

Part-1: Using ApateDNS

1. Given that a private connection is established, the HTTP request is directed to the Remnux VM and the response is generated from the same server. The requested image is from facebook, but the returned image is the default inetsim image.

The screenshot shows a Windows desktop environment. In the background, a Microsoft Internet Explorer window is open at the URL `http://facebook.com/img.png`. The browser's content area displays a black rectangle with the text "This is the INetSim default image". In the foreground, the ApateDNS application is running. It features a "Capture Window" tab with a table of DNS requests and a "DNS Hex View" tab. The table shows a single entry for a request to facebook.com at 13:44:29, which was successfully resolved. Below the table, a log of events shows the server starting at 13:43:39. At the bottom of the ApateDNS window, there are input fields for "DNS Reply IP" (set to 192.168.10.2), "# of N/D/DOMAIN's" (set to 0), and "Selected Interface" (set to AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport). The taskbar at the bottom shows the Start button, Windows Explorer, Command Prompt, ApateDNS, and the browser window.

Time	Domain Requested	DNS Returned
13:44:29	facebook.com	FOUND

[-] Attempting to find DNS by DHCP or Static DNS.
[-] Using IP address 192.168.10.2 for DNS Reply.
[-] DNS set to 127.0.0.1 on AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport.
[-] Sending valid DNS response of first request.
[-] Server started at 13:43:39 successfully.

DNS Reply IP (Default: Current Gateway/DNS):
of N/D/DOMAIN's:
Selected Interface:

Start Server
Stop Server

Start 7 Windows Explorer Command Prompt ApateDNS http://facebook.com/img...

*enp0s3

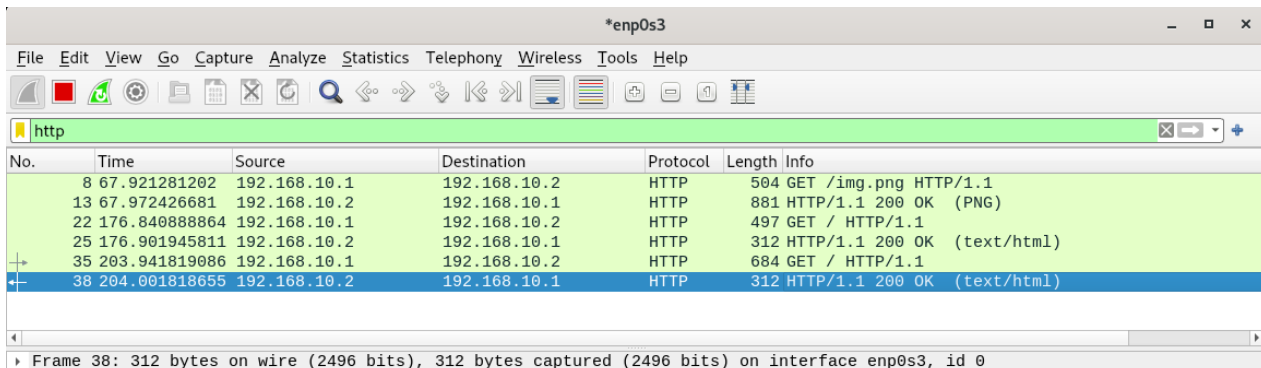
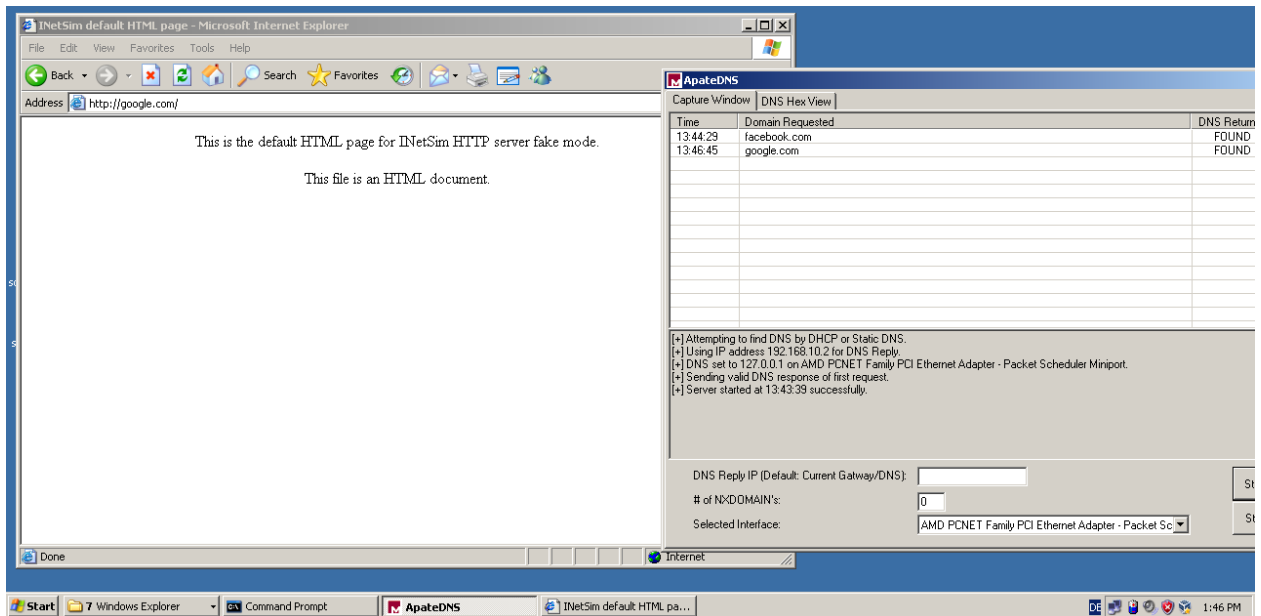
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

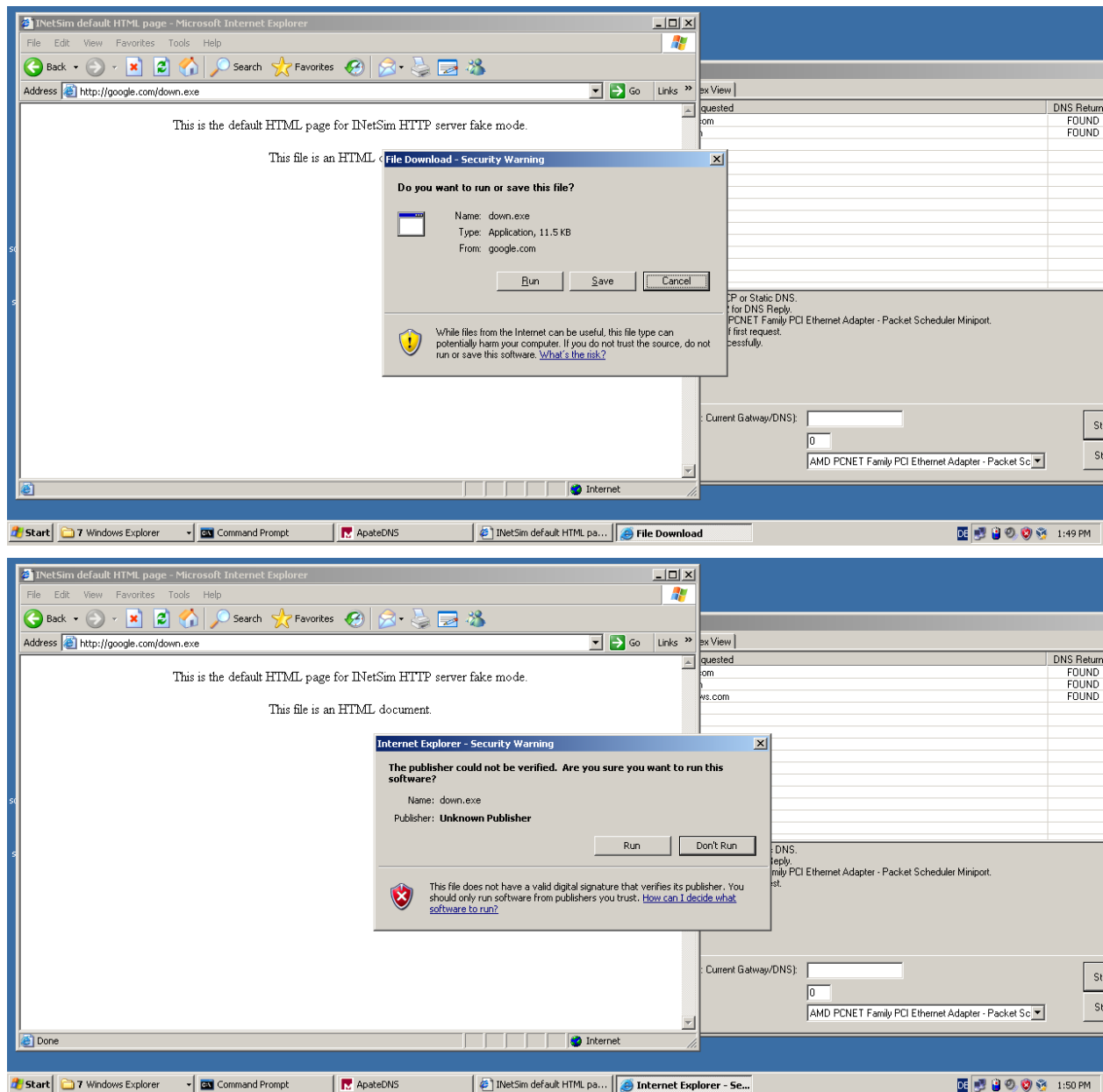
No.	Time	Source	Destination	Protocol	Length	Info
8	67.921281202	192.168.10.1	192.168.10.2	HTTP	504	GET /img.png HTTP/1.1
13	67.972426681	192.168.10.2	192.168.10.1	HTTP	881	HTTP/1.1 200 OK (PNG)

