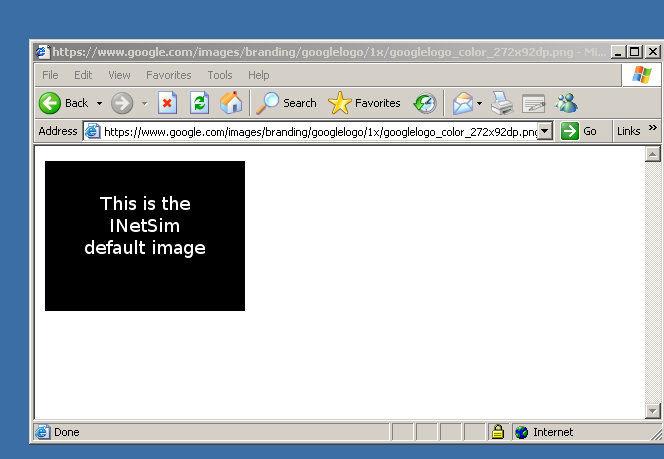
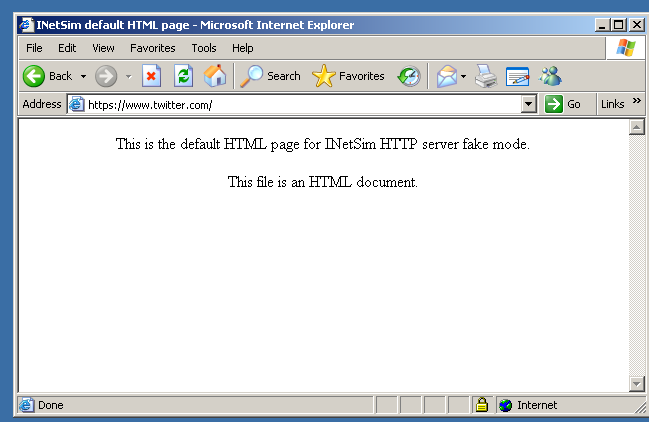
**Activity 1:** **Open a browser on the XP machine. Send a request for an image file from a hypothetical (or real) HTTP server. What happens when you do this?**

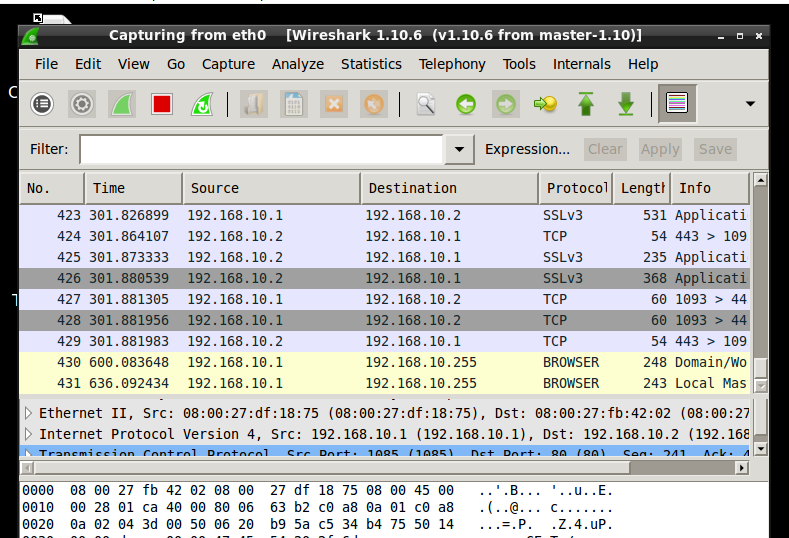
INetSim redirects the image requests to a default/sample image. As shown below in the screenshot:



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

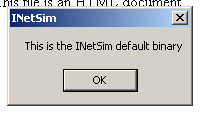
INetSim redirects the webpage (or html) requests to a sample document. Basically, on each webpage request, this content is returned by the server.

