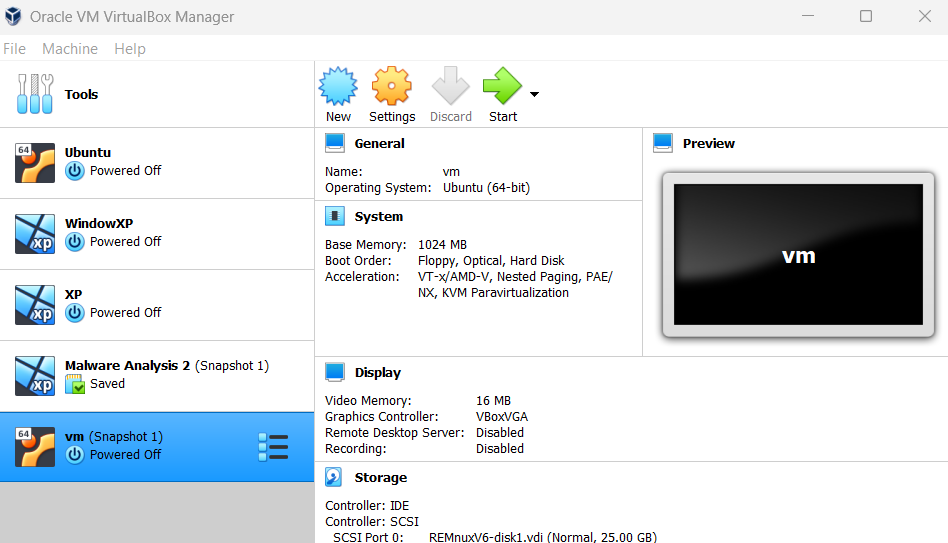
**Step I - INSTALL VMs**

* Install Windows XP - Victim VM
* Install REMnux - Gate VM
  + Update Built-in toollssudo update-remnux full
  + Install guest utils:sudo apt-get install virtualbox-guest-utils
  + Reboot :sudo reboot now



**Step II - NETWORK SETUP**

* REmnux-VM

Enable network adapter 1 and attach it to Internal Network

Click on the arrow pointing down to the left of the option Name, and you will be able to select your Internal networks

By default VirtualBox has intnet already created for you.

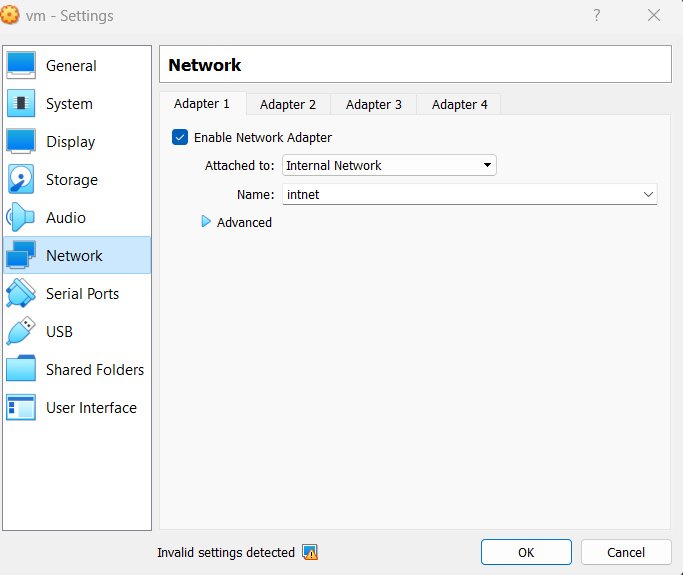
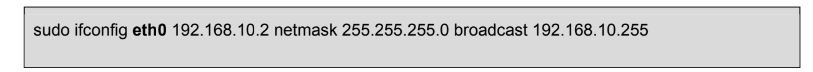
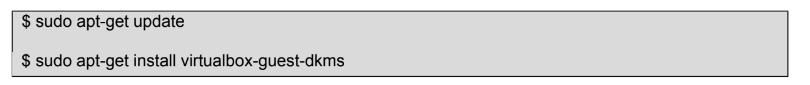
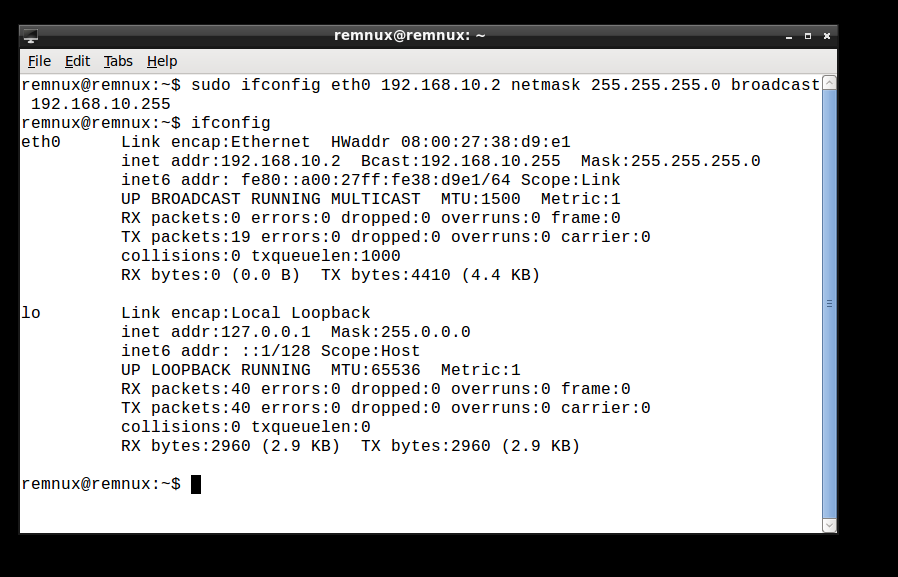


