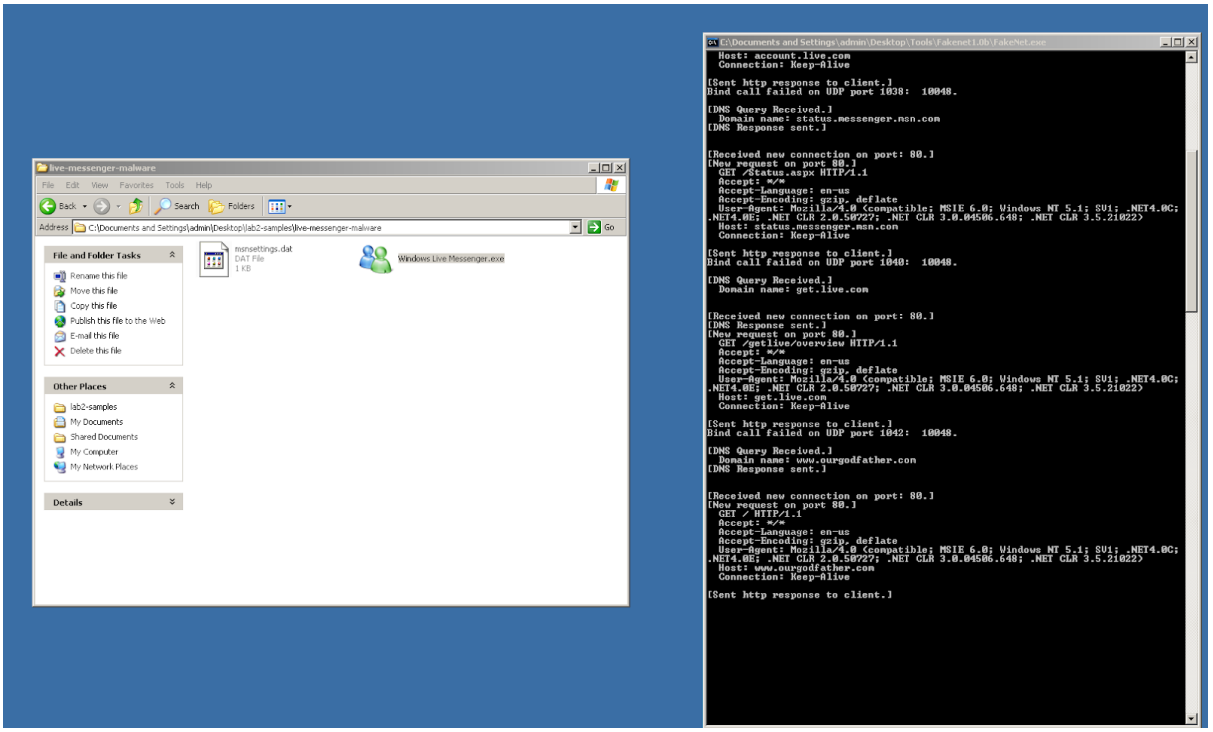
Part 2 Fakenet

(My Wireshark screenshots got deleted, so couldn't add them)

Malware 1

The network behavior observed does not align with that of insetsim. Initially, it begins by executing two DNS protocols. Subsequently, it follows with the three-way TCP handshake and initiates an HTTP GET request targeting "malwareanalysis.com." After this request, the webpage content is loaded through a series of TCP packets. Following successful data transmission, it concludes the communication by sending an HTTP Status code of 200 and ultimately terminating the connection. This process is characterized by the occurrence of two DNS queries and FIN ACKs.

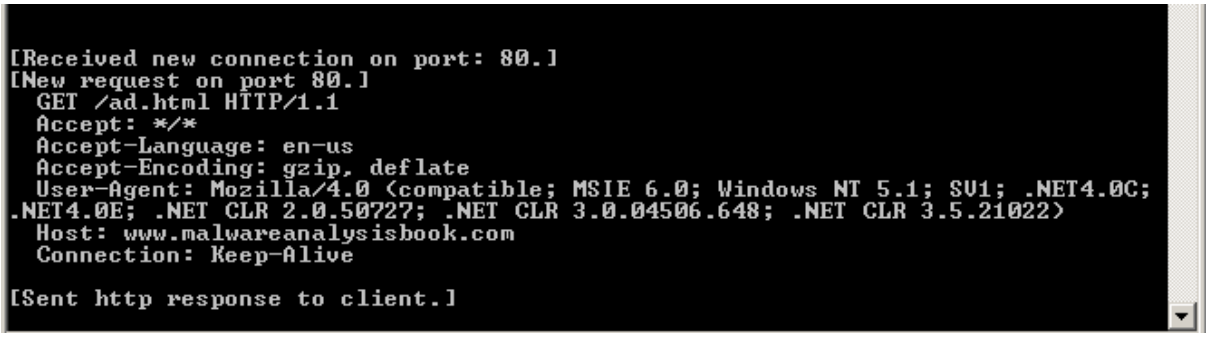
Comparing the outputs of both InetSim and Fakenet, it's evident that they share many similarities in behavior, except for the DNS queries.



Malware 2

This behavior differs significantly from the previous scenario, as it directly sends a GET request to the "practicalmalware/updater" domain, whereas InetSim initially sent a request to "windowsupdater.com." Following this action, it receives a TCP ACK (Acknowledgment) and

proceeds to transmit data to a webpage. The communication concludes with the transmission of an HTTP 200 OK status code.



Malware 3

In this case, the malware exhibits a different behavior by directly sending a DNS query for the "ourgodfather.com" page. Subsequently, it executes the TCP three-way handshake and initiates a GET request for that domain. Following this, it continuously sends data via TCP requests.
The communication is eventually terminated with an HTTP status code of 200. Additionally, it issues another HTTP request, possibly for either continuation of the data transfer or non-traffic data.