Name: Ashish Das

Reg. No.: 19BCE1160

Faculty: Nagraj S. V.

Exercise Number: 1

05/08/2021

Hash Functions for verifying the integrity of files or messages

Aim: - To understand how the hash functions are used for verifying the integrity of files or messages.

Tools Used: FileFormat.Info – Hash Checker (http://www.fileformat.info/tool/hash.htm)

Question 1:

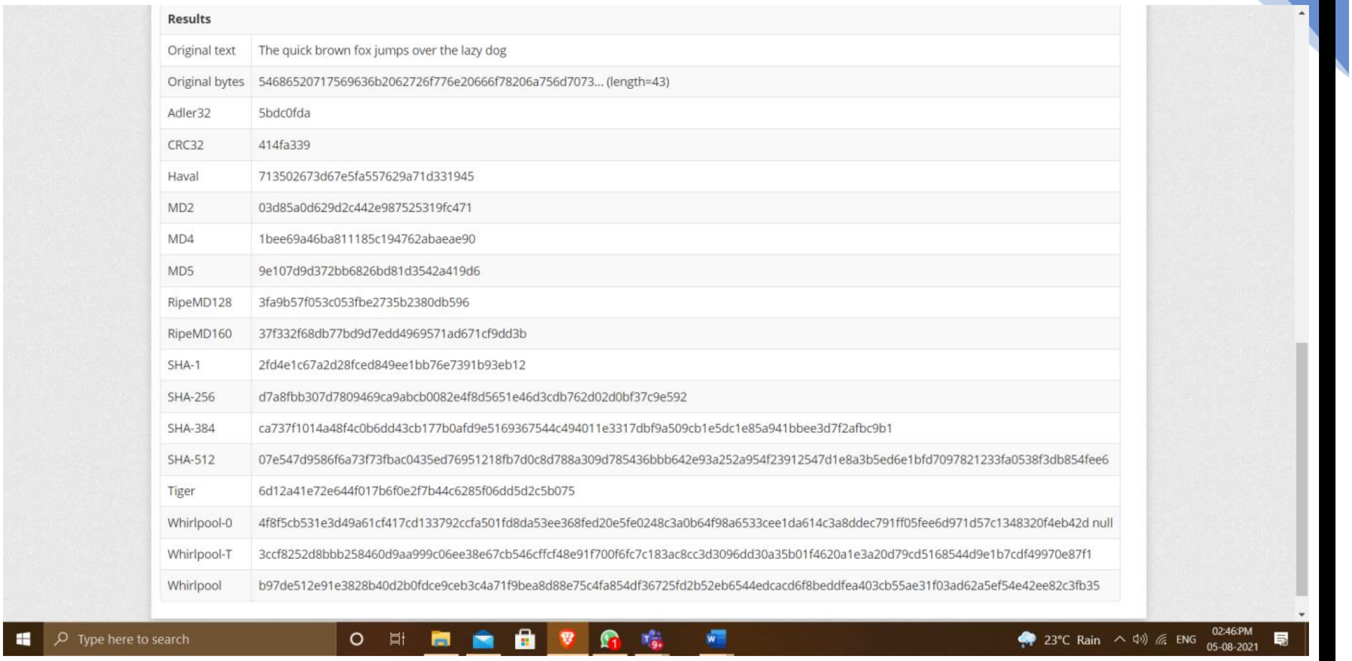
Make use of any online tool to compute the MD5, SHA-1, SHA-256 hash values of the two strings given below

1) The quick brown fox jumps over the lazy dog
2) The quick brown fox jumps over the lazy dogs

Note that the two strings above are slightly different yet their hash values are quite different.

