Trent University
COIS/FRSC 2750H WEB
Winter 2020, Assignment 2

Question 3 involves using a hex editor. The question can be done using either Windows, Mac OS/X, or Linux. If you have a choice, please use Windows. Marked out of 60.

1. [8 marks] Sometimes it is useful to be able to tell if a credit card number is valid or not. For each of the following credit card numbers, perform the Luhn check algorithm to get the sum (see the tutorial clip on Blackboard), indicate if the credit card number is valid and if it is not, what would the valid credit card number be? Please show your work.

a. 4550 2027 1375 1785

Digits	4	5	5	0	2	0	2	7	1	3	7	5	1	7	8	5
Weight	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1
Product	8	5	1 5*2=10; 1+0=1	0	4	0	4	7	2	3	5 7*2=14; 1+4=5	5	2	7	7 8*2=16; 1+6=7	5

The sum of all the products = 65, which doesn't end with a 0
Invalid credit card number

We can add 5 to 65 to make the sum divisible by 10. So, we can add 5 to numbers in odd places, for example, to 0 in 4th place. So, a valid credit card number would be:
4555 2027 1375 1785

b. 5451 3895 6482 8612

Digits	5	4	5	1	3	8	9	5	6	4	8	2	8	6	1	2
Weight	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1
Product	1 5*2=10 1+0=1	4	1 5*2=10 1+0=1	1	6	8	9 9*2=18 1+8=9	5	3 6*2=12 1+2=3	4	7 8*2=16; 1+6=7	2	7 8*2=16; 1+6=7	6	2	2

The sum of all the products = 68, which doesn't end with a 0
Invalid credit card number

We can add 2 to 68 to make the sum divisible by 10. So, we can add 2 numbers to a digit in the odd place. So, adding 2 to digit at 4th place. So, a valid credit card number would be:
5453 3895 6482 8612

c. 4638 1254 6629 3404

Digits	4	6	3	8	1	2	5	4	6	6	2	9	3	4	0	4
Weight	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1

Product	8	6	6	8	2	2	1 5*2=10 1+0=1	4	3 6*2=12 1+2=3	6	4	9	6	4	0	4

The sum of all the products = 73, which doesn't end with a 0
Invalid credit card number

We can subtract 3 from 73 to make the sum divisible by 10. So, we can subtract 3 from numbers to a digit in the odd place. So, subtracting 3 to digit at 4th place. So, a valid credit card number would be:
4635 1254 6629 3404

d. 1234 9876 6543 6789

Digits	1	2	3	4	9	8	7	6	6	5	4	3	6	7	8	9
Weight	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1
Product	2	2	6	4	9 9*2=18 1+8=9	8	5 7*2=14; 1+4=5	6	3 6*2=12 1+2=3	5	8	3	3 6*2=12 1+2=3	7	7 8*2=16; 1+6=7	9

The sum of all the products = 87, which doesn't end with a 0
Invalid credit card number

We can add 3 to 87 to make the sum divisible by 10. So, we can add 3 numbers to a digit in the odd place. So, adding 3 to digit at 4th place. So, a valid credit card number would be:
1237 9876 6543 6789

---

2. [16 marks] Let's see what we can find by using some network tools.

a. [3 marks] Let's see what we can find using whois. Go to https://ping.eu select WHOIS and enter staples.ca (Staples Canada). Be sure to click on the Full Info box and enter the captcha to access the details. What do you see (cut and paste the details into your answer)? How could good guys and bad guys make use of this information?

Domain Name	staples.ca
Registry Domain ID	D623929-CIRA
Registrar WHOIS Server	whois.ca.fury.ca
Registrar URL	Markmonitor.com
Updated Date	2019-10-31T09:22:26Z
Creation Date	2000-10-17T14:18:59Z

Registry Expiry Date	2021-12-02T05:00:00Z
Registrar	MarkMonitor International Canada Ltd.