Figure 2: Enabling adapter 1 and attaching it to Internal network

Now, I am starting my RemnuxVM.

Configure IP address of Remnux





Configure INetSim

Init.d config file: /etc/default/inetsim

Main Config : /etc/inetsim/inetsim.conf

Reports : /var/log/inetsim/reports

Main Log: /var/log/inetsim/

Data Files: /var/lib/inetsim/

For this setup, you will have to, first, access the Main Config file with sudo rights.

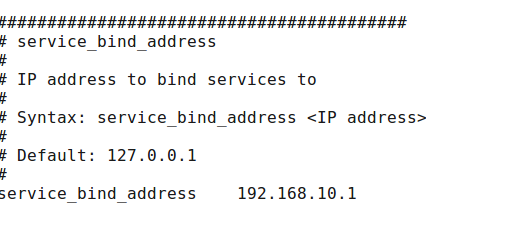
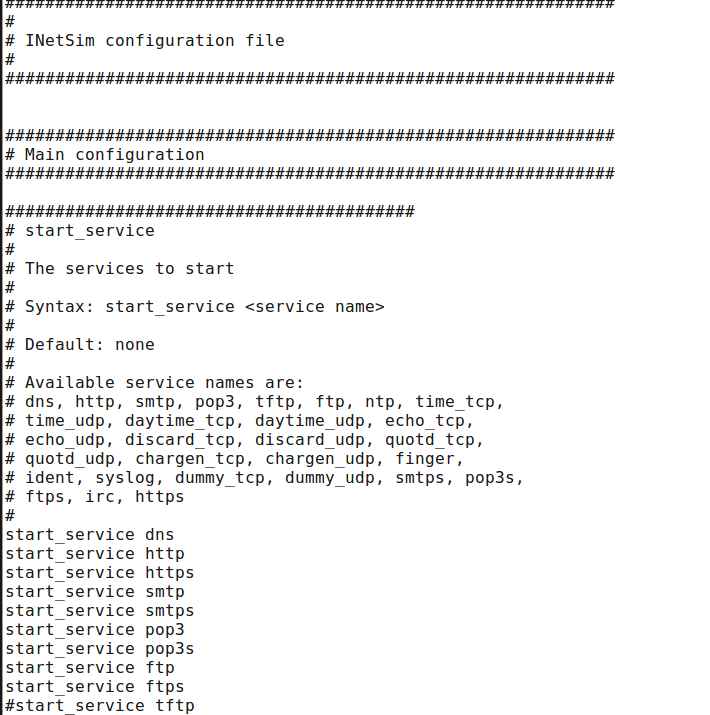