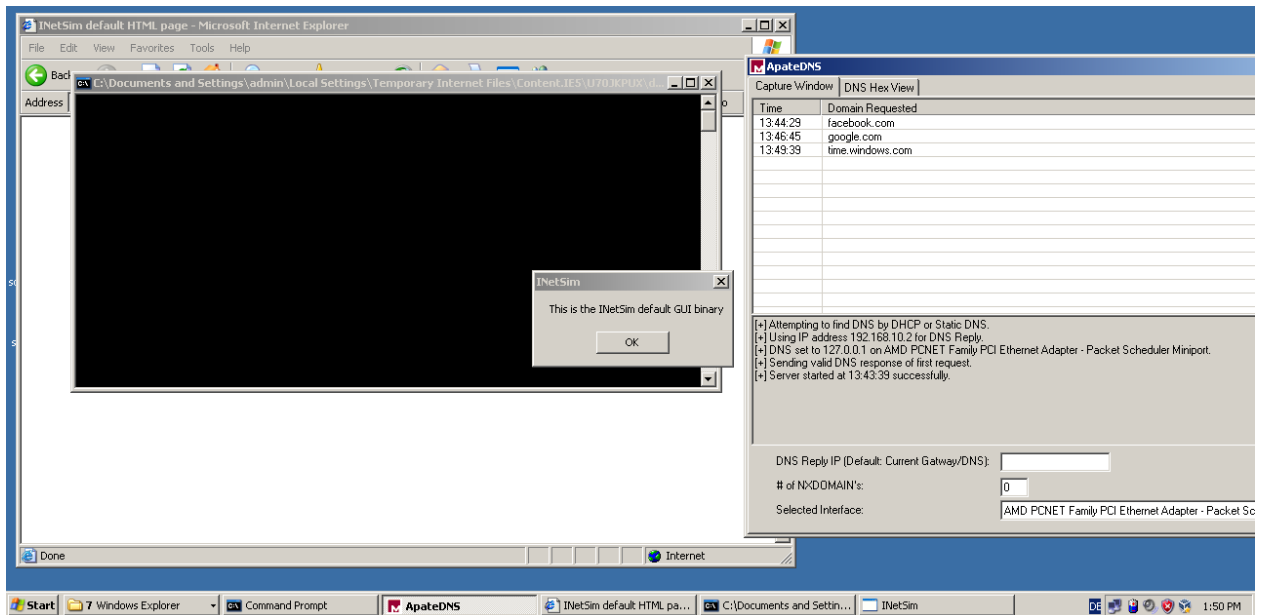
Frame 8: 504 bytes on wire (4032 bits) 504 bytes captured (4032 bits) on interface enp0s3 id 0

2. When I initiate a HTTP request to a web page, it's captured by the server, which presently is the Remnux VM. The packets that Wireshark has captured can be seen in the pictures below.



3. When I request for a “down.exe”. The default inetsim GUI application is downloaded. And the packets and request captured can be seen by the wireshark in the Remnux VM.





*enp0s3						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
8	67.921281202	192.168.10.1	192.168.10.2	HTTP	504	GET /img.png HTTP/1.1
13	67.972426681	192.168.10.2	192.168.10.1	HTTP	881	HTTP/1.1 200 OK (PNG)
22	176.840888864	192.168.10.1	192.168.10.2	HTTP	497	GET / HTTP/1.1
25	176.901945811	192.168.10.2	192.168.10.1	HTTP	312	HTTP/1.1 200 OK (text/html)
35	203.941819086	192.168.10.1	192.168.10.2	HTTP	684	GET / HTTP/1.1
38	204.001818655	192.168.10.2	192.168.10.1	HTTP	312	HTTP/1.1 200 OK (text/html)
49	367.088105117	192.168.10.1	192.168.10.2	HTTP	692	GET /down.exe HTTP/1.1
55	367.112494052	192.168.10.2	192.168.10.1	HTTP	150	HTTP/1.1 200 OK (x-msdos-program)

Sample 1

www.malwareanalysisbook.com is the domain sample 1 is trying to connect. Get request for ad.html is being made and then html text for default inetsim http server is being rendered.

The screenshot displays a Windows XP desktop environment. The primary window is Microsoft Internet Explorer, titled "INetSim default HTML page - Microsoft Internet Explorer". The address bar shows "http://www.malwareanalysisbook.com/ad.html". The main content area displays the text: "This is the default HTML page for INetSim HTTP server fake mode." and "This file is an HTML document."

Overlaid on the bottom right is the "Apat-eDNS" application window. It features a "Capture Window" tab showing a list of DNS requests:

Time	Domain Requested
13:44:29	facebook.com
13:46:45	google.com
13:49:39	time.windows.com
15:41:02	www.malwareanalysisbook.com
15:42:05	www.malwareanalysisbook.com

Below the table, a status box contains the following log entries:

- [+] Attempting to find DNS by DHCP or Static DNS.
- [+] Using IP address 192.168.10.2 for DNS Reply.
- [+] DNS set to 127.0.0.1 on AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport.
- [+] Sending valid DNS response of first request.
- [+] Server started at 13:43:39 successfully.

At the bottom of the Apat-eDNS window, there are configuration fields: "DNS Reply IP (Default: Current Gateway/DNS):", "# of NXDOMAIN's: 0", and "Selected Interface: AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport".

Below the Apat-eDNS window is the "*enp0s3" network interface window. It shows a list of captured packets. The selected packet is an HTTP GET request:

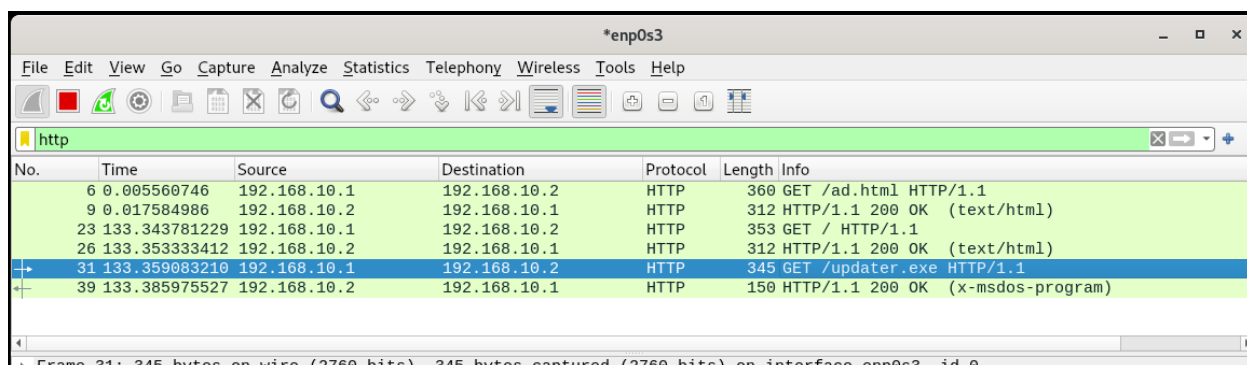
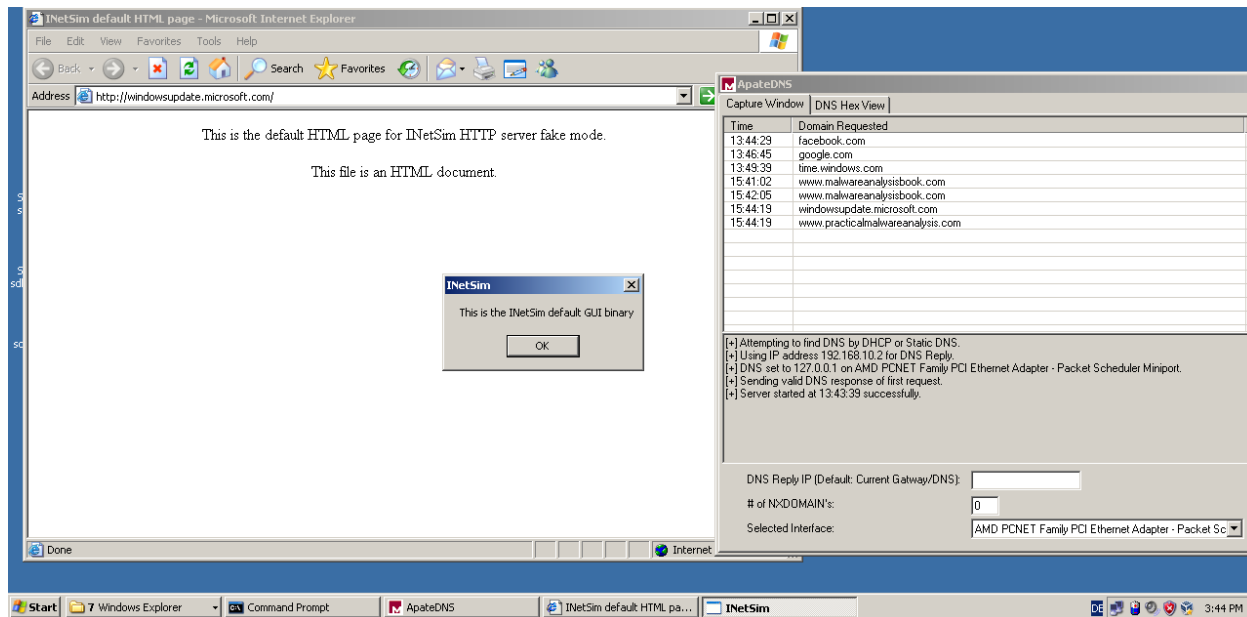
No.	Time	Source	Destination	Protocol	Length	Info
6	0.005560746	192.168.10.1	192.168.10.2	HTTP	360	GET /ad.html HTTP/1.1
9	0.017584986	192.168.10.2	192.168.10.1	HTTP	312	HTTP/1.1 200 OK (text/html)

Sample 2

windowsupdate.microsoft.com is the domain sample 2 is trying to connect. Get request for updater.exe is being made and then x-msdos-program is being received.

www.practicalmalwareanalysis.com is also a domain which is requested.