Registrar IANA ID:
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:

Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status	clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registry Registrant ID	16333847-CIRA
Registrant Name	Staples, Inc. TMA 372897

Registrant Organization:

Registrant Street	500 Staples Drive
Registrant City	Framingham
Registrant State/Province	MA
Registrant Postal Code	01702
Registrant Country	US
Registrant Phone	+1.5082535000

Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:

Registrant Email	DomainMgmt@staples.com
Registry Admin ID	16475322-CIRA
Admin Name	Christine Harrington
Admin Organization	STAPLES, INC. TMA372897
Admin Street	500 Staples Drive
Admin City	Farmingham
Admin State/Province	MA
Admin Postal Code	01702
Admin Country	US

Admin Phone	+1.5082535000

Admin Phone Ext:
Admin Fax:
Admin Fax Ext:

Admin Email	DomainMgmt@staples.com
Registry Tech ID	16475322-CIRA
Tech Name	Christine Harrington
Tech Organization	STAPLES, INC. TMA372897
Tech Street	500 Staples Drive
Tech City	Farmingham
Tech State/Province	MA
Tech Postal Code	01702
Tech Country	US
Tech Phone	+1.5082535000

Tech Phone Ext:
Tech Fax:
Tech Fax Ext:

Tech Email	DomainMgmt@staples.com

Registry Billing ID:
Billing Name:
Billing Organization:
Billing Street:
Billing City:
Billing State/Province:
Billing Postal Code:
Billing Country:
Billing Phone:
Billing Phone Ext:
Billing Fax:
Billing Fax Ext:
Billing Email:

Name Server	a1-51.akam.net
Name Server	a12-65.akam.net
Name Server	a13-65.akam.net
Name Server	a14-66.akam.net
Name Server	a3-64.akam.net
Name Server	a6-66.akam.net
DNSSEC	unsigned

URL of the ICANN Whois Inaccuracy Complaint Form	https://www.icann.org/wicf/
>>> Last update of WHOIS database	2020-03-27T17:15:14Z <<<

For more information on Whois status codes, please visit https	//icann.org/epp

I can see domain name, domain Id, when the domain was created, what is its expiry date, updated date, registrar information(contact-email and phone number), registrant name, administrative contact (name, address, postal code, phone, email), technical contact and name servers.

This information is useful to good guys :
➔ This helps them do a background research of the store or website to ensure that it is a good business or not. For example, as a customer I would want to ensure that there is nothing suspicious about the business I am about to purchase my product from.
➔People wanting to start their own businesses and other users and organizations have facilities to carry out trademark clearances and to help expose any kind of theft and misuse in accordance to the laws.

This information is useful to bad guys:
➔They can use the contact information for sending spam emails, they can get information about the target whoever they want to hack.
➔They can use information to extract data by hacking and have access to the credit card information
➔There is a possibility for identity theft. Cyber criminals can gain unrestricted access and create account and do bad stuff in the name of some other business.

b. [3 marks] Let's see what Ping does. Go to https:ping.eu, select Ping and enter staples.ca (Staples Canada). What do you see? How could good guys and bad guys make use of this information?

--- PING staples.ca (2.17.160.144) 56(84) bytes of data. ---
64 bytes from 2.17.160.144: icmp_seq=1 ttl=58 time=**30.3** ms
64 bytes from 2.17.160.144: icmp_seq=2 ttl=58 time=**30.3** ms
64 bytes from 2.17.160.144: icmp_seq=3 ttl=58 time=**30.3** ms
64 bytes from 2.17.160.144: icmp_seq=4 ttl=58 time=**30.3** ms

--- staples.ca ping statistics ---

packets transmitted **4**

received	**4**
packet loss	**0** %
time	**16** ms

--- Round Trip Time (rtt) ---

min	**30.267** ms
avg	**30.302** ms
max	**30.319** ms
mdev	**0.214** ms

Ping shows how long it takes for a packet to reach the host website. So here I can see the time taken by a 64 bytes packet to reach in milliseconds – 30.3ms,30.3ms,30.3ms,30.3ms for each packet respectively. I can also see how many packets transmitted-4, and the packets lost in the way-0, packets received-4 and total time 16ms. There is also Round Trip Time – minimum, average, maximum, and mdev.

This can be helpful for good guys:
➔It helps decide if a host is reachable by IP
➔Business or organizations can realize how much time their processes takes and thus improve customer experience and maybe increase revenue.
➔Business agility can be improved and security can be improved.
➔Speed tests can be done for company to realise their network capability.
➔A criminal's cell phones last location can be found.

