 00 00 00 10 00 00 00 .....
00000166 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 .....
00000176 00 00 00 00 00 00 00 00 00 00 94 29 00 00 B4 00 .....")..
00000186 00 00 00 60 00 00 E0 01 00 00 00 50 00 .....ä...P.
00000193 00 8C 01 00 00 00 00 00 00 00 00 00 00 00 .....(E...
000001A0 00 70 00 00 1C 00 00 00 40 23 00 00 70 00 p.....@#.p.
000001AE 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000001BE 00 00 00 00 00 00 00 00 00 00 80 23 00 00 08 01 .....°#....
000001CE 00 00 00 00 00 00 00 00 00 00 20 00 00 C8 01 .....È.
000001DE 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000001EE 00 00 00 00 00 00 00 00 00 00 2E 74 65 78 74 00 .....text.
000001FE 00 00 86 0F 00 00 00 10 00 00 10 00 00 00 04 .....t.....
0000020E 00 00 00 00 00 00 00 00 00 00 00 00 20 00 .....
0000021E 00 60 2E 72 64 61 74 61 00 00 E6 11 00 00 00 20 .....rdata.e....
0000022E 00 00 00 12 00 00 00 14 00 00 00 00 00 00 .....
0000023E 00 00 00 00 00 00 40 00 00 40 2E 64 61 74 61 00 .....@.@.data.
0000024E 00 00 38 06 00 00 00 40 00 00 00 02 00 00 00 26 .....8...@.....&
0000025E 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 .....@
0000026E 00 C0 2E 70 64 61 74 61 00 00 8C .....Ä.pdata..E
00000279 01 00 00 00 50 .....P
0000027E 00 00 00 .....

```

Not as easy as one thought (2) – machine instruction compare



Need special support from compiler/linker toolchains

- 1980's Apollo DSEE (Domain Software Engineering Environment) reproduced an executable in a bit-by-bit identical manner