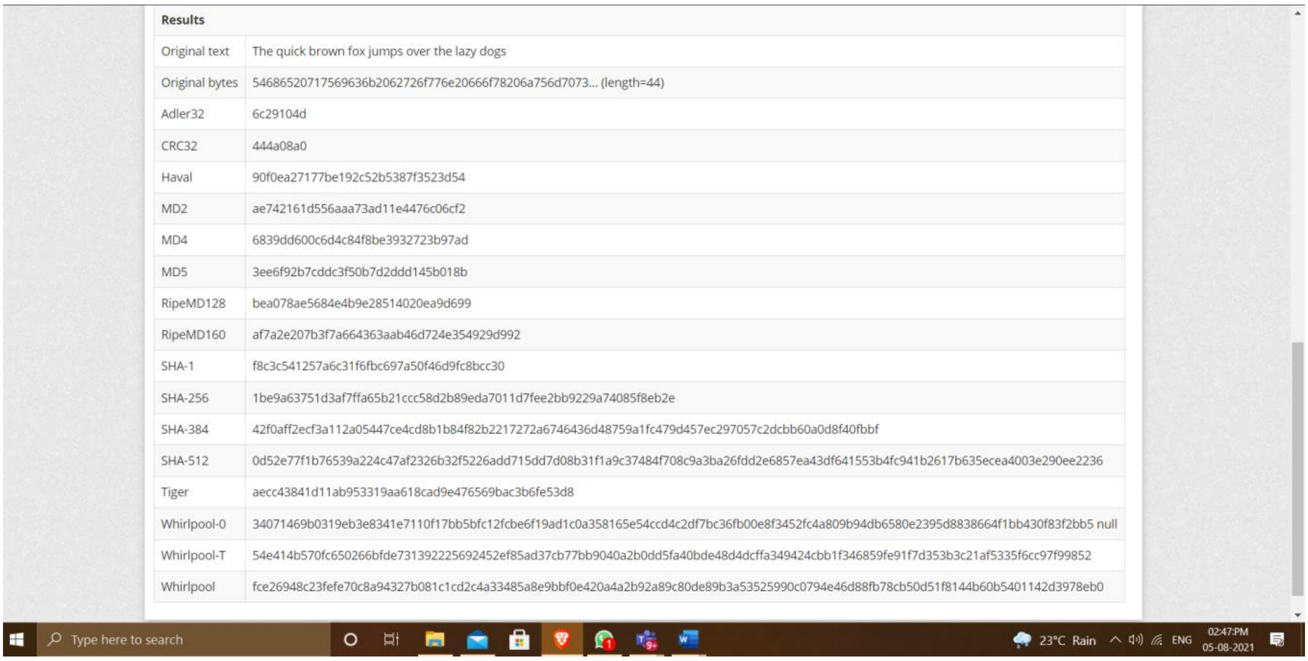
Screenshots:

1) The quick brown fox jumps over the lazy dog



Results	
Original text	The quick brown fox jumps over the lazy dog
Original bytes	54686520717569636b2062726f776e20666f78206a756d7073... (length=43)
Adler32	5bdc0fda
CRC32	414fa339
Haval	713502673d67e5fa557629a71d331945
MD2	03d85a0d629d2c442e987525319fc471
MD4	1bee69a46ba811185c194762abaeae90
MD5	9e107d9d372bb6826bd81d3542a419d6
RipeMD128	3fa9b57f053c053fbe2735b2380db596
RipeMD160	37f332f68db77bd9d7edd4969571ad671cf9dd3b
SHA-1	2fd4e1c67a2d28fced849ee1bb76e7391b93eb12
SHA-256	d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592
SHA-384	ca737f1014a48f4c0b6dd43cb177b0afd9e5169367544c494011e3317dbf9a509cb1e5dc1e85a941bbee3d7f2afbc9b1
SHA-512	07e547d9586f6a73f73fbac0435ed76951218fb7d0c8d788a309d785436bbb642e93a252a954f23912547d1e8a3b5ed6e1bfd7097821233fa0538f3db854fee6
Tiger	6d12a41e72e644f017b6f0e2f7b44c6285f06dd5d2c5b075
Whirlpool-0	4f8f5cb531e3d49a61cf417cd133792ccfa501fd8da53ee368fed20e5fe0248c3a0b64f98a6533cee1da614c3a8ddec791ff05fee6d971d57c1348320f4eb42d null
Whirlpool-T	3ccf8252d8bbb258460d9aa999c06ee38e67cb546cffcf48e91f700f6fc7c183ac8cc3d3096dd30a35b01f4620a1e3a20d79cd5168544d9e1b7cdf49970e87f1
Whirlpool	b97de512e91e3828b40d2b0fdce9ceb3c4a71f9bea8d88e75c4fa854df36725fd2b52eb6544edcacd6f8beddfea403cb55ae31f03ad62a5ef54e42ee82c3fb35