This information can be used by bad guys:
➔They know how much time it takes for packets to reach the host so they could interfere in between and steal information.
➔They can do network hacking and gather information from a network and computers using internet.

c. [3 marks] Now let's see what is the function of the tool traceroute. Go to https://www.uptrends.com/tools/traceroute and enter the URL for the Sydney, Australia website (in English) – www.cityofsydney.nsw.gov.au as the site you want to test. Run the test three times using Toronto, Paris, and Seoul as staring points (be sure to click on Test Again to try a different starting point. This will give you the three paths consisting of a number of hops (steps) For each path, give the Step# and the IP address (not to worry if a particular step for one of the paths does not have an IP address … leave that step blank).

URL used Perth, Australia website https://www.perth.wa.gov.au/ because the given URL was not working.

TORONTO	
STEP#	**IP ADDRESS**
1	66.11.155.241
2	66.11.145.83
3	38.88.240.193
4	154.24.18.141
5	154.54.85.169
6	38.32.56.202

7	104.44.237.163
8	104.44.20.179
9	104.44.7.163
10	104.44.17.147
11	104.44.19.253
12	104.44.18.150
13	104.44.28.43
14	104.44.17.22
15	104.44.7.199
16	104.44.11.108

PARIS	
STEP#	**IP ADDRESS**
1	51.159.30.1
2	51.158.8.164
3	195.154.2.168
4	37.49.237.119
5	104.44.236.99
6	104.44.11.233
7	104.44.28.109
8	104.44.17.64
9	104.44.19.165
10	104.44.7.143
11	104.44.11.118

SEOUL	
STEP#	**IP ADDRESS**
1	37.252.244.73
2	63.218.149.197
3	
4	63.223.15.202
5	63.217.17.94
6	104.44.237.197
7	104.44.11.125
8	104.44.7.194
9	104.44.11.102

d. [3 marks] For each of the three paths, use http://whatismyipaddress.com/ to look up the IP addresses that the data travels from source to destination. For each path, list the countries that data travels. If successive steps are in the same country, do not repeat the country. For example: if the IP addresses indicate that the data travels from Canada to England to England to India to England to Japan, we are looking for Canada, England, India, England, Japan.

For the path starting from Toronto, the data travels through countries Canada and United States

For the path starting from Paris, the data travels though countries France and United States. *I Noticed that IP address from 104.44 are in the country United States.*

For the path starting form Seoul, the data travels through countries South Korea, Australia, Singapore and United States.

e. [2 marks] What is surprising about your results in Part (e).

➔One surprising thing that I noticed was that all the data in each of the three paths, end in country United States.

➔Also, the data travels a lot around in the country United States. *The IP address starting with 104.44 is for the country United States definitely.*

➔I think, since Canada and France are geographically closer to United States, therefore the data directly came from their countries to United State. However, since South Korea is farther away, hence the data stopped in Australia, Singapore in order to have information sent to United States. However, its just my assumption.

➔There were many packets sent from Canada to US

f. [2 mark] What implications do the routes shown have with respect to privacy issues?

Information is being sent via different routes each time. For example, one time, I clicked Test again, however, chose the same starting point and noticed that the last 2 digits of the IP address changed(mostly the ones in United States). This means that there are different route and hence difficult for hackers to interfere and get access to any information, since they can't predict what the next route would be. Thus, keeping the information safe and abiding by the privacy issues.

---

3. [21 marks] Let's see how files are stored on a computer. Windows users should go to http://www.hexworkshop.com/ and download the latest demo version of Hex Workshop. Mac and Linux users should go to http://www.sweetscape.com/010editor/ and download the free trial version of the 010 Editor. Install the software on your computer. Open the hex editor. The left panel will contain addresses, the middle panel contains the bit values stored (in hexadecimal) and the next panel contains possible character values for the bits stored. See the clip on Hex Workshop on Blackboard. If you are using the 010 Editor, please be sure that in the top left-hand side of the panel "Edit As: Hex" is selected. If you see "Edit As: Text", use the drop-down arrow to change it.

a. [1 marks] Most files have signatures so that the computer knows what kind of a file it is so let's see what some common signatures are. Open an rtf file (Word can make these). What are the first 10 hex digits you see?

The first 10 hex digits of a rft file are :
7B 5C 72 74 66 31 5C 61 6E 73

b. [2 marks] Open a pdf file – what are the first 10 hex digits you see? Some files also have trailers that tell the computer that the file has ended. What is the trailer for a pdf file in hex?