- Visual Studio 2019 C++ compiler/linker supports “/experimental:deterministic” and “/pathmap:<SOURCE>=<DEST>” flags
- Visual Studio 2019 CSC compiler supports “-deterministic” and “-pathmap:<SOURCE>=<DEST>” flags
- LLVM Clang toolchain, GCC toolchain -- see <https://reproducible-builds.org/> for information

How do I discover that a Windows 10 based executable file is reproducible?

Use “link /dump /headers” against the executable file in question to inspect the Debug Directories in its image header

Debug Directories

Time	Type	Size	RVA	Pointer	
35707659	cv	25	003A3A40	3A0440	Format: RSDS, {11BC9A51-3F11-40CA-359E-CDF50F0122C1}, 1, ntkrnlmp.pdb
35707659	coffgrp	145C	003A3A68	3A0468	50475500 (PGU)
35707659	repro	24	003A4EEC	3A18EC	51 9A BC 11 11 3F CA 40 35 9E CD F5 0F 01 22 C1 82 9F 4D 74 1A 84 81 FD 12 13 E7 04 59 76 70 35

show only diffs

checksum

Private build

Official build

time stamp

PDB ID

rsrc diffs

confirmed by link dump headers

confirmed by RSRC editor

rsrc size

VER_FILEOS (00040004)

VER_PRIVATE (1 bit)

```

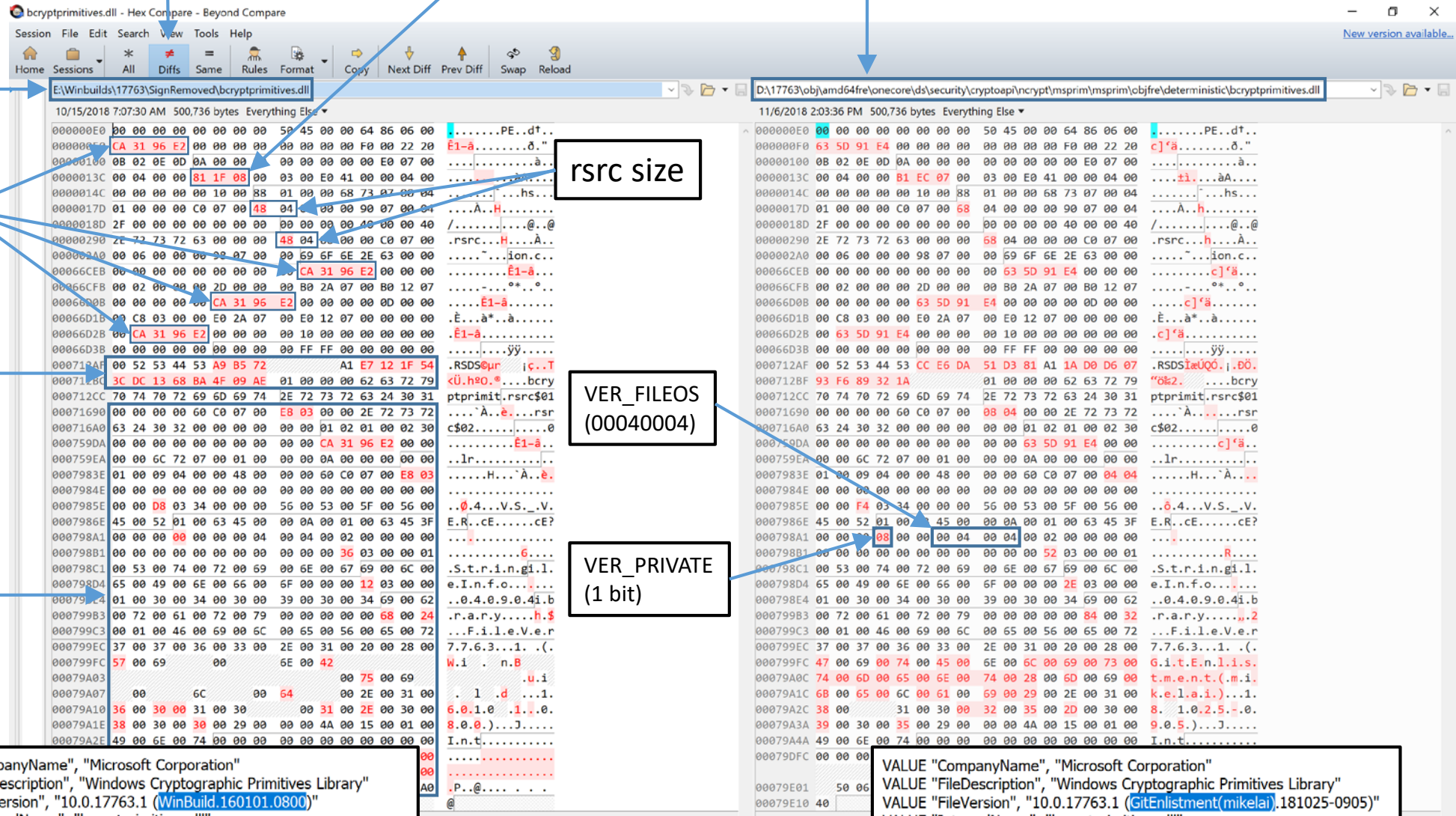
VALUE "CompanyName", "Microsoft Corporation"
VALUE "FileDescription", "Windows Cryptographic Primitives Library"
VALUE "FileVersion", "10.0.17763.1 (WinBuild.160101.0800)"
VALUE "InternalName", "bcryptprimitives.dll"
VALUE "LegalCopyright", "\xA9 Microsoft Corporation. All rights reserved."