Figure 5: binding eth0 static address to the services handled by INetSim

Window XP

Enable network adapter 1 and attach to Internal Network

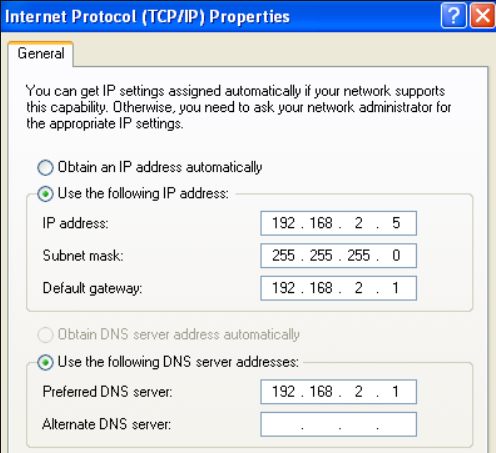
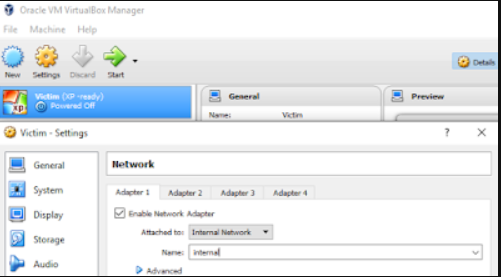


Figure 6: selecting internal network to be attached to the only network adapter for Victim

Start Victim and configure your network adapter:

Figure 9: Configuring the Internal Network adapter to use Gate IP address as its gateway and set a static IP

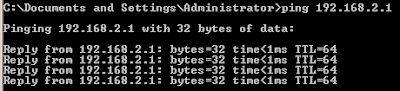


Figure 10: Pinging Gate (Gateway)

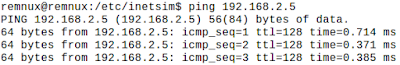
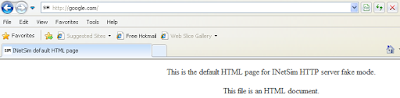