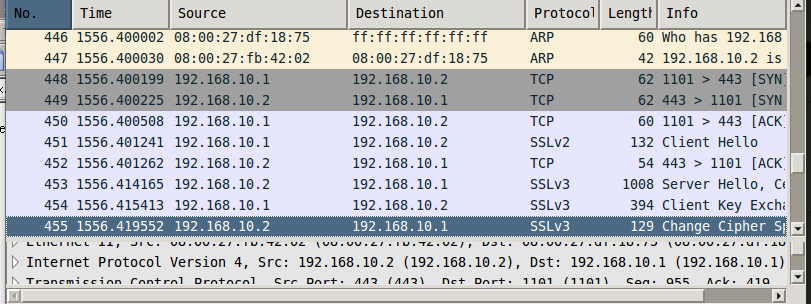




**Activity #3: Try downloading an executable (either .com or .exe file) from any website. What happens when you make this request?**

A default or sample .exe file is downloaded. Opening this file will display the message of INetSim. This is because a default file has been sent to the client from INetSim server running on the REMnux virtual machine. Same like the redirection of image or webpage.

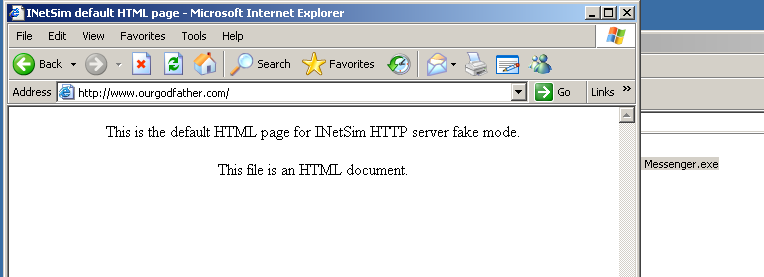




**Activity #4: Malware analysis on ApateDNS and INetSim**

**Malware #1: Live Messenger**

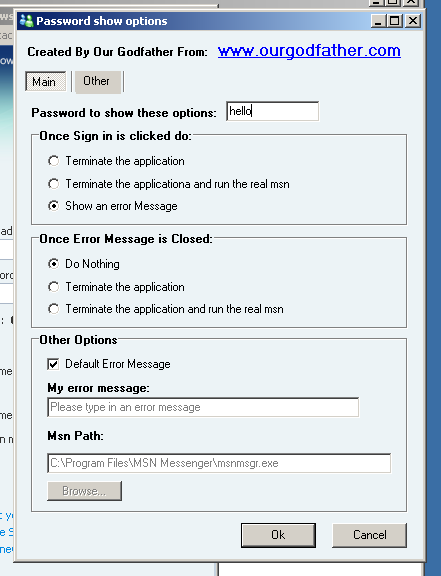
This malware simply opens a website [www.ourgodfather.com](http://www.ourgodfather.com) when the Live Messenger is closed. The domain being requested is [www.ourgodfather.com](http://www.ourgodfather.com). As shown in the screenshot below:



Graphical user interface, application

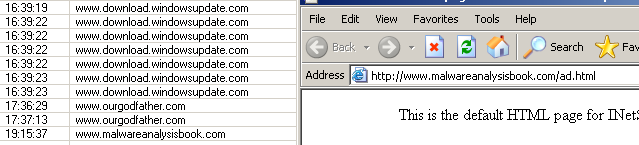
Description automatically generated

**Interesting Point:** Entering “hello” in the email address field will open the settings of the malware. This backdoor was found by chance. The screenshot of settings page is given below:



**Malware Sample 1:**

This malware just requests for the domain [www.malwareanalysisbook.com](http://www.malwareanalysisbook.com) and opens up a page [www.malwareanalysisbook.com/ad.html](http://www.malwareanalysisbook.com/ad.html).

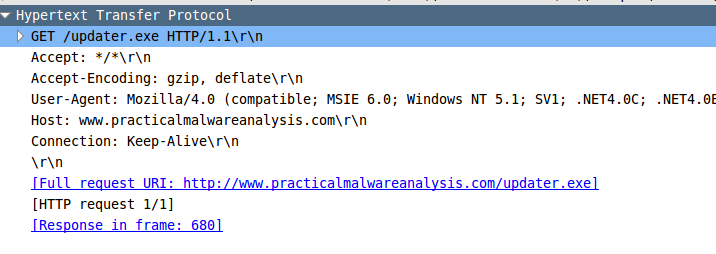


Graphical user interface, application, Word

Description automatically generated

**Malware Sample 2:**

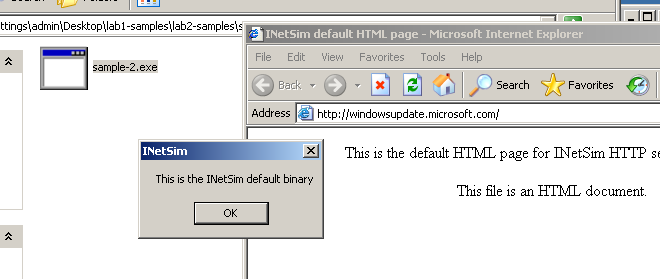
The malware performs the following actions in sequence:

* HTTP Request for [www.windowsupdate.microsoft.com](http://www.windowsupdate.microsoft.com)
* HTTP Request for [www.practicalmalwareanalysis.com/updater.exe](http://www.practicalmalwareanalysis.com/updater.exe)  
  

Domains Requested:

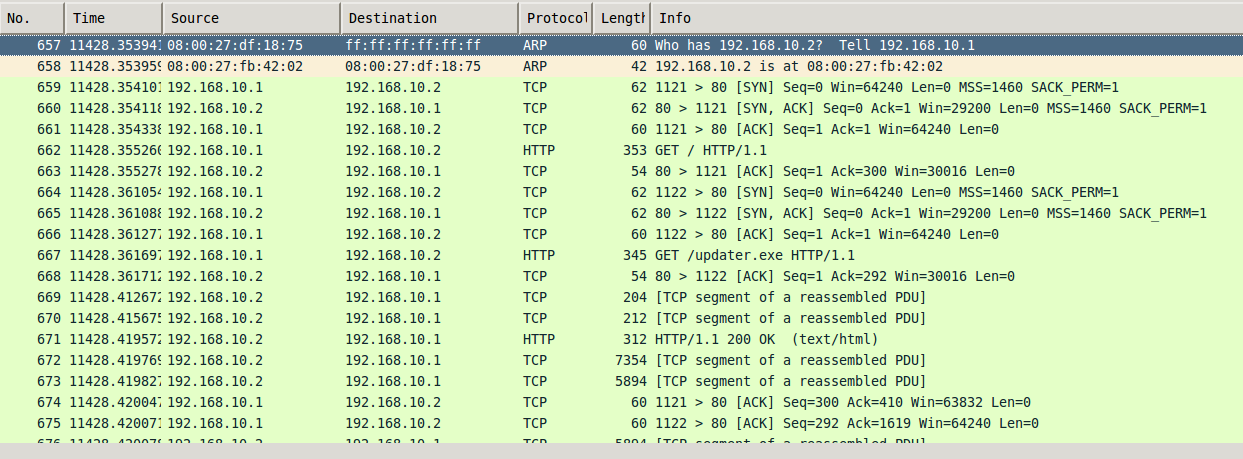
* [www.windowsupdate.microsoft.com](http://www.windowsupdate.microsoft.com)
* www.practicalmalwareanalysis.com

INetSim returns a sample page on the first request and an .exe file on the second request. What this malware does is to attempt to download a malicious file disguised as windows update. Since the webpage for Windows update is opened while the file is being downloaded, user might think that this .exe file is from Microsoft. However, the file is requested from aforementioned website. Screenshots are given below for reference:



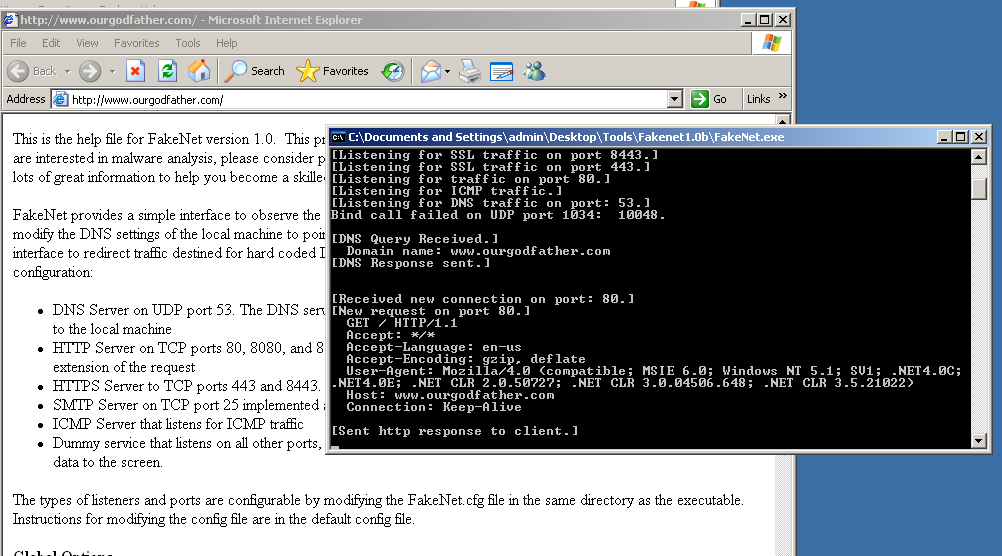
Graphical user interface

Description automatically generated with medium confidence



**Activity Part II: Observing Malware using FakeNet**

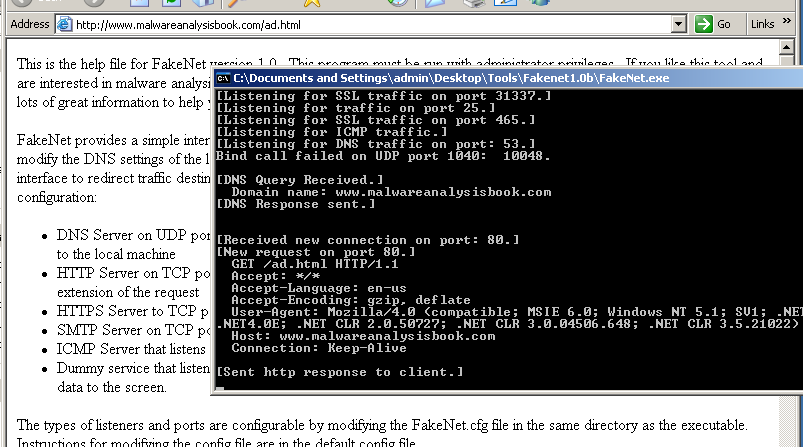
**Live Messenger Malware:**



Graphical user interface, application, table

Description automatically generated

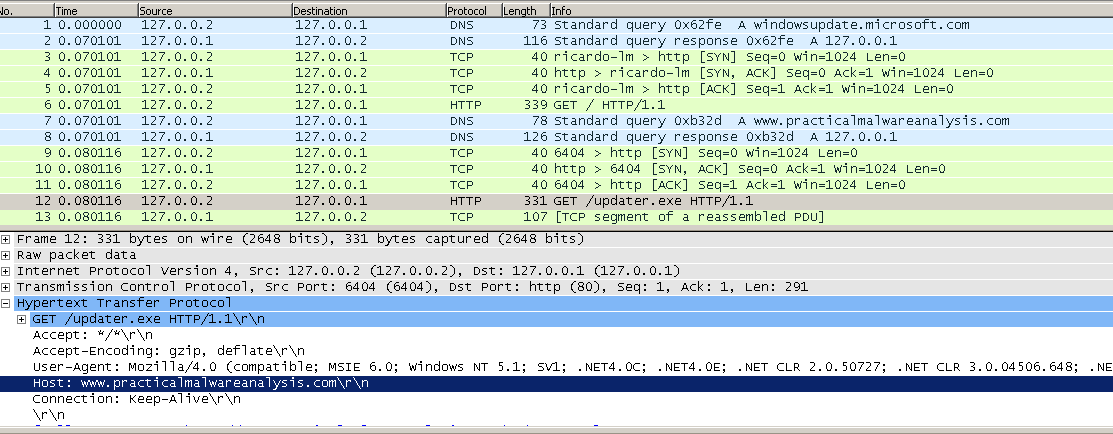
**Malware Sample 1:**



Graphical user interface, application, table, Excel

Description automatically generated

**Malware Sample 2:**

Graphical user interface, application

Description automatically generated

**Observations & Contrast with INetSim:**

FakeNet performs the similar duty as INetSim. The requests are redirected, and sample webpage is shown. Same procedure is for .exe file, a sample program of FakeNet is downloaded instead. The WireShark files show the same observations & results as obtained earlier. Thus, **making no difference in overall working**.

However, FakeNet is more convenient as there is no need of a separate virtual machine. Further, interface is user friendly and PCAP files are saved automatically.