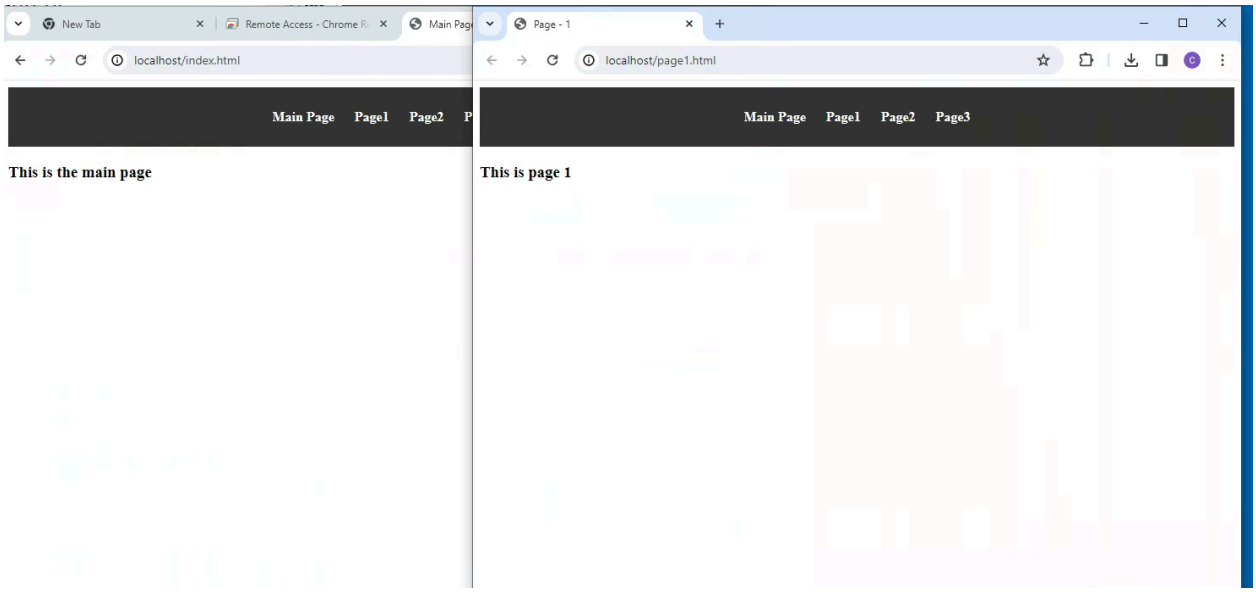
Lab4-1_WindowsApacheLogs
SYS-320
Ben W
SP24

Deliverables:

1. Web page up and running



2. Full Access logs + script

```
# Powershell Script
# SYS-320 - Ben W

cd C:\xampp\apache\logs\

Get-Content access.log
```

```
cd C:\xampp\apache\logs\

Get-Content access.log
::1 - - [09/Feb/2024:10:31:57 -0500] "GET / HTTP/1.1" 200 225 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
::1 - - [09/Feb/2024:10:31:57 -0500] "GET /js/header.js HTTP/1.1" 200 883 "http://localhost/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
::1 - - [09/Feb/2024:10:31:57 -0500] "GET /favicon.ico HTTP/1.1" 404 295 "http://localhost/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
::1 - - [09/Feb/2024:10:32:00 -0500] "GET /page1.html HTTP/1.1" 200 217 "http://localhost/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
::1 - - [09/Feb/2024:10:32:01 -0500] "GET /page2.html HTTP/1.1" 200 217 "http://localhost/page1.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
::1 - - [09/Feb/2024:10:32:04 -0500] "GET /index.html HTTP/1.1" 200 225 "http://localhost/page2.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
::1 - - [09/Feb/2024:10:33:01 -0500] "GET /index.html HTTP/1.1" 304 - "http://localhost/index.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
::1 - - [09/Feb/2024:10:33:02 -0500] "GET /js/header.js HTTP/1.1" 304 - "http://localhost/index.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
::1 - - [09/Feb/2024:10:33:03 -0500] "GET /page2.html HTTP/1.1" 304 - "http://localhost/index.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
::1 - - [09/Feb/2024:10:33:04 -0500] "GET /page3.html HTTP/1.1" 200 217 "http://localhost/page2.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
::1 - - [09/Feb/2024:10:33:06 -0500] "GET /page1.html HTTP/1.1" 304 - "http://localhost/page3.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
::1 - - [09/Feb/2024:10:33:32 -0500] "GET /page1.html HTTP/1.1" 304 - "http://localhost/index.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
::1 - - [09/Feb/2024:10:33:33 -0500] "GET /js/header.js HTTP/1.1" 304 - "http://localhost/page1.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:38 -0500] "GET /pagethatdoesntexist00 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:38 -0500] "GET /favicon.ico HTTP/1.1" 404 296 "http://10.0.17.38/pagethatdoesntexist00" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:40 -0500] "GET /pagethatdoesntexist01 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:43 -0500] "GET /pagethatdoesntexist02 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:46 -0500] "GET /pagethatdoesntexist03 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:47 -0500] "GET /pagethatdoesntexist04 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:50 -0500] "GET /pagethatdoesntexist05 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
::1 - - [09/Feb/2024:10:38:32 -0500] "-" 408 - "-" "-"
```