VALUE "OriginalFilename", "bcryptprimitives.dll"
VALUE "ProductName", "Microsoft\xAE Windows\xAE Operating System"
VALUE "ProductVersion", "10.0.17763.1"

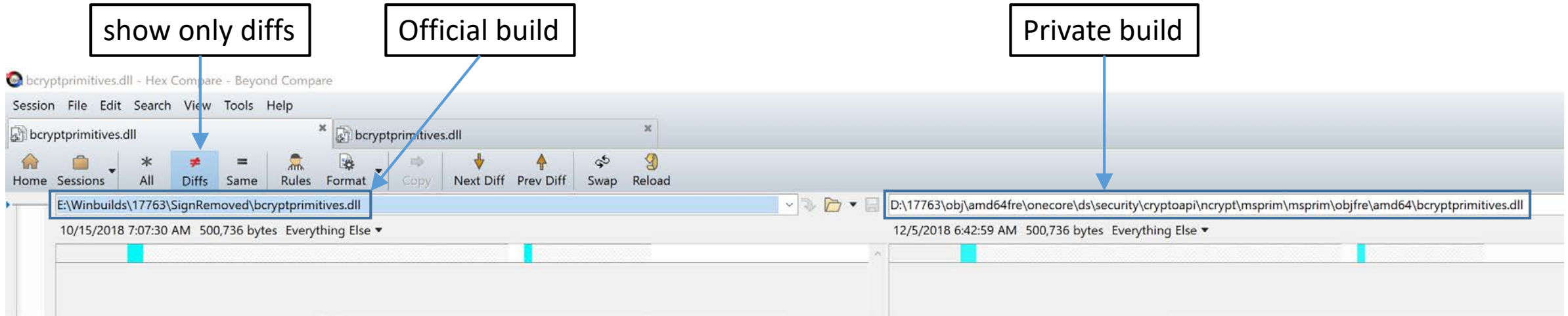
```

```

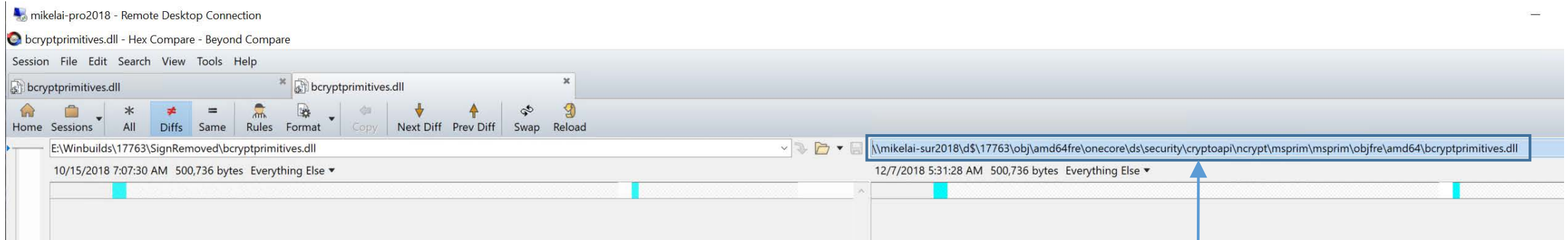
VALUE "CompanyName", "Microsoft Corporation"
VALUE "FileDescription", "Windows Cryptographic Primitives Library"
VALUE "FileVersion", "10.0.17763.1 (GitEnlistment(mikela).181025-0905)"
VALUE "InternalName", "bcryptprimitives.dll"
VALUE "LegalCopyright", "\xA9 Microsoft Corporation. All rights reserved."
VALUE "OriginalFilename", "bcryptprimitives.dll"
VALUE "ProductName", "Microsoft\xAE Windows\xAE Operating System"
VALUE "ProductVersion", "10.0.17763.1"

```





Showing empty – i.e. no difference



Also works when private build occurs in a remote machine

Private build with deterministic Option (trimming)

Private build without deterministic Option (no trimming)

More diffs to explain

The image displays a side-by-side comparison of two versions of the file `bcryptprimitives.dll` using Beyond Compare. The left window shows the file from a 'Private build with deterministic Option (trimming)', and the right window shows it from a 'Private build without deterministic Option (no trimming)'. Both files are 500,736 bytes and were last modified on 11/7/2018. The left view shows a dense list of differences (diffs) highlighted in red, indicating many changes between the two builds. The right view shows a much sparser list of differences, indicating that the deterministic build process successfully eliminated many of the differences present in the non-deterministic build. A blue arrow points from the text 'More diffs to explain' to the left view's diff list.



