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

    b. 5451 3895 6482 8612

    c. 4638 1254 6629 3404

    d. 1234 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?

    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?

    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).

    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.

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

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

    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?

    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)?

    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.

    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?

    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?

    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)?

    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. [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.

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?

   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.

   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.

   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?

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!!