GREP and Regular Expressions Laboratory Exercise-WK4
Cyber Crime Investigations and Forensics II: CYB-356-Z1
Professor: Dennis Labossiere
Date: 07/29/2018
Examiner Name: Brian T. Carr

Table of Contents

List of Illustrative Materials

Tables

Figures

Executive Summary

Background

On 7/23/2018, The Forensic Examiner at Heath and Ledger LLC was informed about possible suspicious activity on the company's network. The Examiner was provided with logfiles containing network activity. Senior Project Manager Winston Jameson had both informed the Examiner of the suspicious activity and extracted the logfiles for the Examiner's analysis.

Request

The Senior Project Manager at Heath and Ledger LLC, Winston Jameson requested that the Forensic Examiner analyze the logfiles provided to determine if there was any evidence confirming suspicious activity. To determine data integrity the Examiner has been requested to compare the md5 hash value of the downloaded .zip file to the md5 hash value located on the same webpage. Specifically, Mr. Jameson would like the Examiner to implement regular expressions to efficiently search the text files.

Summary of Findings

The Examiner performed an analysis of the logfiles provided and was unable to locate any instances of suspicious activity on the network. The Examiner was able to successfully determine which files contain permanent and temporary redirects. The Examiner was able to determine which domain names appeared in the logfiles. The Examiner also determined each unique email address that was located within the logfiles.

The Examiner determined that 12-12.out.txt contained the code 301 revealing it is permanent redirect, and 11-20.out.txt contained multiple 302 temporary redirects. The Examiner successfully located the domains within the logfiles as seen in *figure 8*. The Examiner also discovered all usernames and domains while eliminating duplicates and outputting it to a text file.

Evidence

Table 1 outlines the evidence items of this case.

Description	Designation	Filename	MD5 Hash
Evidence Provided	Preservation Copy	Logfiles.zip	0637cd0905ddd3cf781d95230b7e798d
Evidence Created	Preservation Copy	PRES_Logfiles/11-20.out.txt	8afe02de4f58a7c22e5d577b03cd30a4
Evidence Created	Preservation Copy	PRES_Logfiles/12-12.out.txt	b1549d23a26a2fdcbdb6c99c7892f80a
Evidence Created	Preservation Copy	PRES_Logfiles/11-25.out.txt	a14a8111dae4debefc081d29faefa820
Evidence Created	Preservation Copy	PRES_Logfiles/11-19.out.txt	1721bdf81867f68526ac59c6882e054e
Evidence Created	Preservation Copy	PRES_Logfiles/12-03.out.txt	7cf6124456f8a117762185e7ae4519a1
Evidence Examined	Working Copy	WC_Logfiles/11-20.out.txt	8afe02de4f58a7c22e5d577b03cd30a4
Evidence Examined	Working Copy	WC_Logfiles/12-12.out.txt	b1549d23a26a2fdcbdb6c99c7892f80a
Evidence Examined	Working Copy	WC_Logfiles/11-25.out.txt	a14a8111dae4debefc081d29faefa820
Evidence Examined	Working Copy	WC_Logfiles/11-19.out.txt	1721bdf81867f68526ac59c6882e054e
Evidence Examined	Working Copy	WC_Logfiles/12-03	7cf6124456f8a117762185e7ae4519a1
Evidence Created	Preservation Copy	Logfiles/11-20.out.txt	8afe02de4f58a7c22e5d577b03cd30a4
Evidence Created	Preservation Copy	Logfiles/12-12.out.txt	b1549d23a26a2fdcbdb6c99c7892f80a
Evidence Created	Preservation Copy	Logfiles/11-25.out.txt	a14a8111dae4debefc081d29faefa820
Evidence Created	Preservation Copy	Logfiles/11-19.out.txt	1721bdf81867f68526ac59c6882e054e
Evidence Created	Preservation Copy	Logfiles/12-03.out.txt	7cf6124456f8a117762185e7ae4519a1
Evidence Created	Examination Logfiles	ScriptLab4.tar.gz	32ab55badb375a54826f753bcac396f4

