

Vu Nguyen

UID: u1483046

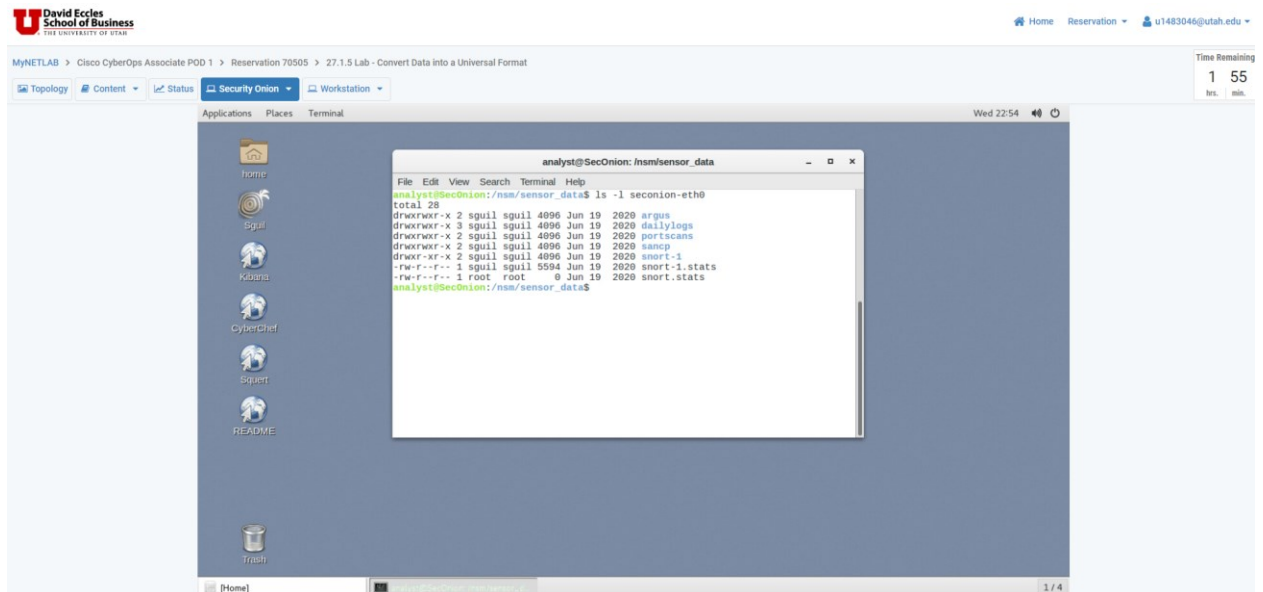
# Assignment 27 - Formatting and REGEX (Lab and Quiz)

## 1. Lab 27.1.5, Part 1, Step 1e:

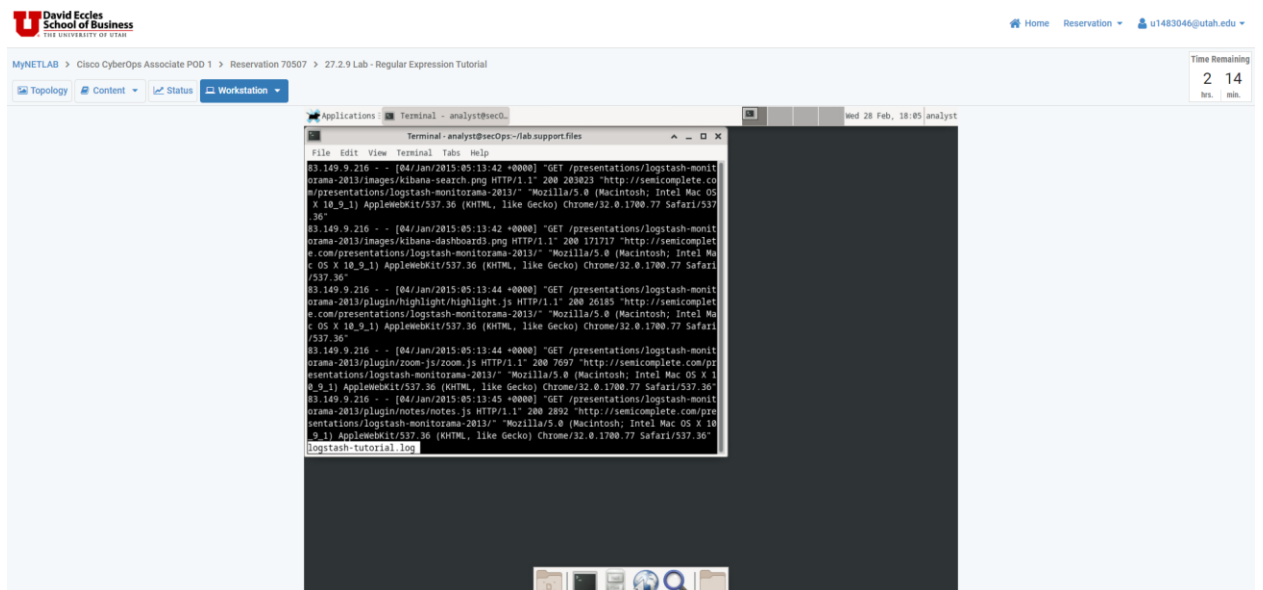
The screenshot shows a MyNETLAB workstation interface. The top navigation bar includes the David Eccles School of Business logo, the course path "MyNETLAB > Cisco CyberOps Associate POD 1 > Reservation 70505 > 27.1.5 Lab - Convert Data into a Universal Format", and a "Workstation" tab. A timer in the top right corner shows "Time Remaining: 2 hrs, 02 min". The terminal window, titled "analyst@secops", displays the following content:

```
analyst@secops:~$ ls -l
drwxr-xr-x 7 analyst analyst 4096 Mar 21 2018 .
-rw-r--r-- 1 analyst analyst 473363 Mar 21 2018 sample.img
-rw-r--r-- 1 analyst analyst 65 Mar 21 2018 sample.img.SHA256.sig
drwxr-xr-x 3 analyst analyst 4096 Mar 21 2018 scripts
-rw-r--r-- 1 analyst analyst 25553 Mar 21 2018 SQL_Lab.pcap
drwxr-xr-x 2 analyst analyst 4096 Aug 11 2020 traceoute_files
analyst@secops lab.support.files$
analyst@secops lab.support.files$ awk 'BEGIN {FS="|"}' ($3==strftime("%c,%Y"))
(print) applicationX_in_epoch.log
awk: cmd. line:1: BEGIN {FS="|"} ($3==strftime("%c,%Y")) (print)
awk: cmd. line:1: ^ syntax error
analyst@secops lab.support.files$ awk 'BEGIN {FS="|"}' ($3==strftime("%c", $3))
(print) applicationX_in_epoch.log
2|Z|Mon 18 Aug 2008 11:00:00 AM EDT|AF|0
3|N|Tue 19 Aug 2008 11:00:00 AM EDT|AF|89
4|N|Sun 07 Sep 2008 11:00:00 AM EDT|AS|12
5|Z|Mon 08 Sep 2008 11:00:00 AM EDT|AS|67
6|N|Tue 09 Sep 2008 11:00:00 AM EDT|EU|23
7|R|Wed 18 Sep 2008 11:00:00 AM EDT|OC|89
8|Wed 31 Dec 1969 07:00:00 PM EST
analyst@secops lab.support.files$ nano applicationX_in_epoch.log
analyst@secops lab.support.files$ awk 'BEGIN {FS="|"}' ($3==strftime("%c", $3))
(print) applicationX_in_epoch.log > applicationX_in_human.log
analyst@secops lab.support.files$
```