This means that by going to this website, an exe file is being downloaded for execution.



Messenger

www.ourgodfather.com is the domain it is trying to connect to. Get request is being made and then html text for default inetsim http server is being rendered.

The screenshot shows a Windows XP desktop with two main applications open: Internet Explorer and ApatcDNS.

Internet Explorer: The address bar shows `http://www.ourgodfather.com/`. The main content area displays the default HTML page for INetSim HTTP server fake mode, which includes the text: "This is the default HTML page for INetSim HTTP server fake mode." and "This file is an HTML document."

ApatcDNS: The "Capture Window" tab is active, showing a list of domain requests. The list includes:

Time	Domain Requested
13:44:29	facebook.com
13:46:45	google.com
13:49:39	time.windows.com
15:41:02	www.malwareanalysisbook.com
15:42:05	www.malwareanalysisbook.com
15:44:19	windowsupdate.microsoft.com
15:44:19	www.practicalmalwareanalysis.com
15:47:30	www.ourgodfather.com

Below the list, there is a status bar with the following text:

- [+] Attempting to find DNS by DHCP or Static DNS.
- [+] Using IP address 192.168.10.2 for DNS Reply.
- [+] DNS set to 127.0.0.1 on AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport.
- [+] Sending valid DNS response of first request.
- [+] Server started at 13:43:39 successfully.

The "DNS Reply IP (Default: Current Gateway/DNS):" field is set to `192.168.10.2`. The "Selected Interface:" dropdown is set to "AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport".

Wireshark: The packet capture window is open, showing a list of captured packets. The selected packet is an HTTP GET request to `www.ourgodfather.com`.

No.	Time	Source	Destination	Protocol	Length	Info
9	0.017584986	192.168.10.2	192.168.10.1	HTTP	312	HTTP/1.1 200 OK (text/html)
23	133.343781229	192.168.10.1	192.168.10.2	HTTP	353	GET / HTTP/1.1
26	133.353333412	192.168.10.2	192.168.10.1	HTTP	312	HTTP/1.1 200 OK (text/html)
31	133.359083210	192.168.10.1	192.168.10.2	HTTP	345	GET /updater.exe HTTP/1.1
39	133.385975527	192.168.10.2	192.168.10.1	HTTP	150	HTTP/1.1 200 OK (x-msdos-program)
57	324.128769057	192.168.10.1	192.168.10.2	HTTP	346	GET / HTTP/1.1
60	324.139550814	192.168.10.2	192.168.10.1	HTTP	312	HTTP/1.1 200 OK (text/html)

=== Report for session '1728' ===

Real start date : 2023-11-03 08:42:58
Simulated start date : 2023-11-03 08:42:58
Time difference on startup : none

2023-11-03 08:44:29 First simulated date in log file
2023-11-03 08:44:29 HTTP connection, method: GET, URL: <http://facebook.com/img.png>, file name: /var/lib/inetsim/http/fakefiles/sample.png
2023-11-03 08:46:17 HTTP connection, method: GET, URL: <http://facebook.com/>, file name: /var/lib/inetsim/http/fakefiles/sample.html
2023-11-03 08:46:45 HTTP connection, method: GET, URL: <http://google.com/>, file name: /var/lib/inetsim/http/fakefiles/sample.html
2023-11-03 08:49:28 HTTP connection, method: GET, URL: <http://google.com/download.exe>, file name: /var/lib/inetsim/http/fakefiles/sample_gui.exe
2023-11-03 08:49:28 Last simulated date in log file

=== Report for session '1912' ===

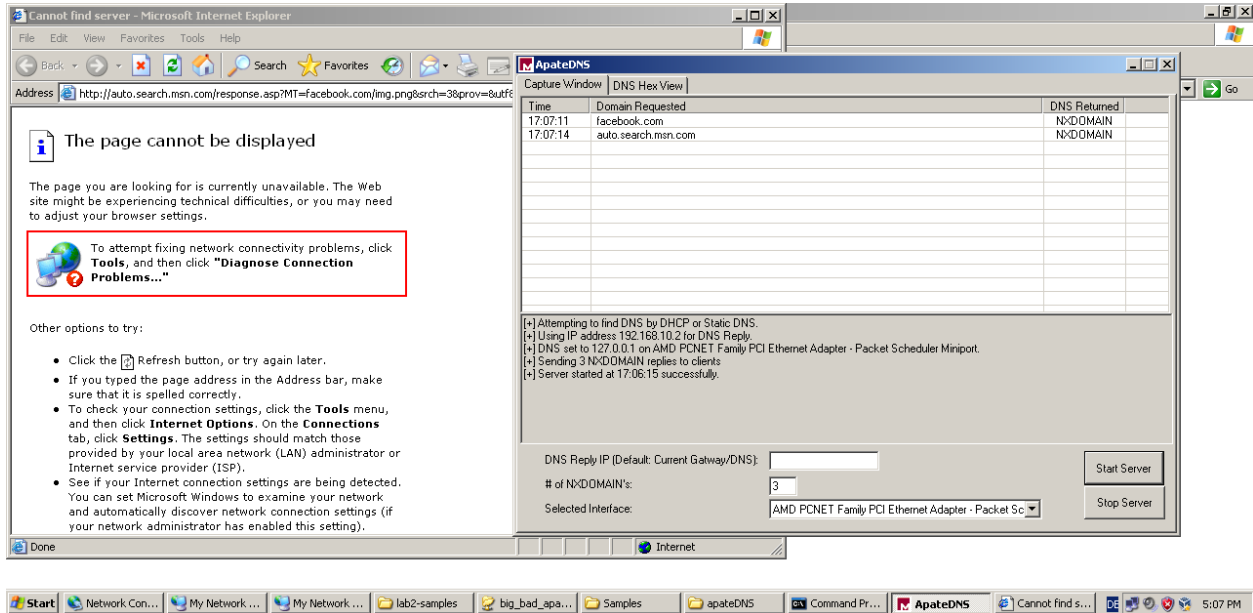
Real start date : 2023-11-03 10:41:57
Simulated start date : 2023-11-03 10:41:57
Time difference on startup : none

2023-11-03 10:42:05 First simulated date in log file
2023-11-03 10:42:05 HTTP connection, method: GET, URL: <http://www.malwareanalysisbook.com/ad.html>, file name: /var/lib/inetsim/http/fakefiles/sample.html
2023-11-03 10:44:19 HTTP connection, method: GET, URL: <http://windowsupdate.microsoft.com/>, file name: /var/lib/inetsim/http/fakefiles/sample.html
2023-11-03 10:44:19 HTTP connection, method: GET, URL: <http://www.practicalmalwareanalysis.com/updater.exe>, file name: /var/lib/inetsim/http/fakefiles/sample_gui.exe
2023-11-03 10:47:30 HTTP connection, method: GET, URL: <http://www.ourgodfather.com/>, file name: /var/lib/inetsim/http/fakefiles/sample.html
2023-11-03 10:47:30 Last simulated date in log file

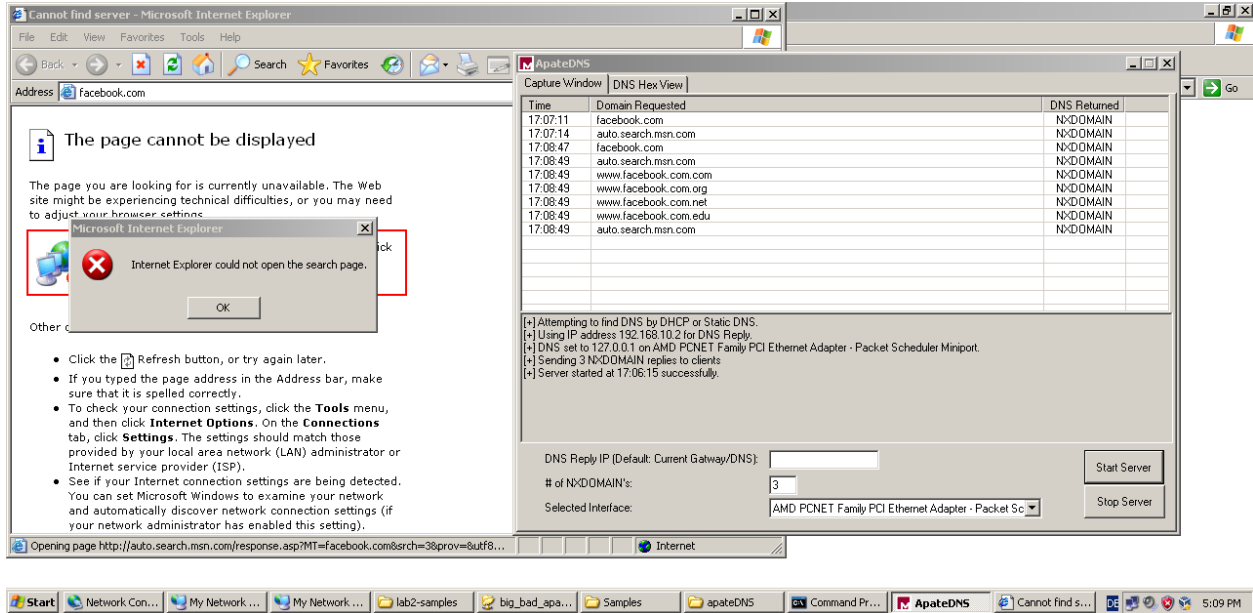
of NXDOMAINS =3

Throughout this, the domains are not being found and multiple domains are requested if the domain searched is not found