Table 1: Case evidence items

Collection and Analysis

Collection

On 7/23/2018, the forensic Examiner at Heath and Ledger LLC, was provided a Uniform Resource Locator (URL) which lead him to a web server hosting the logfiles. The Examiner retrieved the necessary information by implementing Wget v1.17.1. The Examiner executed the command:
$ wget https://s3-us-west-2.amazonaws.com/digitalforensicsworkbook/Logfiles.zip
The Examiner executed the command inside of the GREP_and_Regular/ directory. The Examiner can be seen implementing this command in *figure 1*. The Examiner successfully retrieved the .zip file which was now located at ~/Desktop/GREP_and_Regular/Logfiles.zip and continued to retrieve its MD5 hash value as shown in *figure 2*. Once the md5 hash value was determined the Examiner compared the value to the value provided on the web page where Logfiles.zip was to confirm data integrity. The Examiner can confirm that the downloaded Logfiles.zip matched the md5 hash value provided.

The Examiner created both preservation copies and working copies by unzipping the Logfiles.zip file three times, each into a separate directory. Once the Examiner created /WC_Logfiles/, /PRES_Logfiles/, and /Logfiles/. Both /PRES_Logfiles, and /Logfiles/ are preservation copies, and /WC_Logfiles/ will contain the working copies. The Examiner hashed all files in the ~/Desktop/GREP_and_Regular/ directory with Hashdeep. The Examiner's implementation of the Hashdeep v4.4 command can be seen in *figure 4*.

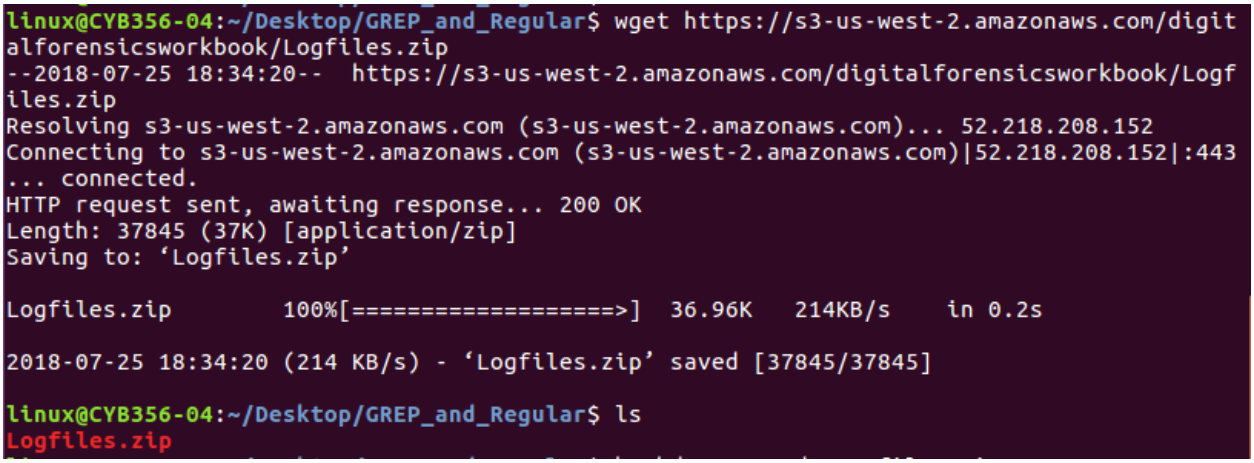

Figure 1: Wget Command Retrieving Logfiles.zip.

```
Logfiles.zip        100%[===================>]  36.96K   214KB/s    in 0.2s

2018-07-25 18:34:20 (214 KB/s) - ‘Logfiles.zip’ saved [37845/37845]

linux@CYB356-04:~/Desktop/GREP_and_Regular$ ls
Logfiles.zip
linux@CYB356-04:~/Desktop/GREP_and_Regular$ hashdeep -c md5 Logfiles.zip
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: /home/linux/Desktop/GREP_and_Regular
## $ hashdeep -c md5 Logfiles.zip
##
37845,0637cd0905ddd3cf781d95230b7e798d,/home/linux/Desktop/GREP_and_Regular/Logfiles.zip
linux@CYB356-04:~/Desktop/GREP_and_Regular$
```