## 2. Lab 27.1.5, Part 3, Step 3c:



## 3. Lab 27.2.9, Part 3, Step 1d (doesn't have to be in the same location of my screen):



#### 4. Lab 27.2.10, Part 1, Step 1g:

David Eccles School of Business  
THE UNIVERSITY OF UTAH

Home Reservation u1483046@utah.edu

MyNETLAB > Cisco CyberOps Associate POD 1 > Reservation 70508 > 27.2.10 Lab - Extract an Executable from a PCAP

Time Remaining: 2 36 hrs. min.

Applications ninda.download.pcap Wireshark - Follow TCP Stream (tcp.stream eq 0) ninda.download.pcap

File Edit View Help

Wireshark - Follow TCP Stream (tcp.stream eq 0) ninda.download.pcap

GET /WS2.Ninda.Ann.exe HTTP/1.1  
User-Agent: Wget/1.19.1 (linux-gnu)  
Accept: \*/\*  
Accept-Encoding: identity  
Host: 209.165.202.133:8080  
Connection: keep-alive

HTTP/1.1 200 OK  
Server: nginx/1.12.0  
Date: Tue, 02 May 2017 14:26:50 GMT  
Content-Type: application/octet-stream  
Content-Length: 345888  
Last-Modified: Fri, 14 Apr 2017 19:17:25 GMT  
Connection: keep-alive  
ETag: "5d8f12845-54480"  
Accept-Ranges: bytes

Frame 4: 238 B on interface (eth0) [Captured]  
Ethernet II, Src: Intel E1000 (08:00:00:00:00:00), Dst: Intel E1000 (08:00:00:00:00:00)  
Internet Protocol Version 4, Src: 10.0.0.1, Dst: 209.165.202.133  
Transmission Control Protocol, Src Port: 8080, Dst Port: 8080, Seq: 1000000000, Win: 65535, Len: 0  
Hypertext Transfer Protocol

16 4c 37 9  
0018 00 0b 2f 6  
0019 ca 85 bd d  
0020 00 1a 37 8  
0021 e5 11 47 4  
0022 2e 41 6d 6

Find: Filter Out This Stream Print Save as... Back X Close

Profile: Default

#### 5. Lab 27.2.10, Part 2, Step 1c:

David Eccles School of Business  
THE UNIVERSITY OF UTAH

Home Reservation u1483046@utah.edu

MyNETLAB > Cisco CyberOps Associate POD 1 > Reservation 70508 > 27.2.10 Lab - Extract an Executable from a PCAP

Time Remaining: 2 35 hrs. min.

Applications ninda.download.pcap Wireshark - Export HTTP object list

File Edit View Help

Wireshark - Export HTTP object list

Packet	Hostname	Content Type	Size	Filename
365	209.165.202.133:8080	application/octet-stream	345 KB	WS2.Ninda.Ann.exe

Text Filter: Save All X Close Save

Frame (1282 bytes) Reassembled TCP (345346 bytes)

Packets: 316 - Displayed: 316 (100.0%) Profile: Default