DIFO 2017 - Lab 1 Report

Group number: Group 14

Group members: Wisam Faik, Md Piar Hossain, Cecilia To

# Exercise 1 - Hashing

# Acquire data based on acquisition to ensure integrity of evidence as read-only.

# Chain-of-custody – by having hash values for all evidence acquire.

Our objection for this exercise was to find the hash values of the four files inside exercise 1.

1. What files (and/or folders) did you hash?

’hello’, ’hello(2)’, ’hello(3)’ and ’hello(4)’ files were all hashed using md5deep64.exe, sha256deep64.exe and whirlpooldeep64.exe.

The commands used were:

i) this is using md5deep64:

> C:\...path…\md5deep64.exe hello

da5c61e1edc0f18337e46418e48c1290 ” hello”

> C:\...path…\md5deep64.exe ”hello (2)”

> C:\...path…\md5deep64.exe ”hello (3)”

> C:\...path…\md5deep64.exe ”hello (4)”

da5c61e1edc0f18337e46418e48c1290 ” hello”

ii) this is using sha256deep64:

> C:\Users\cs2lab\Desktop\Forensics\_Tools\md5deep-4.4\sha256deep64.exe hello

> fad878bd261840a4ea4a8277c546d4f46e79bbeb60b059cee41f8b50e28d0e88 C:\Users\cs2lab\Desktop\Lab1\Exercise1\_Hashing\test\hello

iii) this is using whirlpooldeep64:

> C:\Users\cs2lab\Desktop\Forensics\_Tools\md5deep-4.4\whirlpooldeep64.exe hello

>1f4388f4a81a6cfacde955cf5fd84c4e76f12876db3356e2a84efda91f8c44407b3626b770d9752f9b0aa05927e7fb7c66e07ea96ea47ece2ca78a40cedb9d7e 2017:09:08:05:51:37 C:\Users\cs2lab\Desktop\ Lab1\Exercise1\_Hashing\hello

1. Which algorithms did you choose?

Initially, we only used md5 algorithms but we noticed using md5 ’hello’ with ’hello (4) files have same hash value where ’hello (2)’ with ’hello (3)’ file have the same hash value. Because of this finding, we decided to uswe sha256 and whirlpool algorithms to ensure and confirm if these files truely have the same hash values. While using sha256 and whirlpool algorithms, we discovered the hash values were not the same for all four files.

Our conc for longer lenght of bit hash in the message length

The algorithms chosen for hashing ’hello’, ’hello(2)’, ’hello(3)’ and ’hello(4)’ were sha256, sha512 from whirlpooldeep64 and md5. The reason algorithm sha256 and whirlpool generated different hashbalvues because sha256 digests input message length up to 264 bits in length and whirlpool digests input message length up to 2256 which results into different hash values. Whirlpool generates 512 bits length and sha256 generates 256 bits length.

1. Suppose you would need to calculate the hash sums of several files and folders, how could you do that using the tools and resources provided? Provide a description and exact commands.

According to the <http://md5deep.sourceforge.net/>, ’-r’ flag can be used to hash all files within a folder recursively. This ’–r’ option doesn’t hash the folder only the files inside a folder.

PS C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing> C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017

\Lab1\Exercise1\_Hashing\whirlpooldeep64.exe -t -r C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\

test

1f4388f4a81a6cfacde955cf5fd84c4e76f12876db3356e2a84efda91f8c44407b3626b770d9752f9b0aa05927e7fb7c66e07ea96ea47ece2ca78a40

cedb9d7e 2017:09:14:12:27:34 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\hello

959593fe62721c9d058831eaa742f103d1b853b43a81a94dd30cc89a6dafb6926b64bdd7b0ef16a4c566601f81af95988fb952720482562a6269728e

f5f5d5fb 2017:09:14:12:27:34 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\hello (3)

aae0a840704962b3026cf5b2058aa1a3d7752e6d562e0a843ce0abf7107666fb475ac45df08587c468f7754847f2be4cebd1172dedfebfaa6527c8da

2b1bc364 2017:09:14:12:27:34 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\hello (2)

4324731f2340b0d5ce741f566abd7ebf8a1c18a15e4835bd8c25bdc974ec275a6e088982422456060bf145d7013cd0aa8ac1b62ee3f8149bfd6490e6

a5a95efa 2017:09:14:12:27:34 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\hello (4)

ecd8a5ca2e94899420d1b4ba150f23e4fcfa70fd74062f9e341a55e26db375adcedc4becacd90450928d91c1d78087a66304c5cb010ade8ff03a9235

69167640 2017:09:14:12:27:22 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\test\_md5\_hello.

txt

cd5324f733eff09d647e25bedb4e9d20dc0765ad1ccfcdfd25316fb1df03914634d767fb311d00c6e19c6ec9f6d1430c24a4f87d947477a377cce054

2402c8c7 2017:09:14:12:27:22 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\test\_sha256\_hel

lo.txt

0d8a4947324854e785120f458cf49c3f050d3c6f7053d961eb89b8898e0bf9eafd1aa1025f06de20de869ee881bd0b00d368aa4387f5b2dfff04107e

