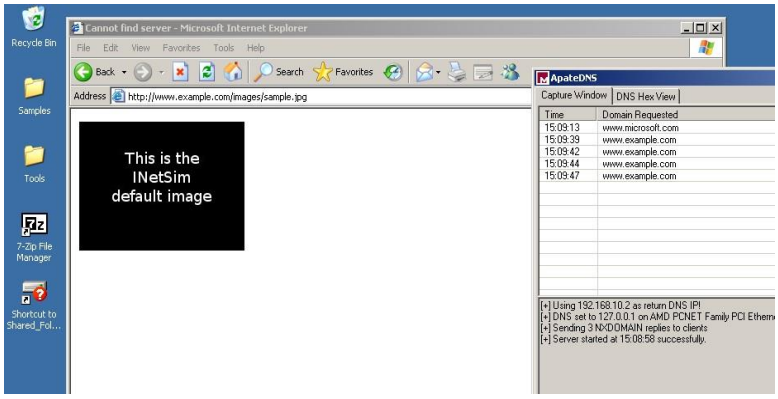
Information Security

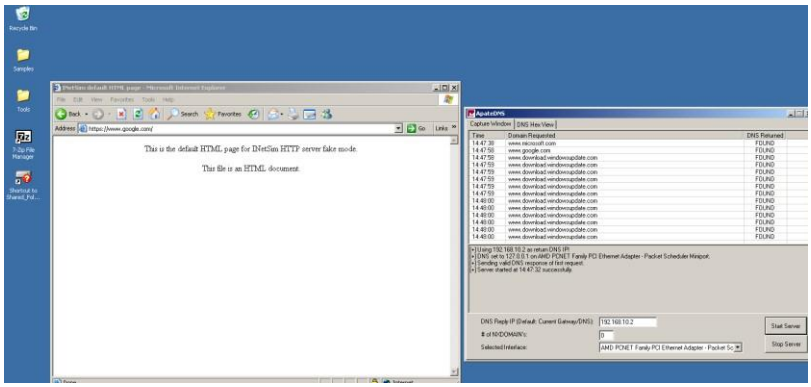
Assignment 2: Malware Analysis:

Part 1:

