Assignment 5: Chanakya Gaur: Regular Expressions

1. What is a “regular expression? [2 points]

Regular Expressions are patterns which are similar to arithmetic expressions that have operands, operators, sub-expressions and a value. Regular expressions allow forensic analyst to search through large quantities of text information for patterns of data such as credit card and telephone numbers.

2. Regarding “regular expressions,” what is a “literal” and what is an “operator”? [4 points]

Operators are functional whereas literals are meant to be inert. Literals are meant for representation and have no functionality.

3. In the RegEx language, which symbol is used to allow an operator character to be treated as a

literal? [2 points]

Ans: “\”

4. In the RegEx language, which symbol is used to `match any one thing’? [2 points]

Ans: “.”

5. In the RegEx language, which symbol is used to `match any decimal digit? [2 points]

Ans: “\d”

6. In the RegEx language, which symbol is used to `match any lowercase letter’? [2 points]

Ans: [a-z] “\l”

7. In the RegEx language, which symbol is used to `match any space or tab character’? [2 points]

Ans: “\s” “\t”

8. In the RegEx language, which symbol matches `any uppercase letter’? [2 points]

Ans: [A-Z] “\u”

9. In the RegEx language, which symbol matches `any whole word’? [2 points]

Ans: “\y”

10. In the RegEx language, which symbol matches `a hex character’? [2 points]

Ans: “\x”

11. In the RegEx language, what are used to “group the elements that must be treated as a group and not an individual character”? [2 points]

Ans: “(…)”

12. In the RegEx language, what are used to designate that the preceding function group should be repeated a number of time? [2 points]

Ans: “{n}”

13. In the RegEx language, what are used to designate all of “the possible options for a single

variable”? [2 points]

Ans: “^”

14. In the RegEx language, what symbol is used to designate “the start of a word”? [2 points]

Ans:” \<”

15. In the RegEx language, what symbol is used to designate “the end of a word”? [2 points]

Ans: “\>”

16. In the RegEx language, what symbol is used to designate the `or’ operator, as in `this or that’? [2 points]

Ans:” |” This | that

17. In the RegEx language, what symbol is used to “match 1 or 0 preceding instances” of a value? [2 points]

Ans: “?”

18. In the RegEx language, what symbol is used as a “range delimiter”? [2 points]

Ans: “\_”

19. Re-write the expression (a|b) using square brackets. [2 points]

Ans: [ab]

20. Will the two expressions below return the same hits? [5 points]

\<((\d\d\d\d)(\-| )){3}\d\d\d\d\>

\<\d\d\d\d)(\-| )\d\d\d\d(\-| )\d\d\d\d)(\-| )\d\d\d\d)\>

Ans: Yes, they will both return the same result.

21. Select the “Live Search” tab on the FTK tool. “Delete all search results” from the “Live search

Results” window. Use the built-in RegEx search capability to search for all of the VISA credit

cards found within the Mantooth.E01 evidence image file. What is the RegEx expression that is

used (4 points) and which three (3) credit card numbers does it find (2 points each)? [10 points]

* 4805-5555-1234-5566
* 4858-2545-5456-5555
* 4454-5588-5124-2458

22. Create a regular expression that can be used to find the expiration date of a credit card. An

example expiration date is “Exp 09/12”. Notice that the date is in a month and year format. In

this example, the expiration date is September (09), in the year 2012 (12). When you write the

expression, assume that the leading zero (0) may or may not be present. Thus, the expression

should also find a date in the following format “Exp 9/12”. Furthermore, assume that any two

digit year is acceptable (00-99). In your answer, provide the regular expression, and also provide a screen-print of your computer that sows the first “hit” that you receive when you use your regular expression. (Please crop the picture and enlarge it so it is easier to see.) [22 points]

(EXP)\s(0[1-9]|1[012]/((0-9)[0-9])

23. How is the syntax for the Technical Report 1 (TR1) expression language different than the RegEx expression language? (Just state what is added to the beginning and to the end of a RegEx expression to make it a TR1 expression.) [5 points]

TR1 expressions needs to be quoted and must begin with ##

24. TR1 expressions are used with FTK by entering them into the “Index Search” tab. What is the TR1 expression that you would use to find all hits for the dates from 1990 to 1999? [Note: The training manual has an error in it. Can you find it? Be sure to test your answer with FTK before you answer this question.] [10 points]

25. What are the two kinds of filters that Forensic ToolKit (FTK) provides? [4 points]

Compound and Tab Filters

26. View the Email tab on FTK for the MantoothUSB image. Expand the “Email by Date” container and notice there are 69 emails in the “Submitted” sub-container, and 61 emails in the

“Delivered” sub-container. (See the picture below.)

42

27. View the graphics for the MantoothUSB image within the Graphics tab. In this case, there are about 3,744 graphics files (this value is found just below the Graphics tab window). This is a reasonable number of files to have to review as part of an examination. However, if this were “real evidence,” the number of graphics might be 100,000 or more, which can be a significant number to review. Thus, it is beneficial to filter the graphics to hide the less relevant ones. [5 points]