Enterprise

[Change Edition](#) ▾

Attribute Name	Attribute Value
Product Group	windows-desktop
Edition Type	Official
Edition Family	Client
Is Virtual Edition?	True
Parent Edition	Professional
Disk Footprint	15,255,828,860
Device Images (FFUs)	0
Neutral Packages	1282
Hosted APIsets	701
Binaries	6465
WoW Binaries	495
All Files	16085

Usage scenarios

Source hash database for query

The screenshot displays the SQL Server Enterprise interface. On the left, the Server Explorer shows a server named 'spArchive_18362ClientEnt' with a database 'spArchive_18362ClientEnt.mdf' containing a table 'SourceFiles'. The main window shows a SQL query executed in the 'Results' tab, returning a list of source files with their hashes.

```
1 | select distinct CPU, PeFileName, SrcFullPath, SrcHash, SrcHashType from SourceFiles s where s.PeRepro = 1 and s.IsManaged = 0 and s.PeFileName LIKE 'acpi.%' order by
```

CPU	PeFileName	SrcFullPath	SrcHash	SrcHashType
594	x64	acpi.sys	sdki\inc\winsvc.h	253ADA6F60FE0871154901306649EA934AE1BE1ECDCDA97E6B9FF1FE4FC3C0C
595	x64	acpi.sys	shared\inc\lacpioclt.h	18240F9EB77F7BB62BE6A610D479DC791C9DA73CD8195429D3C0BC7006493EA
596	x64	acpi.sys	shared\inc\basetsd.h	8EAEF7BB1985F584E8305463494334FC55AAD56D98E59E7346273CECACF81A5A
597	x64	acpi.sys	shared\inc\bugcodes.h	275E8DFA242D0D65898BEA9E24999E192FAB2F0DA6B1C5544CAB303FB127D5BE
598	x64	acpi.sys	shared\inc\cfg.h	D506D5316258300D2A6338C142CFF313AEB347EA2EA5FE848B05508AA8A3AFC4
599	x64	acpi.sys	shared\inc\concurrencyal.h	16ABCA3329E94A06E9B22A48F87B19A02E0D771F7E991A2FFD6C1B8A96F34D9D
600	x64	acpi.sys	shared\inc\devioct.h	10E224F99AF4F1D82B0260EC2E3FC6CABF4101B9CB3D47DD9797A4274C0E036D
601	x64	acpi.sys	shared\inc\devpkkey.h	BC1C5FC0FF02F8ABE4F8D70CEE675097F55F00112D0E68E9E7F46E712CC49F0E
602	x64	acpi.sys	shared\inc\devpropdef.h	25016C23AA834937DFE9C32A5E800D8ACFEFBB407E39203170F03A2666D2B5C80
603	x64	acpi.sys	shared\inc\dontuse.h	32F810E18BBF1AB64E2C71D99E18E6C2255BC4C885ED34B51905C75C5D39E7C3
604	x64	acpi.sys	shared\inc\dpfilter.h	577C410A77DB4FC3FD070550E5D7E2DE6A732B621BC5C4FEDF9ACA0A8B735C5
605	x64	acpi.sys	shared\inc\driverspecs.h	9CF7E9E1C9B55C7C351E87FF5A98E362B6FFDB511C3309AB9CF46B62B0DACE42