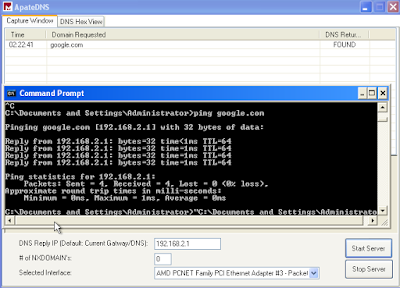
Figure 11: Pinging Victim from Gate

Test my browser to see if Victim is talking to INetSim

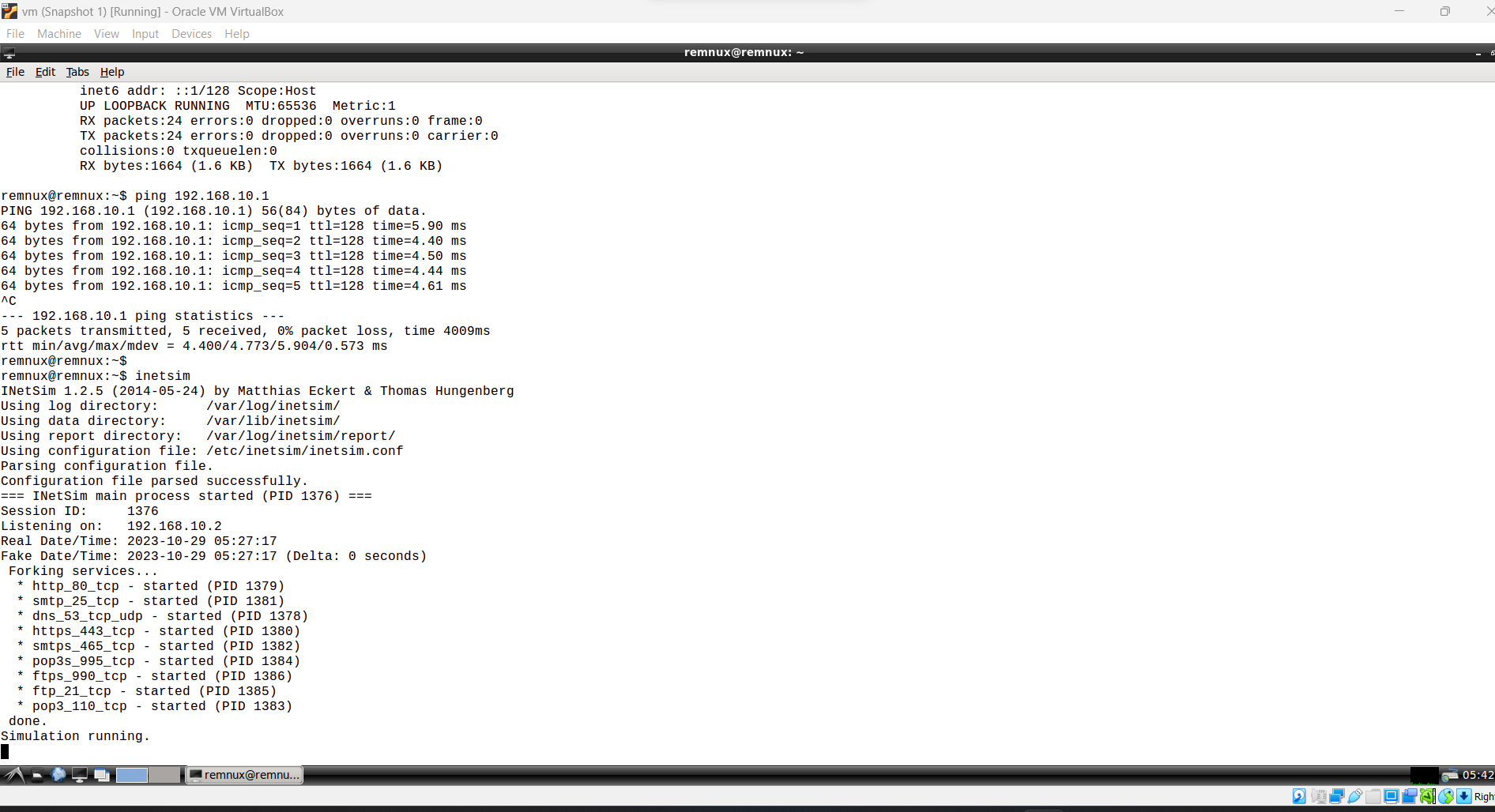


Launch ApateDNS, and set DNS Reply IP to 192.168.2.1 in order to redirect traffic to our Gate

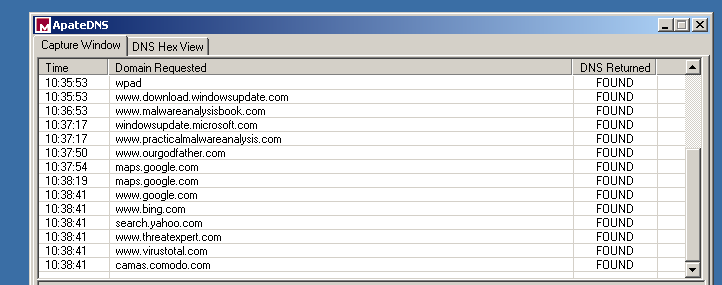
Next, start the server and test it by pinging google.com from command prompt