2) The quick brown fox jumps over the lazy dogs



Results	
Original text	The quick brown fox jumps over the lazy dogs
Original bytes	54686520717569636b2062726f776e20666f78206a756d7073... (length=44)
Adler32	6c29104d
CRC32	444a08a0
Haval	90f0ea27177be192c52b5387f3523d54
MD2	ae742161d556aaa73ad11e4476c06cf2
MD4	6839dd600c6d4c84f8be3932723b97ad
MD5	3ee6f92b7cddc3f50b7d2ddd145b018b
RipeMD128	bea078ae5684e4b9e28514020ea9d699
RipeMD160	af7a2e207b3f7a664363aab46d724e354929d992
SHA-1	f8c3c541257a6c31f6fbc697a50f46d9fc8bcc30
SHA-256	1be9a63751d3af7ffa65b21ccc58d2b89eda7011d7fee2bb9229a74085f8eb2e
SHA-384	42f0aff2ecf3a112a05447ce4cd8b1b84f82b2217272a6746436d48759a1fc479d457ec297057c2dcbb60a0d8f40fbbf
SHA-512	0d52e77f1b76539a224c47af2326b32f5226add715dd7d08b31f1a9c37484f708c9a3ba26fdd2e6857ea43df641553b4fc941b2617b635ecea4003e290ee2236
Tiger	aecc43841d11ab953319aa618cad9e476569bac3b6fe53d8
Whirlpool-0	34071469b0319eb3e8341e7110f17bb5bfc12fcbe6f19ad1c0a358165e54ccd4c2df7bc36fb00e8f3452fc4a809b94db6580e2395d8838664f1bb430f83f2bb5 null
Whirlpool-T	54e414b570fc650266bfde731392225692452ef85ad37cb77bb9040a2b0dd5fa40bde48d4dcffa349424cbb1f346859fe91f7d353b3c21af5335f6cc97f99852
Whirlpool	fce26948c23fefe70c8a94327b081c1cd2c4a33485a8e9bbf0e420a4a2b92a89c80de89b3a53525990c0794e46d88fb78cb50d51f8144b60b5401142d3978eb0

Inference:

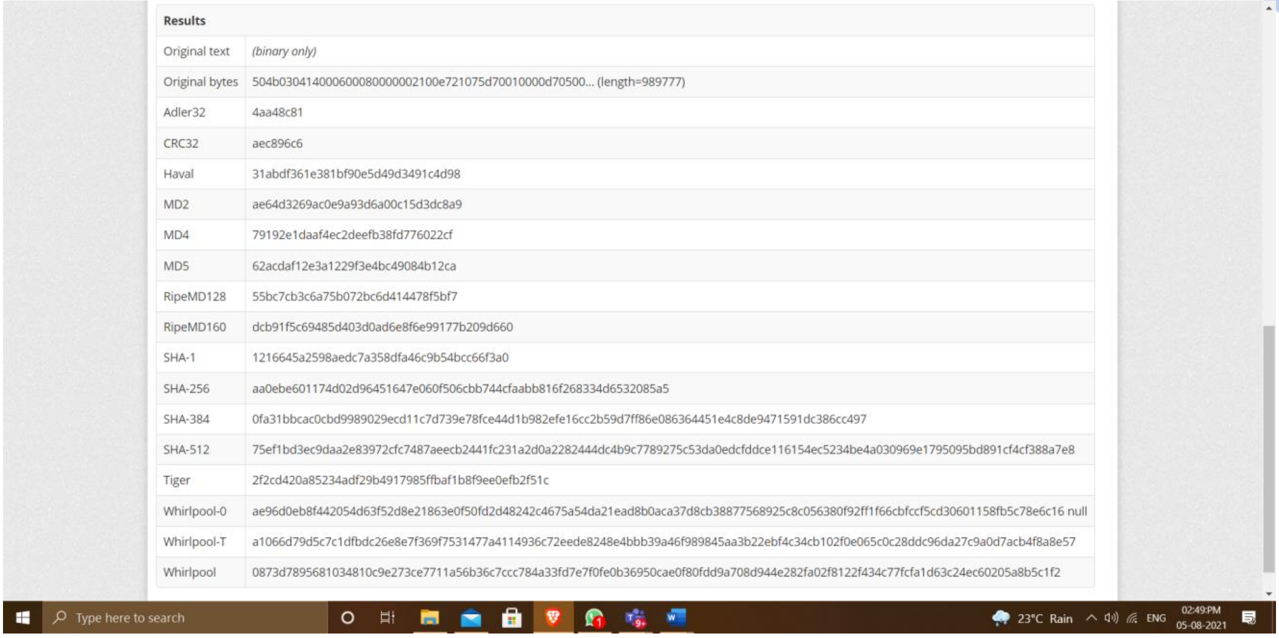
We can clearly see in the above two screenshots that despite the only change in the strings being one addition of s the difference seen in their hash value is quite significant.