606	x64	acpi.sys	shared\inc\eventprov.h	37FF9D09D9D80E1C69D24AE157FAEACA1B42F898943A3138BD0E73AFFC11086D
607	x64	acpi.sys	shared\inc\entrace.h	B32AE953E6B3E4813DD251ED52CD566EA211184AE61BE8804DB884D7D64CF80
608	x64	acpi.sys	shared\inc\guiddef.h	0C08463FBC5A23A8862E57699E2F30DD14CD3B8A4A0903E4FCA9392A57942DAE
609	x64	acpi.sys	shared\inc\initguid.h	422EBCF50B8E8AD2F21A06E7281540F759237EABE37E445605FC45CC45D88314
610	x64	acpi.sys	shared\inc\ip2string.h	16FE1F7FBFC3BD334E50A00CC4D365629A6E4D006049C102BD8BD43C06198D46
611	x64	acpi.sys	shared\inc\kernelypes.h	E844C7726C42736DF74445B36351DC01E29BCCCE7D57EA208F77F61AA4C2B191
612	x64	acpi.sys	shared\inc\ksamd64.inc	63194CDE422A909DEC2131C82A320C165CF666122FCD53D59145FC962202DD02
613	x64	acpi.sys	shared\inc\kmtypes.h	68D284D00AE33282FB265880F8166F2B5DC60C0A7A26DB652450A5B44D4EE11
614	x64	acpi.sys	shared\inc\ksamd64.inc	EE11AFCEC5349E943A8D3543711699D06E97BEF7DEE677D628931B7C247B31AC
615	x64	acpi.sys	shared\inc\minwin\apiset.h	700A79B181668539BBC2FE9DA27C3D1D36E3DEF3341E8ED16E6011E99C524DFD
616	x64	acpi.sys	shared\inc\minwin\apisetconv.h	5892590DBEA96D90176BD6BC67944C95F97E8E67A617E39ED9F78CCFD35E40D
617	x64	acpi.sys	shared\inc\minwin\minwindef.h	A9CF08BE8407A196104124D5ADE2308E204E47D3252BCD2AD20D0F2137843D62
618	x64	acpi.sys	shared\inc\minwin\ntdef.h	B2849BBACFC957459F5DA0C7A5D4E851E3F7D204DA01439DEBB104AD406CBA22
619	x64	acpi.sys	shared\inc\ntiolog.h	E3B7DD0C78F5D493D087D3433A5EC38937809EB3BB7E376F7BAC29AD14E08A71
620	x64	acpi.sys	shared\inc\ntstatus.h	4E56B087C5F2B0993DFE0ACE51AA1E816C993AFC6033E4A0E6C990AE6F0071D9
621	x64	acpi.sys	shared\inc\poppack.h	A5D0DEF5CFE96D634A41EE9A97749C147165F8656CDFED5DF53BC24C8ADB1210
622	x64	acpi.sys	shared\inc\pshpack1.h	DEE27F2712B9E72CA78A404834735303D16BDB21C8AA3ADDACA7DBC22664529
623	x64	acpi.sys	shared\inc\pshpack2.h	971D19074639C3B6134BB40776CB2F817C53CB0D5D748B52468F571932BBCC49
624	x64	acpi.sys	shared\inc\pshpack4.h	1CB4D07A218EC43C7935B431B16146FC0F3D29D43BD192F12959051D62C48D57
625	x64	acpi.sys	shared\inc\pshpack8.h	47F3972A1211E3A5AC32B18FAE1A824DB087DC7DC562D152E9CCAB9B297FAEF0
626	x64	acpi.sys	shared\inc\pshpack16.h	346FBB98672D2B0B32DCAADC9A6F736DAB45AA8AFF8661B3E05E05D852C53DF3