The first 10 hex digits for a pdf file is:
25 50 44 46 2D 31 2E 37 0D 25
The trailer for a pdf file is ..%%EOF..
The trailer for pdf file in hex is : 25 25 45 4F 46 0D 0A

c. [1 mark] Open the trent.gif file available in the Assignment 2 zipped folder on Blackboard. What are the first 10 hex digits you see (i.e. the signature)?

The first 10 hex digits are:
47 49 46 38 39 61 85 01 81 00

d. [1 mark] Let's try one last type of file (and ASCII text file). Open COIS2750H_A2.txt and then determine the signature for this type of file.

The signature for this file is :
54 68 69 73 20 69 73 20 61 20

e. [4 marks] A good way to see if a file has been altered is to do a checksum. Open the file 4550out-s19.doc posted to Blackboard in Hex Workshop. Go to Tools and then Generate Checksum. Select CRC (32 bit) (or CRC-32 in the 010 Editor) as your algorithm, select Entire Document, and generate the checksum. How many digits are there in the hex checksum? What are the first 8 digits of the hex checksum? Do another checksum but this time select MD4 (128 bit) (or MD4 in 010 editor) as the algorithm. How many hex digits are there in this checksum? What are the first 8 hex digits?

There are 8 digits in the check sum and the first 8 are: 8CB65A9E

For MD4(128 bit), there are now 32 digits in the checksum
The first 8 are: 63DD2E1D

f. [2 mark] Now let's see what effect changing the content of the file has on the checksum. Make a copy the 4550out-s19.doc file and rename it test.doc (in case we need it in court). Perform this copy from the Operating System (do not use "Save As" from within MS Word). Let's first check out the values of the checksums. Run the CRC (32 bit) and MD4 (128 bit)? algorithms on test.doc and compare them to the results from Part (e). What are the first 8 digits of each checksum and how much did the checksums change?

CRC (32 bit) 8 digits : 791FC267
MD4 (128 bit) 8 digits : D1471A37

The checksums have changed totally, and they are no where similar for both CRC (32 bit) and MD4 (128 bit).

g. [2 marks] Now let's see what happens when we change the contents of our file copy. From within MS Word, change the first letter of the document text from upper case to lower case (i.e. Computing to computing), save it and then open test.doc in the hex editor. What are the first 8 digits of the hex checksum using CRC (32 bit) and what are the first 8 digits in hex using MD4 (128 bit)? How much did the checksums change from Part (f)?

CRC (32 bit) 8 digits : 791FC267
MD4 (128 bit) 8 digits : D1471A37

The checksums didn’t change ta all from part(f)

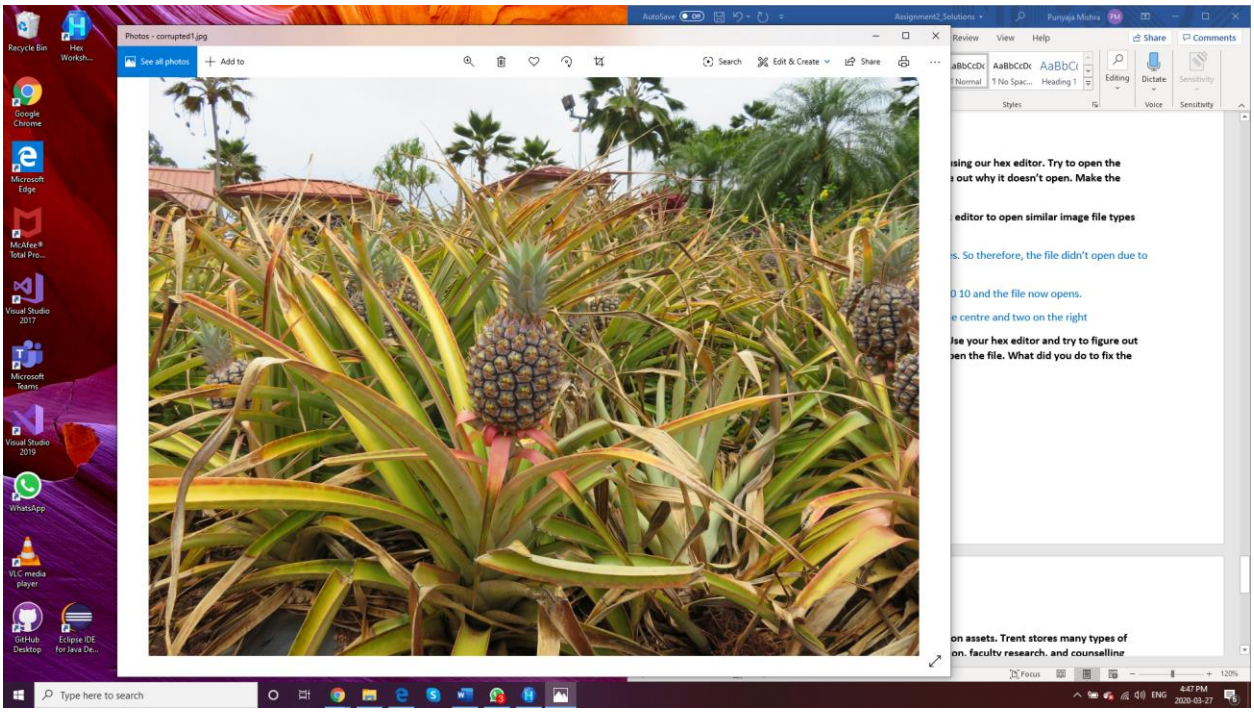
h. [4 marks] Now let’s try to recover corrupted files using our hex editor. Try to open the corrupted1.jpg file. Now use your hex editor and try to figure out why it doesn’t open. Make the needed changes needed to open the file. What did you