Figure 2: MD5 Value of Logfiles.zip Retrieved with Hashdeep.

```
linux@CYB356-04:~/Desktop/GREP_and_Regular$ unzip Logfiles.zip
Archive:  Logfiles.zip
[Logfiles.zip] Logfiles/11-19.out.txt password:
  inflating: Logfiles/11-19.out.txt
  inflating: Logfiles/11-20.out.txt
  inflating: Logfiles/11-25.out.txt
  inflating: Logfiles/12-02.out.txt
  inflating: Logfiles/12-03.out.txt
  inflating: Logfiles/12-12.out.txt
linux@CYB356-04:~/Desktop/GREP_and_Regular$
```

Figure 3: Unzip Command Used on Logfiles.zip

```
linux@CYB356-04:~/Desktop$ hashdeep -c md5 -r ~/Desktop/GREP_and_Regular/
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: /home/linux/Desktop
## $ hashdeep -c md5 -r /home/linux/Desktop/GREP_and_Regular/
##
42984,8afe02de4f58a7c22e5d577b03cd30a4,/home/linux/Desktop/GREP_and_Regular/PRES_Logfiles/11-20.out.txt
354435,b1549d23a26a2fdcbdb6c99c7892f80a,/home/linux/Desktop/GREP_and_Regular/PRES_Logfiles/12-12.out.txt
18741,a14a8111dae4debefc081d29faefa820,/home/linux/Desktop/GREP_and_Regular/PRES_Logfiles/11-25.out.txt
28674,1731bdf81867f68526ac59c6882e054e,/home/linux/Desktop/GREP_and_Regular/PRES_Logfiles/11-19.out.txt
55185,7cf6124456f8a117762185e7ae4519a1,/home/linux/Desktop/GREP_and_Regular/PRES_Logfiles/12-03.out.txt
37845,0637cd0905ddd3cf781d95230b7e798d,/home/linux/Desktop/GREP_and_Regular/PRES_Logfiles.zip
55516,97ed6061bdabf24dd5a907895e8ae667,/home/linux/Desktop/GREP_and_Regular/PRES_Logfiles/12-02.out.txt
42984,8afe02de4f58a7c22e5d577b03cd30a4,/home/linux/Desktop/GREP_and_Regular/Logfiles/11-20.out.txt
37845,0637cd0905ddd3cf781d95230b7e798d,/home/linux/Desktop/GREP_and_Regular/WC_Logfiles.zip
18741,a14a8111dae4debefc081d29faefa820,/home/linux/Desktop/GREP_and_Regular/Logfiles/11-25.out.txt
354435,b1549d23a26a2fdcbdb6c99c7892f80a,/home/linux/Desktop/GREP_and_Regular/Logfiles/12-12.out.txt
55185,7cf6124456f8a117762185e7ae4519a1,/home/linux/Desktop/GREP_and_Regular/Logfiles/12-03.out.txt
28674,1731bdf81867f68526ac59c6882e054e,/home/linux/Desktop/GREP_and_Regular/Logfiles/11-19.out.txt
55516,97ed6061bdabf24dd5a907895e8ae667,/home/linux/Desktop/GREP_and_Regular/Logfiles/12-02.out.txt
37845,0637cd0905ddd3cf781d95230b7e798d,/home/linux/Desktop/GREP_and_Regular/Logfiles.zip
42984,8afe02de4f58a7c22e5d577b03cd30a4,/home/linux/Desktop/GREP_and_Regular/WC_Logfiles/11-20.out.txt
354435,b1549d23a26a2fdcbdb6c99c7892f80a,/home/linux/Desktop/GREP_and_Regular/WC_Logfiles/12-12.out.txt
18741,a14a8111dae4debefc081d29faefa820,/home/linux/Desktop/GREP_and_Regular/WC_Logfiles/11-25.out.txt
55185,7cf6124456f8a117762185e7ae4519a1,/home/linux/Desktop/GREP_and_Regular/WC_Logfiles/12-03.out.txt
28674,1731bdf81867f68526ac59c6882e054e,/home/linux/Desktop/GREP_and_Regular/WC_Logfiles/11-19.out.txt
55516,97ed6061bdabf24dd5a907895e8ae667,/home/linux/Desktop/GREP_and_Regular/WC_Logfiles/12-02.out.txt
linux@CYB356-04:~/Desktop$
```

Figure 4: Hashdeep v4.4 Implemented on /GREP_and_Regular/

Analysis

The Examiner had collected the evidence by implementing Wget v1.17.1 and created preservation and working copies by unzipping Logfiles.zip three times, each extraction to a different location. The Examiner then retrieved all the Hash values by implementing Hashdeep v4.4. Once the ~/Desktop/GREP_and_Regular/WC_Logfiles/ set up the Examiner began to implement GREP searches. The Examiner's first GREP search was:
$grep -winr "301" ~/Desktop/GREP_and_Regular/WC_Logfiles/ which can be seen in *figure 5*. When implementing this GREP literal expression, the Examiner was looking for which file contained the "301" permanent redirect. As seen in *Figure 5* the only file containing a "301" redirect was /home/linux/Desktop/GREP_and_Regular/WC_Logfiles/12-12.out.txt.

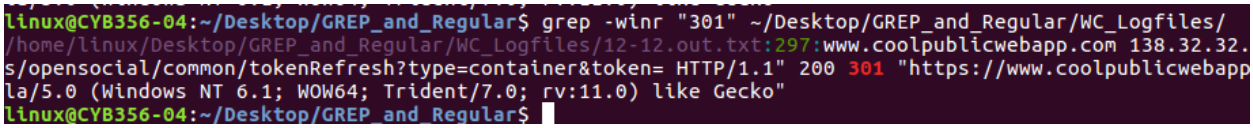

Figure 5:First Literal GREP Search

Next the Examiner used GREP to implement a literal expression searching for "302" which is a temporary redirect. The Examiner made use of the same syntax which retrieved the "301" permanent redirects. The file containing multiple "302" temporary redirects was ~/Desktop/GREP_and_Regular/WC_Logfiles/11-20.out.txt.

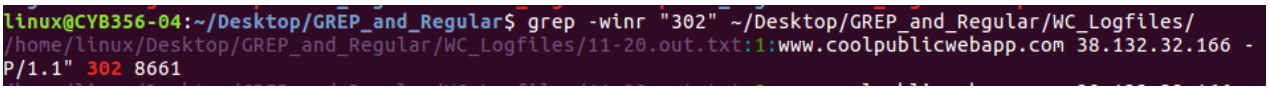

Figure 6: Second Literal GREP Search

Once the Examiner was finished implementing literal GREP expressions the next step in the lab procedure was to implement regular expressions with GREP. The first regular expression the Examiner constructed was:
$grep -inre '\b30[1-2]\b' ~/Desktop/GREP_and_Regular/WC_Logfiles/ this regular expression is the equivalent of the first two literal expressions. The regular expression can be seen in *figure 7*.

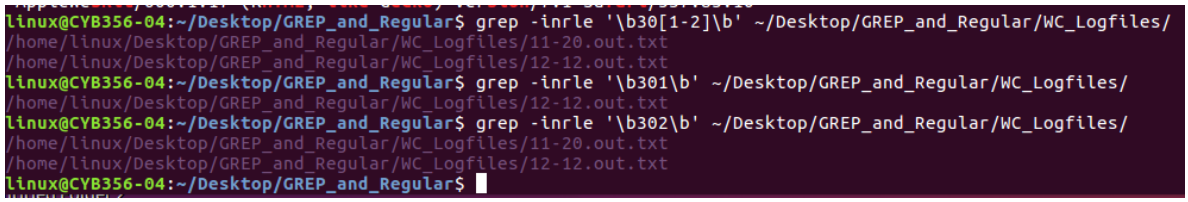

Figure 7: First Regular Expression

The Examiner's next task was to write a regular expression searching the logs for domain names. The Examiner used the syntax:
$ grep -Eniorh '(@[[:alnum:]]_.-]+?\.[[:alpha:]].]{2,6})' "$@" * | sort -m | more
The regular expression implemented by the Examiner was built to look recursively through the current directory. The Examiner chose not to include the directory he wants to recursively search because it located within his current directory /GREP_and_Regular/. The Examiner notes that