627	x64	acpi.sys	shared\inc\reshub.h	C1B4646848E36F2205E2AFD81F3382103BA1E5EA38D273AA2136FB288277DA62
628	x64	acpi.sys	shared\inc\sai.h	52B609C0DD87D8563834FF669D3AFBA2842AF5CF6D1383520001665406E5049
629	x64	acpi.sys	shared\inc\skddkver.h	1BE7036A2DE81216D8708047C28BFD34B7928FAA8D5DD1DC45023637BDF31134
630	x64	acpi.sys	shared\inc\sdv_driverspecs.h	99FD81F9464150F56963C3BBFAFAA95F93B837C221C4237E6E399A85E00EA9F39
631	x64	acpi.sys	shared\inc\specstrings.h	7FA62AA9A8F64B1E68D6F75D7F4B04D2B1B14BB6C58A01E53BC7F27168028A
632	x64	acpi.sys	shared\inc\specstrings_strict.h	49B12898B42BCF53E5F8F75E6DB1A5D3FFB7A9F394E50DF3351E0824D4A8B42
633	x64	acpi.sys	shared\inc\specstrings_undef.h	6ABA76EABBE627EDADBA5AB29304D9E2FF4EB9DA165FD81A9095C851F405A01
634	x64	acpi.sys	shared\inc\traceloggingprovider.h	606AEB1B67081860FB64415C700375D27B91045F8FE9F625987CBC179BA7806E
635	x64	acpi.sys	shared\inc\wmguid.h	6511CF20BD2DFDC9E7B2D7AC1AA8D9E275EA2F058D0FAAA9C2ACC33B7CFAD
636	x64	acpi.sys	shared\inc\winapi\family.h	843B2A47AD66E6CBB5F65738631428DDBA60B2D21975878A5CC051BA6A488AAD
637	x64	acpi.sys	shared\inc\windef.h	94B86C38376E0C1AAE76F2A16E0A1EADBB6E78FA32DE4447DB1AC2B9B231761
638	x64	acpi.sys	shared\inc\winerror.h	8DD515801194F64BB7133268E605A0E691E163F4A37AD16B49DB4599A06FF3D3
639	x64	acpi.sys	shared\inc\winpackagfamily.h	8F74E254896094A3884E6975FD24B3493846514065F47D2666DF53CDEA45B8EA
640	x64	acpi.sys	shared\inc\wmistr.h	7BDC4FA3601A3C6DF97E8518B7BD98C3052F889367E3A30F5BCF4A9334D0A5B

Server Explorer | Toolbox | Query executed successfully at 12:44:22 PM | (LocalDB)\MSSQLLocalDB (14....) | NTDEV\mikelai (57) | spArchive_18362ClientEnt | 00:00:10 | 640 rows

Compatible with SARIF (Static Analysis Results Interchange Format)

According to <https://docs.oasis-open.org/sarif/sarif/v2.1.0/sarif-v2.1.0.html>

EXAMPLE:

```
"artifacts": [  
  {  
    "location": {  
      "uri": "file:///C:/Code/main.c"  
    },  
    "sourceLanguage": "c",  
    "hashes": {  
      "sha-256": "b13ce2678a8807ba0765ab94a0ecd394f869bc81"  
    }  
  }  
]
```

Identify delta source files for an update

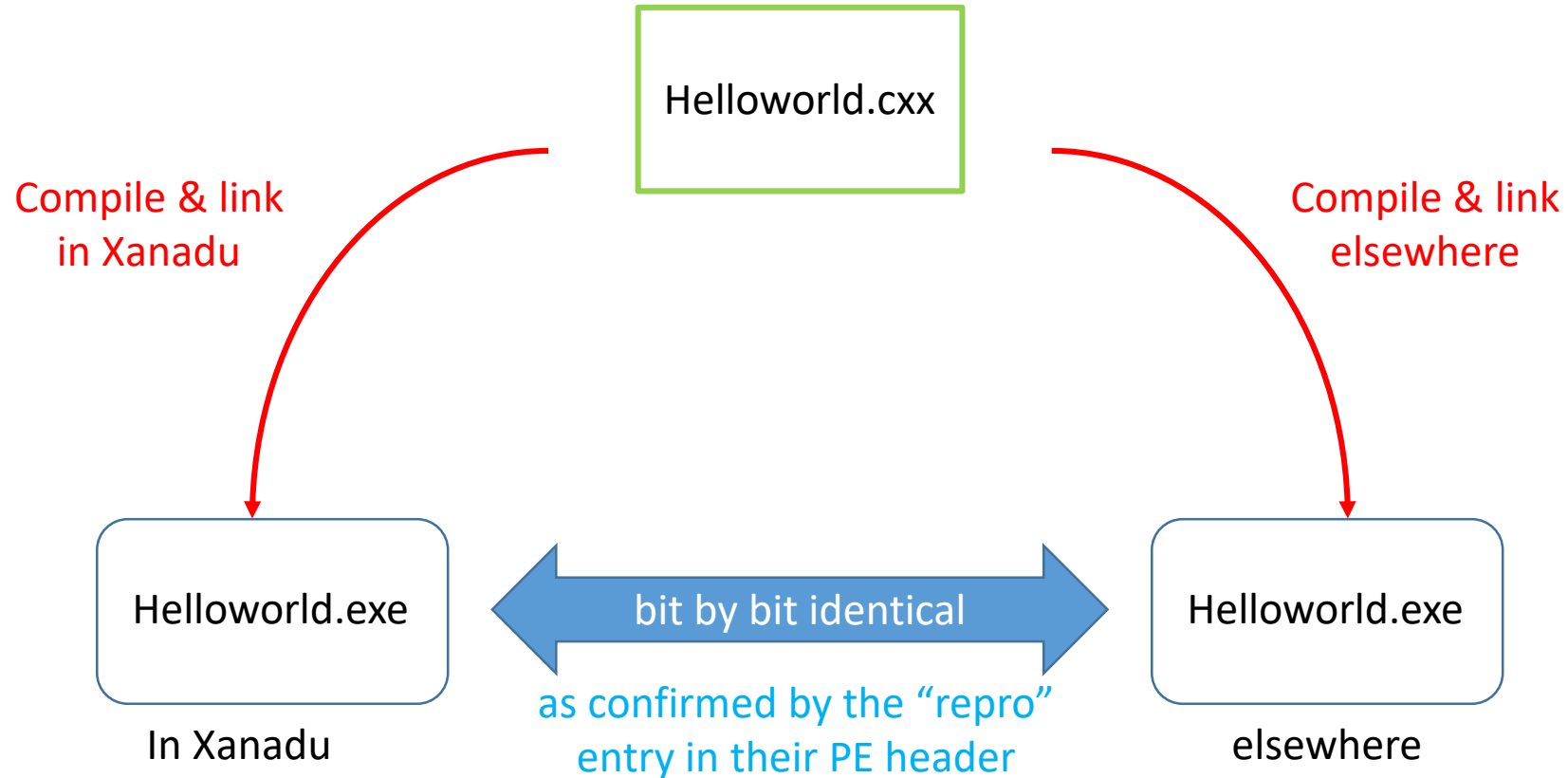
2	Old PE:	d:\media\18362clientent\mountidx3\windows\system32\drivers\acpi.sys (x64)		