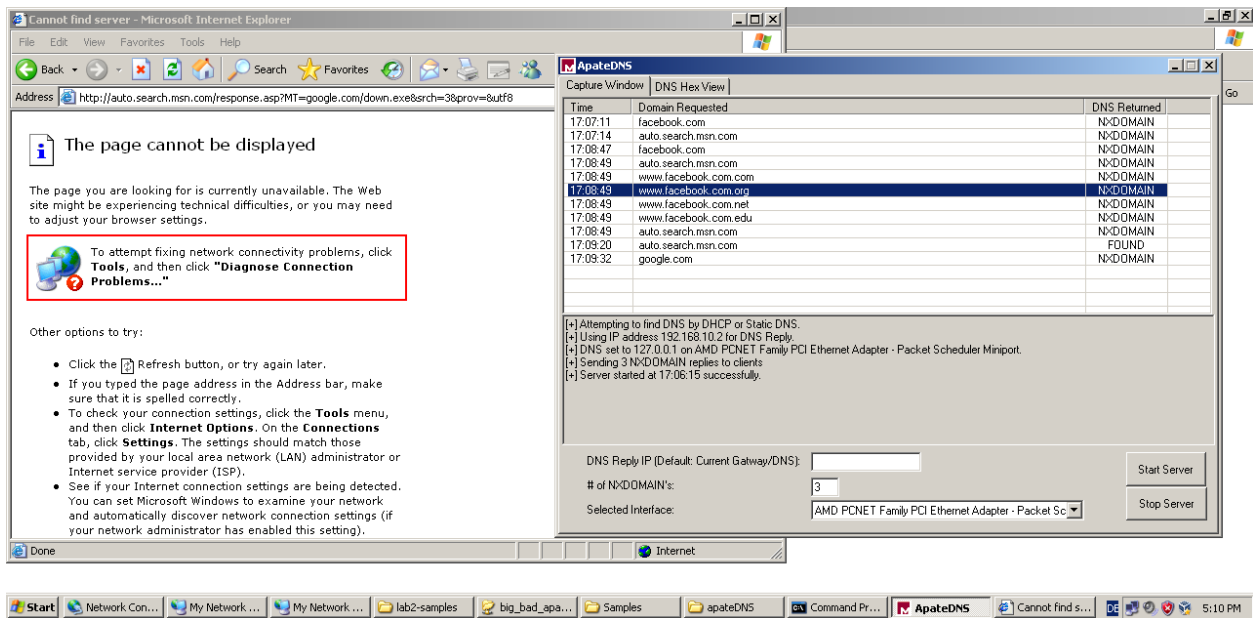
1.



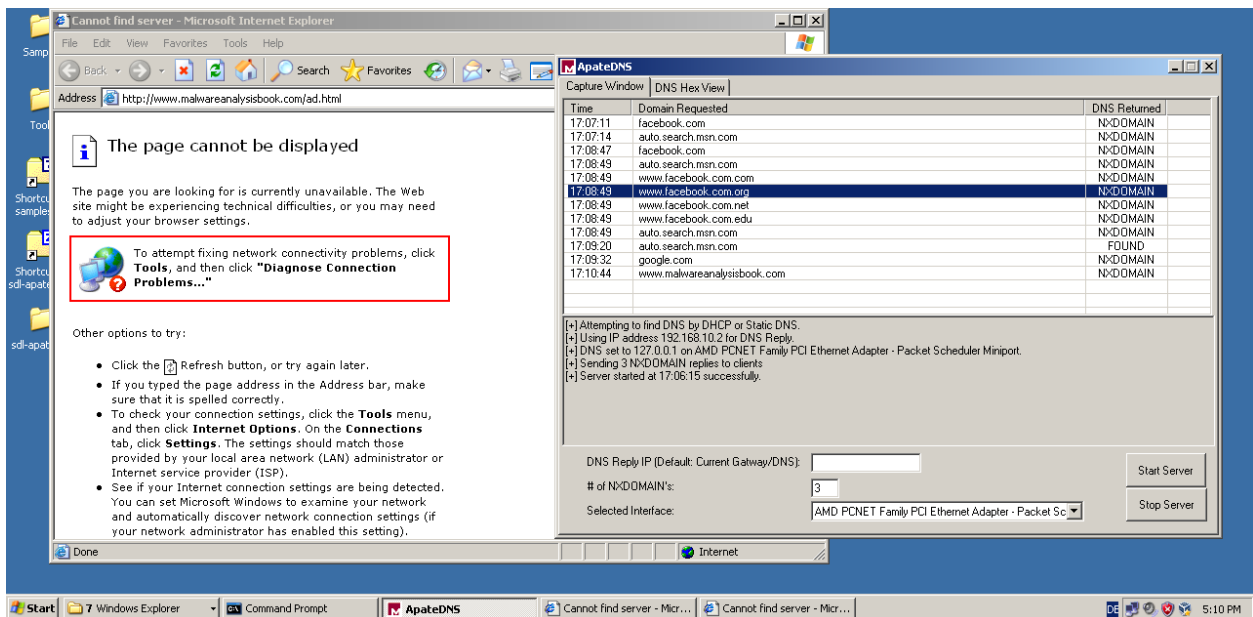
2.



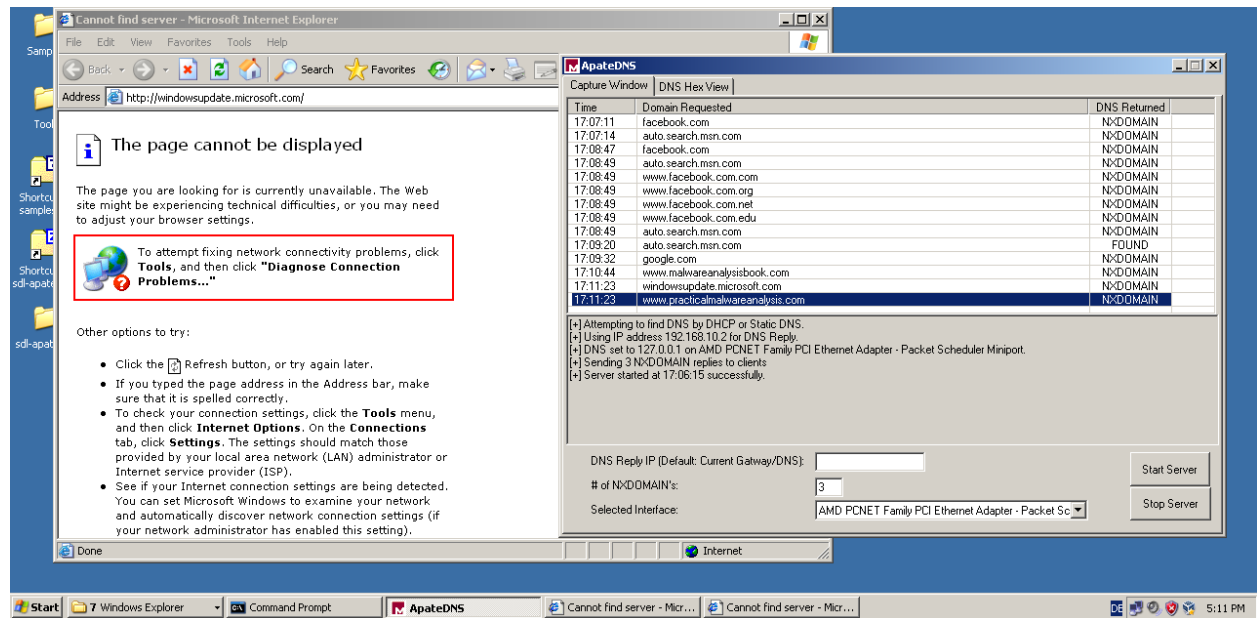
3.