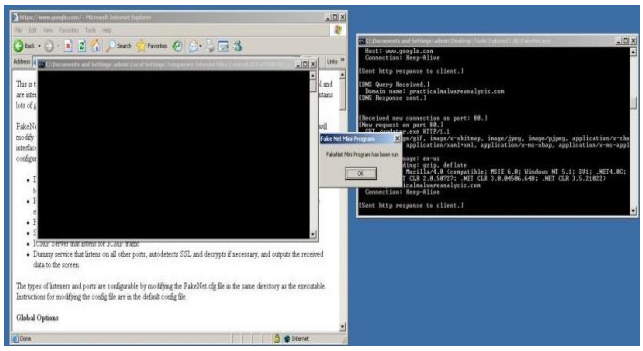
Q1

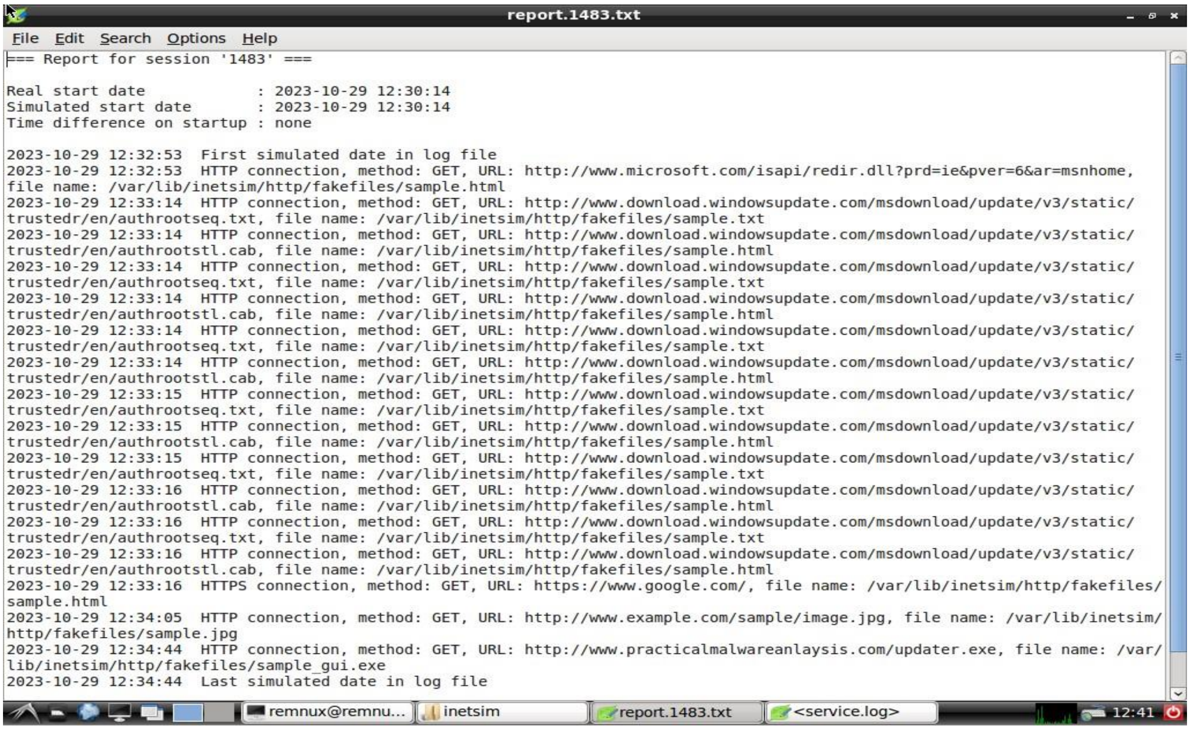


Q2



Q3





```
=== Report for session '1483' ===

Real start date           : 2023-10-29 12:30:14
Simulated start date      : 2023-10-29 12:30:14
Time difference on startup : none

2023-10-29 12:32:53  First simulated date in log file
2023-10-29 12:32:53  HTTP connection, method: GET, URL: http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome, file name: /var/lib/inetsim/http/fakefiles/sample.html
2023-10-29 12:33:14  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt, file name: /var/lib/inetsim/http/fakefiles/sample.txt
2023-10-29 12:33:14  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab, file name: /var/lib/inetsim/http/fakefiles/sample.html
2023-10-29 12:33:14  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt, file name: /var/lib/inetsim/http/fakefiles/sample.txt
2023-10-29 12:33:14  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab, file name: /var/lib/inetsim/http/fakefiles/sample.html
2023-10-29 12:33:14  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt, file name: /var/lib/inetsim/http/fakefiles/sample.txt
2023-10-29 12:33:14  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab, file name: /var/lib/inetsim/http/fakefiles/sample.html
2023-10-29 12:33:15  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt, file name: /var/lib/inetsim/http/fakefiles/sample.txt
2023-10-29 12:33:15  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab, file name: /var/lib/inetsim/http/fakefiles/sample.html
2023-10-29 12:33:15  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt, file name: /var/lib/inetsim/http/fakefiles/sample.txt
2023-10-29 12:33:16  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab, file name: /var/lib/inetsim/http/fakefiles/sample.html
2023-10-29 12:33:16  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt, file name: /var/lib/inetsim/http/fakefiles/sample.txt
2023-10-29 12:33:16  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab, file name: /var/lib/inetsim/http/fakefiles/sample.html
2023-10-29 12:33:16  HTTPS connection, method: GET, URL: https://www.google.com/, file name: /var/lib/inetsim/http/fakefiles/sample.html
2023-10-29 12:34:05  HTTP connection, method: GET, URL: http://www.example.com/sample/image.jpg, file name: /var/lib/inetsim/http/fakefiles/sample.jpg
2023-10-29 12:34:44  HTTP connection, method: GET, URL: http://www.practicalmalwareanlaysis.com/updater.exe, file name: /var/lib/inetsim/http/fakefiles/sample_gui.exe
2023-10-29 12:34:44  Last simulated date in log file
```

Q4

Malware Sample1:

1) The samples are trying to contact the domain "get.Live.com." This domain is mentioned in the "Host" field of the HTTP request.
2)
    - URL: http://get.Live.com/getlive/overview
    - Host: get.Live.com
    - Connection: Keep-Alive

3) The sequence of events in the malware sample's network activities is as follows:
    - The malware establishes a connection with the IP address 192.168.10.1 on port 1076.
    - It sends an HTTP GET request to the domain "get.Live.com"
    - The server INetSim responds with a fake "html" file (sample.html) and sends the response headers.
    - The connection is terminated after the response, marking the end of this specific network activity.