3	New PE:	d:\media\kb4512941v011\windows10.0-kb4512941-x64\amd64_dual_acpi.inf_31bf3856ad364e35_10.0.18362.329_none_b5ad09708ddd3578\acpi.sys (x64)		
4				
5	Label	CPU	Source Hash	Source Path
6	18362ClientEnt	x64	C8189D3CB51B99B57932E0B4994D6B05FC306349E475B2307C94FAA6C6027C7B	ddk\inc\ntddk.h
7	KB4512941V011	x64	9F64E685979B4340C9ECB0863B50C4E9C24C2AF8903AFEC9E37246943C99450F	ddk\inc\ntddk.h
8	18362ClientEnt	x64	FE4A0FF22FC952F276D09BFA44D5F65C24CD6FAD4D6660D8223C30B5A75CDB50	ddk\inc\wdm.h
9	KB4512941V011	x64	7C3C6F8E254FC81C2682813B6F7C723614E96E0DEA712D3BB285EF6A6E3A6326	ddk\inc\wdm.h
10	18362ClientEnt	x64	073796FB5EF24AB3B8EE0383F658A537D268A2B105F6DC5307A31B58BCA4E92F	internal\minwin\priv_sdk\inc\hvgdk_mini.h
11	KB4512941V011	x64	DA7936DA0F48EC2F6CDCFABA7C9971F1A33C90206F6EACABB13EF8305EEAEF81	internal\minwin\priv_sdk\inc\hvgdk_mini.h
12	18362ClientEnt	x64	FDC299B0700CA24D2F9625228DC354348E68E309A59E3513186442C482D9136C	internal\minwin\priv_sdk\inc\iumtypes.h
13	KB4512941V011	x64	30A6C17473338D4B54DB23A3A50087823F8CA102A04CA03FD60D4D7FB5DE8BDA	internal\minwin\priv_sdk\inc\iumtypes.h
14	18362ClientEnt	x64	278D777B408BB49DDF5A71DB34CB22D4421CD7F9E060ED13D1E94E1E5AB8FAF5C	internal\minwin\priv_sdk\inc\kernel-processor-power-events.h
15	KB4512941V011	x64	90217EBDB320D953A96779D8F2C2FDC0F2073223C313BA5E657B1C513CC891E5	internal\minwin\priv_sdk\inc\kernel-processor-power-events.h
16	18362ClientEnt	x64	D009EAE94F996512FA0BA3AC036903715B5EFE566F8B10A49123BB3F15241BF1	internal\minwin\priv_sdk\inc\ntpoapi_p.h
17	KB4512941V011	x64	54183CC924B9C254F2B457F9368137929BE0DC2564F818A30605E15D8755BFC5	internal\minwin\priv_sdk\inc\ntpoapi_p.h
18	18362ClientEnt	x64	64E64A96488F854A266E1F4844C713ABC1983AA8E2D0BF7E57A070948CC7995E	internal\sdks\inc\minwin\ntosp.h
19	KB4512941V011	x64	2DB41A2E487A0D81794320165669F4D5E58F046AAF222491DF18CD277E380808	internal\sdks\inc\minwin\ntosp.h
20	18362ClientEnt	x64	842A433BA4EEE8E893E4FB338741216C76E185427F639A2982D467B4EBE820F5	internal\sdks\inc\minwin\zwapi.h
21	KB4512941V011	x64	479BBD7BB0DB3C421850209930BBC25FF2BDEF3AF081E7FC9D42A8E82A746C7	internal\sdks\inc\minwin\zwapi.h