Sample 1

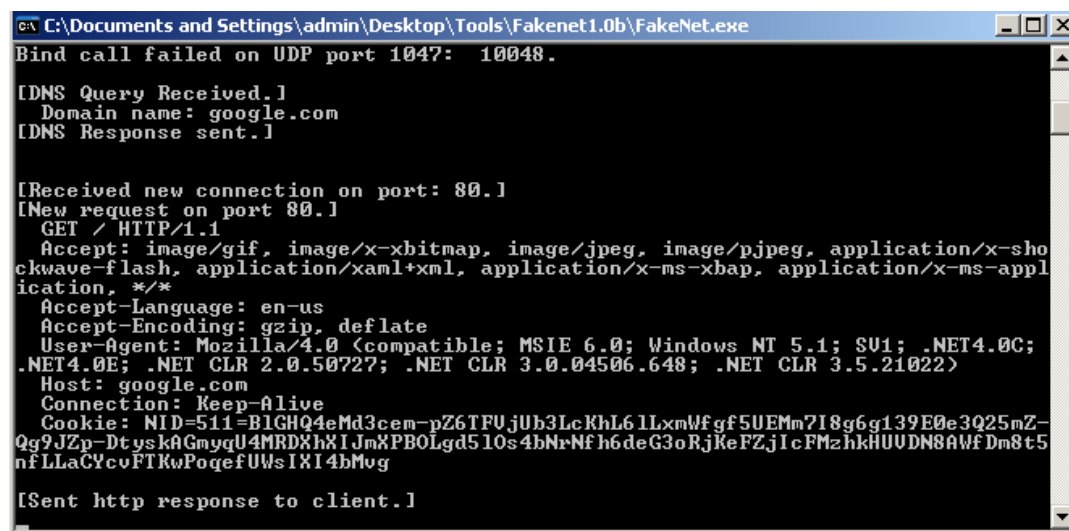
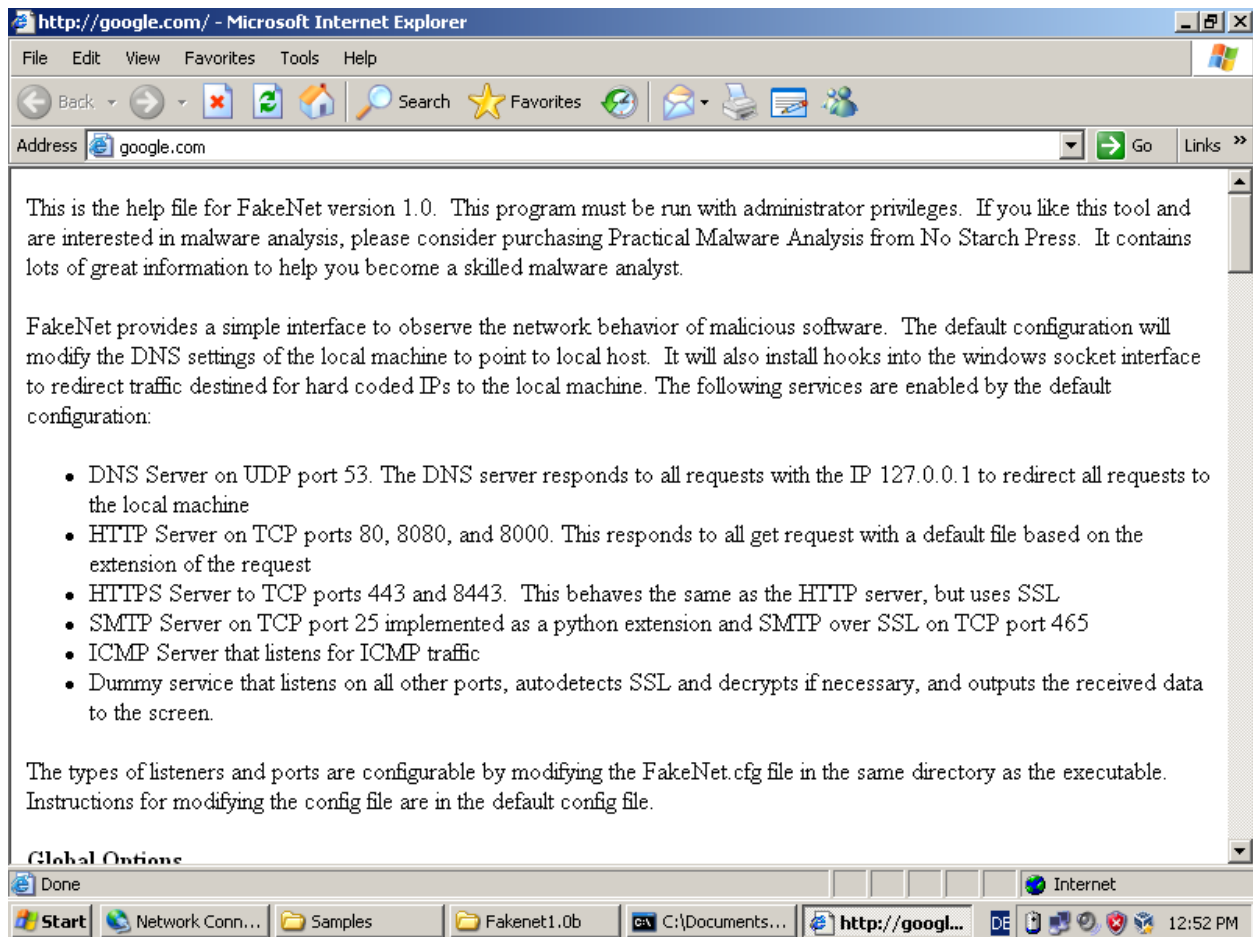


Sample 2

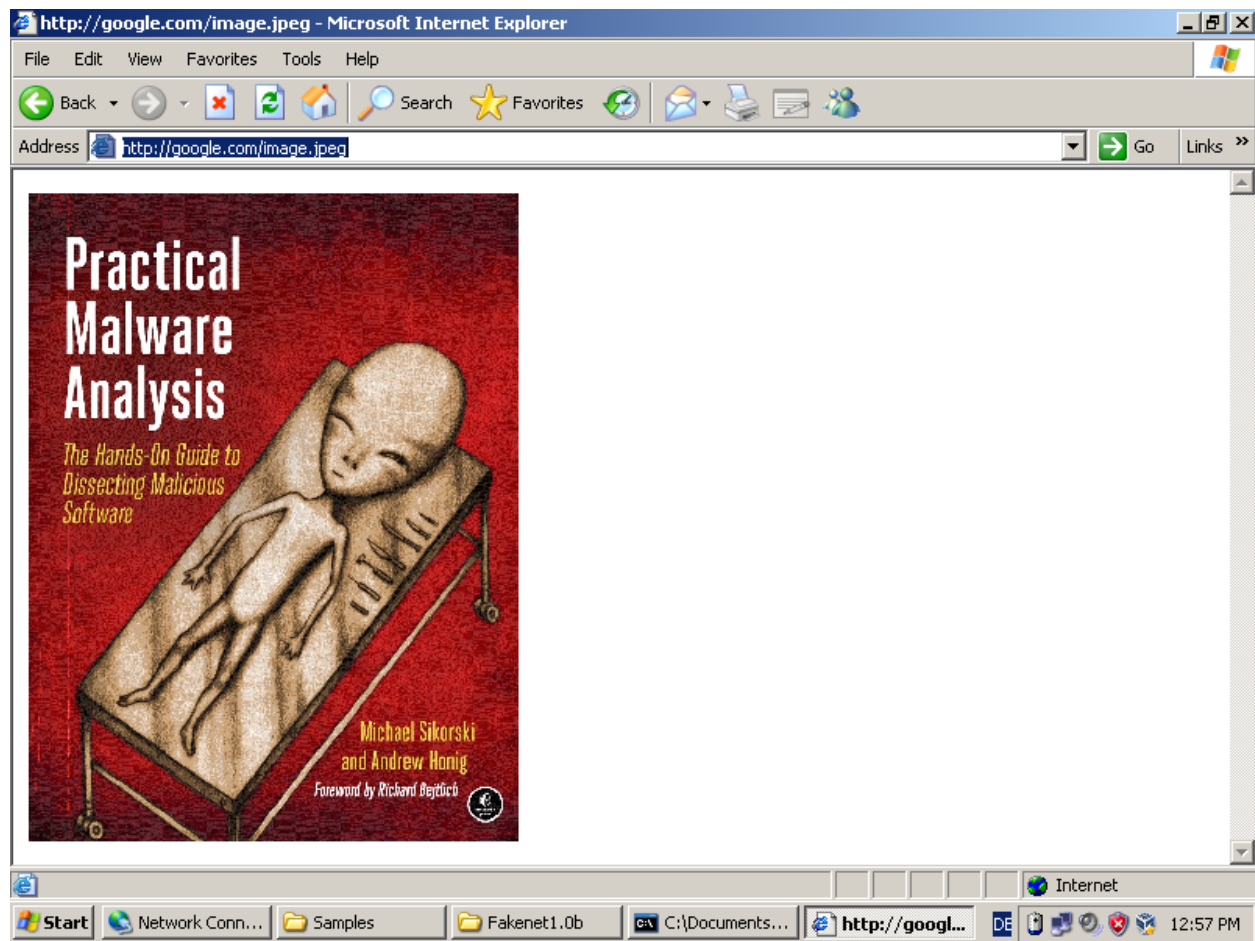


Part-2: Using FakeNet

1.



