Information System Security

Homework 1 – Report

Objective: *Get splunk.com' s subdomain IP addresses and filter out the duplicate ones.*

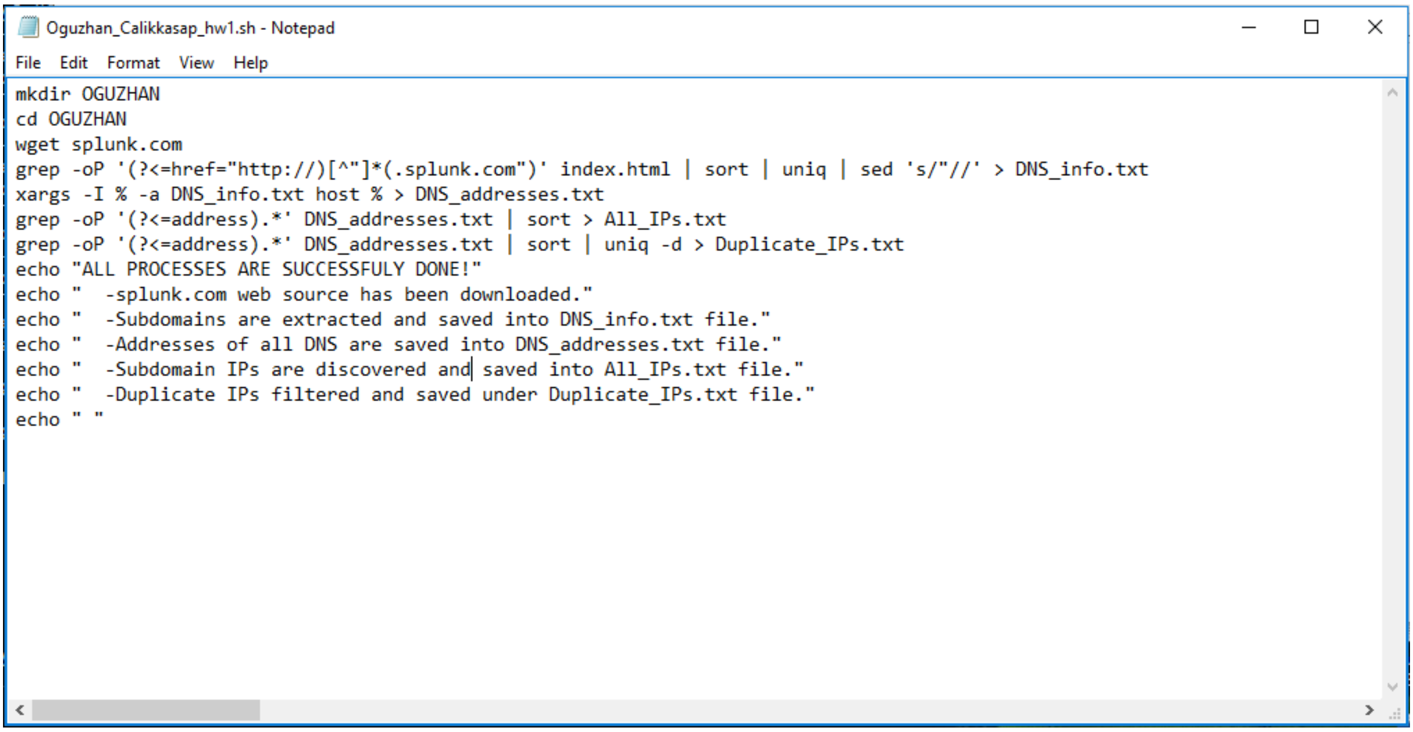
Name: Oğuzhan Çalıkkasap

Environment Used:

I have used Windows 10 Bash Shell which enables me to command with Linux native commands on Windows.

This is a new feature comes with the new Windows 10 release.