00bd03bb 2017:09:14:12:27:22 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\testwhirlpool\_h

ello.txt

19fa61d75522a4669b44e39c1d2e1726c530232130d407f89afee0964997f7a73e83be698b288febcf88e3e03c4f0757ea8964e59b63d93708b138cc

42a66eb3 2017:09:14:12:27:22 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\test\_hello.txt

cd4228bc5292bb243bd7a18d5db8419895c1393e52c3ddbf6561ce599085fc935bfe6dde74d13566b0a2f6decbb4e6a6c64bb5a0c753911698b695be

522247db 2017:09:14:12:27:22 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\test\_wp\_hello.t

xt

d34fe1349fe6e6ef33010a48af7b04498eefc8702563e3d40bb34cb01705c6d0f2a5cb1a969ddcdb37f3547e531addad1b6ad3c1f8cc9c582a68185b

8440c91f 2017:09:14:12:27:22 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\time\_compare\_te

st\_hello.txt

PS C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing> C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017

\Lab1\Exercise1\_Hashing\md5deep64.exe -t -r C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test

da5c61e1edc0f18337e46418e48c1290 2017:09:14:12:27:34 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hash

ing\test\hello

cdc47d670159eef60916ca03a9d4a007 2017:09:14:12:27:34 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hash

ing\test\hello (2)

cdc47d670159eef60916ca03a9d4a007 2017:09:14:12:27:34 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hash

ing\test\hello (3)

da5c61e1edc0f18337e46418e48c1290 2017:09:14:12:27:34 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hash

ing\test\hello (4)

b076b440e2ac6e392a7172a60b107042 2017:09:14:12:27:22 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hash

ing\test\testwhirlpool\_hello.txt

d41d8cd98f00b204e9800998ecf8427e 2017:09:14:12:27:22 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hash

ing\test\test\_hello.txt

b2e85f921e590c143c301a6713e5fe0d 2017:09:14:12:27:22 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hash

ing\test\test\_md5\_hello.txt

ed82a7abc238002699079a7a30a2b9d0 2017:09:14:12:27:22 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hash

ing\test\test\_sha256\_hello.txt

649be596531b5f0afd118f1d45616c51 2017:09:14:12:27:22 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hash

ing\test\test\_wp\_hello.txt

917311b1746e8706361921326eb6b91b 2017:09:14:12:27:22 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hash

ing\test\time\_compare\_test\_hello.txt

PS C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing>

d)

# Exercise 2 - File Headers

# 

# Exercise 3 – Anti Forensics

# Exercise 4 - Acquisition

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec a diam lectus. Sed sit amet ipsum mauris. Maecenas congue ligula ac quam viverra nec consectetur ante hendrerit. Donec et mollis dolor. Praesent et diam eget libero egestas mattis sit amet vitae augue. Nam tincidunt congue enim, ut porta lorem lacinia consectetur. Donec ut libero sed arcu vehicula ultricies a non tortor. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean ut gravida lorem. Ut turpis felis, pulvinar a semper sed, adipiscing id dolor. Pellentesque auctor nisi id magna consequat sagittis. Curabitur dapibus enim sit amet elit pharetra tincidunt feugiat nisl imperdiet. Ut convallis libero in urna ultrices accumsan. Donec sed odio eros. Donec viverra mi quis quam pulvinar at malesuada arcu rhoncus. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. In rutrum accumsan ultricies. Mauris vitae nisi at sem facilisis semper ac in est.

# Exercise 5 - Cracking

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec a diam lectus. Sed sit amet ipsum mauris. Maecenas congue ligula ac quam viverra nec consectetur ante hendrerit. Donec et mollis dolor. Praesent et diam eget libero egestas mattis sit amet vitae augue. Nam tincidunt congue enim, ut porta lorem lacinia consectetur. Donec ut libero sed arcu vehicula ultricies a non tortor. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean ut gravida lorem. Ut turpis felis, pulvinar a semper sed, adipiscing id dolor. Pellentesque auctor nisi id magna consequat sagittis. Curabitur dapibus enim sit amet elit pharetra tincidunt feugiat nisl imperdiet. Ut convallis libero in urna ultrices accumsan. Donec sed odio eros. Donec viverra mi quis quam pulvinar at malesuada arcu rhoncus. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. In rutrum accumsan ultricies. Mauris vitae nisi at sem facilisis semper ac in est.

# Exercise 6 - Steganography

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec a diam lectus. Sed sit amet ipsum mauris. Maecenas congue ligula ac quam viverra nec consectetur ante hendrerit. Donec et mollis dolor. Praesent et diam eget libero egestas mattis sit amet vitae augue. Nam tincidunt congue enim, ut porta lorem lacinia consectetur. Donec ut libero sed arcu vehicula ultricies a non tortor. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean ut gravida lorem. Ut turpis felis, pulvinar a semper sed, adipiscing id dolor. Pellentesque auctor nisi id magna consequat sagittis. Curabitur dapibus enim sit amet elit pharetra tincidunt feugiat nisl imperdiet. Ut convallis libero in urna ultrices accumsan. Donec sed odio eros. Donec viverra mi quis quam pulvinar at malesuada arcu rhoncus. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. In rutrum accumsan ultricies. Mauris vitae nisi at sem facilisis semper ac in est.