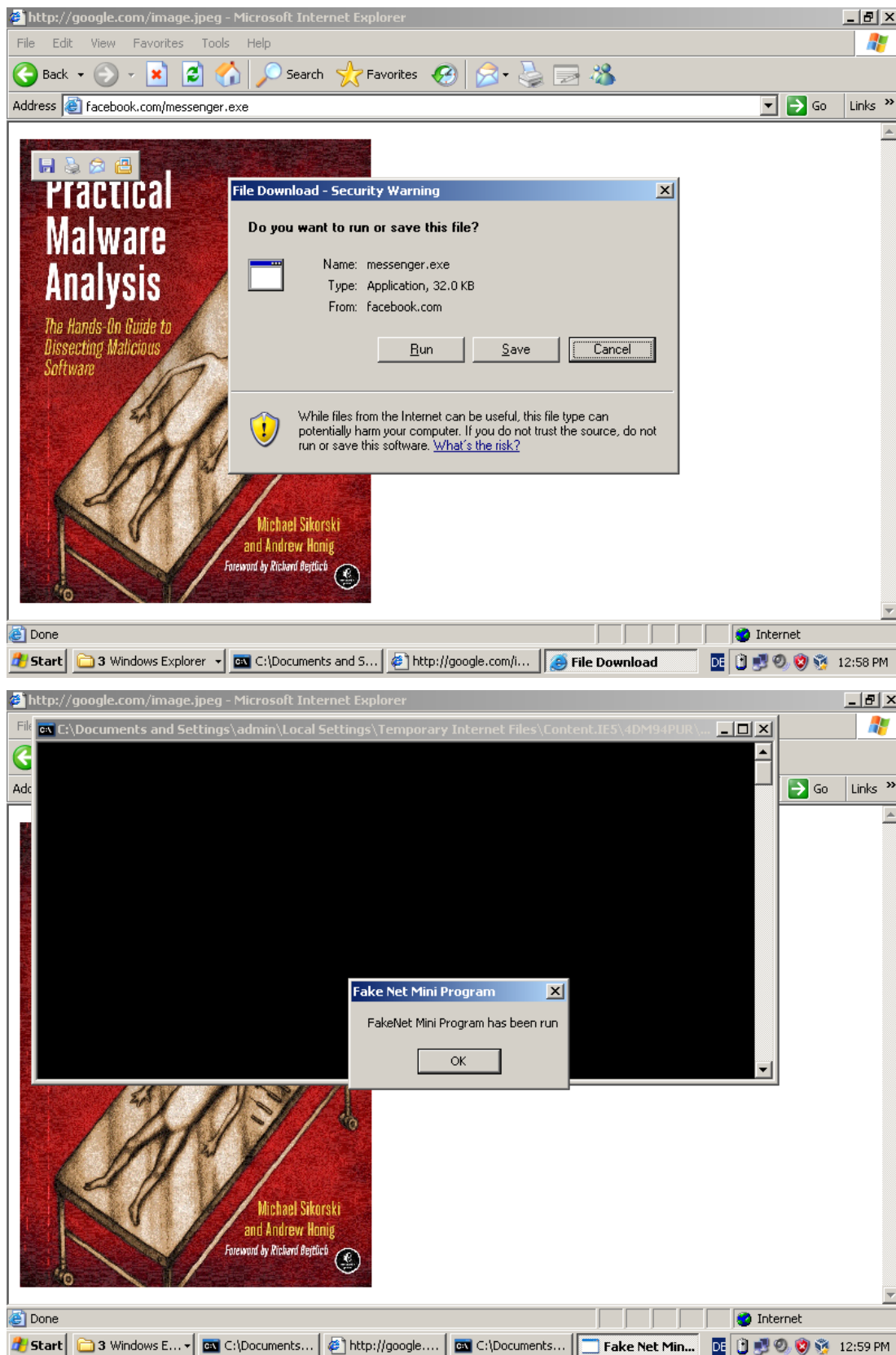
2.



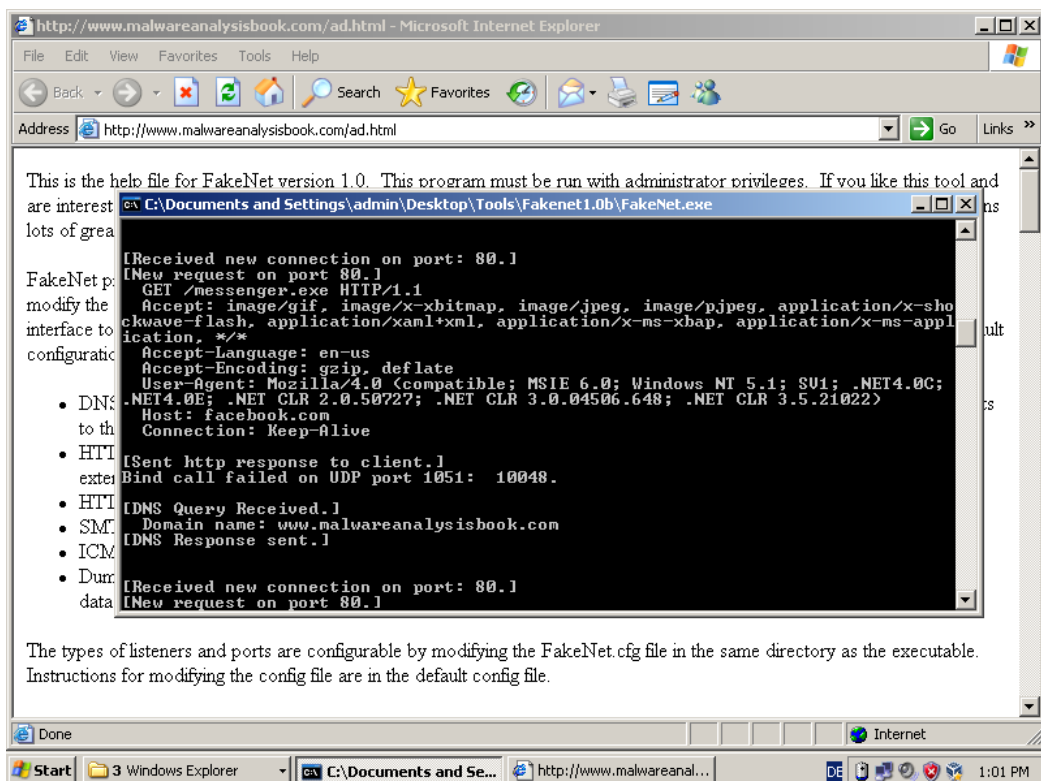
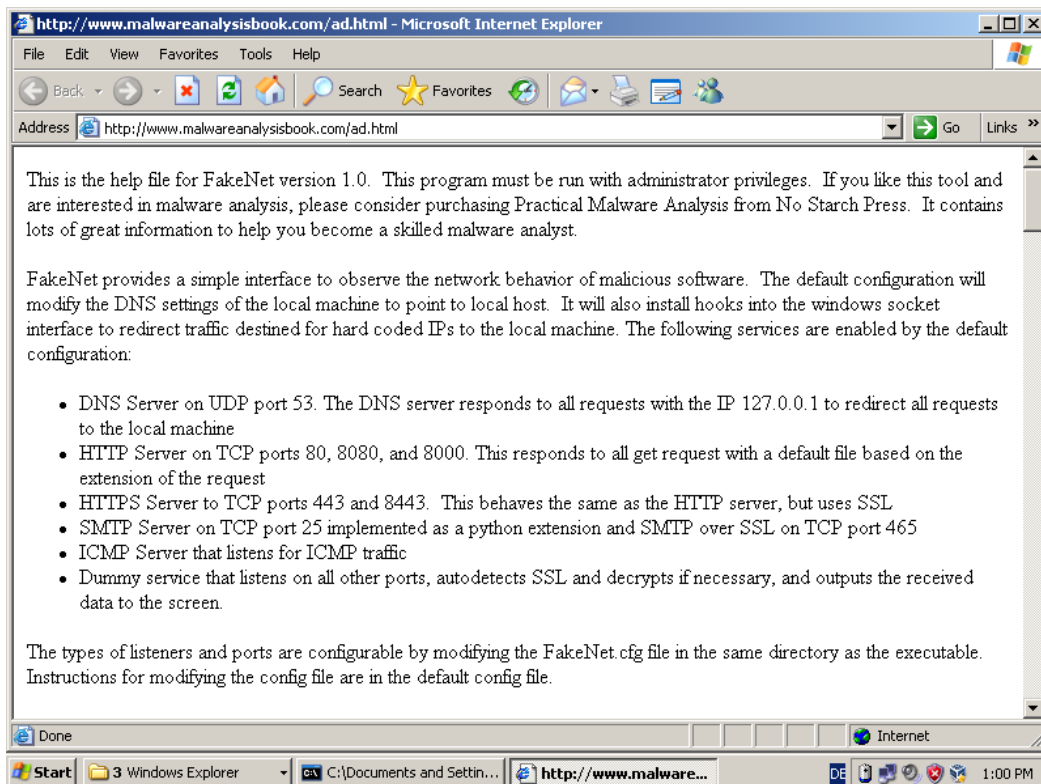
```
C:\Documents and Settings\admin\Desktop\Tools\Fakenet1.0b\FakeNet.exe
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SU1; .NET4.0C;
.NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: google.com
Connection: Keep-Alive
Cookie: NID=511=B1GHQ4eMd3cem-pZ6TFUjUb3LcKhL6lLxmWfgf5UEMm7I8g6g139E0e3Q25mZ-
Qg9JZp-DtyskAGmyqU4MRDXhXIjMxPBOLgd510s4bNrNf h6deG3oRjKeFZjlcFMzhkHUVDN8AWF Dm8t5
nfLLaCYcvFTKwPoqefUWsIXI4bMvg
[Sent http response to client.]

[Received new connection on port: 80.]
[New request on port 80.]
GET /image.jpeg HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-sho
ckwave-flash, application/xaml+xml, application/x-ms-xbap, application/x-ms-appl
ication, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SU1; .NET4.0C;
.NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: google.com
Connection: Keep-Alive
Cookie: NID=511=B1GHQ4eMd3cem-pZ6TFUjUb3LcKhL6lLxmWfgf5UEMm7I8g6g139E0e3Q25mZ-
Qg9JZp-DtyskAGmyqU4MRDXhXIjMxPBOLgd510s4bNrNf h6deG3oRjKeFZjlcFMzhkHUVDN8AWF Dm8t5
nfLLaCYcvFTKwPoqefUWsIXI4bMvg
[Sent http response to client.]
-
```