the output is identical between the syntax including the directory to recursively search, and the syntax with the directory excluded. This regular expression can be seen in *Figure 8*.

```
linux@CYB356-04:~/Desktop/GREP_and_Regular$ grep -Eniorh '(@[[:alnum:]_.-]+?\.[[:alpha:].]{2,6})' "$@" * | sort -m | more
1:@awesomeclient.com
2:@awesomeclient.com
3:@awesomeclient.com
4:@cool-co.com
5:@cool-co.com
6:@awesomeclient.com
7:@awesomeclient.com
8:@cool-co.com
9:@awesomeclient.com
10:@awesomeclient.com
11:@awesomeclient.com
12:@cool-co.com
13:@awesomeclient.com
14:@awesomeclient.com
15:@contractor.awesomeclient.com
1:@awesomeclient.com
2:@awesomeclient.com
3:@awesomeclient.com
4:@awesomeclient.com
5:@awesomeclient.com
6:@awesomeclient.com
7:@awesomeclient.com
8:@awesomeclient.com
9:@awesomeclient.com
10:@awesomeclient.com
11:@cool-co.com
12:@cool-co.com
13:@awesomeclient.com
14:@awesomeclient.com
15:@awesomeclient.com
16:@awesomeclient.com
17:@awesomeclient.com
18:@cool-co.com
19:@awesomeclient.com
--More--
```

Figure 8: Second Regular Expression

The Examiner's final step in the laboratory procedure was to construct a regular expression which would only print out all usernames and domains, including only matching search hit text, excluding line numbers, and finally redirecting the output to a text file called FinalGREP.txt. The Examiner used a GREP regular expression piped into sort which was then piped into 'uniq' and finally output into FinalGREP.txt. The Examiner made use of the -E, -i, -o, -r, and -h switches. -E defines that GREP is using a regular expression. -r requests that GREP searches recursively through the directory. The -o switch makes it so that only matching parts of a line are output. -h suppresses the file name in output. The regular expression constructed by the Examiner checked for an unspecified number of alphanumeric characters before an '@', then another unspecified number of alphanumeric characters representing the domain name, followed by a period, and finally two-to-six non-case-sensitive letters from the alphabet. The output of this GREP regular expression was piped into sort using the '|' operator commonly referred to as a "pipe". Sort sorted the output of the GREP regular expression and then piped it to uniq, which removed duplicate results. The final portion of my syntax output to a text file FinalGREP.txt.

```
linux@CYB356-04:~/Desktop/GREP_and_Regular$ grep -Eiorh '([[:alnum:]_.-]+@[[:alnum:]_.-]+?\.[[:alpha:].]{2,6})' "$@" * | sort | uniq > FinalGREP.txt
linux@CYB356-04:~/Desktop/GREP_and_Regular$ cat FinalGREP.txt
bj.honeycutt@awesomeclient.com
charles.winchester@awesomeclient.com
chris.t.ramsey@awesomeclient.com
frank.burns@cool-co.com
gsmutagi@cool-co.com
jmn@awesomeclient.com
joey.a.ortega@awesomeclient.com
margaret.houlihan@cool-co.com
maxwell.klinger@awesomeclient.com
nik.v.bosnyak@awesomeclient.com
radar.oreilly@awesomeclient.com
rpilipon@cool-co.com
sherman.potter@awesomeclient.com
stephanie.deville@awesomeclient.com
trapper@contractor.awesomeclient.com
linux@CYB356-04:~/Desktop/GREP_and_Regular$
```

Figure 9: Final Regular Expression Output to FinalGREP.txt

Conclusion

The Senior Project Manager at Heath and Ledger LLC. requests that the Forensics Examiner analyze the network logfiles to determine if there is any suspicious activity. During this analysis the Examiner made use of both literal and regular expressions with GREP v2.25.

The Examiner could not positively confirm any instances of suspicious activity, although he did locate multiple one permanent, and multiple temporary redirects. The Examiner did successfully locate domain names in the logfile, and unique username@domain combinations. The Examiner efferently and effectively searched through multiple lengthy text files by implementing GREPv2.25 with regular expressions.

Appendix

Appendix A: Examiner Workstation Specifications

- Computer Name: BrianCarrWorkstation
- Operating System (OS) Name: Windows 10
- OS Version: Student Edition
- System Make/Model: MSi GS63VR Stealth Pro
- System Serial Number: K1612N0043395
- Time Zone of Examiner Machine: Eastern Daylight Time (-4:00 GMT)
- System date/time is consistent with the time zone listed above, as verified by http://nist.time.gov/.

Appendix B: Tools

- GREP (GNU grep) v2.25
- Sort (GNU coreutils) v8.25
- Hashdeep v4.4
- GNU Wget v1.17.1
- Uniq (GNU coreutils) v8.25