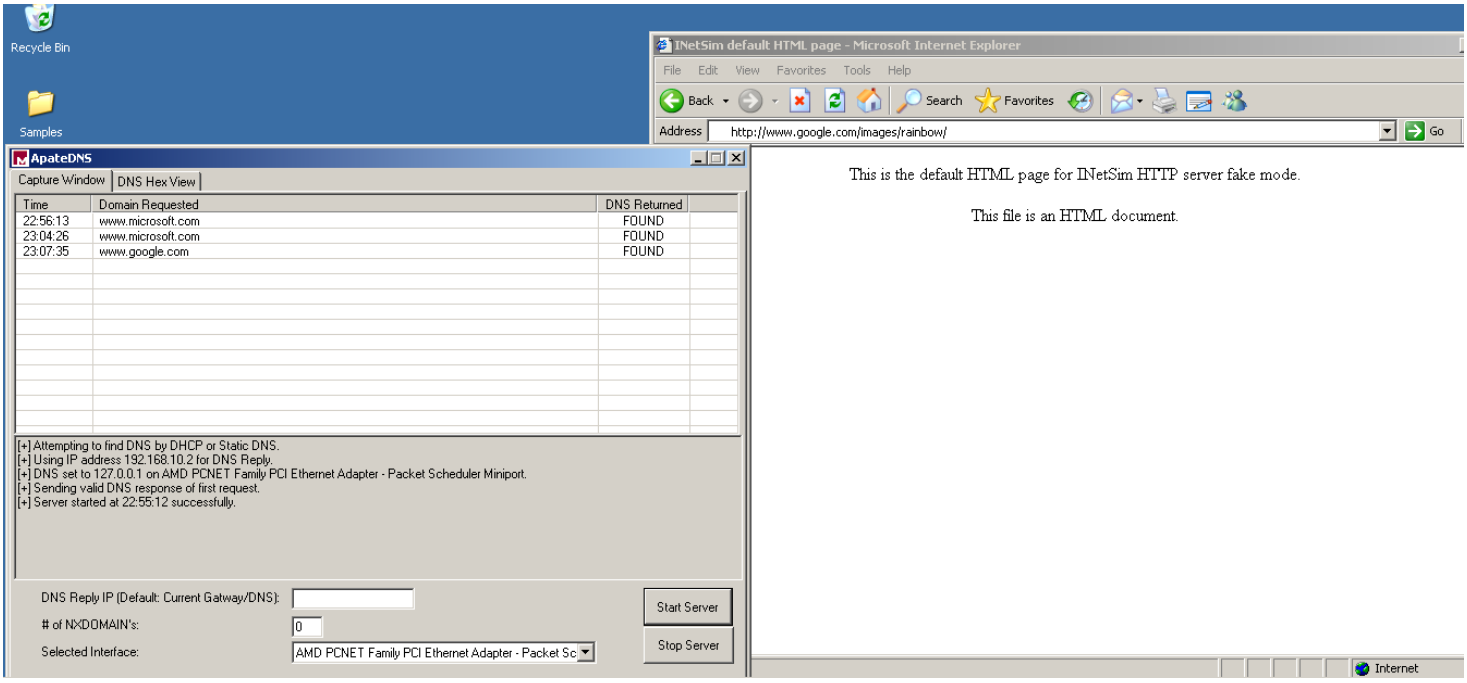
Information Security Assignment 2

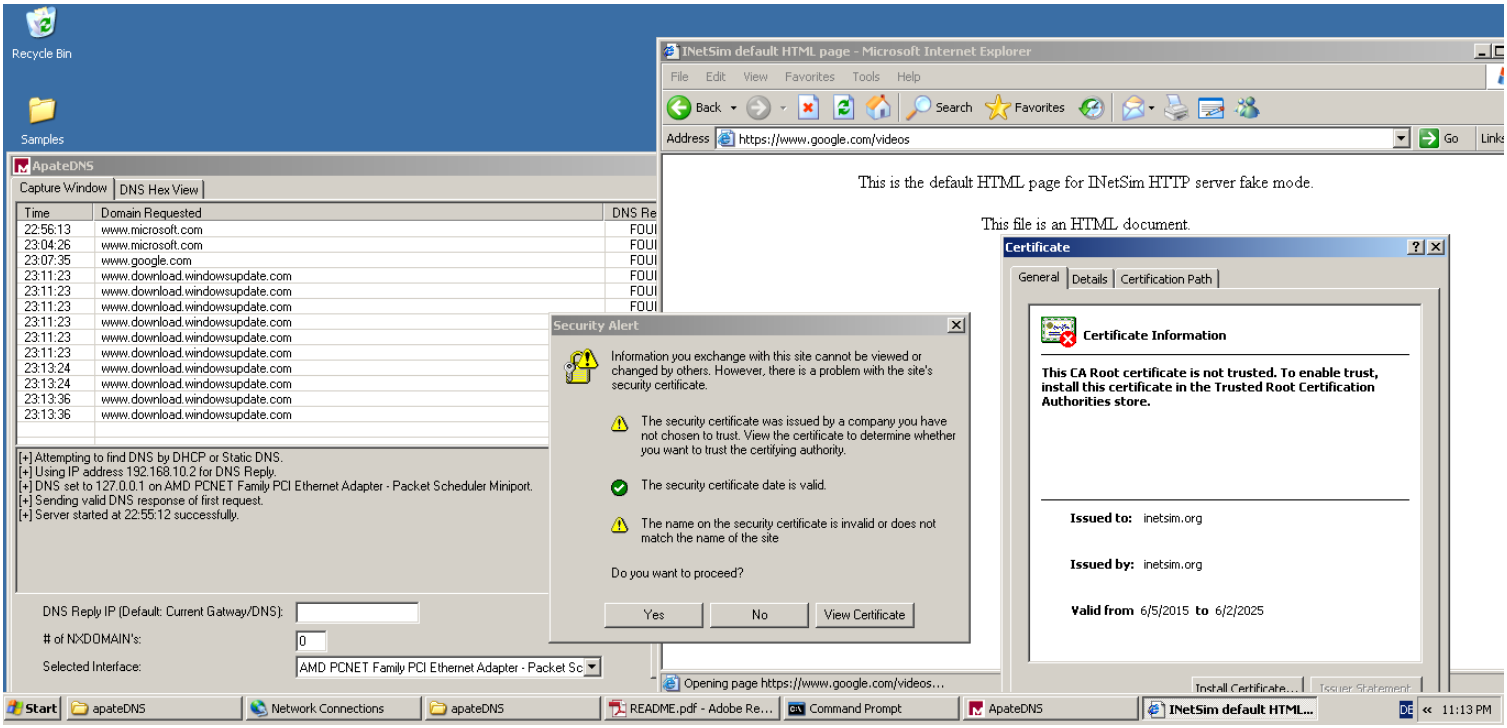
Part 1

Activity 1:



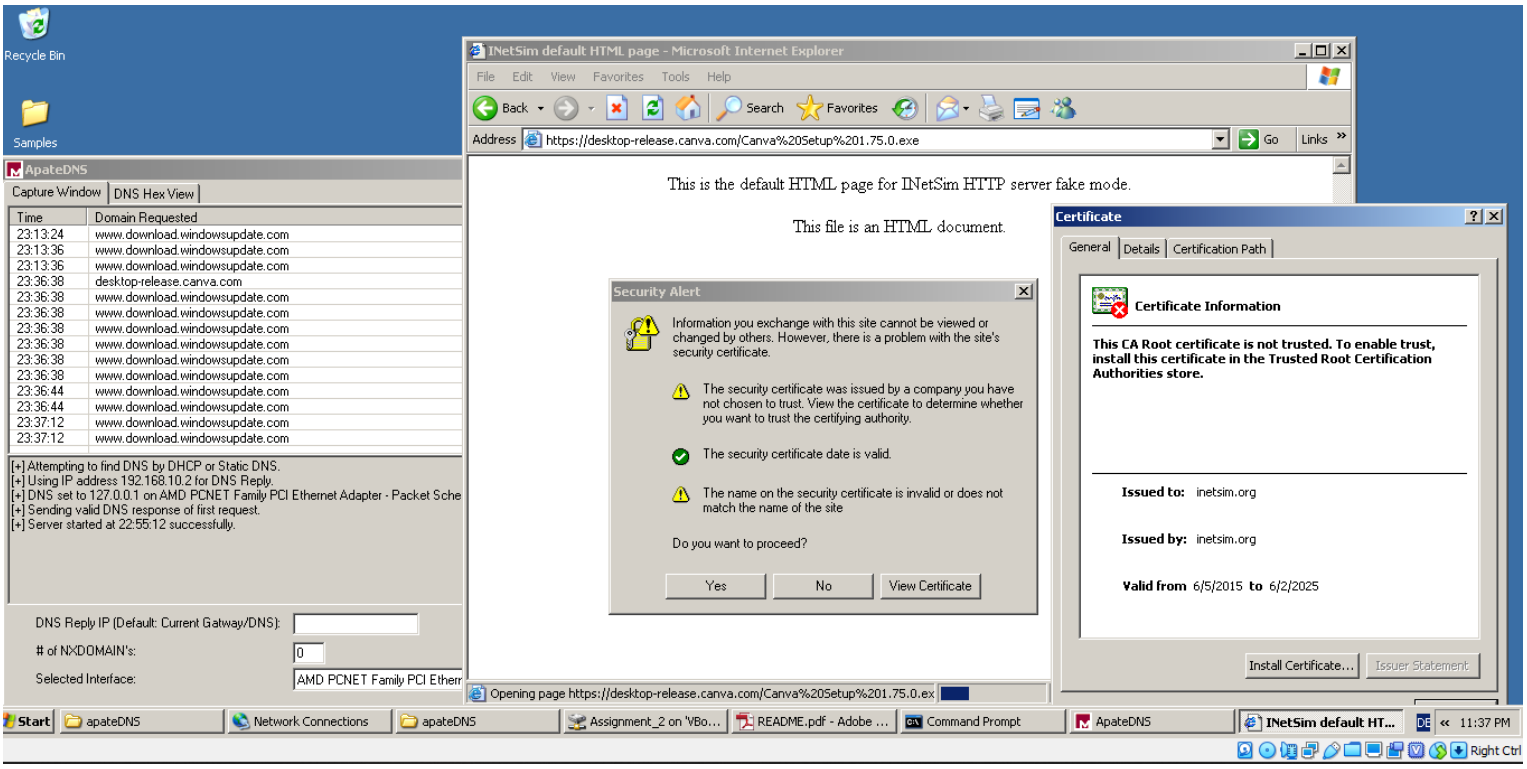
When we try to open a browser on XP machine and send a request for an image file, ApateDNS spoofs the DNS response and what gets opened instead is the default HTML page for INetSim HTTP server because in the case of ApateDNS, the default DNS reply is current gateway and we set the default gateway of XP machine as the REMnux machine's IP where INetSim is running the simulation (INetSim acts as an HTTP server).

Activity 2:



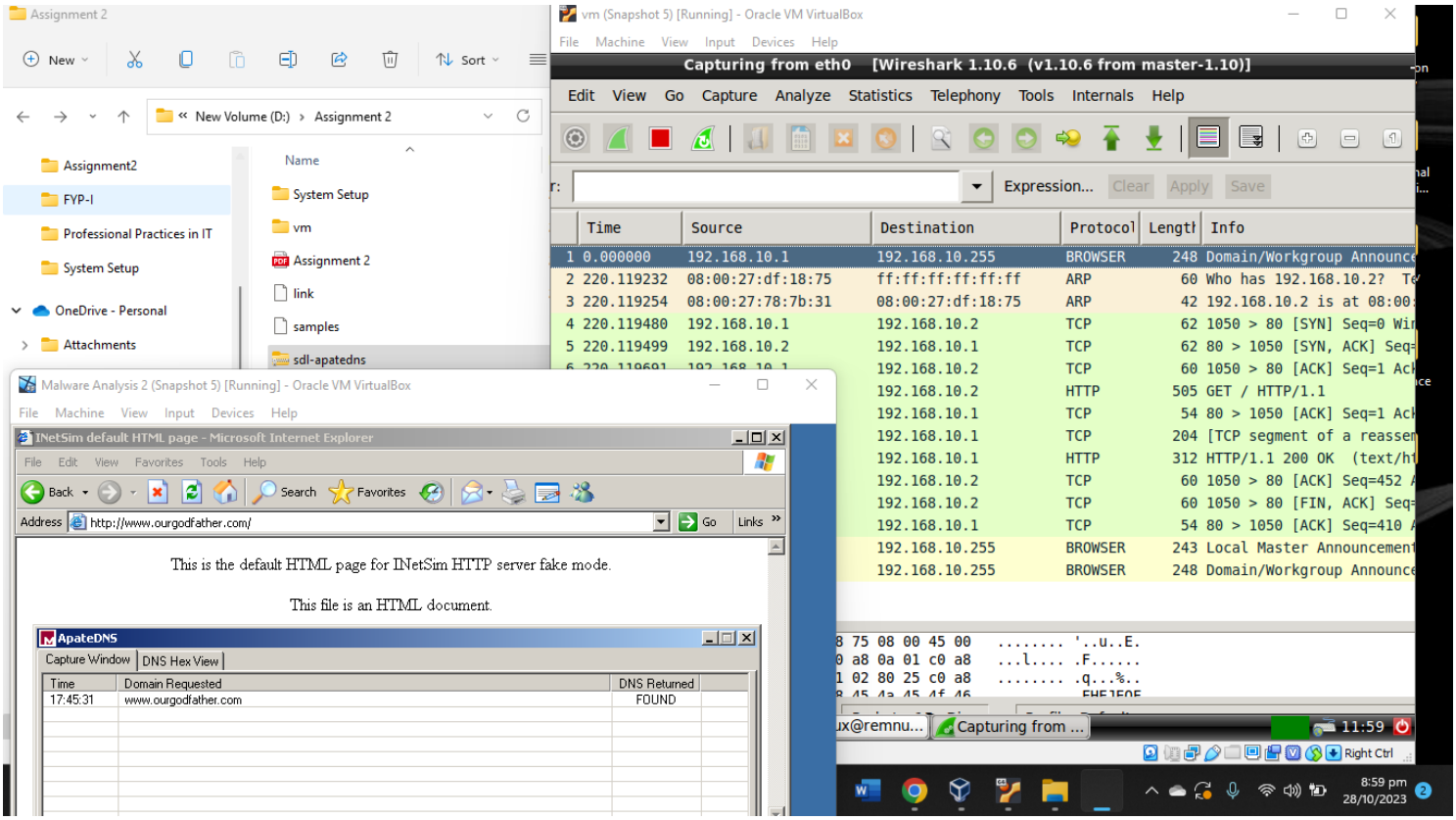
Once we send a request for a webpage through HTTPS, ApateDNS spoofs the DNS response and what gets opened instead is the default HTML page for INetSim HTTP server because in the case of ApateDNS, the default DNS reply is current gateway and we set the default gateway of XP machine as the REMnux machine's IP where INetSim is running the simulation (INetSim acts as an HTTP server). However, in this case, we sent the request through HTTPS, which is a secure protocol, thus we get a security alert as shown in the above screenshot. We can view the certificate through this security alert. It can be seen in the above screenshot that the certificate was not issued by CA, rather it was issued by inetsim.org to inetsim.org which highlights malicious activity.

Activity 3:



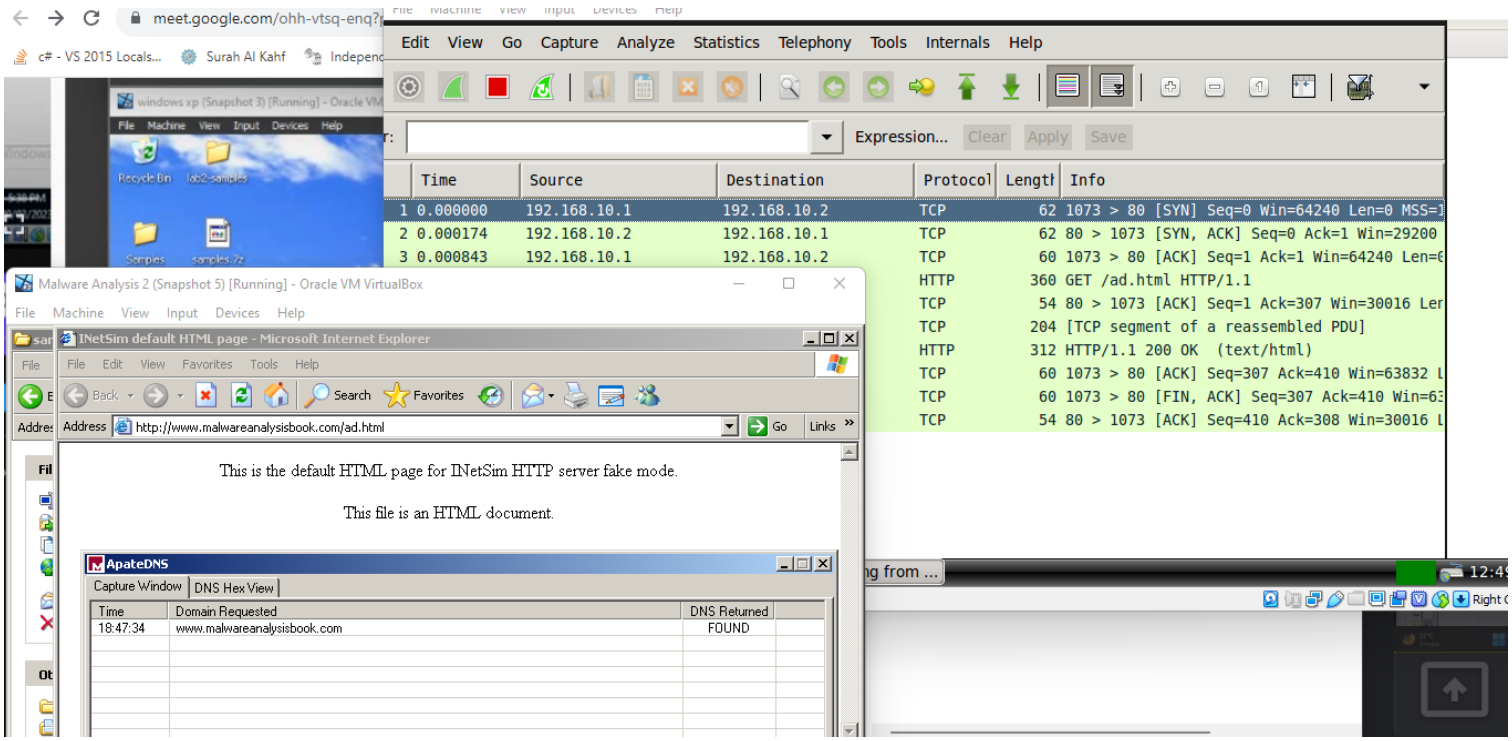
Once we try to download an executable (.exe) file from a website, ApateDNS spoofs the DNS response and what gets opened instead is the default HTML page for INetSim HTTP server because in the case of ApateDNS, the default DNS reply is current gateway and we set the default gateway of XP machine as the REMnux machine's IP where INetSim is running the simulation (INetSim acts as an HTTP server). However, we tried downloading the executable file through HTTPS, which is a secure protocol, thus we get a security alert as shown in the above screenshot. We can view the certificate through this security alert. It can be seen in the above screenshot that the certificate was not issued by CA, rather it was issued by inetsim.org to inetsim.org which highlights malicious activity.

Activity 4 (Live messenger)



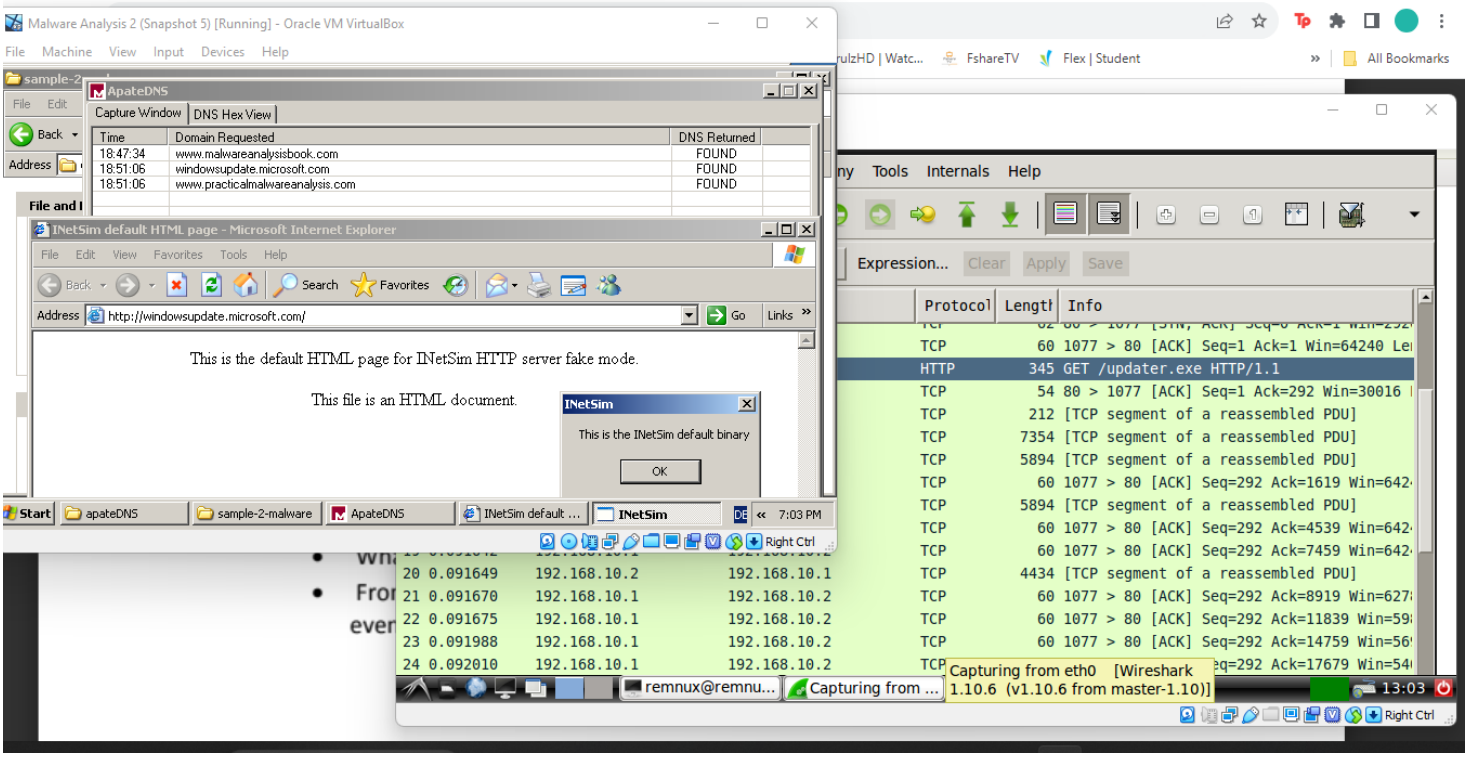
- The sample was trying to contact www.ourgodfather.com.
- HTTP request is being made by the XP machine to the INetSim server as shown by wireshark in the screenshot. In reality, http request was to be made to www.ourgodfather.com but because the DNS reply was spoofed, it was made to the INetSim server on REMnux machine instead. This request occurs after the DNS was spoofed by ApateDNS. On wireshark, it can be seen at line 7 occurring at a timestamp of around 220.
- The malware tries to open www.ourgodfather.com to redirect the user/analyst. www.ourgodfather.com is a Domain Name. Its IP address is needed which will be the DNS response. ApateDNS spoofs this DNS response. In the case of ApateDNS, the default DNS reply is the current gateway of the machine which in the case of XP machine is the IP address of REMnux machine. INetSim is running a simulation on REMnux machine which means INetSim is acting as a server. Thus, http request is made to InetSim server, as a response, we see the default HTML page for INetSim HTTP server in our browser on XP machine.

Activity 4 (Sample 1):



- The sample is trying to contact www.malwareanalysisbook.com
- Http request is being made by the XP machine to the INetSim server as shown by wireshark in the screenshot. In reality, http request was to be made to www.malwareanalysisbook.com but because the DNS reply was spoofed, it was made to the INetSim server on REMnux machine instead. This request occurs after the DNS was spoofed by ApateDNS. On wireshark, it can be seen at line 4 occurring at a timestamp of around 0.
- The malware tries to open www.malwareanalysisbook.com to redirect the user/analyst. www.malwareanalysisbook.com is a Domain Name. Its IP address is needed which will be the DNS response. ApateDNS spoofs this DNS response. In the case of ApateDNS, the default DNS reply is the current gateway of the machine which in the case of XP machine is the IP address of REMnux machine. INetSim is running a simulation on REMnux machine which means INetSim is acting as a server. Thus, http request is made to InetSim server, as a response, we see the default HTML page for INetSim HTTP server in our browser on XP machine.