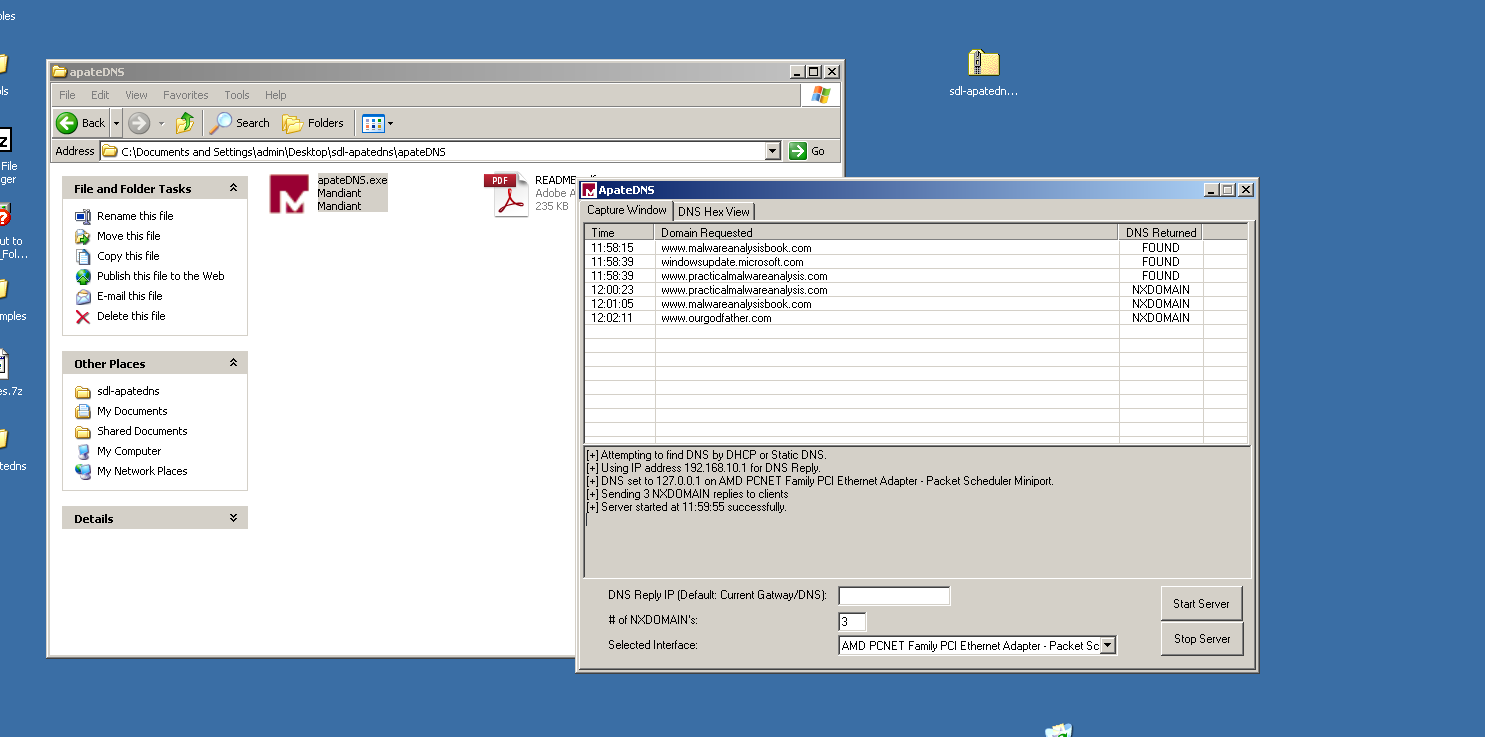
After starting Inetsim



After Executing malwares



After changing to Nx domain=3



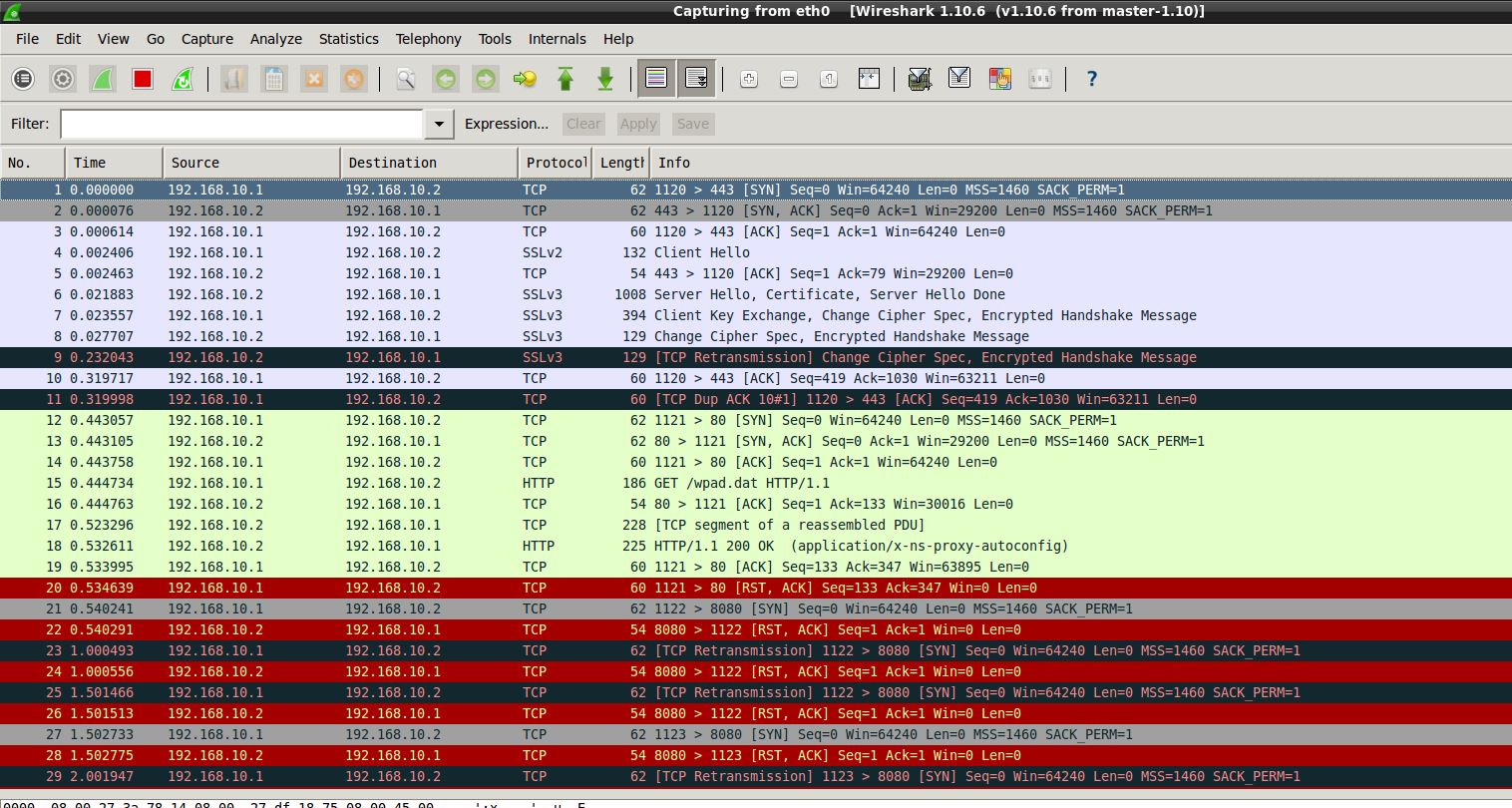
Understand the colors:

Services = Pink

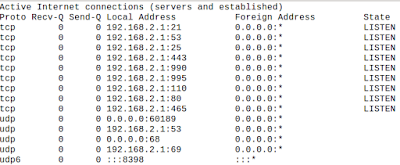
Processes = light purple/light blue ( looks purple to me)

New process = Green

Terminated process = Red



Inetsim listening on the ports



**1. Open a browser on the XP machine. Send a request for an image file from a**

**hypothetical (or real) HTTP server. What happens when you do this?**

When I send a request for an image file from a hypothetical (or real) HTTP server, ApateDNS intercepts the request and redirects it to INetSim. INetSim then generates a simulated response, which will be returned to the browser.

**2. Send another request for a web page through HTTPS. What do you notice?**

When I send a request for a web page through HTTPS, ApateDNS will not be able to intercept the request, as HTTPS is encrypted. Therefore, the request will be sent directly to the destination server.

**3. Try downloading an executable (either .com or .exe file) from any website. What**

**happens when you make this request?**

When I try to download an executable file, ApateDNS will intercept the request and redirect it to INetSim. INetSim then generates a simulated response, which will be returned to the browser.I got an alert that it is an inetsim generated file.

**4. Unzip the file containing the three malware samples (password: infected). Execute**

**each of them and note/record their network behaviour as observed by you and/or**

**logged with the tools.**

**Which domains are the samples trying to contact?**

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

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

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

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

**What http requests (if any) are being made and when do these requests occur?**

Red and black ,blue

**From the logs, traffic capture and tool outputs, can you establish the sequence of**

**events in the malware samples’ network activities?**

The malware sample infects the computer and connects to the internet.