Malware Sample2:

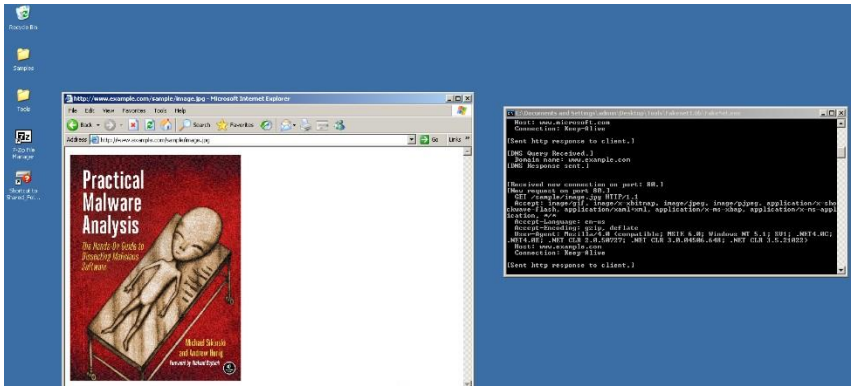
1) The samples are trying to contact the domain "www.malwareanalysisbook.com." This domain is mentioned in the "Host" field of the HTTP request.

2) Method: GET
    - URL http://www.malwareanalysisbook.com/ad.html
    - Host: www.malwareanalysisbook.com o
    Connection: Keep-Alive

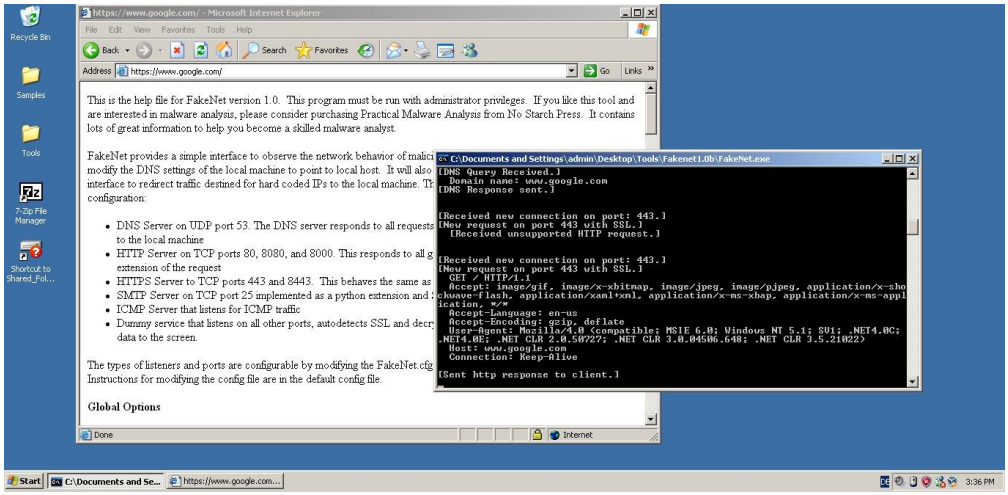
The malware establishes a connection with the IP address 192.168.10.1 on port 1079. It sends HTTP GET request to the domain. "www.malwareanalysisbook.com" requesting the file "ad.html." The server INetSim responds with a fake "html" file (sample.html) and sends the response headers. The connection is terminated after the response, marking the end of this specific network activity.