do to fix the image? Describe the picture. (Hint: use your hex editor to open similar image file types and check their signatures).

I opened another .jpg file and the files had different signatures. So therefore, the file didn’t open due to the wrong signature.

I changed the signature from FF D8 DD E1 AA 10 to FF D8 E0 00 10 and the file now opens.

The image is of a pineapple field and there is a pineapple in the centre and two on the right



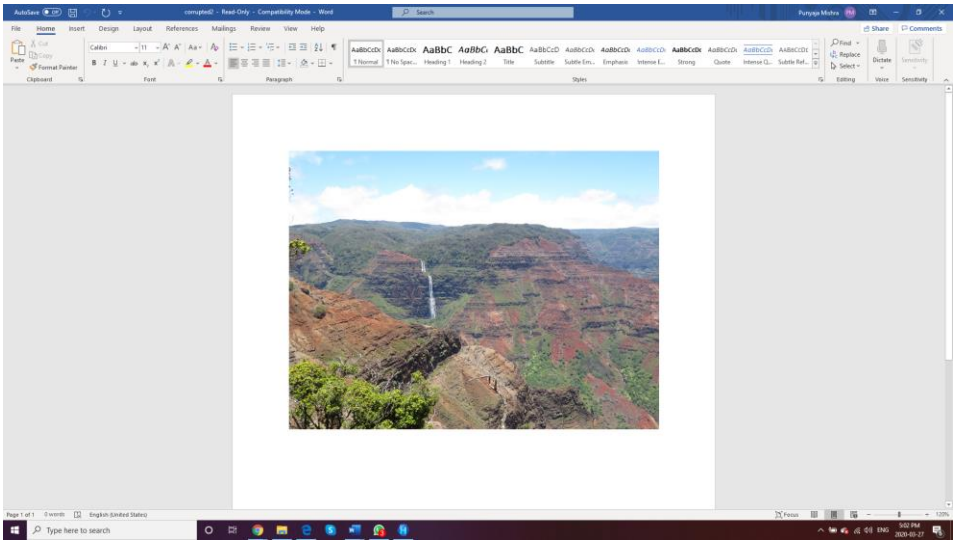
i. [4 mark] Now try to open the corrupted2.gif file. Use your hex editor and try to figure out why it doesn’t open. Make the needed changes needed to open the file. What did you do to fix the file? Describe the contents of the file.

The corrupted2 file is gif. However, the signature is that of a word document.

Gif signature: 47 49 46 38 39 61

And word doc signature is : 00 CF 11 E0 A1 B1 1A

On opening it with word, I could look at the picture



---

4. [15 marks] Let's do some risk analysis on Trent's information assets. Trent stores many types of information and three of these are: parking permit information, faculty research, and counselling centre information.

a. [3 marks] For EACH of the three types of information describe who would want to illegally access this type of information and why?

Hackers would want the parking permit information as they can steal license plate numbers. They can also get access to driver's license, and personal information about the license owner like first name, last name, address, date of birth. They can also get information about the car – model, year, type and try to steal it. Maybe a hacker might try to target someone's permit to use it as their own.