The malware sample contacts a C2 server to receive instructions.

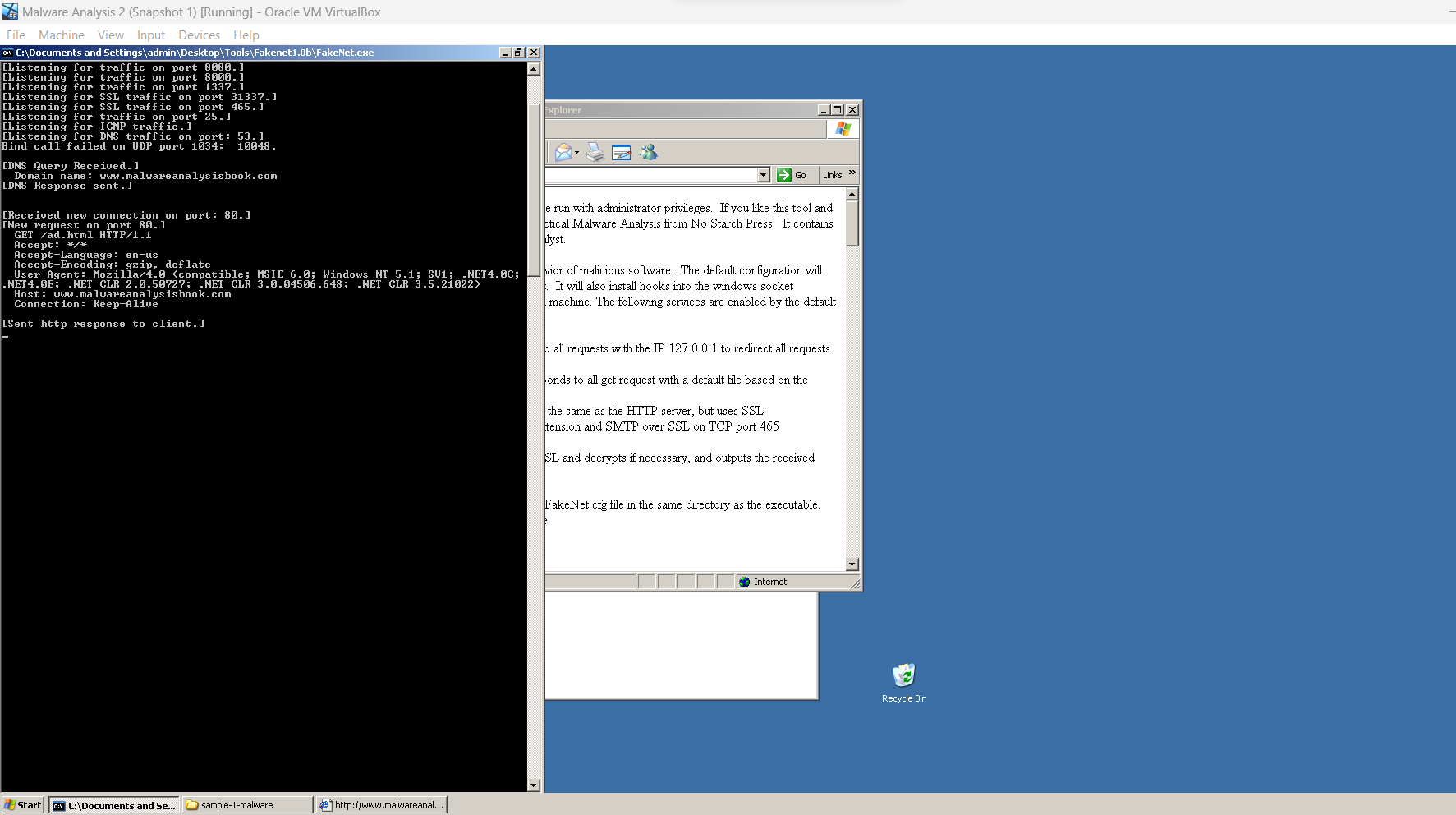
The C2 server instructs the malware sample to download a file from an update server.