Part-2

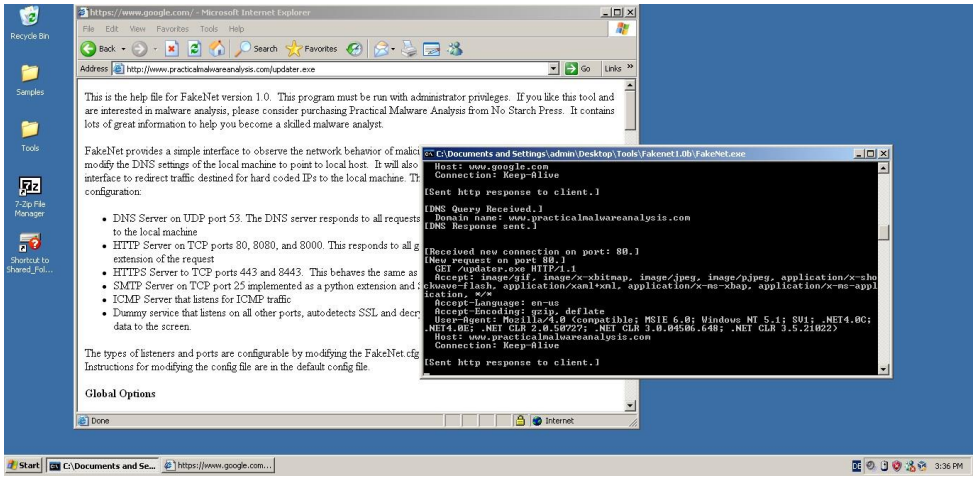
Q1



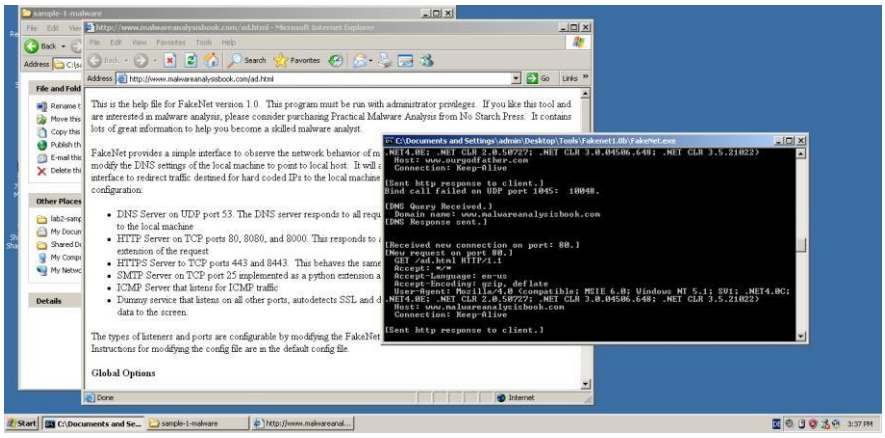
Q2

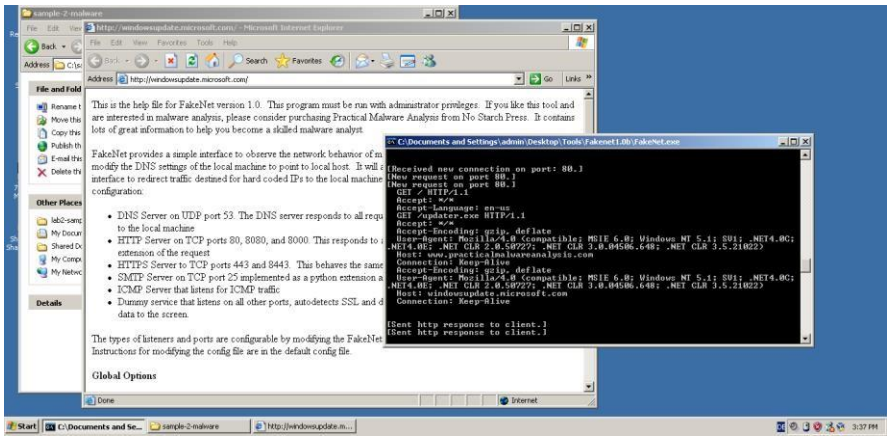


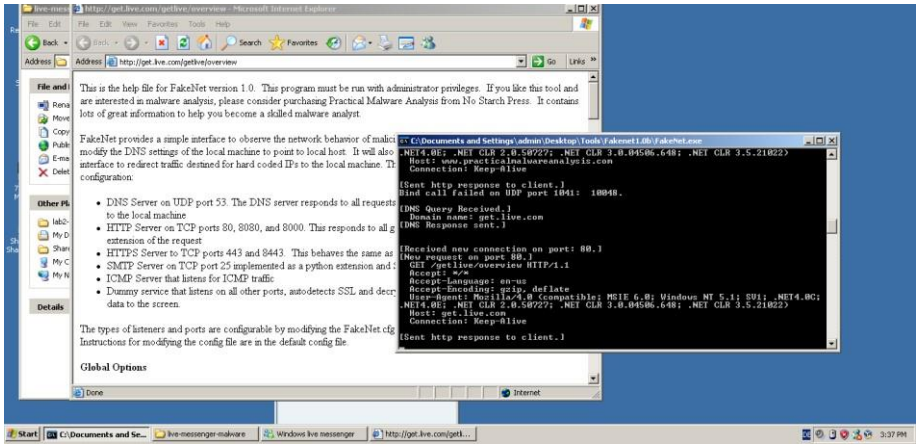
Q3



Q\4







Report of FakeNet: