DIGITAL FORENSICS LAB

Exercise 1	
Name	S Shyam Sundaram
Registration Number	19BCE1560
Slot	L39+L40
Faculty	Dr. Seshu Babu Pulgara
Date	10th August, 2021

AIM

To verify the integrity of files or messages using Hash functions

PART A

Make use of any online tool such as http://www.fileformat.info/tool/hash.htm 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

   MD5: 9e107d9d372bb6826bd81d3542a419d6
   SHA-1: 2fd4e1c67a2d28fced849ee1bb76e7391b93eb12
   SHA-256: d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592

2. The quick brown fox jumps over the lazy dogs

   MD5: 3ee6f92b7cddc3f50b7d2ddd145b018b
   SHA-1: f8c3c541257a6c31f6fbc697a50f46d9fc8bcc30
   SHA-256: 1be9a63751d3af7ffa65b21ccc58d2b89eda7011d7fee2bb9229a74085f8eb2e

3. the quick brown fox jumps over the lazy dog

   MD5: 5e48a737eaff799917707b2815af10fc
   SHA-1: cbf88a749e1a87a236bee745f842f462b97e374f
   SHA-256: b779f6eaff679cbf30b4b784c76eb04abda965800fe2e40f1f47b0a89177fe19

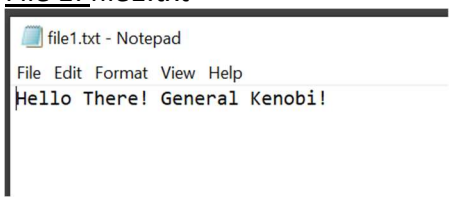
OBSERVATIONS

- For a unique string, the hash value will too, be unique.
- Even a difference of one character (the presence or absence too) can result in a completely different hash value (sentence 1 and 2).
- The case of the characters affects the hash value too. Even the change in case of one letter can result in a completely different hash value (sentence 3).
- Different hash functions and algorithms give a different hash value for the same input.
- The length of the hash value produced by MD5, SHA-1 and SHA-256 result in 32-, 160- and 256-bit long hash values, independent of the length of the input.

PART B

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.

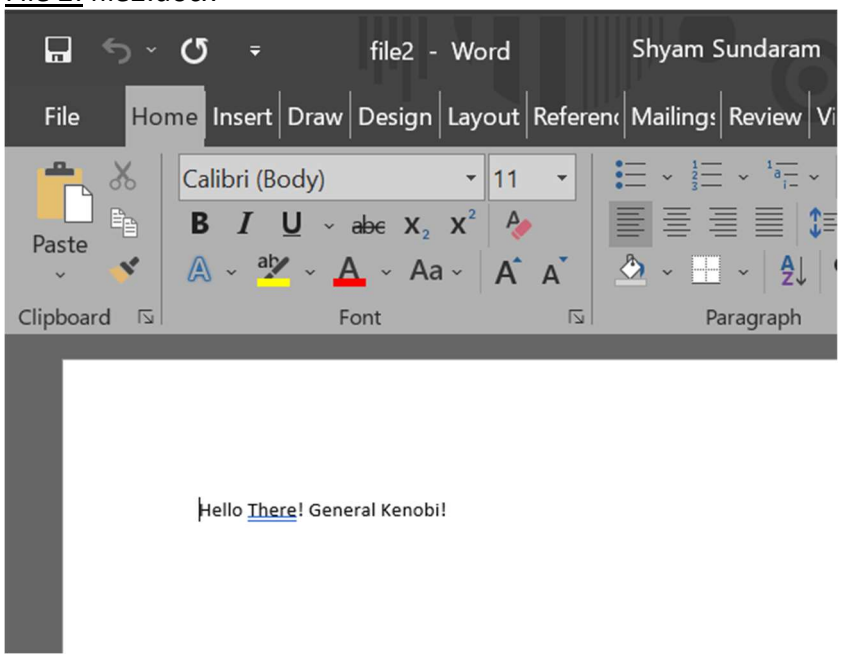
File 1: file1.txt



Hash Values:

Adler32	8cb709a5
CRC32	c2bb8330
Haval	75b23877188383c49da4f8c555b2da6f
MD2	ebb17c6942acb059721d299842f25961
MD4	8d23c442235b80d551e7a3a4050f38ce
MD5	ba84586ceb2834a18a73da0f2f1e7281
RipeMD128	139d2792050482a4f0937eeb9e8d4daa
RipeMD160	ca7874064be270b4655a12529a98995a83c4d780
SHA-1	db62ab2a2ab141add49a1d21fb6367c6852098bd
SHA-256	88ad629fbfd120d3afd5b5747042e5d2446639d818e75a809f2c6c2959e785e1
SHA-384	cf2caf49c78f49b065660db01047384fb73cd5d62a87089ff18d6b5adb20eddb079c9942acb9504b283029b053139f8b
SHA-512	6bf0353dae7590cff31029432017578d268c2e905a2e5f1c32f128d5a505ed8f2f36c2624c95fa11cc3c1ee2f7edc29bade2310610a0ca4768f9691362b0afc3
Tiger	8ef6e39e17addcbba935bfd4921d46717a472f0fd50f6bb4
Whirlpool-0	a690acbbda347d58ce73444cee27bf12b4d9c3e31550c0681a0bad9e345f50d3fd0446dddec46dc63ec60312a399d1169077c255542946832e99668a12383e7e null
Whirlpool-T	ff5cee368898abed38e06d8c17789ea3e4ec7086e7d531f69f433455d78c75cb4896cd7169f0d16820e1319794c6ad8f8cc04e96e13df8d9980bfd3281a1132e
Whirlpool	61943bf7e23596e2abe89b5185f90a7170a3c86f3a30f29cbc968580164cbe29908ca1681485107296c7e8ed6ee16a8018cdd4025e4d45ee9b805ff1e6ffe2f1

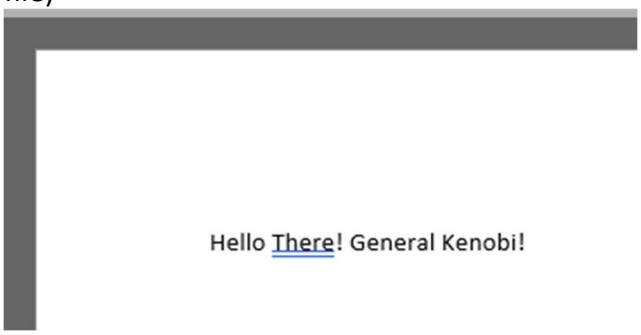
File 2: file2.docx



Hash Values:

Adler32	1c5c7e9d
CRC32	89386860
Haval	f62d18c5a3d0fc1001c84e66d3db47e4
MD2	3154ca0240e1b643e1b4855156738529
MD4	da0bd36451206a0dbce3625862addbe8
MD5	cc949c95801bd0458dad189adc578c9f
RipeMD128	f234fb36cbc35558eb88f7f2d09c367d
RipeMD160	4d2911f718d0b49902e415db753996c58ab95ffa
SHA-1	63b9296f78c4f584b1e8e8fe69787c80ca2cba2d
SHA-256	75497a168c0ba8cd3a9d47b002d756fa8b54bdbf389ead59fb8b90925ef5dfa0
SHA-384	c8e68abfeab43d653239fa6d139a8245432c4bb5f7b9659f3e1d4a4f1c8218b2f2fb6013cbaeb041f6687cce6be09881
SHA-512	39f39511b872a053bdc4c104eb240a56e1a1a38f148ae2bd680c5cf70750a552073c977b4bce75e52da1999440024cb3631ffe1f2f79896b9e1d9149023dd1c0
Tiger	09069feaef4feba87e0ccb37e6c6ab00d2ac0fc31599d14a
Whirlpool-0	eec08cfd32d9a7c189919d20102a8515329b99d82d525ca2264e847af480ffc991a3c6a6bfe9d0c4f3ab99bf9bd2ef7b3070980725f78ff071adaab16bd9084c null
Whirlpool-T	f748ecc3e4de0567c28edf4a6c523fa45bb30d33a3d2ddb0cac040ea14eac53fb2af2c208b78b43adb6c12e270bdd7221f87fb72e53ea9063b06a754410f2fec
Whirlpool	86c5ddd97f30a55cdbdd1da0bf6ba286afa6c1a00f100295daa9d00d7bd8dc30e8317f1967a73b4cedf0c08fe4c5ab2a4059292026031436 82a263b9a9336b18

File 3: file2.docx (The same file content. But the file was deleted and the content was copy pasted to a new document with the same name and extension. Thus, essentially, the same file)



Hash Values:

Adler32	3a57849c
CRC32	16654ae1
Haval	0bd329f445146bdb2377a8dd4690ddc0
MD2	154624fe255a3b4531ee8f1f7e028c76
MD4	dd1eefeedc6b9a0d7a6ce92e5f07d593
MD5	8d3228e9fc3ec36c49da478d830a6ecb
RipeMD128	7d545078364205acfecff56aac1b261f
RipeMD160	519ff6f3ead16a6e64fe32be70501f06bcde98c8
SHA-1	8ceb3e3c27b79b0dd011727fadb361ea0db4a262
SHA-256	bac938e75c1c62362597933be78f6c0817d12924a71574556562fbdbaed38714
SHA-384	4340f251bd5646e52b9ff740093c27c5ba9731410bafc3f23ff4be4f44d1db634094afb7e40b12bf8bee15ffed988bcb
SHA-512	f81953e3cef77152e240c3273a1f671561b7c083292dacb4c8d21090f12efe1eb5da5695ab2b32af27abdc2c40b24812aa0cb3c73a4aa29e7b4d221b58efbf37
Tiger	99f3fce8b1be5b18e858fa7a296b32596abbeb59585eb5ed
Whirlpool-0	a141c0c6367c1aeb365ee4098f5c20b7623b432d4c3fc156d4f8ba0c99f4b11d9769c7bc3407894c3c1deacdf445dbe213d1d6fc93fb7737579e881e66ce0db2 null
Whirlpool-T	845f2d73fbbe424e02ebc45681c55ede880b8f980045354dad68917ce949c40e104198de1d9be496ad0db6649120586bac43d400835b1f26eb88686e1d55ff08
Whirlpool	8e18da49f49a6a42e4bf2b1cb0646f85c553f84dcd813cc5516e1c1fbb9dd2c8531cc199cb8ab9be51311471794ccfbf9707d336eaaba5babdd4796a25c95819

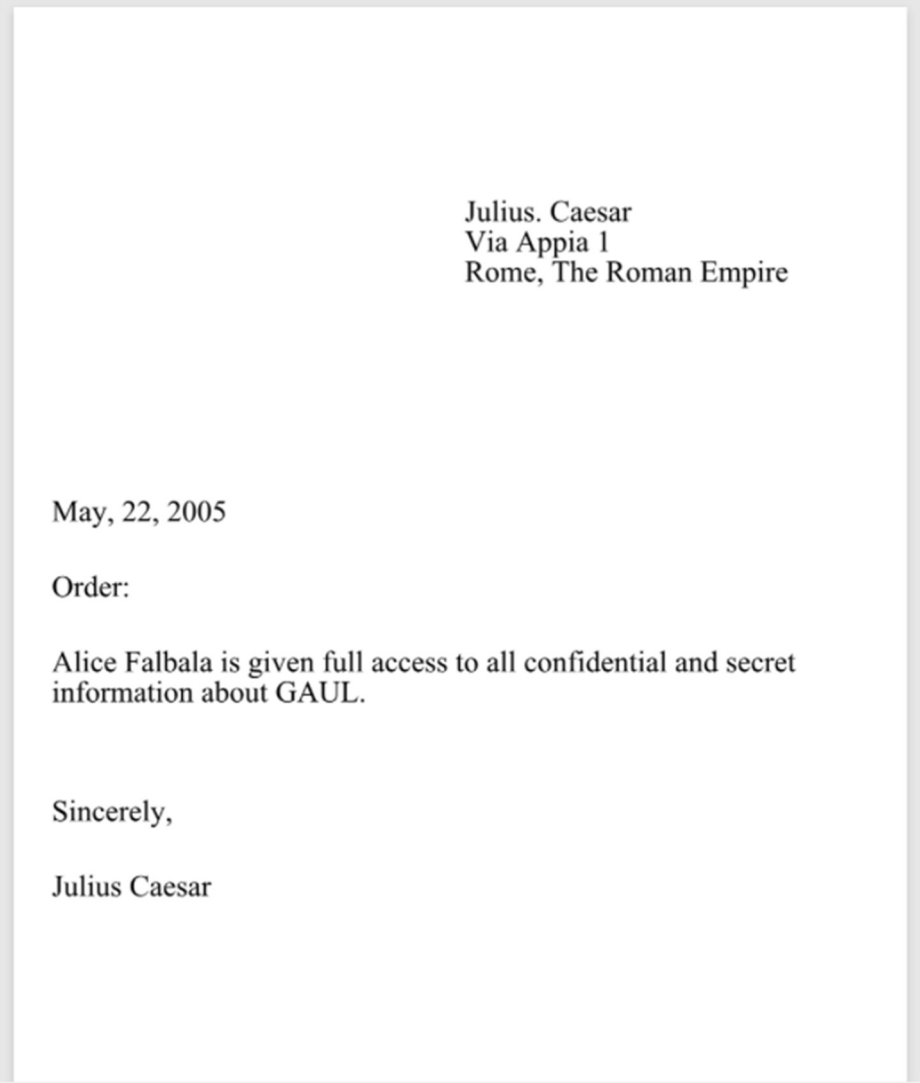
OBSERVATIONS

- The same observations from part A are seen here. Length of the hash values (of MD5, SHA-1 and SHA-256) are independent of the input length (or type). Also, a minute difference in data can give very different hash values.
- Though file1 and file2 have the same content, they are of different file types. One is a text file while the second is an MS Word docx file. Yet, they yield distinct hash values. Thus, files of different type yield different hash values.
- Another very interesting observation is made. File 2 was deleted and another with the same name and type was created. The content was also the same (as seen in input 2 and 3 above). But they still return two different hash values. This indicates that the algorithms implemented use the metadata of the files too (here, it may be the time of creation). Thus, two files created separately no matter how similar, yield two different hash values.

PART C

Two files shown below are different. These are passed as input to the MD5 hash function.

File 1: order.ps



Julius. Caesar
Via Appia 1
Rome, The Roman Empire

May, 22, 2005

Order:

Alice Falbala is given full access to all confidential and secret information about GAUL.

Sincerely,

Julius Caesar

Hash Values:

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

File 2: letter_of_rec.ps

Julius. Caesar
Via Appia 1
Rome, The Roman Empire

May, 22, 2005

To Whom it May Concern:

Alice Falbala fulfilled all the requirements of the Roman Empire intern position. She was excellent at translating roman into her gaul native language, learned very rapidly, and worked with considerable independence and confidence.

Her basic work habits such as punctuality, interpersonal deportment, communication skills, and completing assigned and self-determined goals were all excellent.

I recommend Alice for challenging positions in which creativity, reliability, and language skills are required.

I highly recommend hiring her. If you'd like to discuss her attributes in more detail, please don't hesitate to contact me.

Sincerely,

Julius Caesar

Hash Values:

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

OBSERVATIONS

- Both these files are different in every way: from their names to the contents. Yet, they still yield the same hash value for MD5. Other algorithms result in different hash values. This is what is called as a ‘collision’.