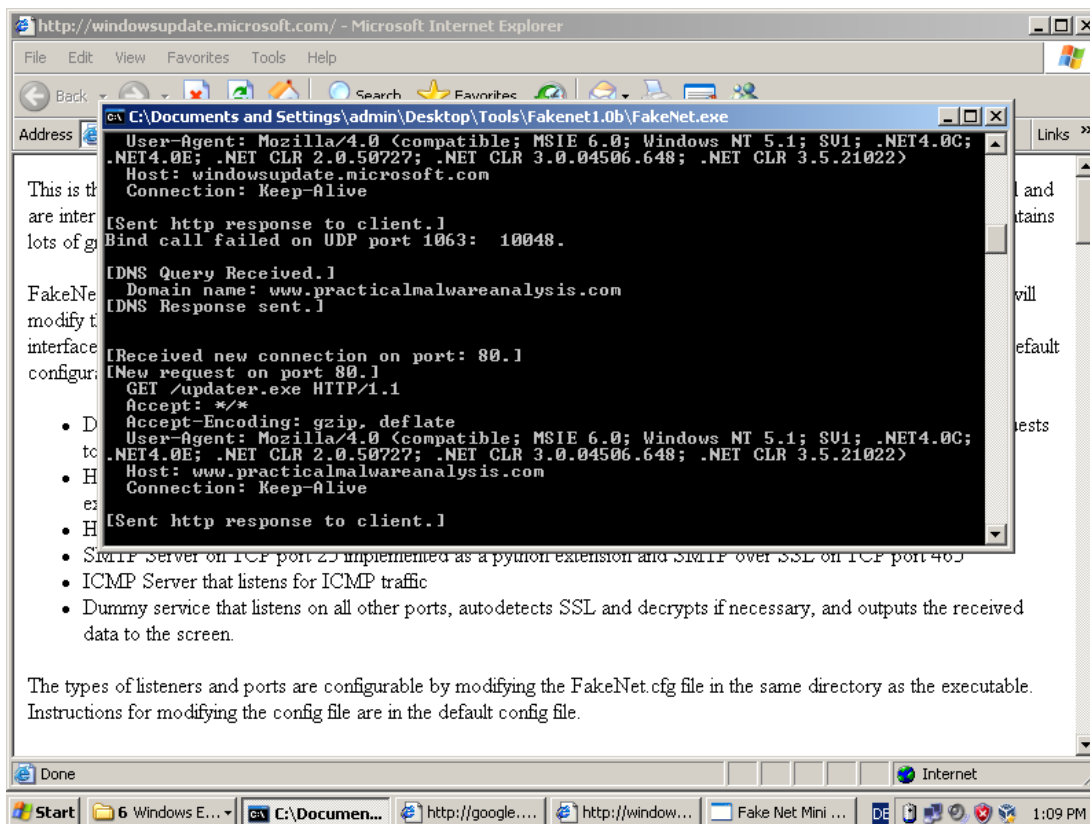
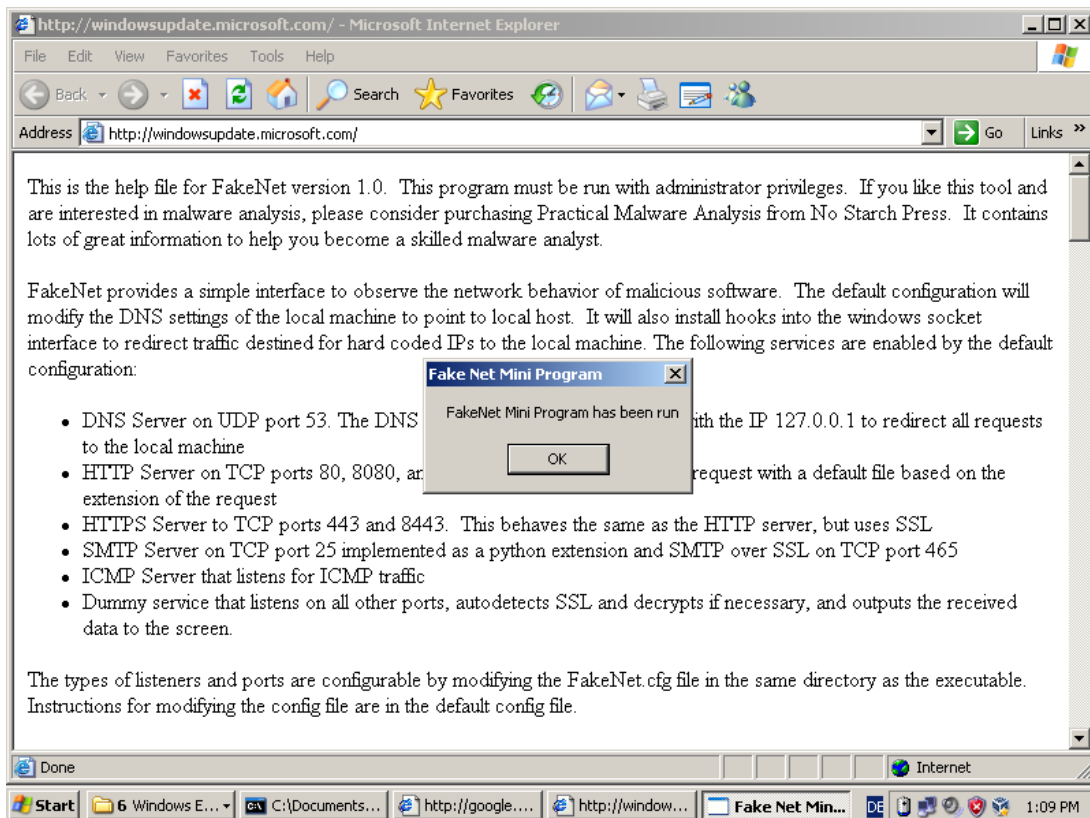
3.



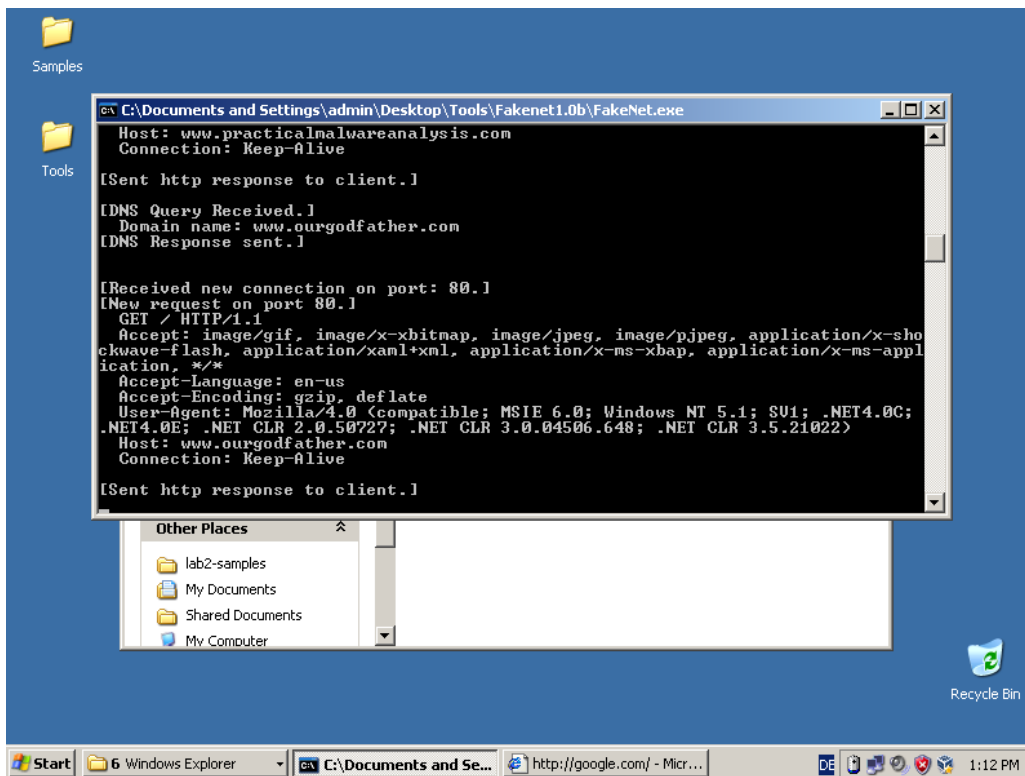
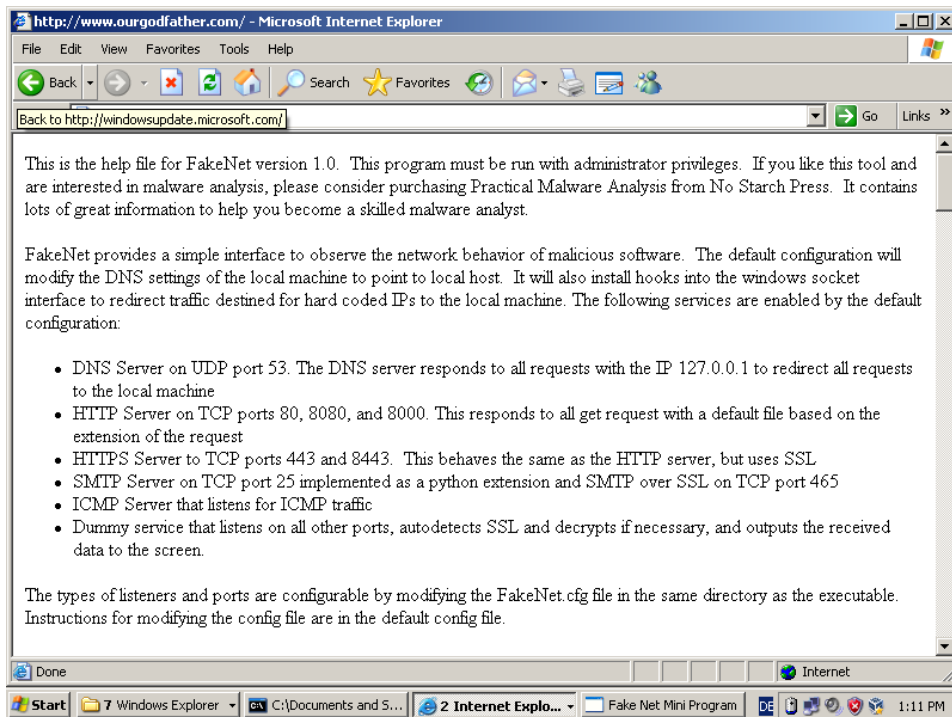
Sample 1