3. Last 5 lines

```
# Powershell Script
# SYS-320 - Ben W

cd C:\xampp\apache\logs\

Get-Content -tail 5 access.log
```

```
PS C:\xampp\apache\logs> # Powershell Script
# SYS-320 - Ben W

cd C:\xampp\apache\logs\

Get-Content -tail 5 access.log
10.0.17.8 - - [09/Feb/2024:10:35:43 -0500] "GET /pagethatdoesntexist02 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:46 -0500] "GET /pagethatdoesntexist03 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:47 -0500] "GET /pagethatdoesntexist04 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:50 -0500] "GET /pagethatdoesntexist05 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
::1 - - [09/Feb/2024:10:38:32 -0500] "-" 408 - "-" "-"
```

4. Only errors

```
# SYS-320 - Ben W

cd C:\xampp\apache\logs\

Get-Content -tail 10 access.log | Select-String ' 404 ',' 400 '
```

```
PS C:\xampp\apache\logs> # Powershell Script
# SYS-320 - Ben W

cd C:\xampp\apache\logs\

Get-Content -tail 10 access.log | Select-String ' 404 ',' 400 '

10.0.17.8 - - [09/Feb/2024:10:35:38 -0500] "GET /pagethatdoesntexist00 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:38 -0500] "GET /favicon.ico HTTP/1.1" 404 296 "http://10.0.17.38/pagethatdoesntexist00" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:40 -0500] "GET /pagethatdoesntexist01 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:43 -0500] "GET /pagethatdoesntexist02 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:46 -0500] "GET /pagethatdoesntexist03 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:47 -0500] "GET /pagethatdoesntexist04 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:50 -0500] "GET /pagethatdoesntexist05 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
```

5. Non ‘200’ responses

```
cd C:\xampp\apache\logs\

Get-Content -tail 10 access.log | Select-String ' 200 ' -NotMatch
```

```
PS C:\xampp\apache\logs> # Powershell Script
# SYS-320 - Ben W

cd C:\xampp\apache\logs\

Get-Content -tail 10 access.log | Select-String ' 200 ' -NotMatch

#Get-Content -tail 10 access.log | Select-String ' 404 ',' 400 '

::1 - - [09/Feb/2024:10:33:32 -0500] "GET /page1.html HTTP/1.1" 304 - "http://localhost/index.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) chrome/121.0.0.0 Safari/537.36"
::1 - - [09/Feb/2024:10:33:33 -0500] "GET /js/header.js HTTP/1.1" 304 - "http://localhost/page1.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:38 -0500] "GET /pagethatdoesntexist00 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:38 -0500] "GET /favicon.ico HTTP/1.1" 404 296 "http://10.0.17.38/pagethatdoesntexist00" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:40 -0500] "GET /pagethatdoesntexist01 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:43 -0500] "GET /pagethatdoesntexist02 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:46 -0500] "GET /pagethatdoesntexist03 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:47 -0500] "GET /pagethatdoesntexist04 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
10.0.17.8 - - [09/Feb/2024:10:35:50 -0500] "GET /pagethatdoesntexist05 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
::1 - - [09/Feb/2024:10:38:32 -0500] "-" 408 - "-" "-"
```

6. Log file errors

```
cd C:\xampp\apache\logs
$errors = ls -File .\*.log | Select-String "error"

$errors[-5..-1]
```

```
PS C:\xampp\apache\logs> C:\Users\champuser\Documents\sys320git\PowershellLabs\Lab04-Cla

install.log:14:Rewrote docs/conf/extra/httpd-multilang-errordoc.conf.in
install.log:15: to c:/Apache24/conf/original/extra/httpd-multilang-errordoc.conf
install.log:40:Duplicated c:/Apache24/conf/original/extra/httpd-multilang-errordoc.conf
install.log:41: to c:/Apache24/conf/extra/httpd-multilang-errordoc.conf
```

7. IP List from logs

```
cd C:\xampp\apache\logs

$notfounds = Get-Content -tail 10 access.log | Select-String ' 404 '

$regex = [regex] "^(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}) .*"


$ipsUnorganized = $notfounds -split $regex

$ips = @()
for ($i=0; $i -lt $ipsUnorganized.Count; $i++) {
    $ips += [pscustomobject]@{ "IP" = $ipsUnorganized[$i]; }
}

$ips | ? { $_.IP -ilike "10.*" }
```

```
PS C:\xampp\apache\logs> C:\Users\champuser\Documents\sys320git\PowershellLab

IP
--
10.0.17.8
10.0.17.8
10.0.17.8
10.0.17.8
10.0.17.8
10.0.17.8
10.0.17.8
```

8. This worked sort of, I changed it to better match the prompted program, but it stopped working so well.

```
# Powershell Script
# SYS-320 - Ben W

cd C:\xampp\apache\logs

$notfounds = Get-Content -tail 10 access.log | Select-String ' 404 '

$regex = [regex] "^(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}) .*"


$ipsUnorganized = $regex.Matches($notfounds)

$ips = @()
for ($i=0; $i -lt $ipsUnorganized.Count; $i++) {
    $ips += [pscustomobject]@{ "IP" = $ipsUnorganized[$i].Value; }
}

$ipoftens = $ips | ? { $_.IP -ilike "10.*" }

$count = $ipoftens | Group-Object IP

$count | Select-Object Count, Name
```

```
PS C:\xampp\apache\logs> C:\Users\champuser\Documents\sys320git\PowershellLabs\Lab04-ClassActivity\Lab04-1_ClassActivity.ps1

Count Name
----- ----
    1 10.0.17.8 - - [09/Feb/2024:10:35:38 -0500] "GET /pagethatdoesntexist00 HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36" 10.0.17.8 - - [09/F...


PS C:\xampp\apache\logs>
```

9. https://github.com/benjamin-weatherill/SYS-320/tree/main/PowershellLabs/Lab04-ClassActivity