Hackers can get access to personal information about the faculties who did the research, like their first and last names, residence address, date of birth and may impersonate them. Also, the research can be stolen by the hackers and either published as their own research. Or, the research can be misused when stolen. Also, let's say if a certain department of the university have been funded by government or is doing some national level research, then people may have hired hackers to steal this research information.

Hackers can misuse details about the counselors. They can get access to personal information about them, like their first and last names, residence address, date of birth and steal their degrees and offer false services by impersonating them. They can also steal data about the students taking these services and personal data including their need to take these services. This data can also be used against the students by threatening them to publicize their personal information.

b. [3 marks] Consider what the impact would be for EACH of the three types of information mentioned above if the information was improperly accessed or damaged. Is the impact Catastrophic (expose school to serious lawsuits, loss of reputation, and/or information cannot be recreated), Serious (some exposure to lawsuits, loss of reputation and/or information is expensive to recreate), or No Big Deal (small chance of lawsuits, information can easily be recreated). Be sure to justify your choice for each type of information.

The impact would be serious if parking information was accessed. Hackers on accessing sensitive information like license plate number can lead to identity fraud, which can become catastrophic. Entire parking system would have to be rebuild with more security against the hackers. There can be lawsuit as hackers can use someone else's permit without paying and use someone else's license plate numbers for crimes.

If hackers get access to counselling centre information then the situation would be catastrophic if they use the degree of the service provider as it is identity fraud. Also, they can get access to student data and the information about their sessions with eh counsellor and it can be serious as their can be loss of reputation for the students.

If hackers got access to information about faculties then it will be catastrophic as they can be responsible for identity fraud. Also, the theft of research data is serious as they can either sell or publish in their own name leading to lawsuits against them. Certain government funded researches can be stolen which can be very catastrophic.

c. [3 marks] Now consider what the likelihood is that EACH type of information could be accessed or damaged: not likely, moderately likely, very likely. Justify why you think the information fits in that category.

The likelihood of parking permit and information being accessed is moderately likely. These kinds of hacks would more likely be done by student hackers to avoid paying parking permit fees. They might target a professor to commit identity fraud as professors have more money than any student, in most cases.

The likelihood of a faculty research information being accessed or damaged depends on the sensitivity of the research. For example as I wrote in the previous program, a government funded research being hacked is very likely. However, someone hacking it for only a faculty information is moderately likely, like by someone who wants to pose as a faculty and thus do an identity theft.

The likelihood of a counselling centre information to be accessed or damaged is not likely. Not many people are interested in knowing personal secrets/troubles about students. It is moderately likely that someone would want to access to information about the counselling staff.

d. [6 marks] Now let's look at how we can manage the risk. Basic techniques are: avoiding the risk, modifying the risk (impact and/or likelihood), transferring the risk to others, and accepting the risk. What techniques would you use for EACH of the types of information and how would you implement it?

The best basic technique to avoid the accessing of parking information is modifying the risk. By modifying risk we can prevent the students from accessing the parking permits they didn't pay for and

also prevent any identity theft. If we increase the security then no student would want to access as there would now be higher chances of getting caught. Also, someone trying to commit an identity fraud would also now have to deal with harder and stronger security thus making it harder for them to commit the crime. Though the likelihood stays the same, but the percentage of successful hacks decreases.

The best basic technique to avoid the faculty research information to be accessed or destroyed to increase the security level around the research data and also the faculty information. The likelihood wouldn't decrease as people can always try to commit identity fraud. However, when doing serious research work, the security needs to be high level because the likelihood not only increases drastically but the consequences are catastrophic. Or, maybe there could be restricted access, like only to faculties responsible for the research should have access to the main, final draft, or data.

The best basic technique to avoid counselling centre information to be accessed or destroyed is to store the information safe. It is less likely for someone to try and steal a student's personal data about the counselling session, however, if the files with such data are stored with strong encryption and in a safe place, then there are even less chances of it being accessed ad hence further decreasing the chances of being hacked. Also, to avoid the possibility of identity theft, there should be stronger security around the data of the counselling staff so the possibility to steal their personal information is more difficult.

Submit your file (in PDF format only) with the answers to the Assignment 2 Dropbox in Blackboard. Be sure that your submission is readable. If we can't read it, we can't mark it.

Good luck and have fun!!