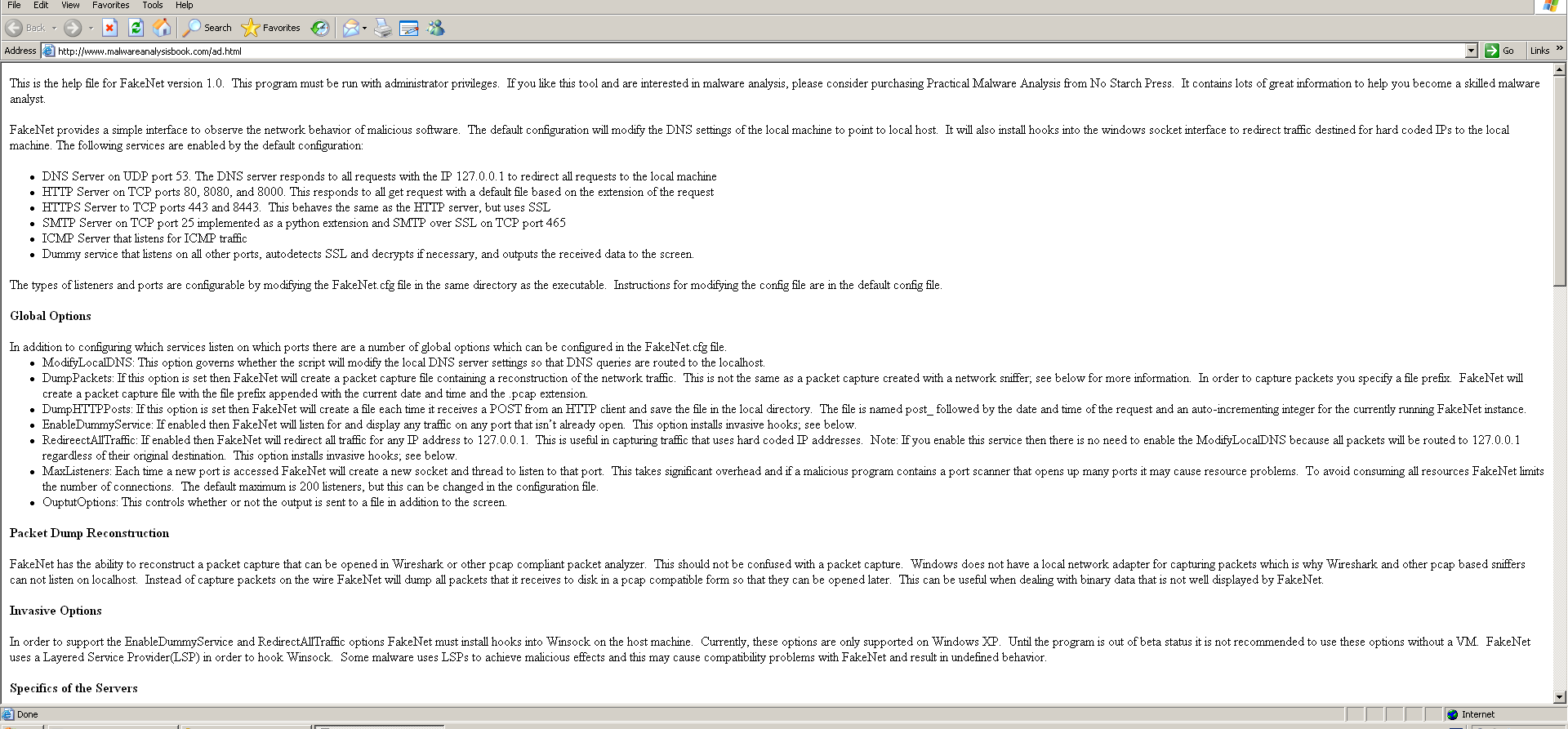
The malware sample downloads the file from the update server and executes it.

The malware sample contacts a data exfiltration server to upload stolen data.

**2nd part: Network services with FakeNet**

**After 1st malware**

****

**Browser looks like:**

**After 2nd malware:**

**After 3rd malware:**