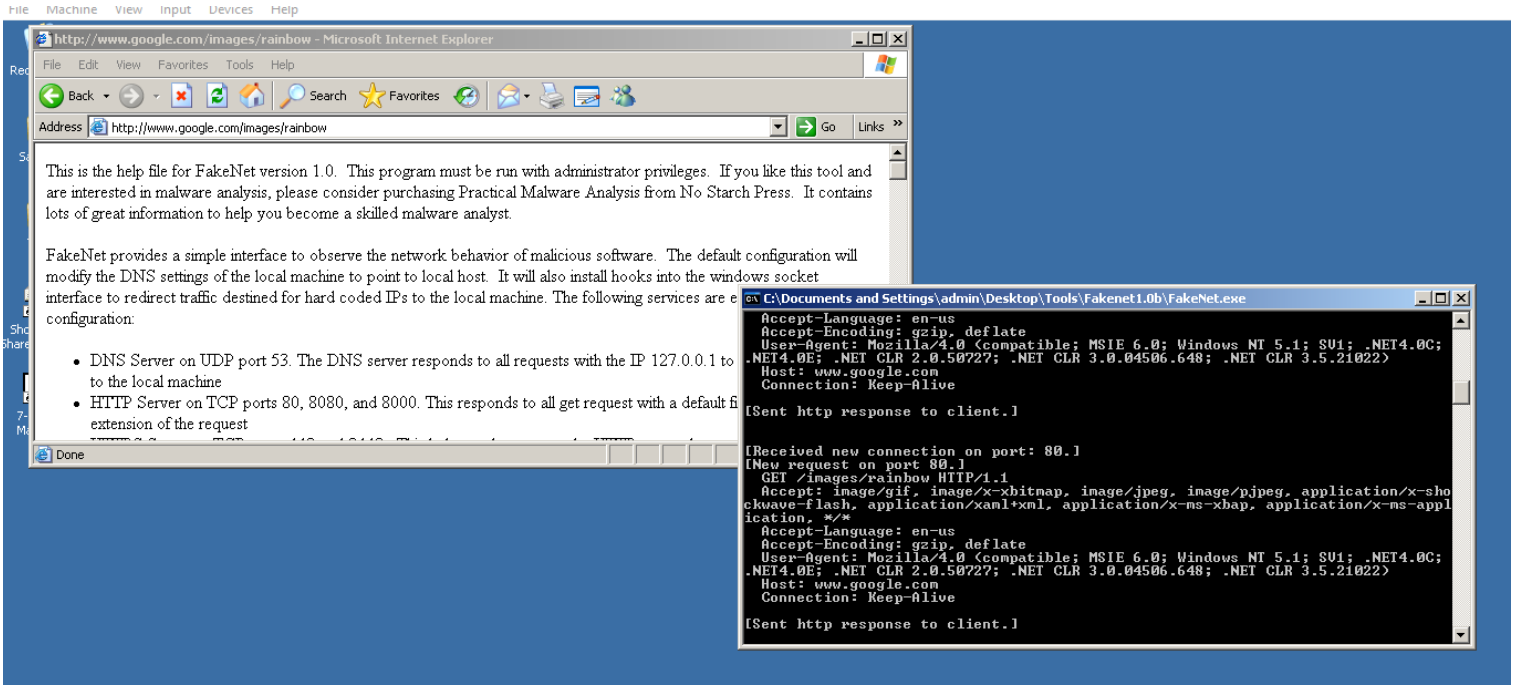
Activity 4 (Sample 2):



- The sample tried to contact www.practicalmalwareanalysis.com
- Http request is being made and this is made by the XP machine to the INetSim server. In reality, http request was to be made to www.practicalmalwareanalysis.com but because the DNS reply was spoofed, it was made to the INetSim server on REMnux machine instead. This request occurs after the DNS was spoofed by ApateDNS. Another HTTP request was made in order to download the updater.exe file.
- The malware tries to open www.practicalmalwareanalysis.com to redirect the user/analyst. www.practicalmalwareanalysis.com is a Domain Name. Its IP address is needed which will be the DNS response. ApateDNS spoofs this DNS response. In the case of ApateDNS, the default DNS reply is the current gateway of the machine which in the case of XP machine is the IP address of REMnux machine. INetSim is running a simulation on REMnux machine which means INetSim is acting as a server. Thus, http request is made to INetSim server, as a response, we see the default HTML page for INetSim HTTP server in our browser on XP machine. In this case, we also see a message box appear.

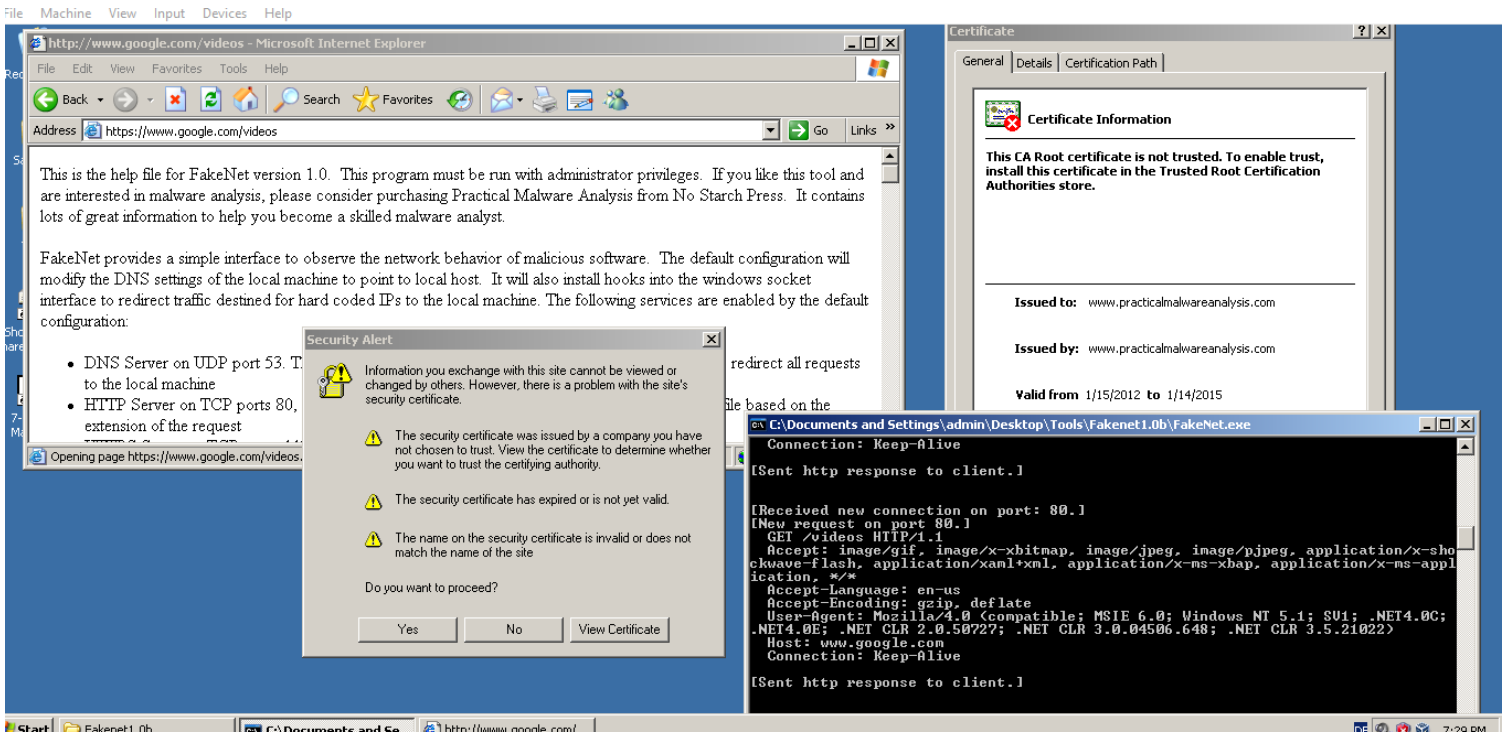
PART 2

Activity 1:



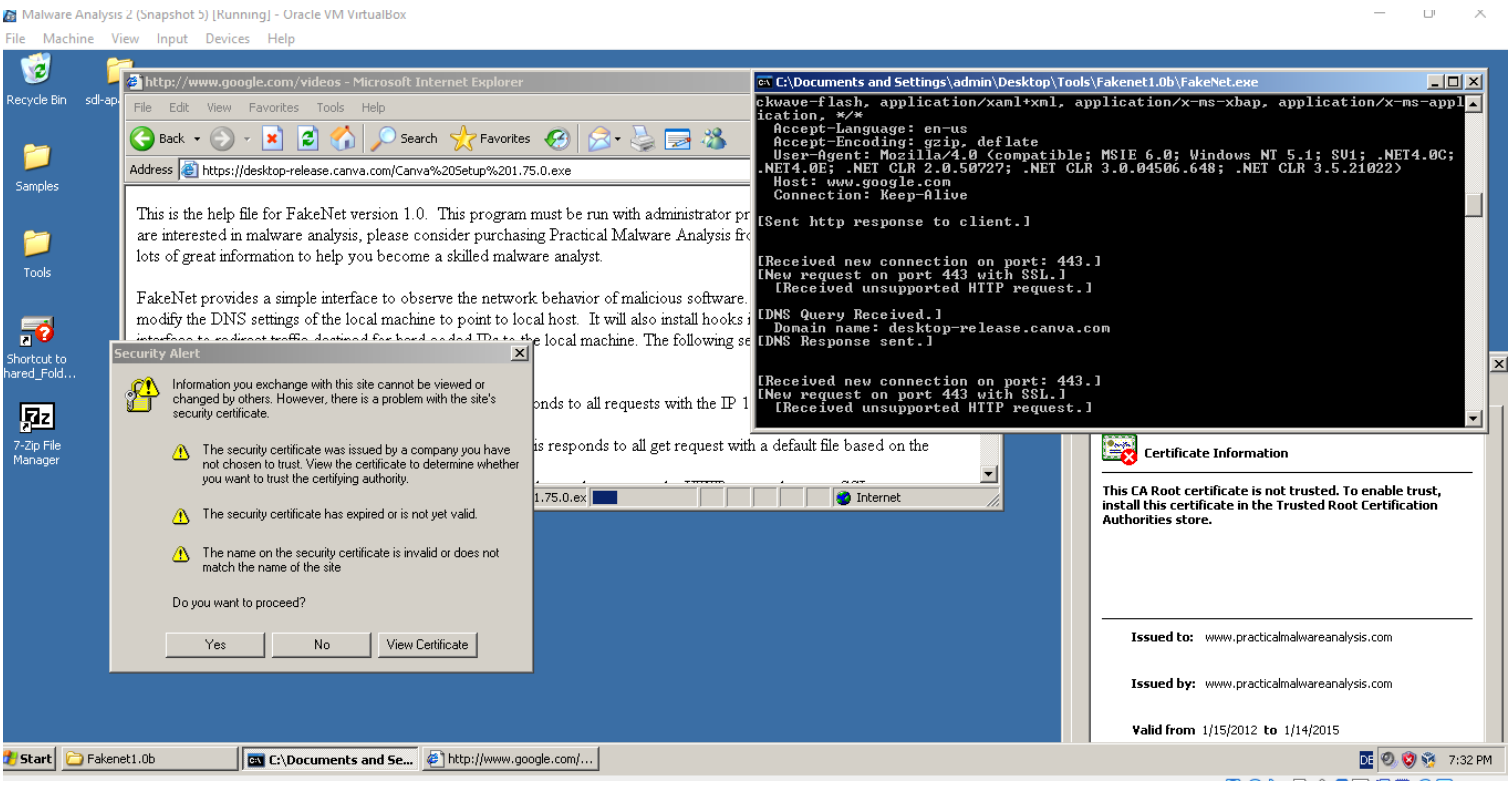
When we try to open a browser on XP machine and send a request for an image file, FakeNet spoofs the DNS response and what gets opened instead (as a result of the http request) is the help file for FakeNet version 1.0.

Activity 2:



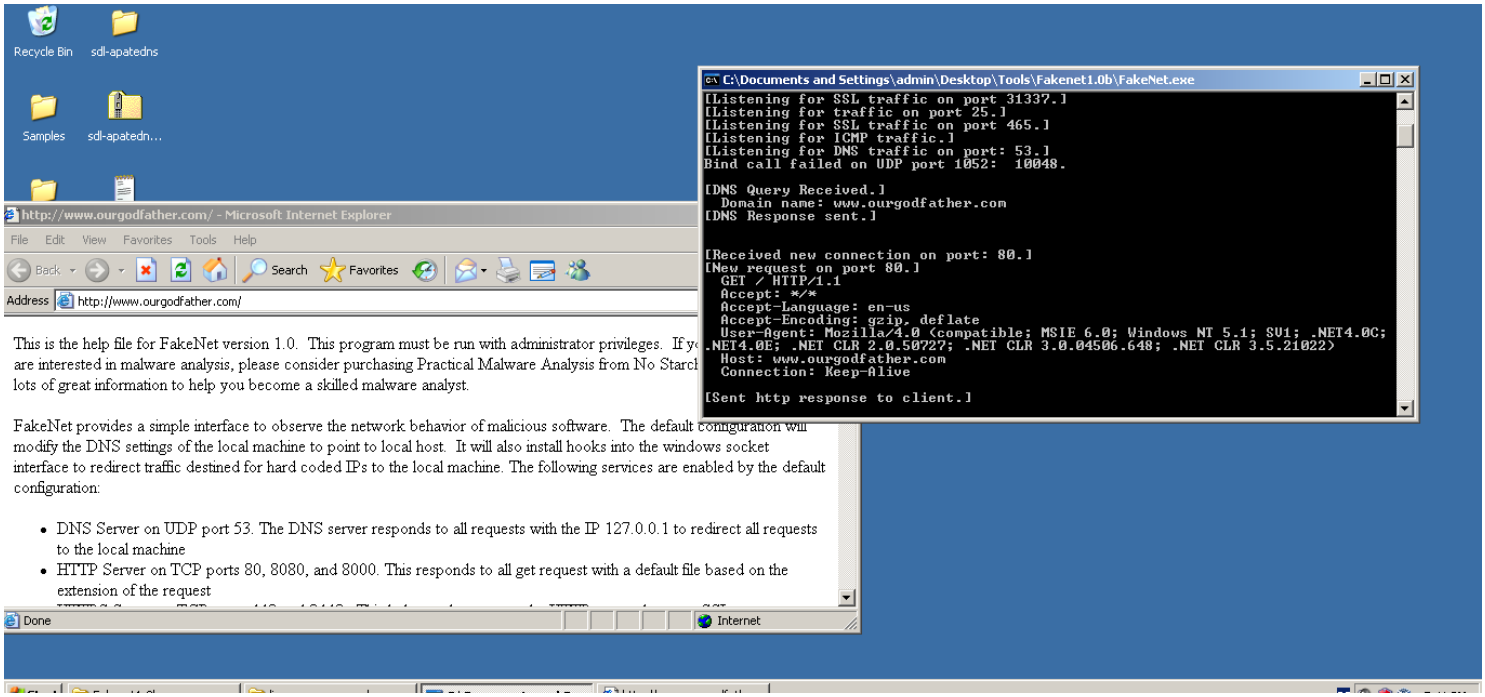
Once we send a request for a webpage through HTTPS, FakeNet spoofs the DNS response and what gets opened instead (as a result of the https request) is the help file for FakeNet version 1.0. However, in this case, we sent the request through HTTPS, which is a secure protocol, thus we get a security alert as shown in the above screenshot. We can view the certificate through this security alert. It can be seen in the above screenshot that the certificate was not issued by CA, rather it was issued by www.practicalmalwareanalysis.com to www.practicalmalwareanalysis.com which highlights malicious activity.

Activity 3:



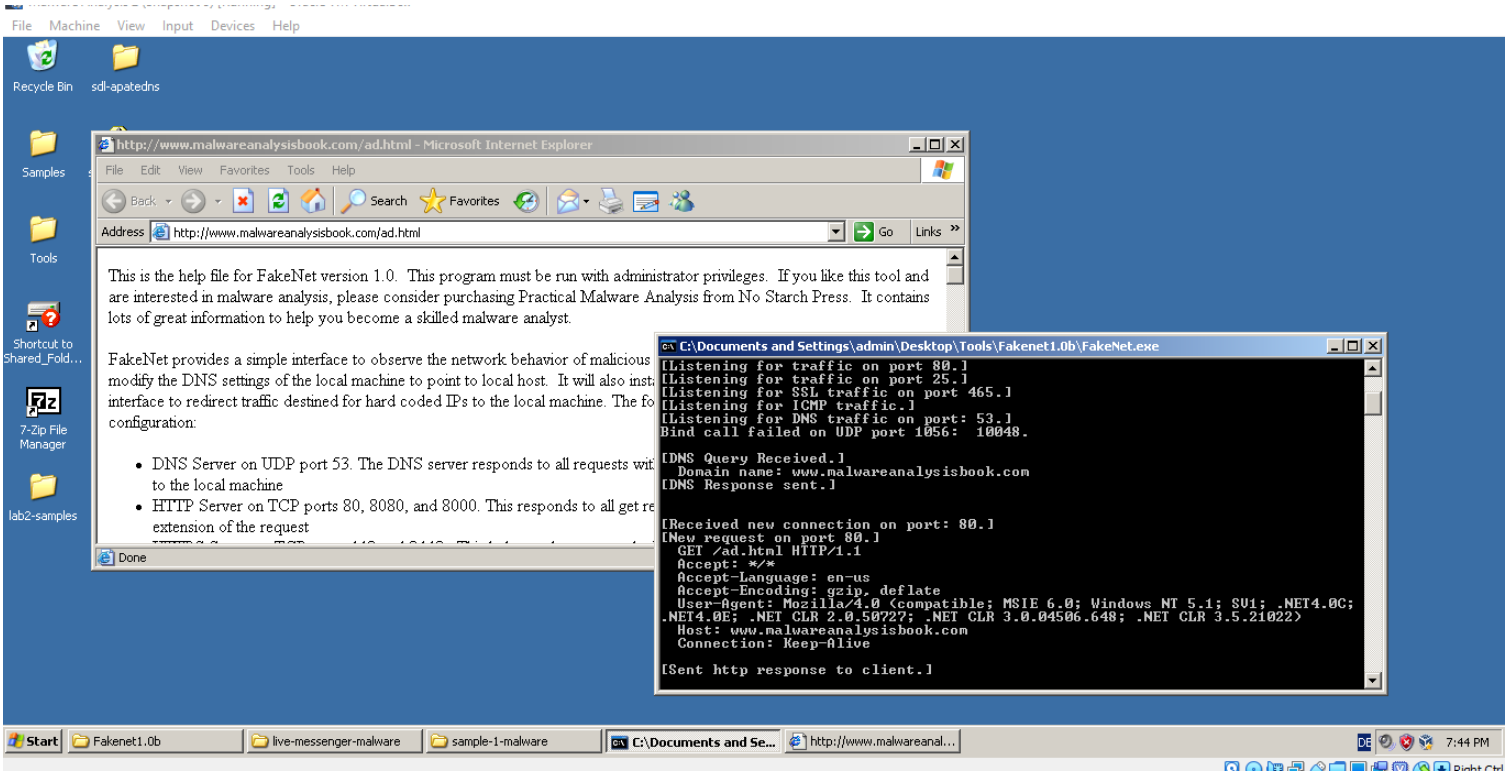
Once we try to download an executable (.exe) file from a website, FakeNet spoofs the DNS response and what gets opened instead is the help file for FakeNet version 1.0. However, we tried downloading the executable file through HTTPS, which is a secure protocol, thus we get a security alert as shown in the above screenshot. We can view the certificate through this security alert. It can be seen in the above screenshot that the certificate was not issued by CA, rather it was issued by www.practicalmalwareanalysis.com to www.practicalmalwareanalysis.com which highlights malicious activity.

Activity 4 (live messenger)



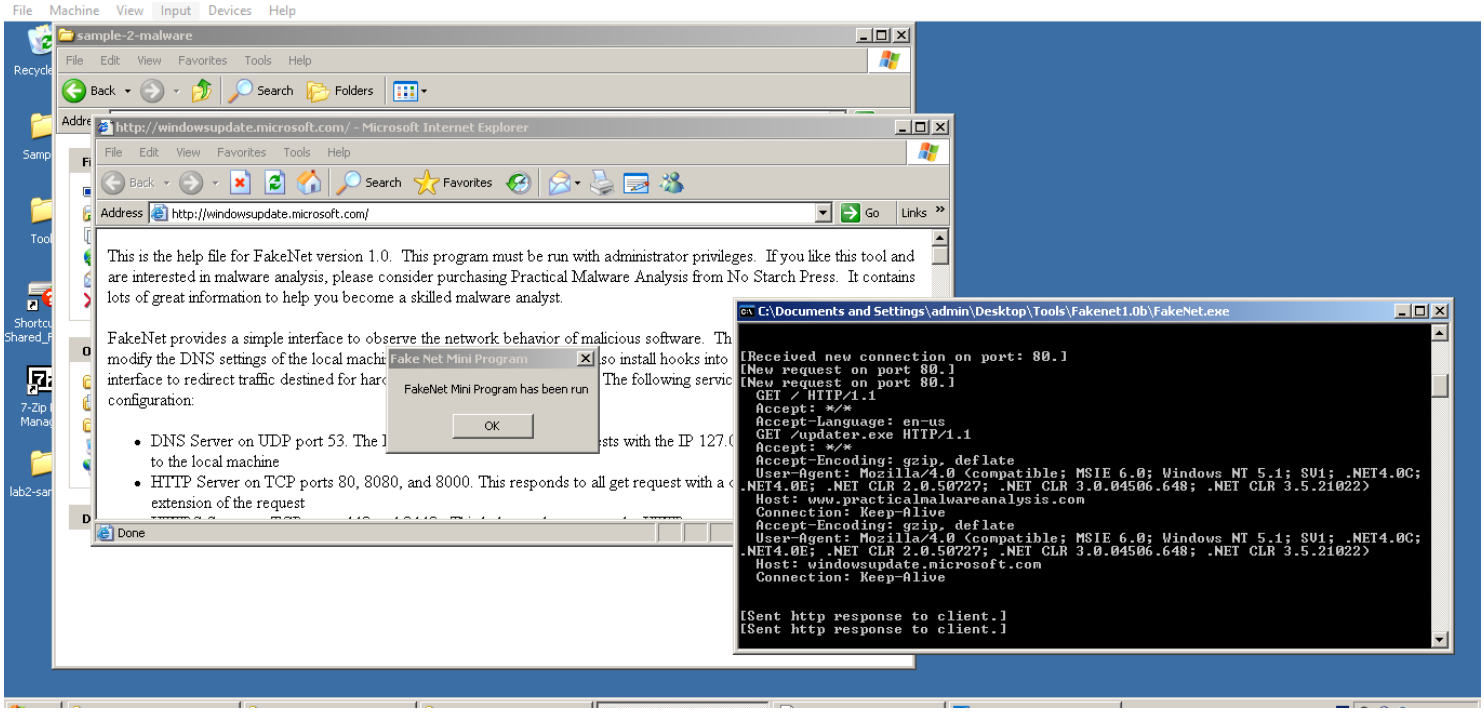
- The sample was trying to contact www.ourgodfather.com.
- HTTP request is being made by the XP machine the response to which is the help file of FakeNet version 1.0. In reality, http request was to be made to www.ourgodfather.com but the DNS reply was spoofed, and as a response to the http request now, the user/analyst sees the FakeNet version 1.0 help file in the browser.
- The malware tries to open www.ourgodfather.com to redirect the user/analyst. www.ourgodfather.com is a Domain Name. Its IP address is needed which will be the DNS response. Fakenet spoofs this DNS response. Now, as a response to the http request, instead of www.ourgodfather.com getting opened in the browser, we see FakeNet version 1.0 help file in the browser on our XP machine.

Activity 4 (Sample 1)



- The sample is trying to contact www.malwareanalysisbook.com
- HTTP request is made by the XP machine, the response to which is the help file of FakeNet version 1.0. In reality, http request was to be made to www.malwareanalysisbook.com but the DNS reply was spoofed, and as a response to the http request now, the user/analyst sees the FakeNet version 1.0 help file in the browser.
- The malware tries to open www.malwareanalysisbook.com to redirect the user/analyst. www.malwareanalysisbook.com is a Domain Name. Its IP address is needed which will be the DNS response. Fakenet spoofs this DNS response. Now, as a response to the http request, instead of www.malwareanalysisbook.com getting opened in the browser, we see FakeNet version 1.0 help file in the browser on our XP machine.

Activity 4 (Sample 2):



- The sample tried to contact www.practicalmalwareanalysis.com
- HTTP request is made by the XP machine, the response to which is the help file of FakeNet version 1.0. In reality, http request was to be made to www.practicalmalwareanalysis.com but the DNS reply was spoofed, and as a response to the http request now, the user/analyst sees the FakeNet version 1.0 help file in the browser. Another HTTP request was made in order to download the updater.exe file.
- The malware tries to open www.practicalmalwareanalysis.com to redirect the user/analyst. www.practicalmalwareanalysis.com is a Domain Name. Its IP address is needed which will be the DNS response. Fakenet spoofs this DNS response. Now, as a response to the http request, instead of www.practicalmalwareanalysis.com getting opened in the browser, we see FakeNet version 1.0 help file in the browser on our XP machine. In this case, we also see a message box appear.

Observations of the malware network behaviour with FakeNet and INetSim:

Yes, the malware network behavior is the same with FakeNet and INetSim. Both spoof the DNS response so that the user is directed to someplace else as a response to the http request on the spoofed IP. In case of ApateDNS, user was redirected to default HTML page for INetSim HTTP server. However, for FakeNet the user was redirected to the FakeNet version 1.0 help file.

Comparison of outputs obtained from both tools:

Output obtained from FakeNet was thorough and more informative. An analyst does not need to download any tool to study the network traffic (e.g wireshark) while using FakeNet. FakeNet shows http requests made and information about whether there were responses to those http requests. It also displays information about DNS queries, DNS responses, and connection establishment with port number.

However, ApateDNS requires a tool like wireshark to study the network traffic as it does not display much information. The only information it shows is about the DNS that was returned.

Another major difference between the two tools (even though not apparent in any activity above) is the fact that ApateDNS can only be used for DNS manipulation, but FakeNet can simulate various network services including not just DNS, but also HTTP, SMTP, FTP etc.