Question 2:

Perform hash calculations for any TWO files of your choice using the following hash functions: Adler32, CRC32, Haval, MD2, MD4, MD5, RipeMD-128, RipeMD-160, SHA-1, SHA-256, SHA-384, SHA-512, Tiger, and Whirlpool

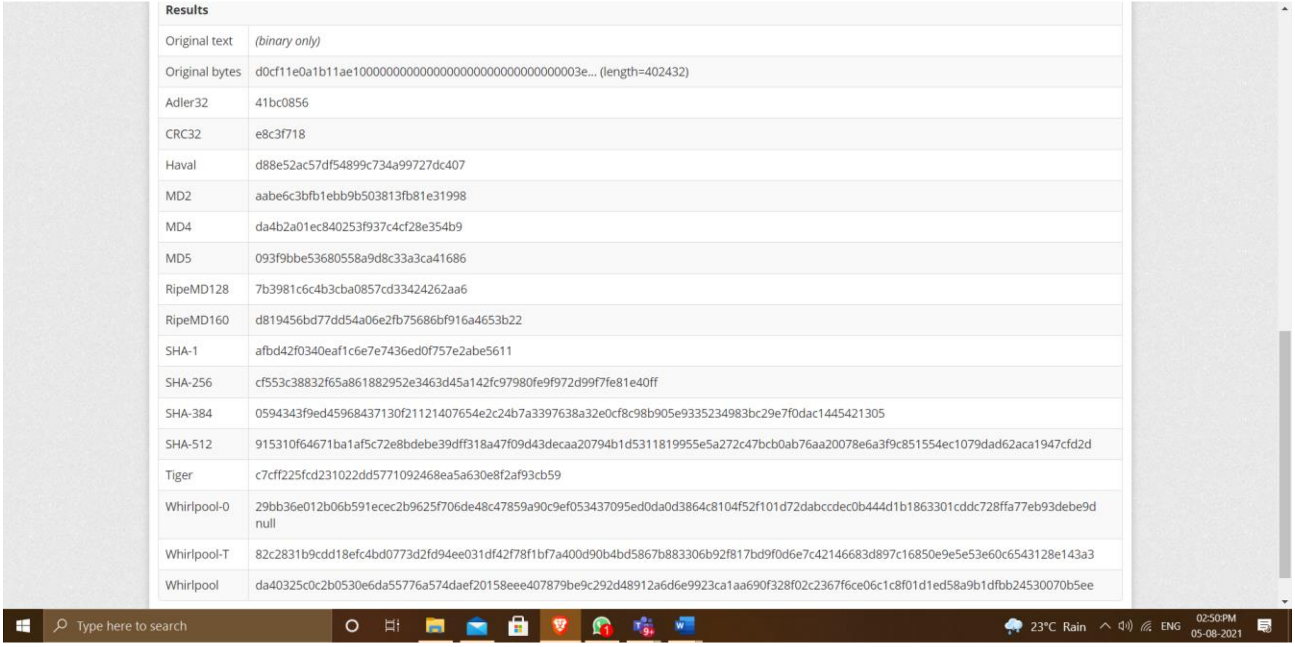
Screenshots:

1) The Hash calculation of the First File



Results	
Original text	*(binary only)*
Original bytes	504b0304140006000800000002100e721075d70010000d70500... (length=989777)
Adler32	4aa48c81
CRC32	aec896c6
Haval	31abdf361e381bf90e5d49d3491c4d98
MD2	ae64d3269ac0e9a93d6a00c15d3dc8a9
MD4	79192e1daaf4ec2deefb38fd776022cf
MD5	62acdaf12e3a1229f3e4bc49084b12ca
RipeMD128	55bc7cb3c6a75b072bc6d414478f5bf7
RipeMD160	dcb91f5c69485d403d0ad6e8f6e99177b209d660
SHA-1	1216645a2598aedc7a358dfa46c9b54bcc66f3a0
SHA-256	aa0ebe601174d02d96451647e060f506cbb744cfaabb816f268334d6532085a5
SHA-384	0fa31bbcac0cbd9989029ecd11c7d739e78fce44d1b982efe16cc2b59d7ff86e086364451e4c8de9471591dc386cc497
SHA-512	75ef1bd3ec9daa2e83972cfc7487aeecb2441fc231a2d0a2282444dc4b9c7789275c53da0edcfddce116154ec5234be4a030969e1795095bd891cf4cf388a7e8
Tiger	2f2cd420a85234adf29b4917985ffbaf1b8f9ee0efb2f51c
Whirlpool-0	ae96d0eb8f442054d63f52d8e21863e0f50fd2d48242c4675a54da21ead8b0aca37d8cb38877568925c8c056380f92ff1f66cbfccf5cd30601158fb5c78e6c16 null
Whirlpool-T	a1066d79d5c7c1dfbdc26e8e7f369f7531477a4114936c72eede8248e4bbb39a46f989845aa3b22ebf4c34cb102f0e065c0c28ddc96da27c9a0d7acb4f8a8e57
Whirlpool	0873d7895681034810c9e273ce7711a56b36c7ccc784a33fd7e7f0fe0b36950cae0f80fdd9a708d944e282fa02f8122f434c77fcfa1d63c24ec60205a8b5c1f2

2) The Hash calculation of the Second File



Results	
Original text	*(binary only)*
Original bytes	d0cf11e0a1b11ae1000000000000000000000000000000003e... (length=402432)
Adler32	41bc0856
CRC32	e8c3f718
Haval	d88e52ac57df54899c734a99727dc407
MD2	aabe6c3bfb1ebb9b503813fb81e31998
MD4	da4b2a01ec840253f937c4cf28e354b9
MD5	093f9bbe53680558a9d8c33a3ca41686
RipeMD128	7b3981c6c4b3cba0857cd33424262aa6
RipeMD160	d819456bd77dd54a06e2fb75686bf916a4653b22
SHA-1	afbd42f0340eaf1c6e7e7436ed0f757e2abe5611
SHA-256	cf553c38832f65a861882952e3463d45a142fc97980fe9f972d99f7fe81e40ff
SHA-384	0594343f9ed45968437130f21121407654e2c24b7a3397638a32e0cf8c98b905e9335234983bc29e7f0dac1445421305
SHA-512	915310f64671ba1af5c72e8bdebe39dff318a47f09d43decaa20794b1d5311819955e5a272c47bcb0ab76aa20078e6a3f9c851554ec1079dad62aca1947cfd2d
Tiger	c7cff225fcd231022dd5771092468ea5a630e8f2af93cb59
Whirlpool-0	29bb36e012b06b591ecec2b9625f706de48c47859a90c9ef053437095ed0da0d3864c8104f52f101d72dabccdec0b444d1b1863301cddc728ffa77eb93debe9d null
Whirlpool-T	82c2831b9cdd18efc4bd0773d2fd94ee031df42f78f1bf7a400d90b4bd5867b883306b92f817bd9f0d6e7c42146683d897c16850e9e5e53e60c6543128e143a3
Whirlpool	da40325c0c2b0530e6da55776a574daef20158eee407879be9c292d48912a6d6e9923ca1aa690f328f02c2367f6ce06c1c8f01d1ed58a9b1dfbb24530070b5ee

Question 3:

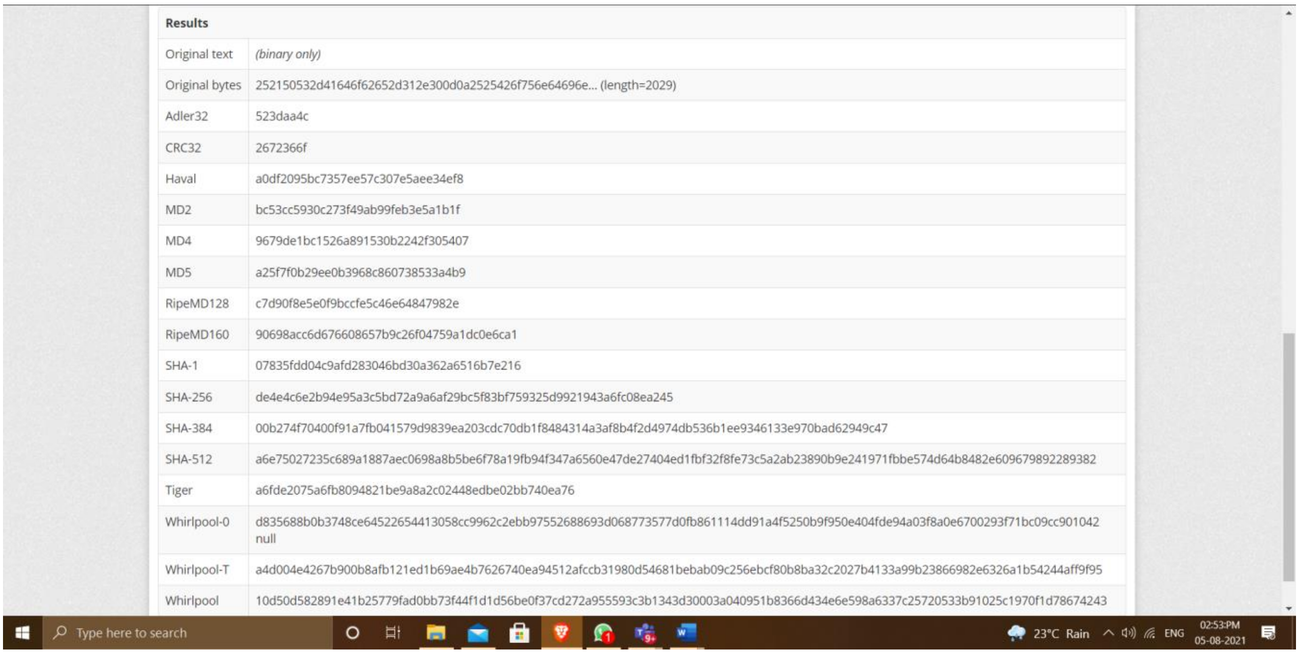
Collision

Consider the two postscript files at http://web.archive.org/web/20071226014140/http://www.cits.rub.de/MD5Collisions/

- Are the two files identical?
- Now compute the MD5 hash values for each of them. Are they equal? If so why does this happen?

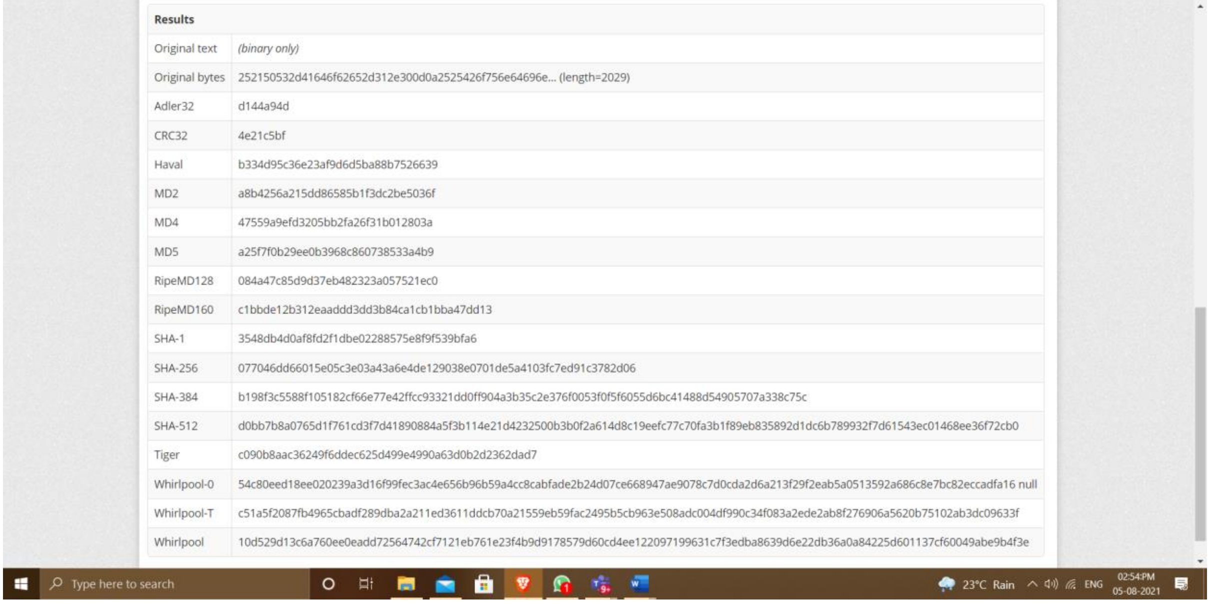
Screenshots:

1) Hash calculation of letter_of_rec.ps



Results	
Original text	*(binary only)*
Original bytes	252150532d41646f62652d312e300d0a2525426f756e64696e... (length=2029)
Adler32	523daa4c
CRC32	2672366f
Haval	a0df2095bc7357ee57c307e5aee34ef8
MD2	bc53cc5930c273f49ab99feb3e5a1b1f
MD4	9679de1bc1526a891530b2242f305407
MD5	a25f7f0b29ee0b3968c860738533a4b9
RipeMD128	c7d90f8e5e0f9bccfe5c46e64847982e
RipeMD160	90698acc6d676608657b9c26f04759a1dc0e6ca1
SHA-1	07835fdd04c9afd283046bd30a362a6516b7e216
SHA-256	de4e4c6e2b94e95a3c5bd72a9a6af29bc5f83bf759325d9921943a6fc08ea245
SHA-384	00b274f70400f91a7fb041579d9839ea203cdc70db1f8484314a3af8b4f2d4974db536b1ee9346133e970bad62949c47
SHA-512	a6e75027235c689a1887aec0698a8b5be6f78a19fb94f347a6560e47de27404ed1fbf32f8fe73c5a2ab23890b9e241971fbbe574d64b8482e609679892289382
Tiger	a6fde2075a6fb8094821be9a8a2c02448edbe02bb740ea76
Whirlpool-0	d835688b0b3748ce64522654413058cc9962c2ebb97552688693d068773577d0fb861114dd91a4f5250b9f950e404fde94a03f8a0e6700293f71bc09cc901042 null
Whirlpool-T	a4d004e4267b900b8afb121ed1b69ae4b7626740ea94512afccb31980d54681bebab09c256ebcf80b8ba32c2027b4133a99b23866982e6326a1b54244aff9f95
Whirlpool	10d50d582891e41b25779fad0bb73f44f1d1d56be0f37cd272a955593c3b1343d30003a040951b8366d434e6e598a6337c25720533b91025c1970f1d78674243

2) Hash Calculation of order.ps



Results	
Original text	*(binary only)*
Original bytes	252150532d41646f62652d312e300d0a2525426f756e64696e... (length=2029)
Adler32	d144a94d
CRC32	4e21c5bf
Haval	b334d95c36e23af9d6d5ba88b7526639
MD2	a8b4256a215dd86585b1f3dc2be5036f
MD4	47559a9efd3205bb2fa26f31b012803a
MD5	a25f7f0b29ee0b3968c860738533a4b9
RipeMD128	084a47c85d9d37eb482323a057521ec0
RipeMD160	c1bbde12b312eaaddd3dd3b84ca1cb1bba47dd13
SHA-1	3548db4d0af8fd2f1dbe02288575e8f9f539bfa6
SHA-256	077046dd66015e05c3e03a43a6e4de129038e0701de5a4103fc7ed91c3782d06
SHA-384	b198f3c5588f105182cf66e77e42ffcc93321dd0ff904a3b35c2e376f0053f0f5f6055d6bc41488d54905707a338c75c
SHA-512	d0bb7b8a0765d1f761cd3f7d41890884a5f3b114e21d4232500b3b0f2a614d8c19eefc77c70fa3b1f89eb835892d1dc6b789932f7d61543ec01468ee36f72cb0
Tiger	c090b8aac36249f6ddec625d499e4990a63d0b2d2362dad7
Whirlpool-0	54c80eed18ee020239a3d16f99fec3ac4e656b96b59a4cc8cabfade2b24d07ce668947ae9078c7d0cda2d6a213f29f2eab5a0513592a686c8e7bc82eccadfa16 null
Whirlpool-T	c51a5f2087fb4965cbadf289dba2a211ed3611ddcb70a21559eb59fac2495b5cb963e508adc004df990c34f083a2ede2ab8f276906a5620b75102ab3dc09633f
Whirlpool	10d529d13c6a760ee0eadd72564742cf7121eb761e23f4b9d9178579d60cd4ee122097199631c7f3edba8639d6e22db36a0a84225d601137cf60049abe9b4f3e

Inference:

- No, the two files are not identical.
- The MD5 hash value of both the files are the same (which can be observed in the above screenshots). This happens due to the hash collision.
-

Result:

- Developed an understanding on how the hash functions are used to verify the integrity of the files as well as about hash collision.