22	18362ClientEnt	x64	69513109A6015D6B3C19B431C5A81112A5C94567FE2CE09F2D65A3349A63BE5A	internal\sdks\inc\wil\staging.h
23	KB4512941V011	x64	FE0947C2DFA272F52D6AC0391AACC84C36A2B1D9943D226905D281C493BB1DE1	internal\sdks\inc\wil\staging.h
24	18362ClientEnt	x64	3A7867622180907F1F6CDD258B7B4071E049C03F264522AE59AB008B704E74D2	minkernel\busdrv\acpi\driver\inc\emguid.h
25	KB4512941V011	x64	BEE3074A1ECAAF1018382AE5E3D922C81C7B37FBE681CFA3E2FAD7E1F0F05B447	minkernel\busdrv\acpi\driver\inc\emguid.h
26	18362ClientEnt	x64	81E793E0D14224555FED270026FBA41F209FAE3FD444E4F9C6EF8FA2597677E6	minkernel\busdrv\acpi\driver\intsup\init.c
27	KB4512941V011	x64	E5ABA551139745BDDE81CEA40564D25F75DF92E134C06E6AC7DCD62A428E6732	minkernel\busdrv\acpi\driver\intsup\init.c
28	18362ClientEnt	x64	45B65827814C0200208E3B93AC5E4E3021F0DB8073BE349E3401B1A53A266D76	minkernel\busdrv\acpi\driver\intsup\irqarb.c
29	KB4512941V011	x64	115E6452B2A9164A9A241B005B936A69EFF0888C66B6CF57C465C9F763A285E2	minkernel\busdrv\acpi\driver\intsup\irqarb.c
30	18362ClientEnt	x64	400FBB40BE02F75F6B2BAA9E0296AB02F864E4C517AF6C21BF1626513C078EE9	minkernel\busdrv\acpi\driver\intsup\irqarb.h
31	KB4512941V011	x64	A43CE9AFBFAAAE04092FD4445CDD2979D9AA4D87B3EC6AF69265915B93AFEBAB	minkernel\busdrv\acpi\driver\intsup\irqarb.h

Implication to updates

- ❑ The more deterministic the executable generation is, the smaller the delta between the original and the update is
- ❑ The smaller the delta is, the tinier the bandwidth is needed to distribute the update

A vision for
the software ecosystem
future

Compilation Location Irrelevancy



Implies:

- 1) support of business recovery,
- 2) potential detection of unauthorized modification,
- 3) security audit / evaluation may be based on easier comparison or matching,
- 4) new business models / processes

Final Suggestion in 4 Steps

1. From the original, identify all the pieces
2. Clone a copy of the pieces
3. Reproduce from the cloned pieces
4. Compare the reproduced with the original

And in the case of OSS development

- ❑ An archive of the development environment that you originally used to build your project is critical
- ❑ A best practice described in <https://www.freecodecamp.org/news/put-your-dev-env-in-github>

Questions