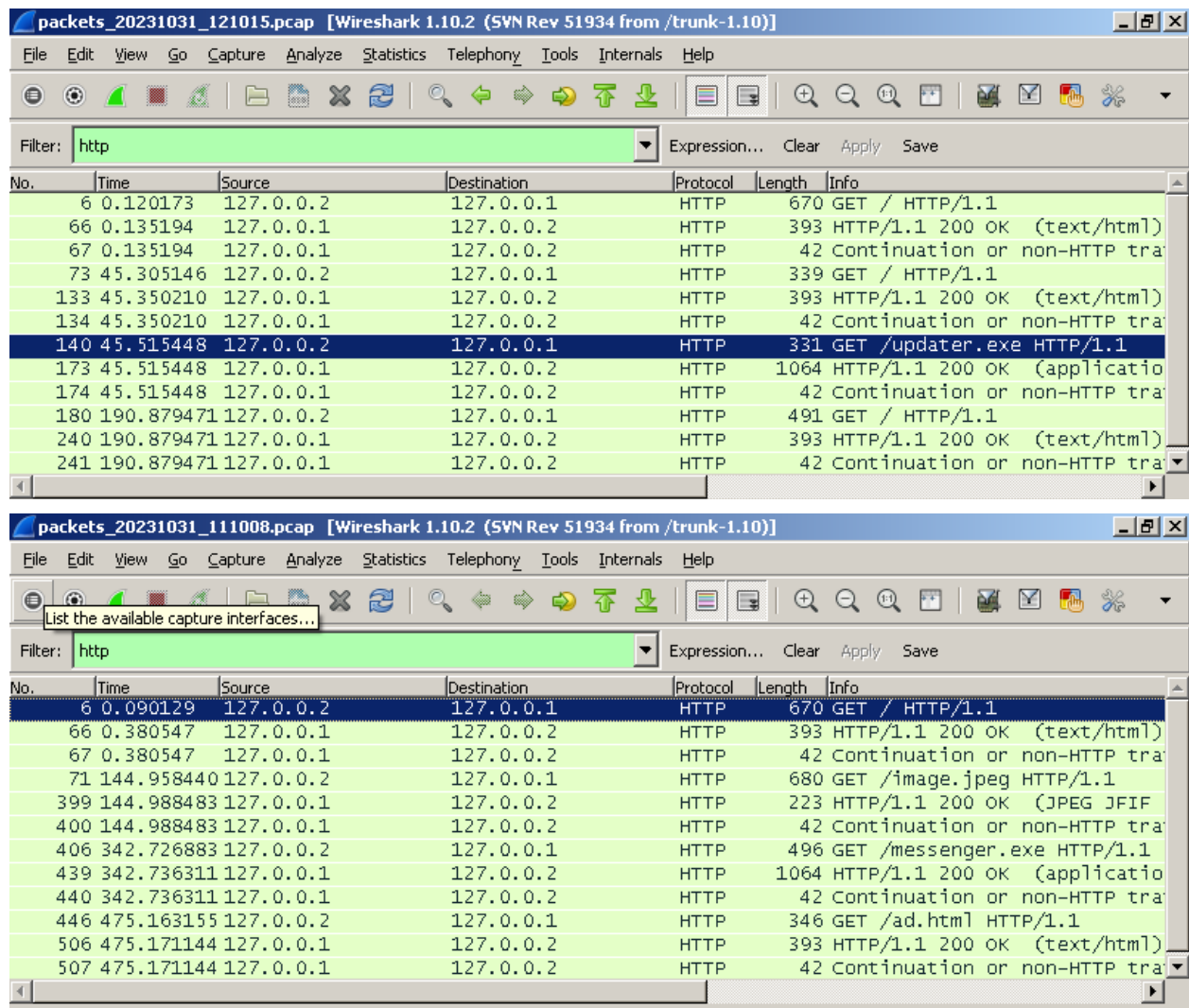
Sample 2



Messenger



PCB file in Wireshark



The top screenshot shows a packet capture of an HTTP GET request for 'updater.exe' from 127.0.0.2 to 127.0.0.1. The bottom screenshot shows a packet capture of an HTTP GET request for 'ad.html' from 127.0.0.2 to 127.0.0.1. Both screenshots show a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.120173	127.0.0.2	127.0.0.1	HTTP	670	GET / HTTP/1.1
66	0.135194	127.0.0.1	127.0.0.2	HTTP	393	HTTP/1.1 200 OK (text/html)
67	0.135194	127.0.0.1	127.0.0.2	HTTP	42	Continuation or non-HTTP tra
73	45.305146	127.0.0.2	127.0.0.1	HTTP	339	GET / HTTP/1.1
133	45.350210	127.0.0.1	127.0.0.2	HTTP	393	HTTP/1.1 200 OK (text/html)
134	45.350210	127.0.0.1	127.0.0.2	HTTP	42	Continuation or non-HTTP tra
140	45.515448	127.0.0.2	127.0.0.1	HTTP	331	GET /updater.exe HTTP/1.1
173	45.515448	127.0.0.1	127.0.0.2	HTTP	1064	HTTP/1.1 200 OK (applicatio
174	45.515448	127.0.0.1	127.0.0.2	HTTP	42	Continuation or non-HTTP tra
180	190.879471	127.0.0.2	127.0.0.1	HTTP	491	GET / HTTP/1.1
240	190.879471	127.0.0.1	127.0.0.2	HTTP	393	HTTP/1.1 200 OK (text/html)
241	190.879471	127.0.0.1	127.0.0.2	HTTP	42	Continuation or non-HTTP tra

No.	Time	Source	Destination	Protocol	Length	Info
6	0.090129	127.0.0.2	127.0.0.1	HTTP	670	GET / HTTP/1.1
66	0.380547	127.0.0.1	127.0.0.2	HTTP	393	HTTP/1.1 200 OK (text/html)
67	0.380547	127.0.0.1	127.0.0.2	HTTP	42	Continuation or non-HTTP tra
71	144.958440	127.0.0.2	127.0.0.1	HTTP	680	GET /image.jpeg HTTP/1.1
399	144.988483	127.0.0.1	127.0.0.2	HTTP	223	HTTP/1.1 200 OK (JPEG JFIF
400	144.988483	127.0.0.1	127.0.0.2	HTTP	42	Continuation or non-HTTP tra
406	342.726883	127.0.0.2	127.0.0.1	HTTP	496	GET /messenger.exe HTTP/1.1
439	342.736311	127.0.0.1	127.0.0.2	HTTP	1064	HTTP/1.1 200 OK (applicatio
440	342.736311	127.0.0.1	127.0.0.2	HTTP	42	Continuation or non-HTTP tra
446	475.163155	127.0.0.2	127.0.0.1	HTTP	346	GET /ad.html HTTP/1.1
506	475.171144	127.0.0.1	127.0.0.2	HTTP	393	HTTP/1.1 200 OK (text/html)
507	475.171144	127.0.0.1	127.0.0.2	HTTP	42	Continuation or non-HTTP tra

Conclusion:

Yes, the overall network behavior of the malware aligns with both FakeNet and INetSim. However, a key difference lies in the source of the default HTML pages, images, and .exe files. Instead of sourcing these from INetSim, they are now being retrieved from FakeNet. Aside from this distinction, the behavior of the malware remains consistent, particularly in terms of the domains requested and actions executed.