A Brief Explanation of My Shell Script:


Oguzhan_Calikkasap_hw1.sh - Notepad
File Edit Format View Help

```
mkdir OGUZHAN
cd OGUZHAN
wget splunk.com
grep -oP '(?<=href="http://)[^"]*(.splunk.com")' index.html | sort | uniq | sed 's/"//' > DNS_info.txt
xargs -I % -a DNS_info.txt host % > DNS_addresses.txt
grep -oP '(?<=address).*' DNS_addresses.txt | sort > All_IPs.txt
grep -oP '(?<=address).*' DNS_addresses.txt | sort | uniq -d > Duplicate_IPs.txt
echo "ALL PROCESSES ARE SUCCESSFULY DONE!"
echo "  -splunk.com web source has been downloaded."
echo "  -Subdomains are extracted and saved into DNS_info.txt file."
echo "  -Addresses of all DNS are saved into DNS_addresses.txt file."
echo "  -Subdomain IPs are discovered and saved into All_IPs.txt file."
echo "  -Duplicate IPs filtered and saved under Duplicate_IPs.txt file."
echo " "
```

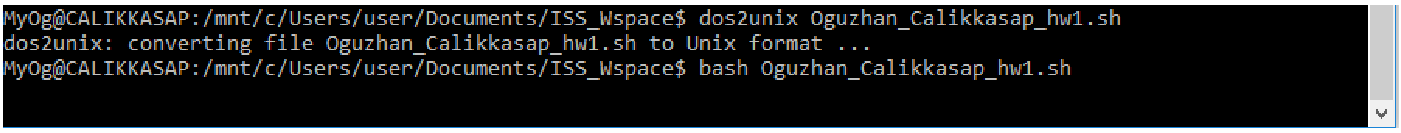
Here you see my code file with .sh extension above.

What I have done is the following:

- I have created a directory named OGUZHAN and changed my current directory to that new one,
- downloaded the source of splunk.com with wget command,
- used grep command in order to filter the DNS names. To do so, I've checked between "href=" and ".splunk.com" contexts in the source html. This is done by utilizing grep "Matcher Selection" where I have interpreted my pattern as a regular Perl expression (-P extension in the code provides me that). Then I used sort and uniq cmds to avoid repeated dns names. Sed cmd is used for removing the quote mark which was left after the preceding operation. Finally, I wrote the result into the DNS_info file.
- I made use of xargs command to get a continuous input (which are DNS names) from DNS_info file and put these input after the host command one by one. Because I needed to type a command in "host DNS_NAME_HERE" form, to be able to get each IP address of the subdomains. –I extension provides getting input from a file and replacing it with the specified placeholder (I used % as placeholder).
- after using host command, I have extracted the IP addresses by getting everything suppressed except the IP digits by grep command again. I have sorted and saved them into the file All-IPs.
- I have, this time, filtered only the duplicate IP addresses by using uniq command and saved them under the Duplicate_IPs file.
- All the remaining echo statements are for giving information to user about what have been done within the program.

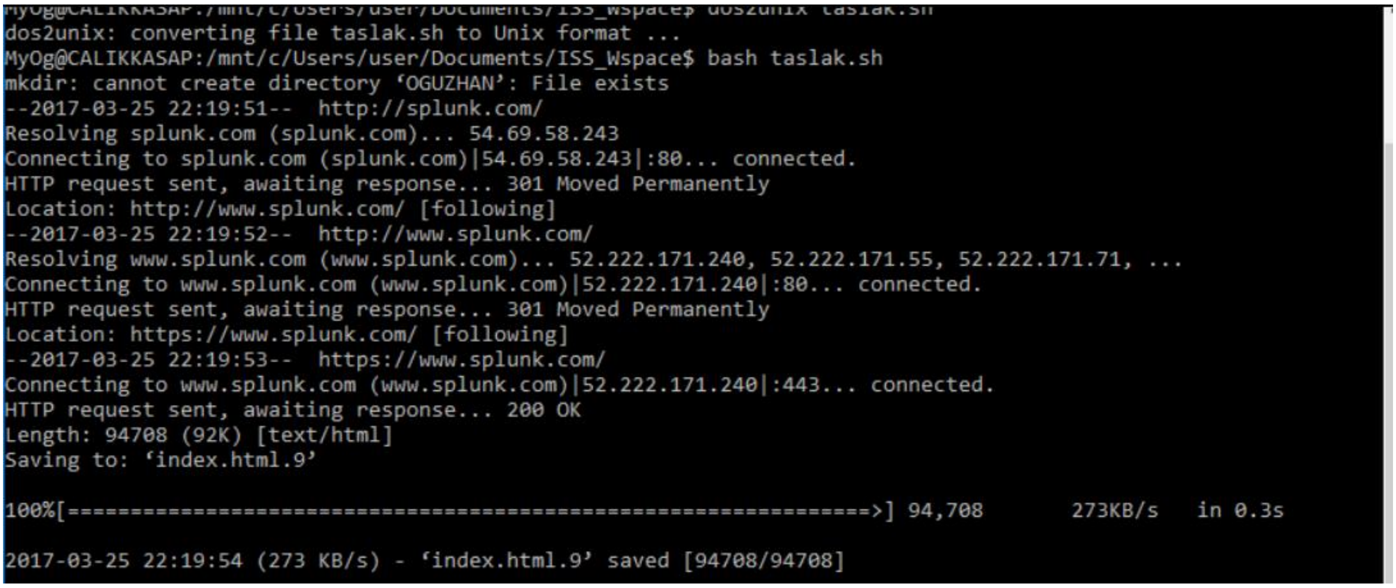
Screenshots of Each Step:

To get the shell script working properly on Linux, I made a little manipulation on my script file, by converting it to the unix language. Then I typed “bash” command to execute (this is the same as “./something” command):



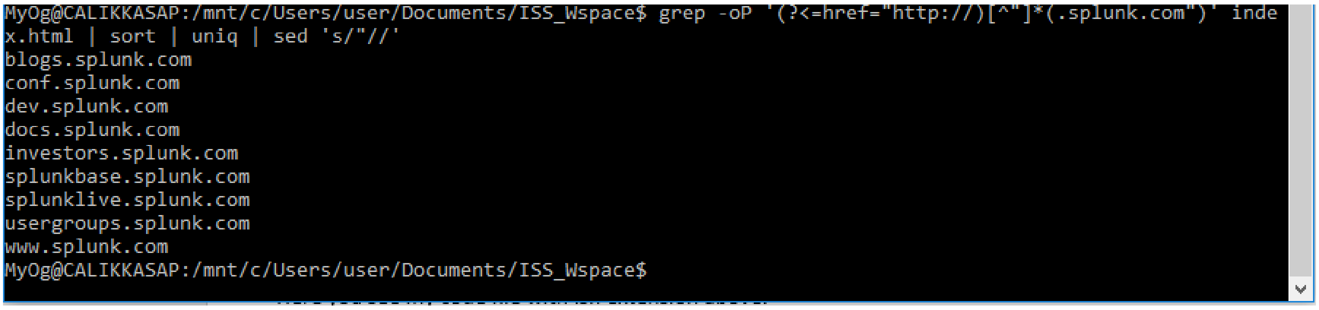
```
MyOg@CALIKKASAP:/mnt/c/Users/user/Documents/ISS_Wspace$ dos2unix Oguzhan_Calikkasap_hw1.sh
dos2unix: converting file Oguzhan_Calikkasap_hw1.sh to Unix format ...
MyOg@CALIKKASAP:/mnt/c/Users/user/Documents/ISS_Wspace$ bash Oguzhan_Calikkasap_hw1.sh
```

After wget command:



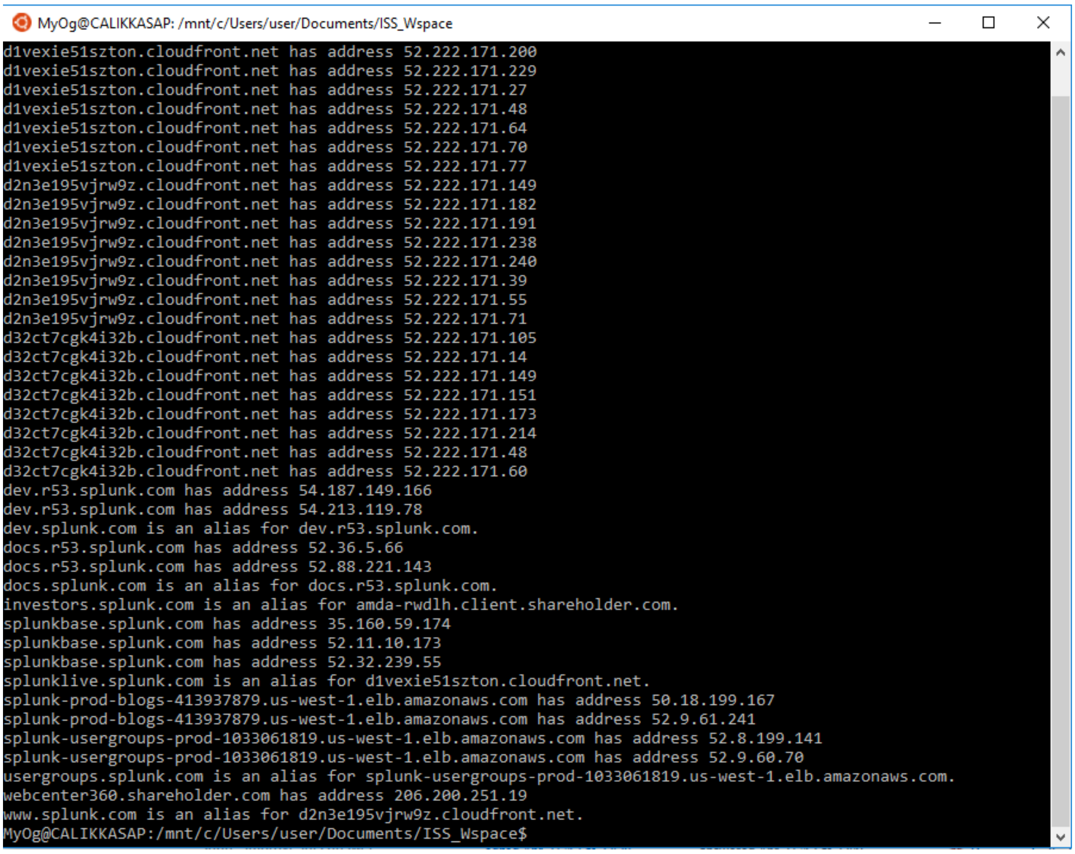
```
MyOg@CALIKKASAP:/mnt/c/Users/user/Documents/ISS_Wspace$ dos2unix taslak.sh
dos2unix: converting file taslak.sh to Unix format ...
MyOg@CALIKKASAP:/mnt/c/Users/user/Documents/ISS_Wspace$ bash taslak.sh
mkdir: cannot create directory ‘OGUZHAN’: File exists
--2017-03-25 22:19:51--  http://splunk.com/
Resolving splunk.com (splunk.com)... 54.69.58.243
Connecting to splunk.com (splunk.com)|54.69.58.243|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.splunk.com/ [following]
--2017-03-25 22:19:52--  http://www.splunk.com/
Resolving www.splunk.com (www.splunk.com)... 52.222.171.240, 52.222.171.55, 52.222.171.71, ...
Connecting to www.splunk.com (www.splunk.com)|52.222.171.240|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.splunk.com/ [following]
--2017-03-25 22:19:53--  https://www.splunk.com/
Connecting to www.splunk.com (www.splunk.com)|52.222.171.240|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 94708 (92K) [text/html]
Saving to: ‘index.html.9’

100%[==============================================================>] 94,708       273KB/s    in 0.3s

2017-03-25 22:19:54 (273 KB/s) - ‘index.html.9’ saved [94708/94708]
```

Output of the first grep command:



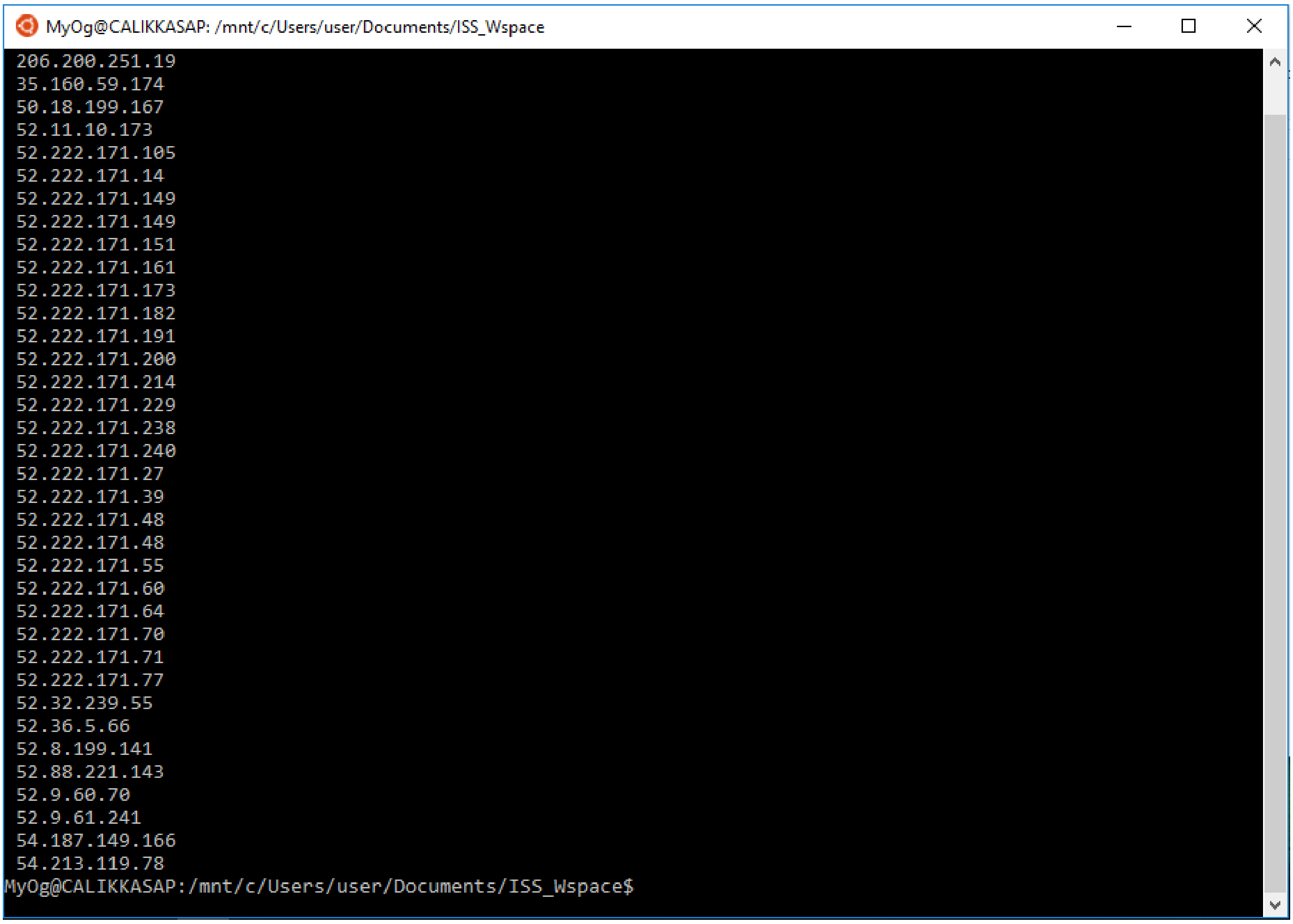
```
MyOg@CALIKKASAP:/mnt/c/Users/user/Documents/ISS_Wspace$ grep -oP '(?<=href="http://)[^"]*(.splunk.com")' inde
x.html | sort | uniq | sed 's/"//'
blogs.splunk.com
conf.splunk.com
dev.splunk.com
docs.splunk.com
investors.splunk.com
splunkbase.splunk.com
splunklive.splunk.com
usergroups.splunk.com
www.splunk.com
MyOg@CALIKKASAP:/mnt/c/Users/user/Documents/ISS_Wspace$
```

Output of the xargs command:



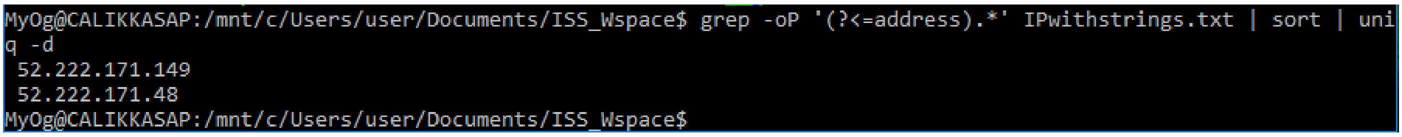
```
d1vexie51szton.cloudfront.net has address 52.222.171.200
d1vexie51szton.cloudfront.net has address 52.222.171.229
d1vexie51szton.cloudfront.net has address 52.222.171.27
d1vexie51szton.cloudfront.net has address 52.222.171.48
d1vexie51szton.cloudfront.net has address 52.222.171.64
d1vexie51szton.cloudfront.net has address 52.222.171.70
d1vexie51szton.cloudfront.net has address 52.222.171.77
d2n3e195vjrw9z.cloudfront.net has address 52.222.171.149
d2n3e195vjrw9z.cloudfront.net has address 52.222.171.182
d2n3e195vjrw9z.cloudfront.net has address 52.222.171.191
d2n3e195vjrw9z.cloudfront.net has address 52.222.171.238
d2n3e195vjrw9z.cloudfront.net has address 52.222.171.240
d2n3e195vjrw9z.cloudfront.net has address 52.222.171.39
d2n3e195vjrw9z.cloudfront.net has address 52.222.171.55
d2n3e195vjrw9z.cloudfront.net has address 52.222.171.71
d32ct7cgk4i32b.cloudfront.net has address 52.222.171.105
d32ct7cgk4i32b.cloudfront.net has address 52.222.171.14
d32ct7cgk4i32b.cloudfront.net has address 52.222.171.149
d32ct7cgk4i32b.cloudfront.net has address 52.222.171.151
d32ct7cgk4i32b.cloudfront.net has address 52.222.171.173
d32ct7cgk4i32b.cloudfront.net has address 52.222.171.214
d32ct7cgk4i32b.cloudfront.net has address 52.222.171.48
d32ct7cgk4i32b.cloudfront.net has address 52.222.171.60
dev.r53.splunk.com has address 54.187.149.166
dev.r53.splunk.com has address 54.213.119.78
dev.splunk.com is an alias for dev.r53.splunk.com.
docs.r53.splunk.com has address 52.36.5.66
docs.r53.splunk.com has address 52.88.221.143
docs.splunk.com is an alias for docs.r53.splunk.com.
investors.splunk.com is an alias for amda-rwdlh.client.shareholder.com.
splunkbase.splunk.com has address 35.160.59.174
splunkbase.splunk.com has address 52.11.10.173
splunkbase.splunk.com has address 52.32.239.55
splunklive.splunk.com is an alias for d1vexie51szton.cloudfront.net.
splunk-prod-blogs-413937879.us-west-1.elb.amazonaws.com has address 50.18.199.167
splunk-prod-blogs-413937879.us-west-1.elb.amazonaws.com has address 52.9.61.241
splunk-usergroups-prod-1033061819.us-west-1.elb.amazonaws.com has address 52.8.199.141
splunk-usergroups-prod-1033061819.us-west-1.elb.amazonaws.com has address 52.9.60.70
usergroups.splunk.com is an alias for splunk-usergroups-prod-1033061819.us-west-1.elb.amazonaws.com.
webcenter360.shareholder.com has address 206.200.251.19
www.splunk.com is an alias for d2n3e195vjrw9z.cloudfront.net.
MyOg@CALIKKASAP:/mnt/c/Users/user/Documents/ISS_Wspace$
```

Output of the second grep command (filters and shows only the IP numbers):



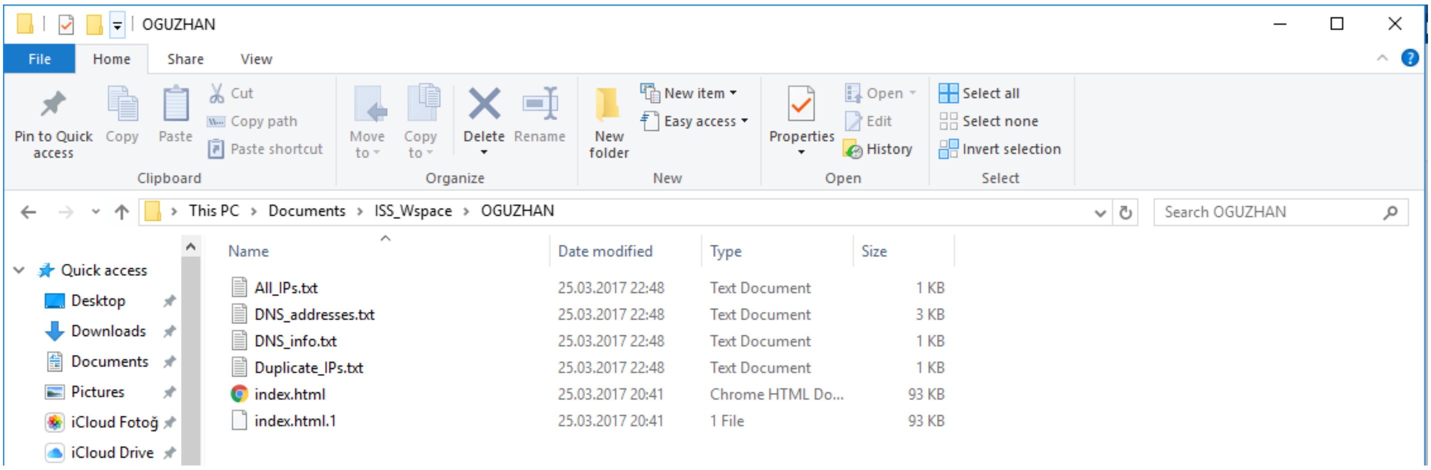
```
 206.200.251.19
 35.160.59.174
 50.18.199.167
 52.11.10.173
 52.222.171.105
 52.222.171.14
 52.222.171.149
 52.222.171.149
 52.222.171.151
 52.222.171.161
 52.222.171.173
 52.222.171.182
 52.222.171.191
 52.222.171.200
 52.222.171.214
 52.222.171.229
 52.222.171.238
 52.222.171.240
 52.222.171.27
 52.222.171.39
 52.222.171.48
 52.222.171.48
 52.222.171.55
 52.222.171.60
 52.222.171.64
 52.222.171.70
 52.222.171.71
 52.222.171.77
 52.32.239.55
 52.36.5.66
 52.8.199.141
 52.88.221.143
 52.9.60.70
 52.9.61.241
 54.187.149.166
 54.213.119.78
MyOg@CALIKKASAP:/mnt/c/Users/user/Documents/ISS_Wspace$
```

Output of the third grep command (shows only the duplicate ones):



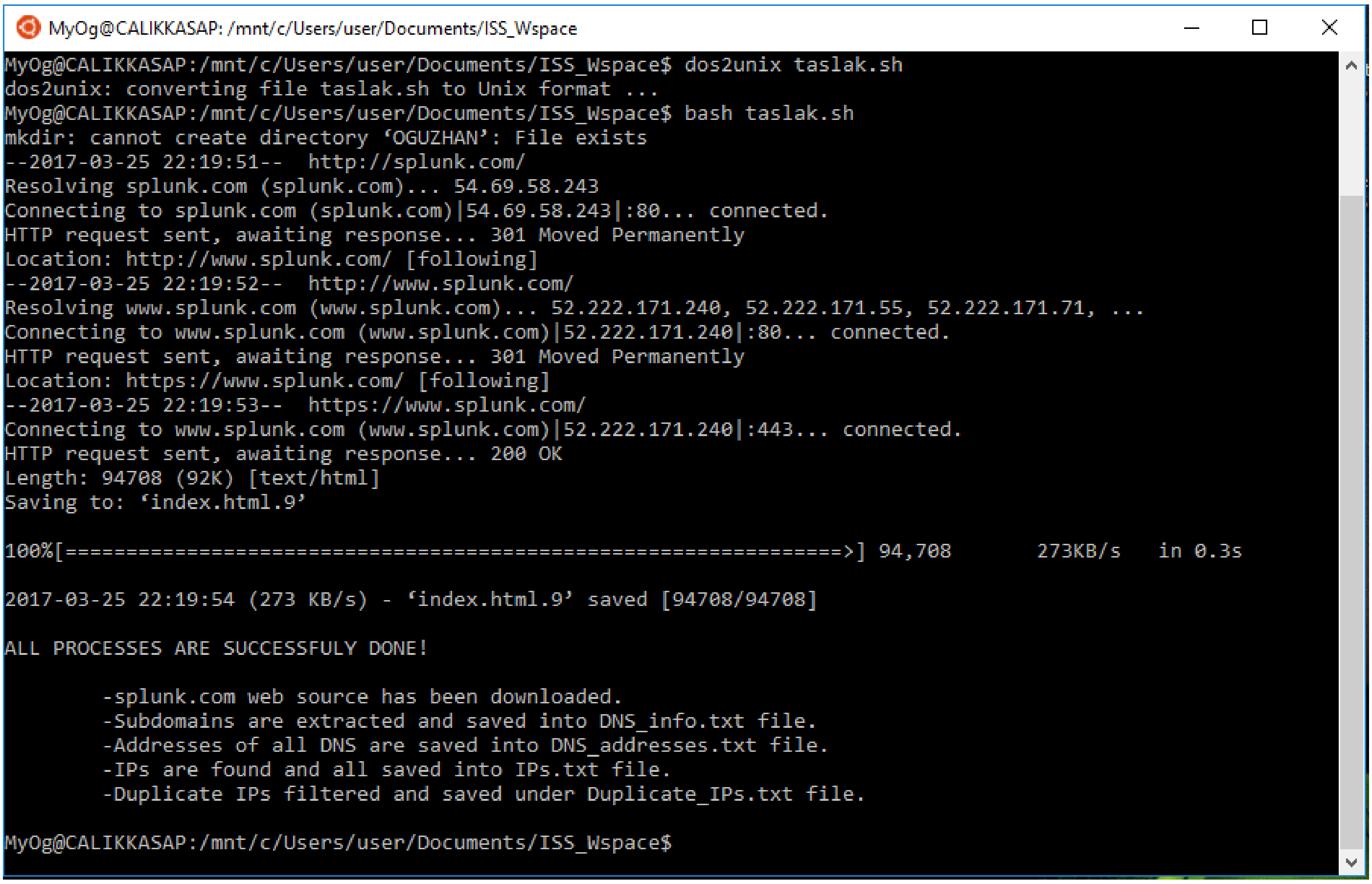
```
MyOg@CALIKKASAP:/mnt/c/Users/user/Documents/ISS_Wspace$ grep -oP '(?<=address).*' IPwithstrings.txt | sort | uni
q -d
 52.222.171.149
 52.222.171.48
MyOg@CALIKKASAP:/mnt/c/Users/user/Documents/ISS_Wspace$
```

Resulting file that has been created by the program:



Name	Date modified	Type	Size
All_IPs.txt	25.03.2017 22:48	Text Document	1 KB
DNS_addresses.txt	25.03.2017 22:48	Text Document	3 KB
DNS_info.txt	25.03.2017 22:48	Text Document	1 KB
Duplicate_IPs.txt	25.03.2017 22:48	Text Document	1 KB
index.html	25.03.2017 20:41	Chrome HTML Do...	93 KB
index.html.1	25.03.2017 20:41	1 File	93 KB

Program information after everything has been done:



```
MyOg@CALIKKASAP:/mnt/c/Users/user/Documents/ISS_Wspace$ dos2unix taslak.sh
dos2unix: converting file taslak.sh to Unix format ...
MyOg@CALIKKASAP:/mnt/c/Users/user/Documents/ISS_Wspace$ bash taslak.sh
mkdir: cannot create directory ‘OGUZHAN’: File exists
--2017-03-25 22:19:51--  http://splunk.com/
Resolving splunk.com (splunk.com)... 54.69.58.243
Connecting to splunk.com (splunk.com)|54.69.58.243|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.splunk.com/ [following]
--2017-03-25 22:19:52--  http://www.splunk.com/
Resolving www.splunk.com (www.splunk.com)... 52.222.171.240, 52.222.171.55, 52.222.171.71, ...
Connecting to www.splunk.com (www.splunk.com)|52.222.171.240|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.splunk.com/ [following]
--2017-03-25 22:19:53--  https://www.splunk.com/
Connecting to www.splunk.com (www.splunk.com)|52.222.171.240|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 94708 (92K) [text/html]
Saving to: ‘index.html.9’

100%[================================================================>] 94,708       273KB/s   in 0.3s

2017-03-25 22:19:54 (273 KB/s) - ‘index.html.9’ saved [94708/94708]

ALL PROCESSES ARE SUCCESSFULY DONE!

        -splunk.com web source has been downloaded.
        -Subdomains are extracted and saved into DNS_info.txt file.
        -Addresses of all DNS are saved into DNS_addresses.txt file.
        -IPs are found and all saved into IPs.txt file.
        -Duplicate IPs filtered and saved under Duplicate_IPs.txt file.

MyOg@CALIKKASAP:/mnt/c/Users/user/Documents/ISS_Wspace$
```