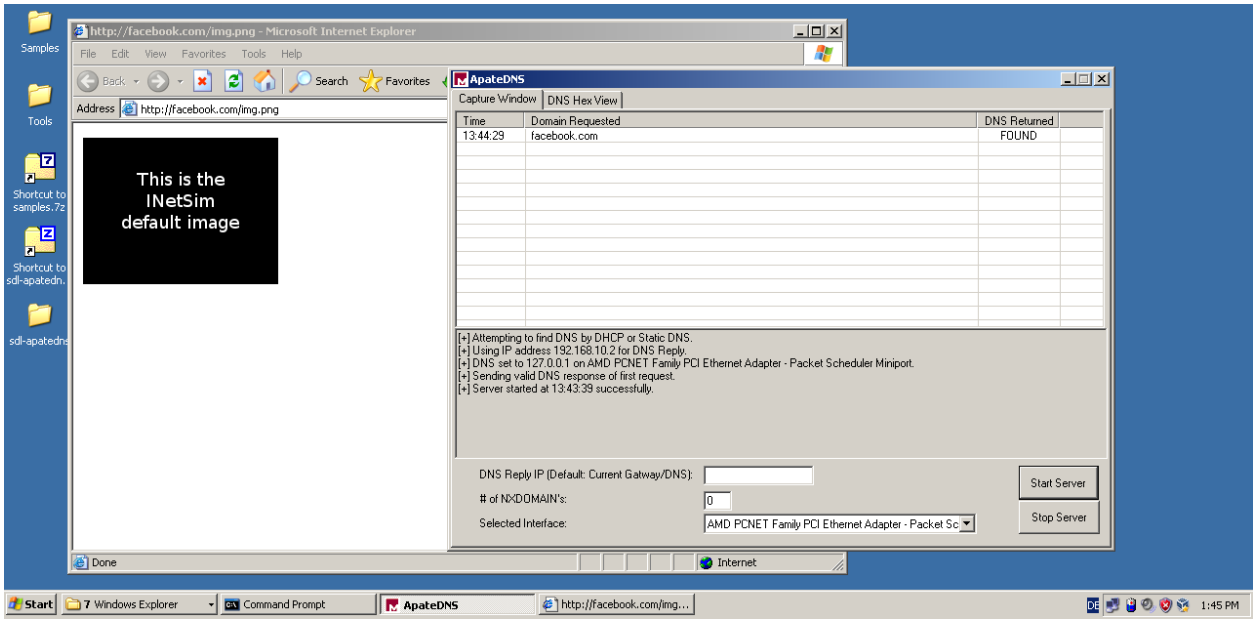
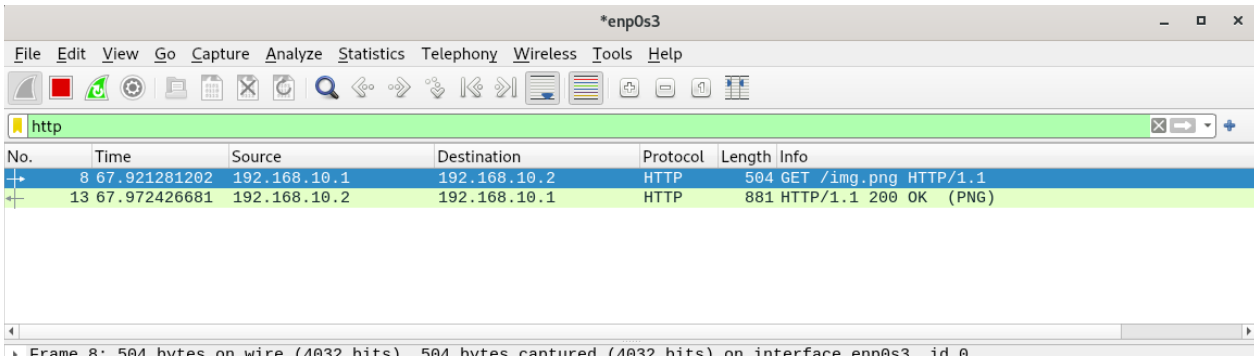
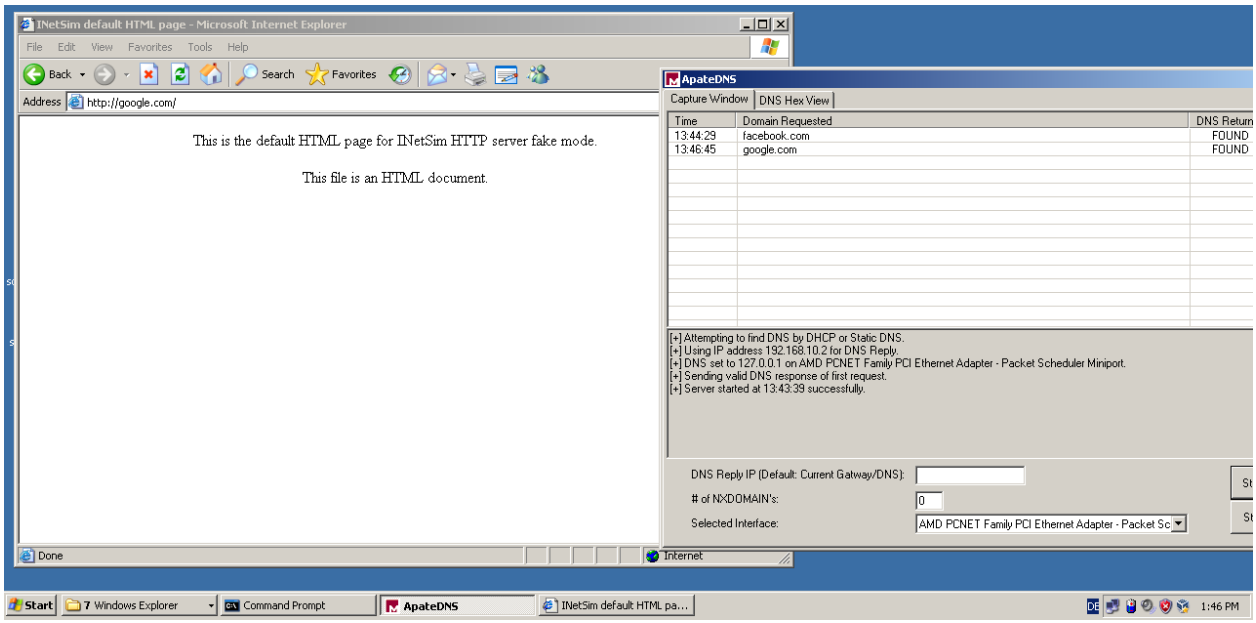
Part-1: Using ApateDNS

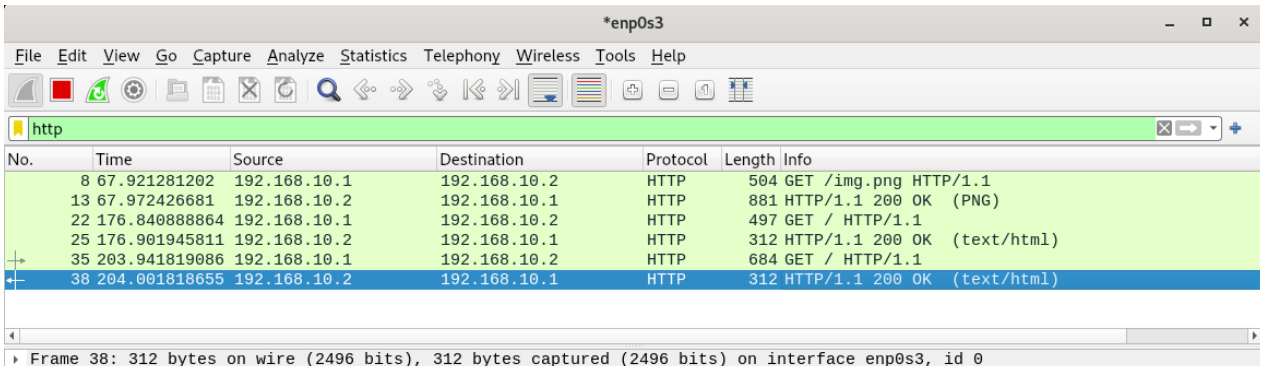
1. Given that a private connection is established, the HTTP request is directed to the Remnux VM and the response is generated from the same server. The requested image is from facebook, but the returned image is the default inetsim image.



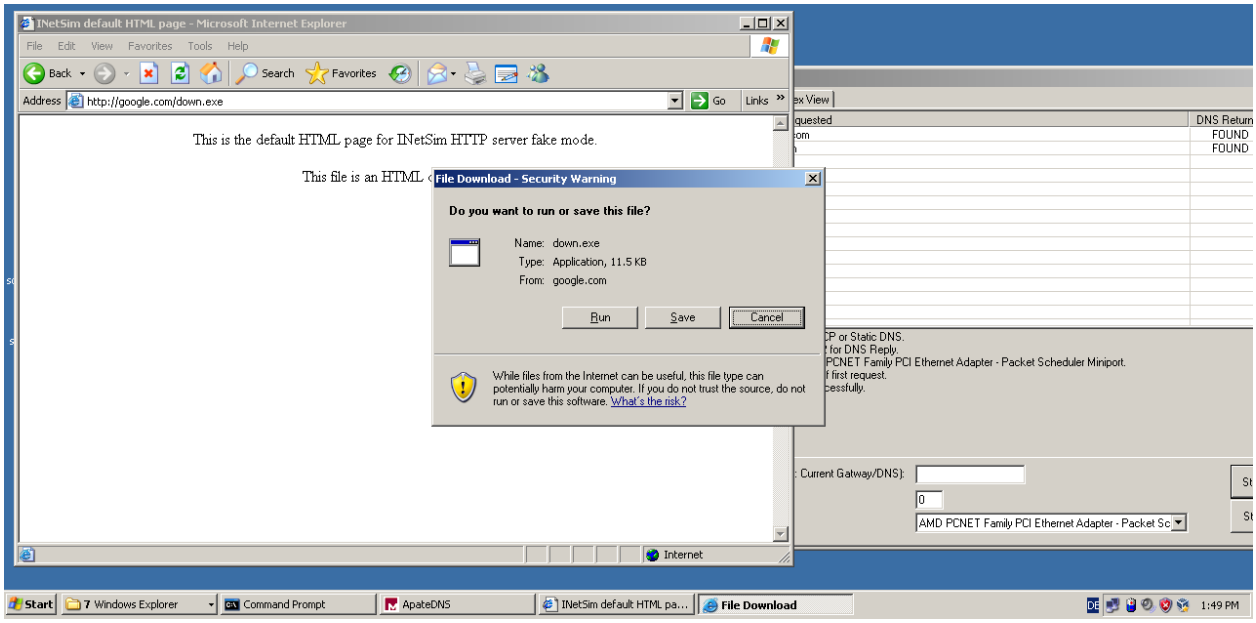


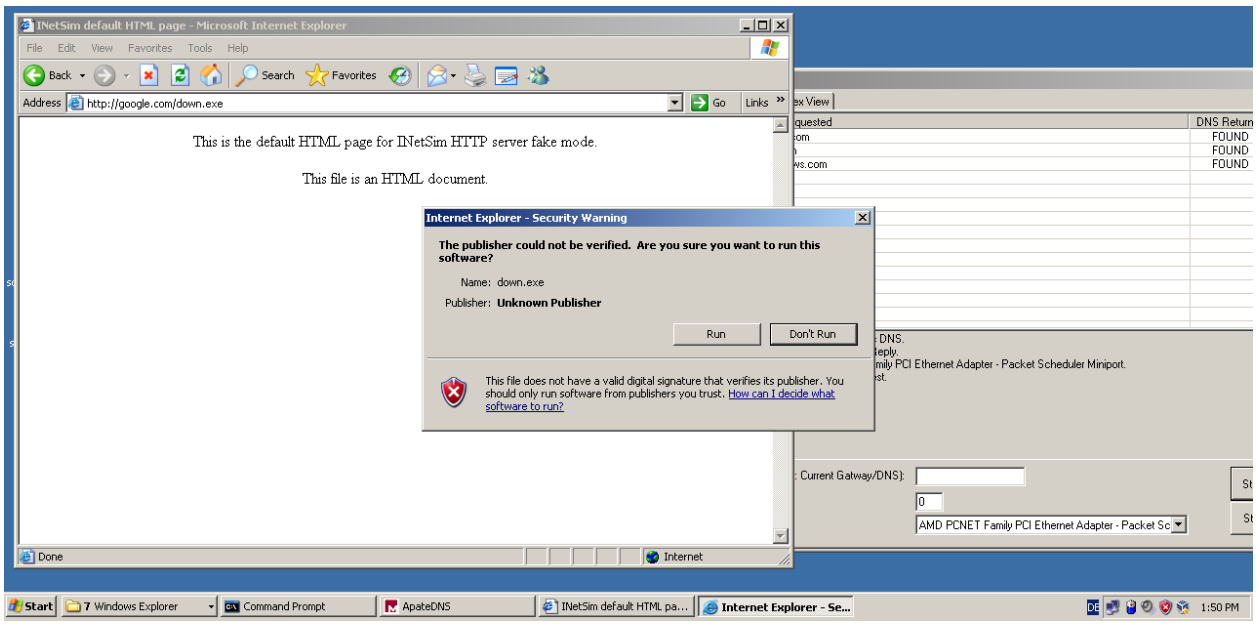
2. When I initiate a HTTP request to a web page, it's captured by the server, which presently is the Remnux VM. The packets that Wireshark has captured can been seen in the pictures below.

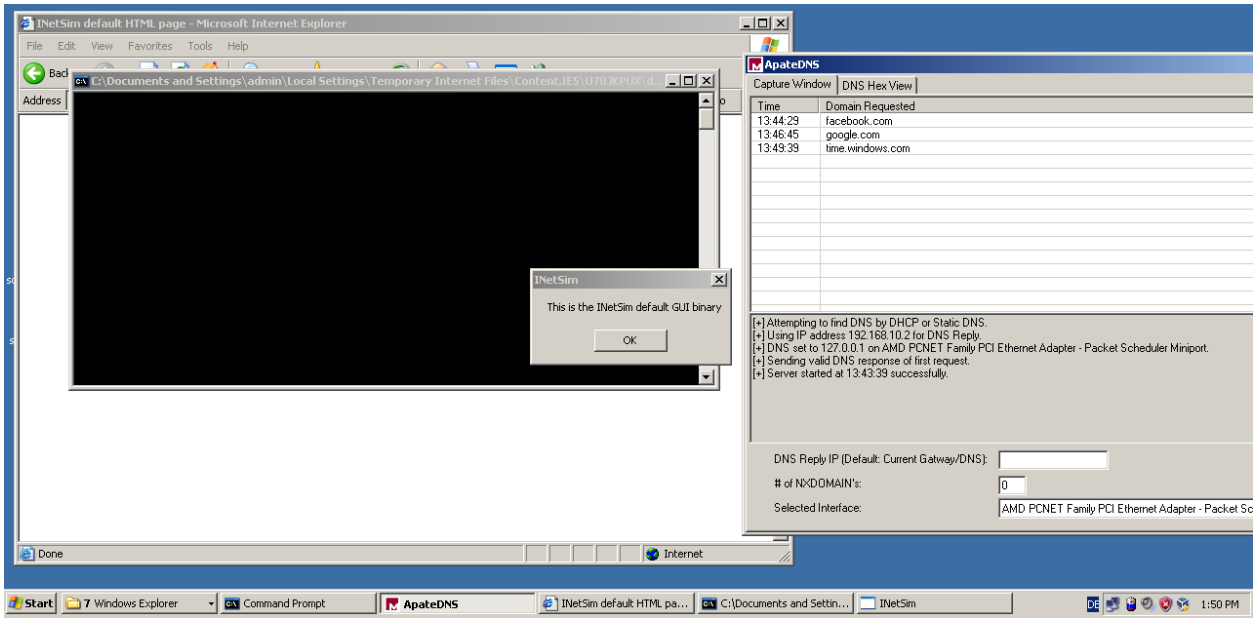


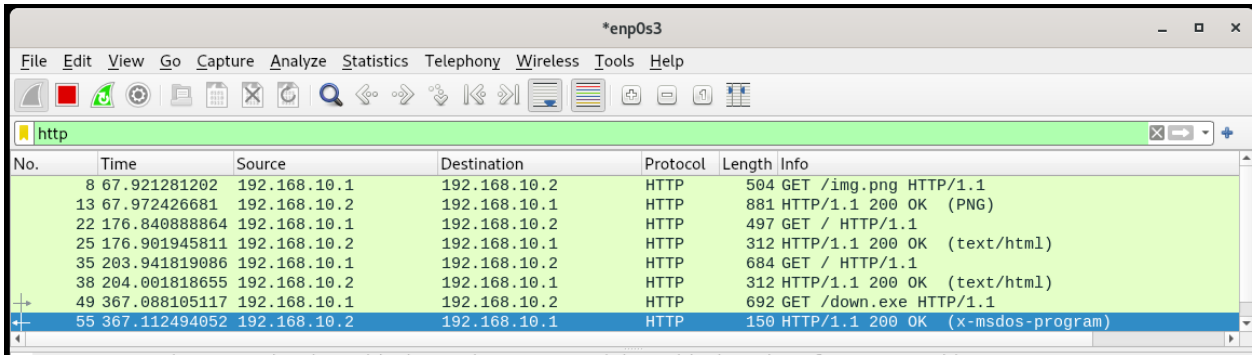


3. When I request for a “down.exe”. The default inetsim GUI application is downloaded. And the packets and request captured can be seen by the wireshark in the Remnux VM.



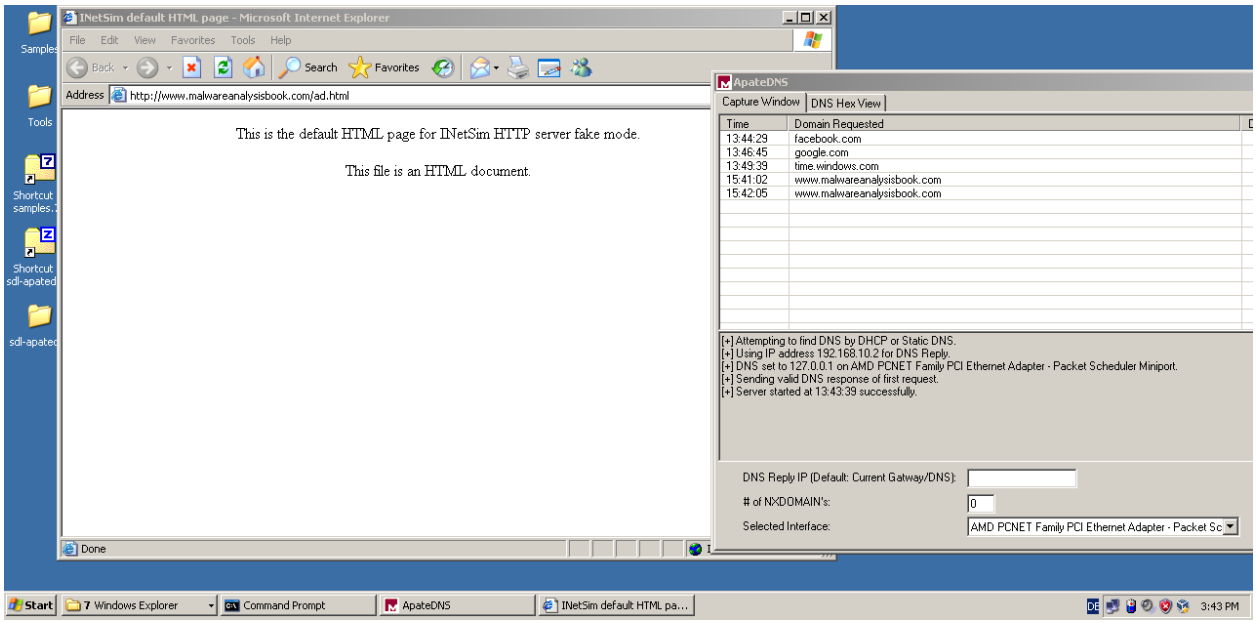


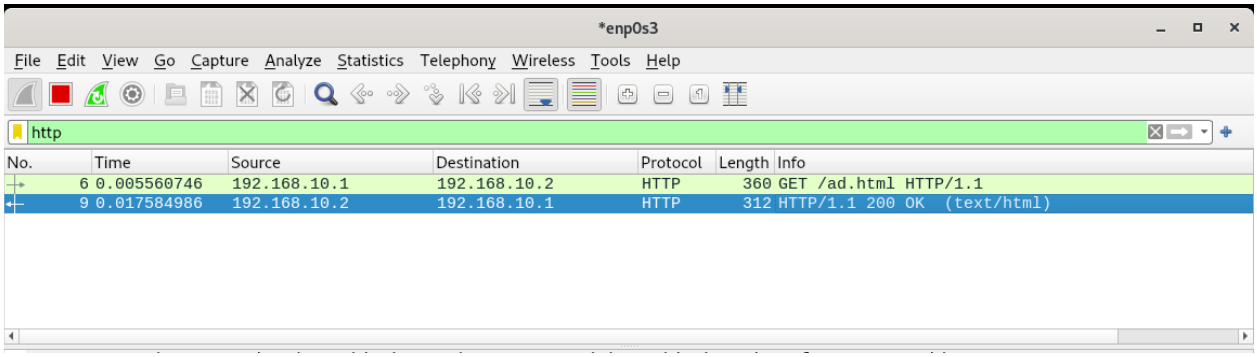

INetSim default HTML page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
C:\Documents and Settings\admin\Local Settings\Temporary Internet Files\Content.IE5\U70JKPUX\d...
INetSim
This is the INetSim default GUI binary
OK
Done
Internet
ApateDNS
Capture Window
DNS Hex View
Time
Domain Requested
13:44:29
facebook.com
13:46:45
google.com
13:49:39
time.windows.com
[+] 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 Gatway/DNS):
# of NXDOMAIN's:
0
Selected Interface:
AMD PCNET Family PCI Ethernet Adapter - Packet Sc
Start
7 Windows Explorer
Command Prompt
ApateDNS
INetSim default HTML pa...
C:\Documents and Settin...
INetSim
1:50 PM


*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

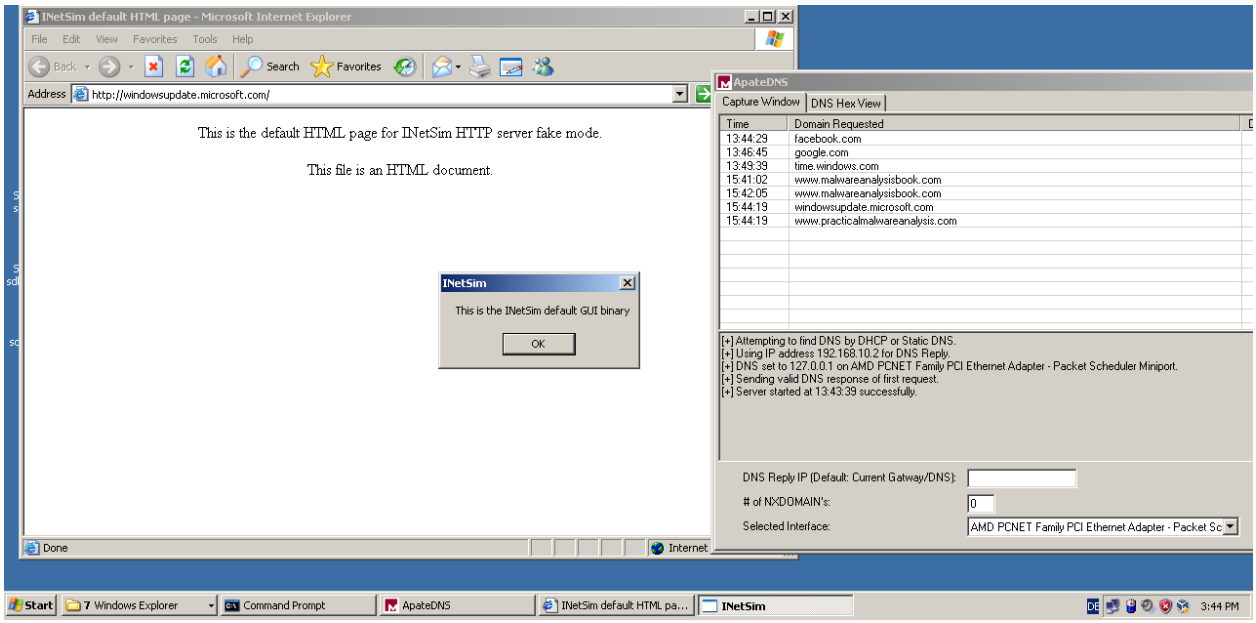
www.malwareanalysisbook.com is the domain sample 1 is trying to connect. Get request for ad.html is being made and then html text for default inetsim http server is being rendered.

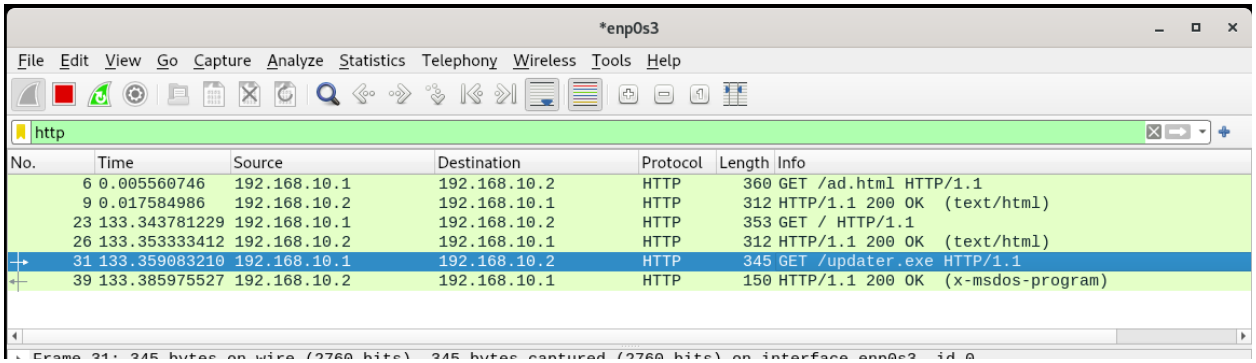




Sample 2

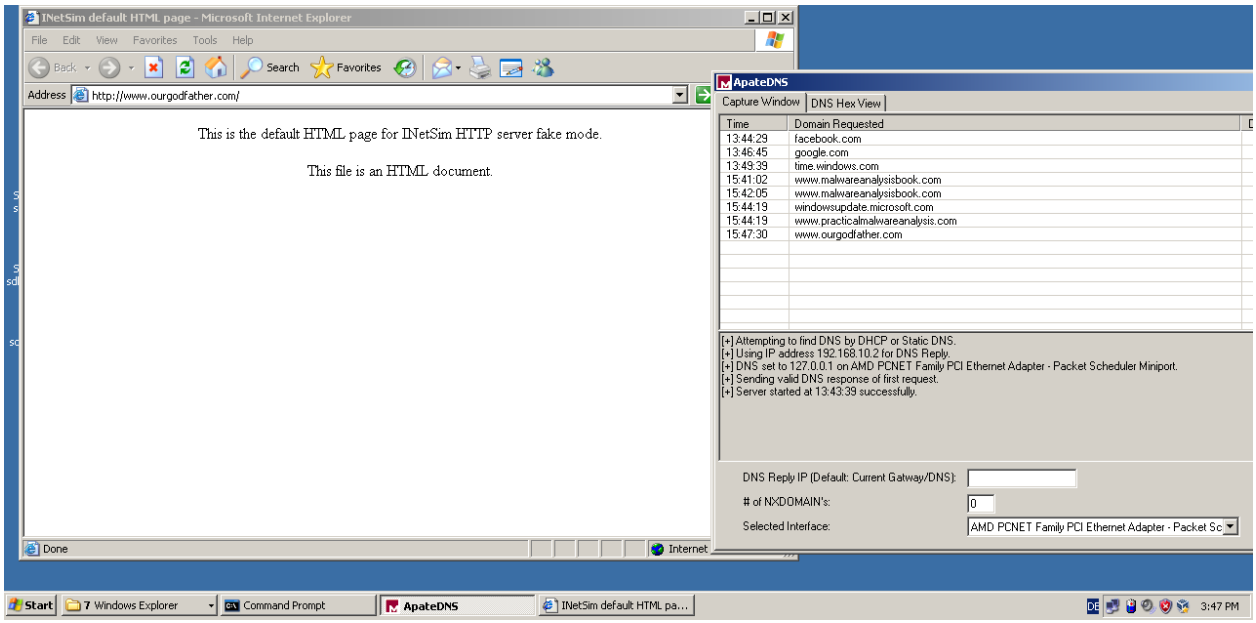
windowsupdate.microsoft.com is the domain sample 2 is trying to connect. Get request for updater.exe is being made and then x-msdos-program is being received.
www.practicalmalwareanalysis.com is also a domain which is requested.
This means that by going to this website, an exe file is being downloaded for execution.

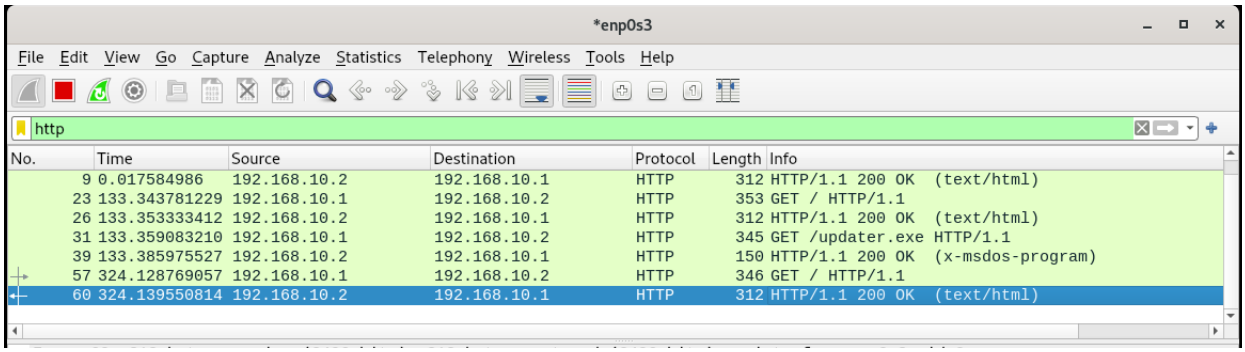




Messenger

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.





=== 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/down.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' ===

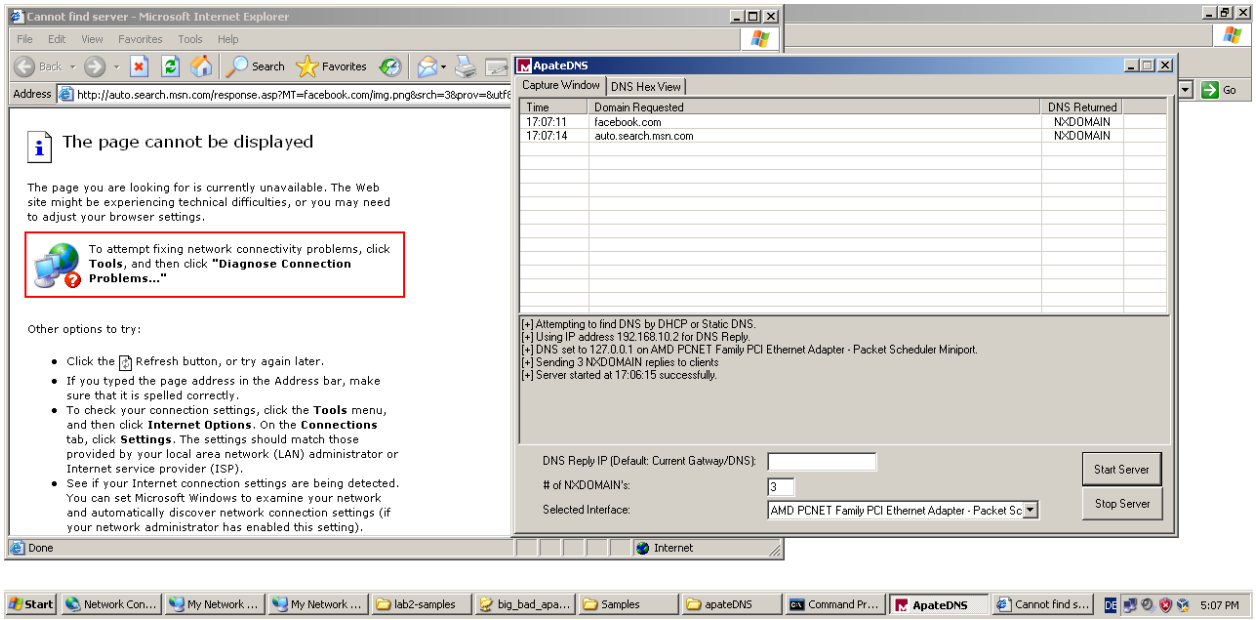
Real start date : 2023-11-03 10:41:57
Simulated start date : 2023-11-03 10:41:57
Time difference on startup : none

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

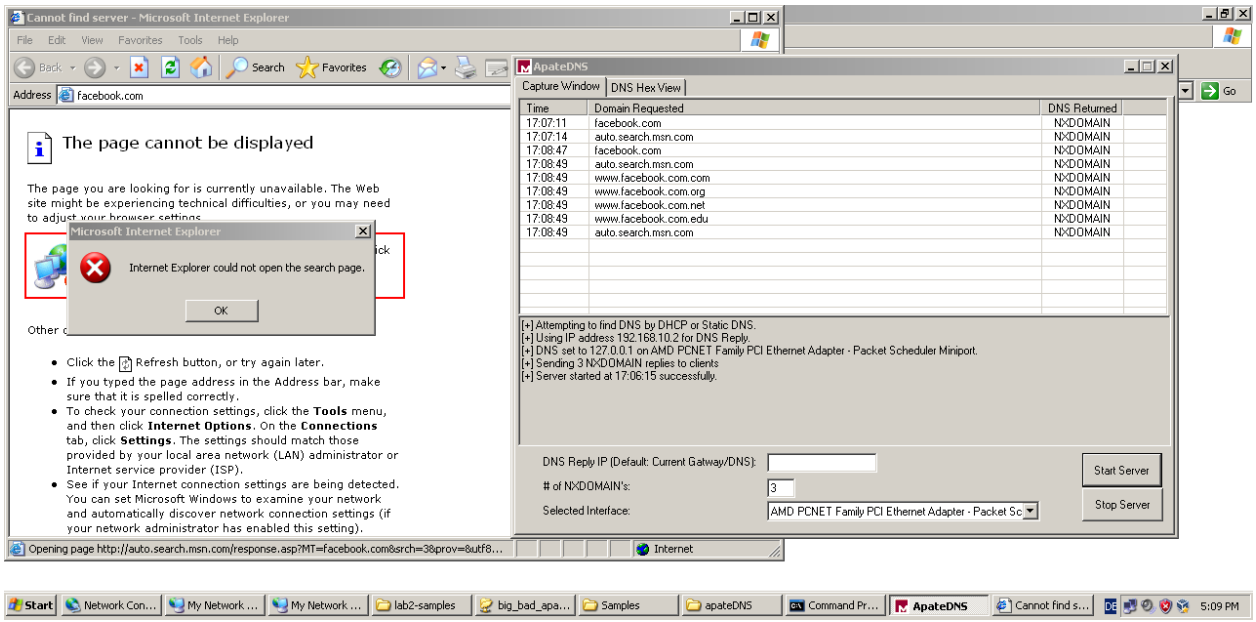
# of NXDOMAINS =3

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

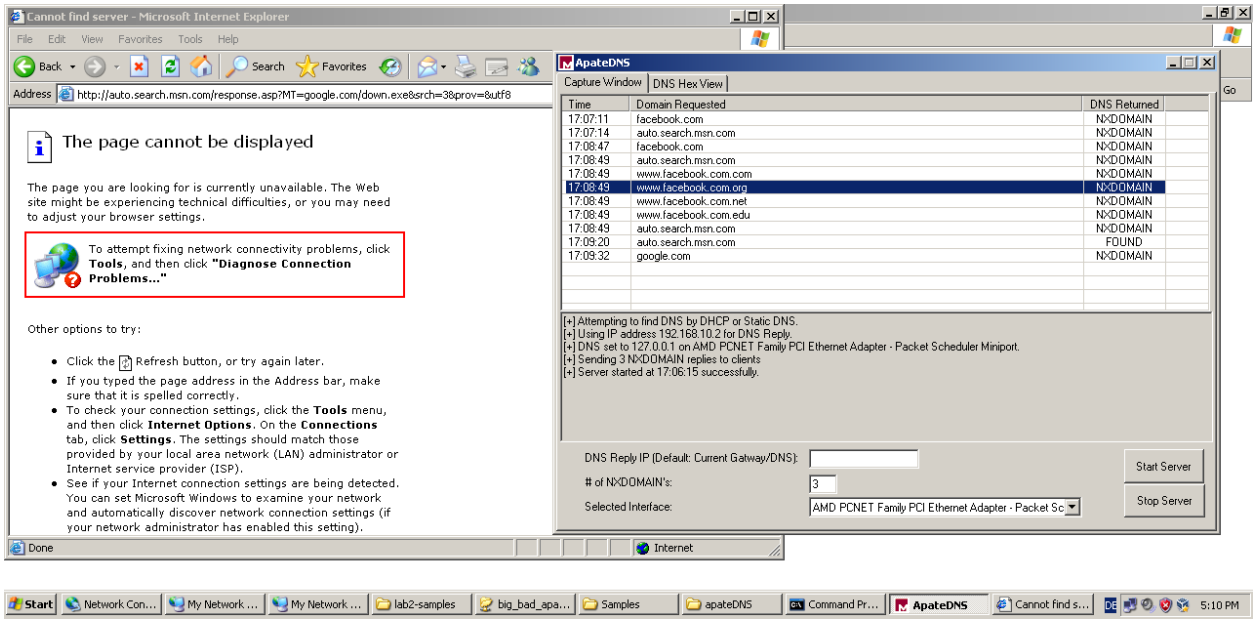
1.



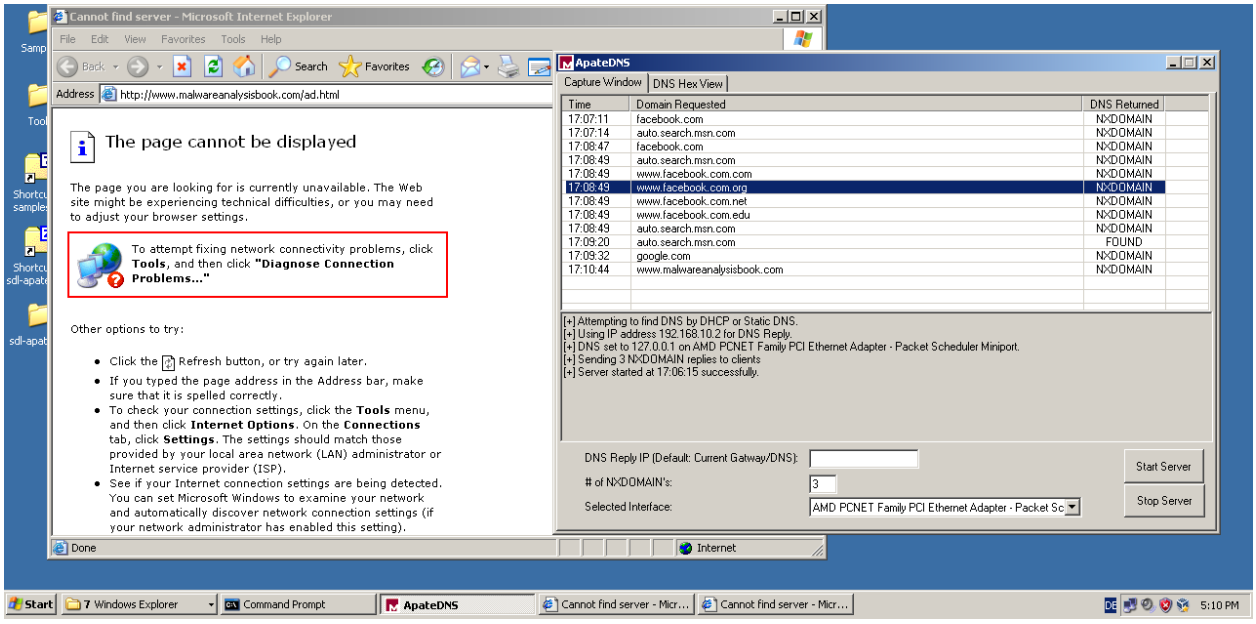
2.



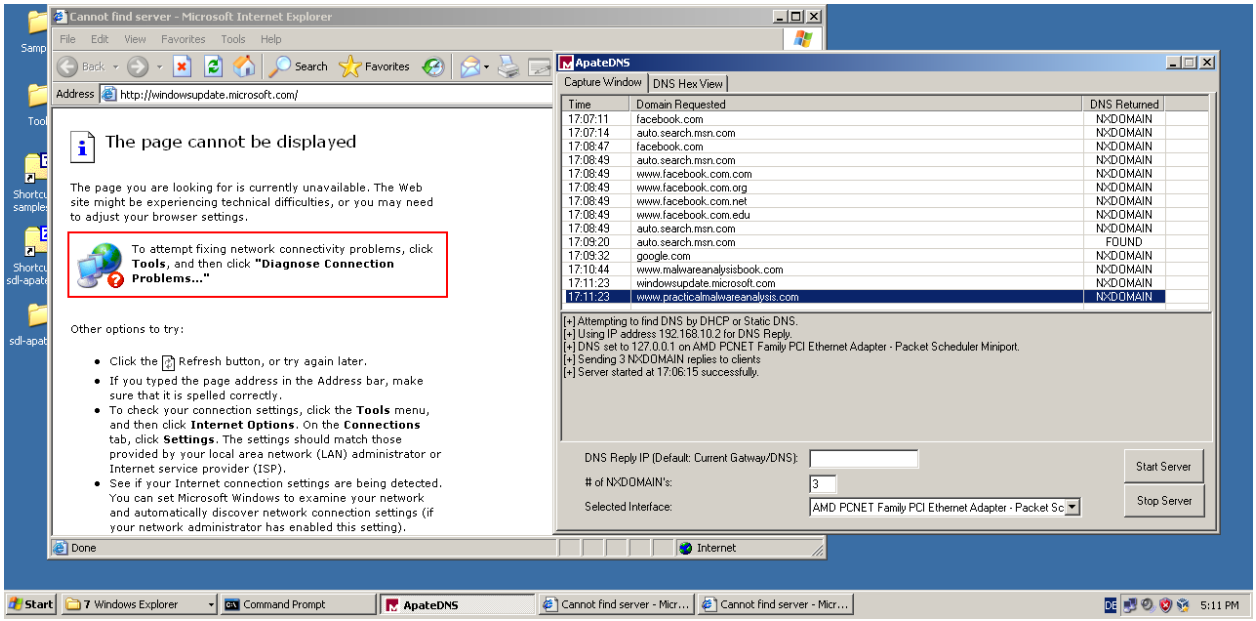
3.


Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://auto.search.msn.com/response.asp?MT=google.com/down.exe&srch=3&prov=&utf8
The page cannot be displayed
The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.
To attempt fixing network connectivity problems, click Tools, and then click "Diagnose Connection Problems..."
Other options to try:
Click the Refresh button, or try again later.
If you typed the page address in the Address bar, make sure that it is spelled correctly.
To check your connection settings, click the Tools menu, and then click Internet Options. On the Connections tab, click Settings. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
See if your Internet connection settings are being detected. You can set Microsoft Windows to examine your network and automatically discover network connection settings (if your network administrator has enabled this setting).
Done
Internet
ApateDNS
Capture Window
DNS Hex View
Time
Domain Requested
DNS Returned
17:07:11 facebook.com NXDOMAIN
17:07:14 auto.search.msn.com NXDOMAIN
17:08:47 facebook.com NXDOMAIN
17:08:49 auto.search.msn.com NXDOMAIN
17:08:49 www.facebook.com.com NXDOMAIN
17:08:49 www.facebook.com.org NXDOMAIN
17:08:49 www.facebook.com.net NXDOMAIN
17:08:49 www.facebook.com.edu NXDOMAIN
17:08:49 auto.search.msn.com NXDOMAIN
17:09:20 auto.search.msn.com FOUND
17:09:32 google.com NXDOMAIN
[+] 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 3 NXDOMAIN replies to clients
[+] Server started at 17:06:15 successfully.
DNS Reply IP (Default: Current Gatway/DNS):
# of NXDOMAIN's: 3
Selected Interface: AMD PCNET Family PCI Ethernet Adapter - Packet Sc
Start Server
Stop Server
Start
Network Con...
My Network ...
My Network ...
lab2-samples
big_bad_apa...
Samples
apateDNS
Command Pr...
ApateDNS
Cannot find s...
5:10 PM

Sample 1

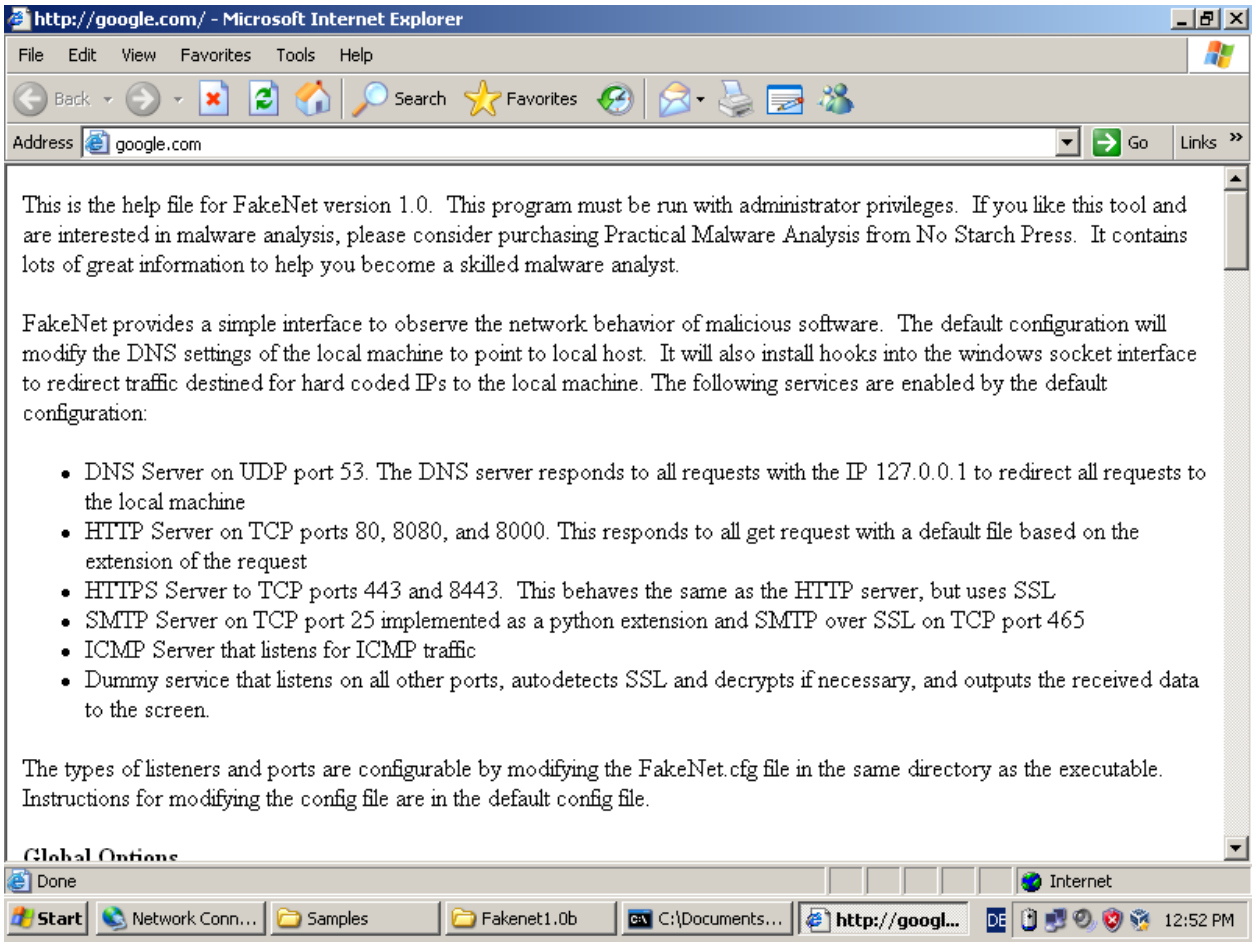

Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.malwareanalysisbook.com/ad.html
The page cannot be displayed
The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.
To attempt fixing network connectivity problems, click Tools, and then click "Diagnose Connection Problems..."
Other options to try:
Click the Refresh button, or try again later.
If you typed the page address in the Address bar, make sure that it is spelled correctly.
To check your connection settings, click the Tools menu, and then click Internet Options. On the Connections tab, click Settings. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
See if your Internet connection settings are being detected. You can set Microsoft Windows to examine your network and automatically discover network connection settings (if your network administrator has enabled this setting).
Done
Internet
ApateDNS
Capture Window
DNS Hex View
Time
Domain Requested
DNS Returned
17:07:11 facebook.com NXDOMAIN
17:07:14 auto.search.msn.com NXDOMAIN
17:08:47 facebook.com NXDOMAIN
17:08:49 auto.search.msn.com NXDOMAIN
17:08:49 www.facebook.com.com NXDOMAIN
17:08:49 www.facebook.com.org NXDOMAIN
17:08:49 www.facebook.com.net NXDOMAIN
17:08:49 www.facebook.com.edu NXDOMAIN
17:08:49 auto.search.msn.com NXDOMAIN
17:09:20 auto.search.msn.com FOUND
17:09:32 google.com NXDOMAIN
17:10:44 www.malwareanalysisbook.com NXDOMAIN
[+] 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 3 NXDOMAIN replies to clients
[+] Server started at 17:06:15 successfully.
DNS Reply IP (Default: Current Gatway/DNS):
# of NXDOMAIN's: 3
Selected Interface: AMD PCNET Family PCI Ethernet Adapter - Packet Sc
Start Server
Stop Server
Start
7 Windows Explorer
Command Prompt
ApateDNS
Cannot find server - Micr...
Cannot find server - Micr...
5:10 PM

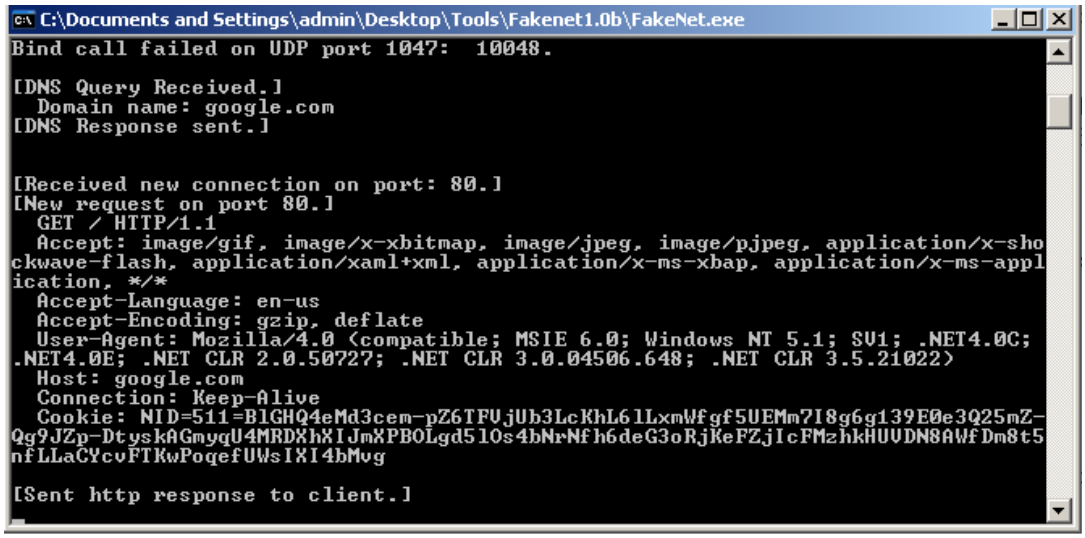
Sample 2


Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://windowsupdate.microsoft.com/
The page cannot be displayed
The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.
To attempt fixing network connectivity problems, click Tools, and then click "Diagnose Connection Problems..."
Other options to try:
Click the Refresh button, or try again later.
If you typed the page address in the Address bar, make sure that it is spelled correctly.
To check your connection settings, click the Tools menu, and then click Internet Options. On the Connections tab, click Settings. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
See if your Internet connection settings are being detected. You can set Microsoft Windows to examine your network and automatically discover network connection settings (if your network administrator has enabled this setting).
Done
Internet
ApateDNS
Capture Window
DNS Hex View
Time
Domain Requested
DNS Returned
17:07:11 facebook.com NXDOMAIN
17:07:14 auto.search.msn.com NXDOMAIN
17:08:47 facebook.com NXDOMAIN
17:08:49 auto.search.msn.com NXDOMAIN
17:08:49 www.facebook.com.com NXDOMAIN
17:08:49 www.facebook.com.org NXDOMAIN
17:08:49 www.facebook.com.net NXDOMAIN
17:08:49 www.facebook.com.edu NXDOMAIN
17:08:49 auto.search.msn.com NXDOMAIN
17:09:20 auto.search.msn.com FOUND
17:09:32 google.com NXDOMAIN
17:10:44 www.malwareanalysisbook.com NXDOMAIN
17:11:23 windowsupdate.microsoft.com NXDOMAIN
17:11:23 www.practicalmalwareanalysis.com NXDOMAIN
[+] 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 3 NXDOMAIN replies to clients
[+] Server started at 17:06:15 successfully.
DNS Reply IP (Default: Current Gatway/DNS):
# of NXDOMAIN's: 3
Selected Interface: AMD PCNET Family PCI Ethernet Adapter - Packet Sc
Start Server
Stop Server
Start
7 Windows Explorer
Command Prompt
ApateDNS
Cannot find server - Micr...
Cannot find server - Micr...
5:11 PM

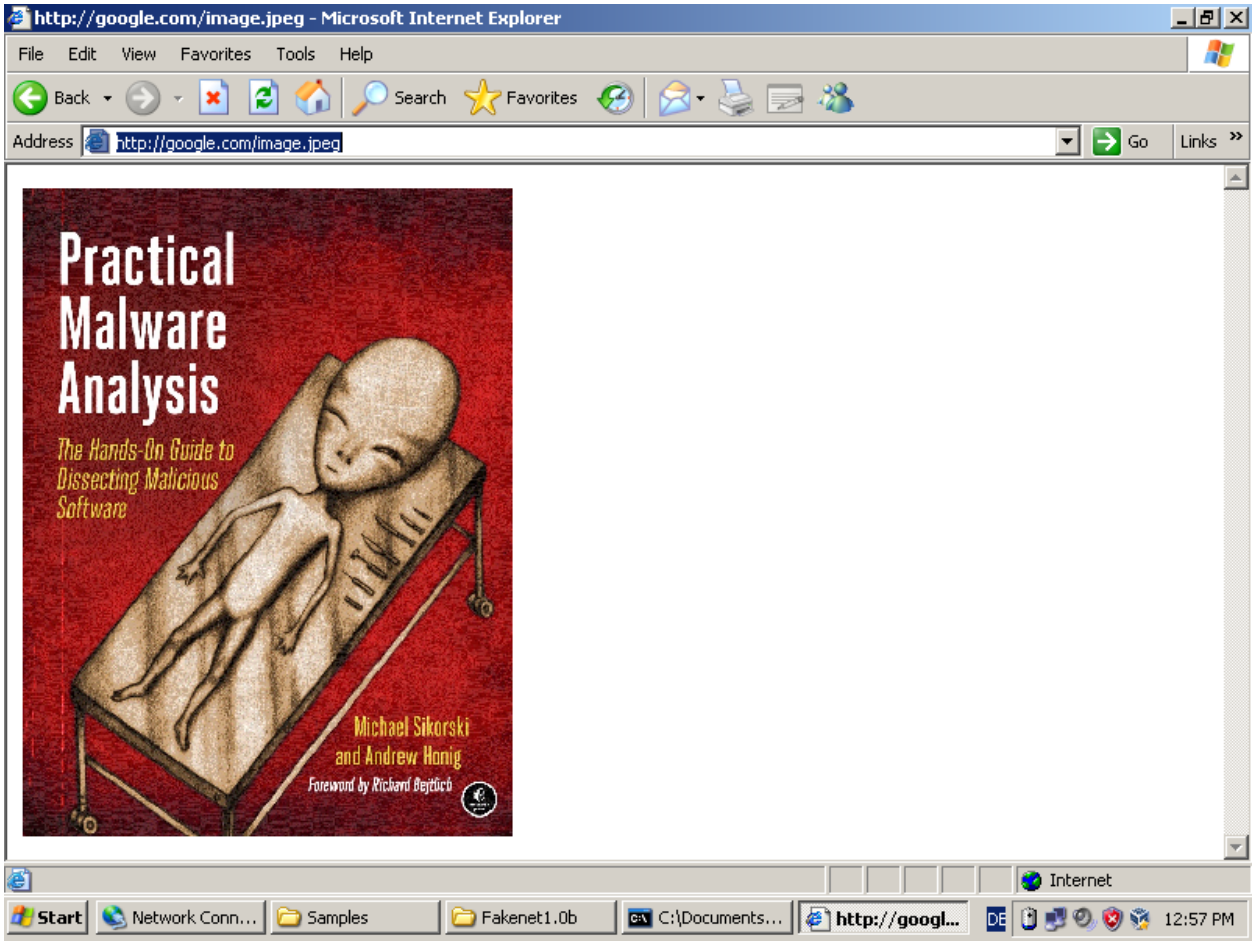
Part-2: Using FakeNet

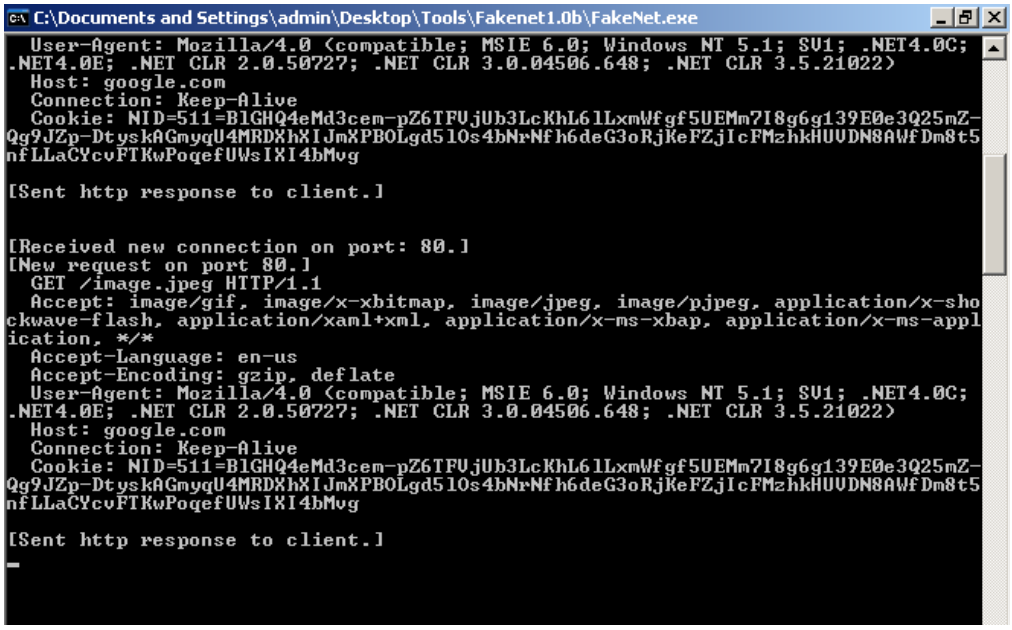
1.



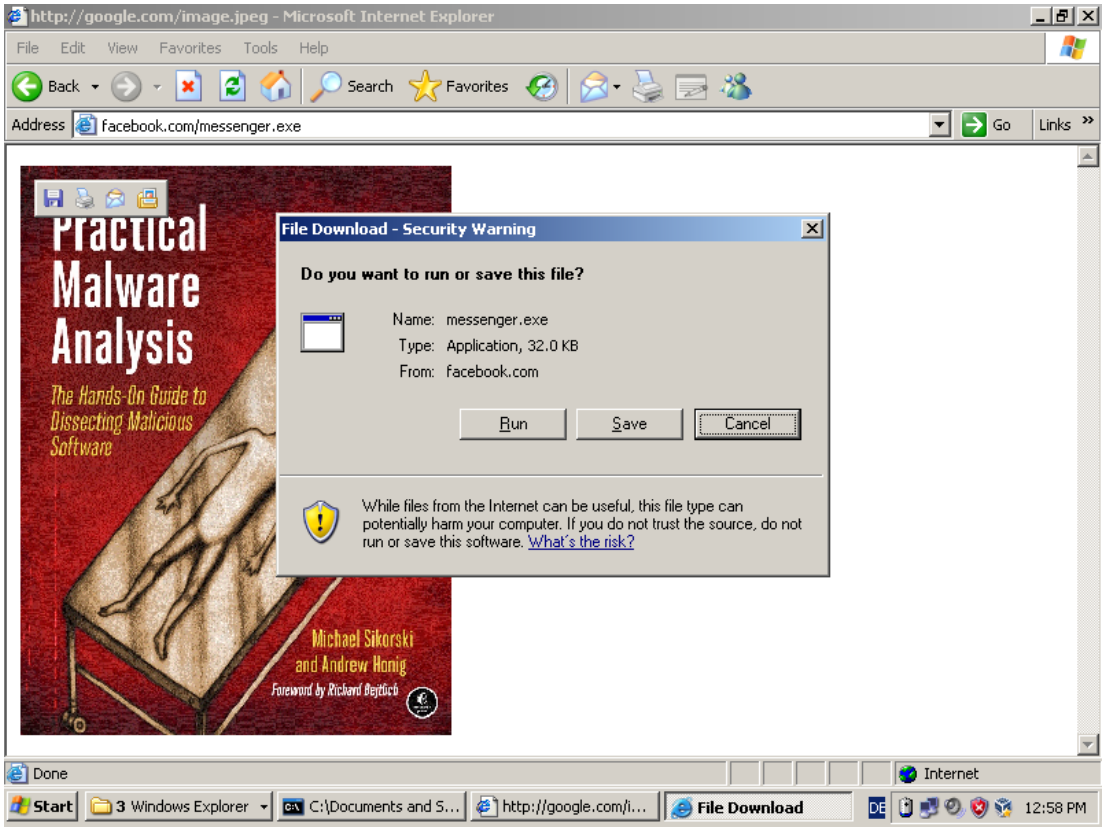


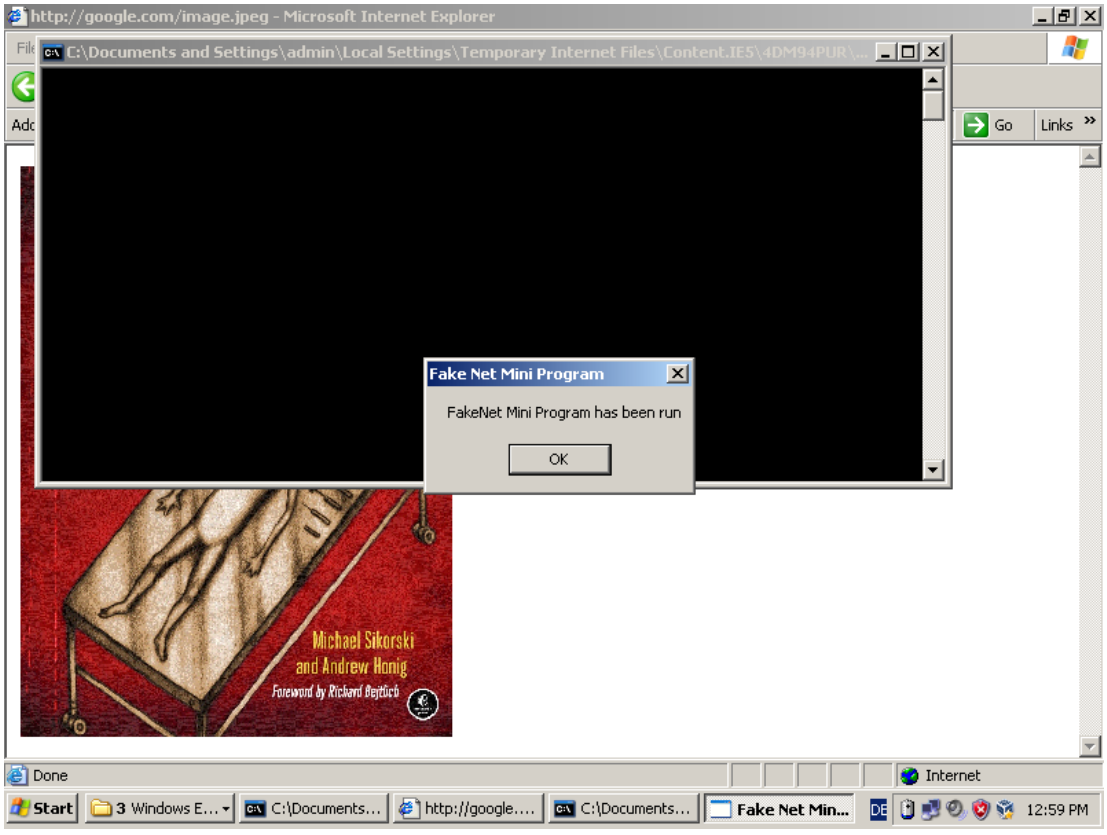
2.


http://google.com/image.jpeg - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://google.com/image.jpeg
Go Links
Practical Malware Analysis
The Hands-On Guide to Dissecting Malicious Software
Michael Sikorski and Andrew Honig
Foreword by Richard Bejtlich
Internet
Start
Network Conn...
Samples
Fakenet1.0b
C:\Documents...
http://googl...
12:57 PM

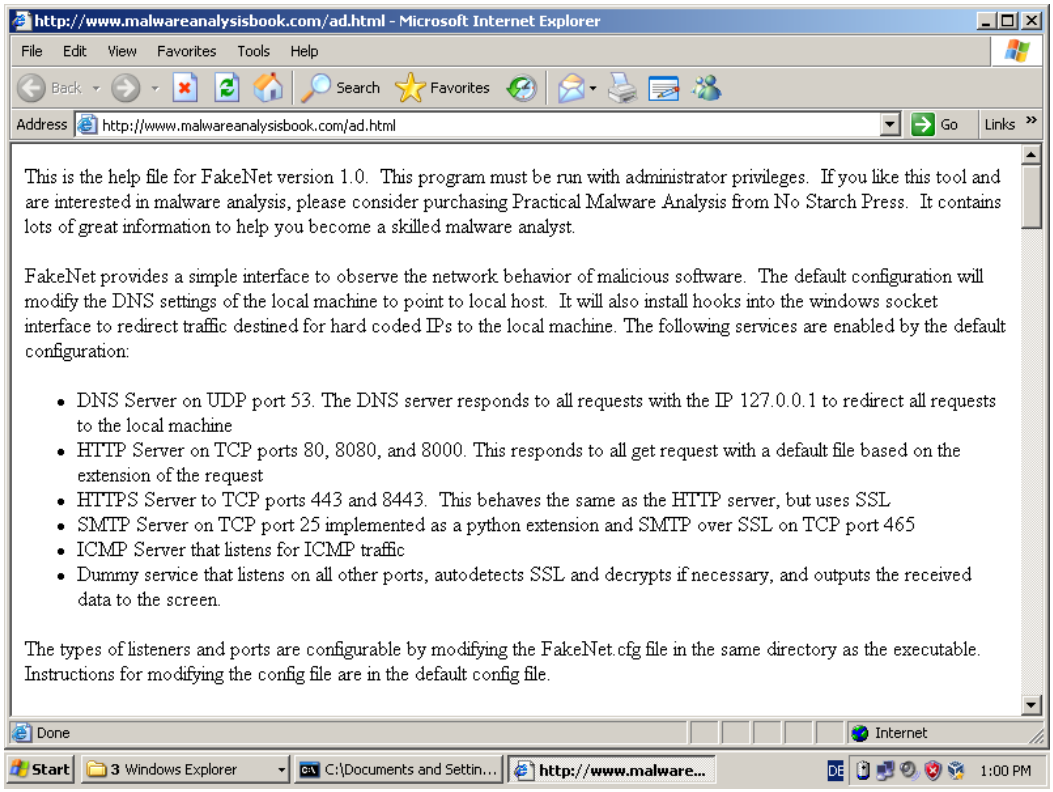

C:\Documents and Settings\admin\Desktop\Tools\Fakenet1.0b\FakeNet.exe
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: google.com
Connection: Keep-Alive
Cookie: NID=511=B1GHQ4eMd3cem-pZ6TFVjUb3LcKhL61LxmWfgf5UEMm7I8g6g139E0e3Q25mZ-Qg9JZp-DtyskAGmyqU4MRDXhXIJmXPBOLgd51Os4bNrNfh6deG3oRjKeFZjIcFMzhkHUVDN8AWfDm8t5nfLLaCYcvFTKwPoqefUWsIXI4bMvg
[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-shockwave-flash, application/xaml+xml, application/x-ms-xbap, application/x-ms-application, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .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-pZ6TFVjUb3LcKhL61LxmWfgf5UEMm7I8g6g139E0e3Q25mZ-Qg9JZp-DtyskAGmyqU4MRDXhXIJmXPBOLgd51Os4bNrNfh6deG3oRjKeFZjIcFMzhkHUVDN8AWfDm8t5nfLLaCYcvFTKwPoqefUWsIXI4bMvg
[Sent http response to client.]

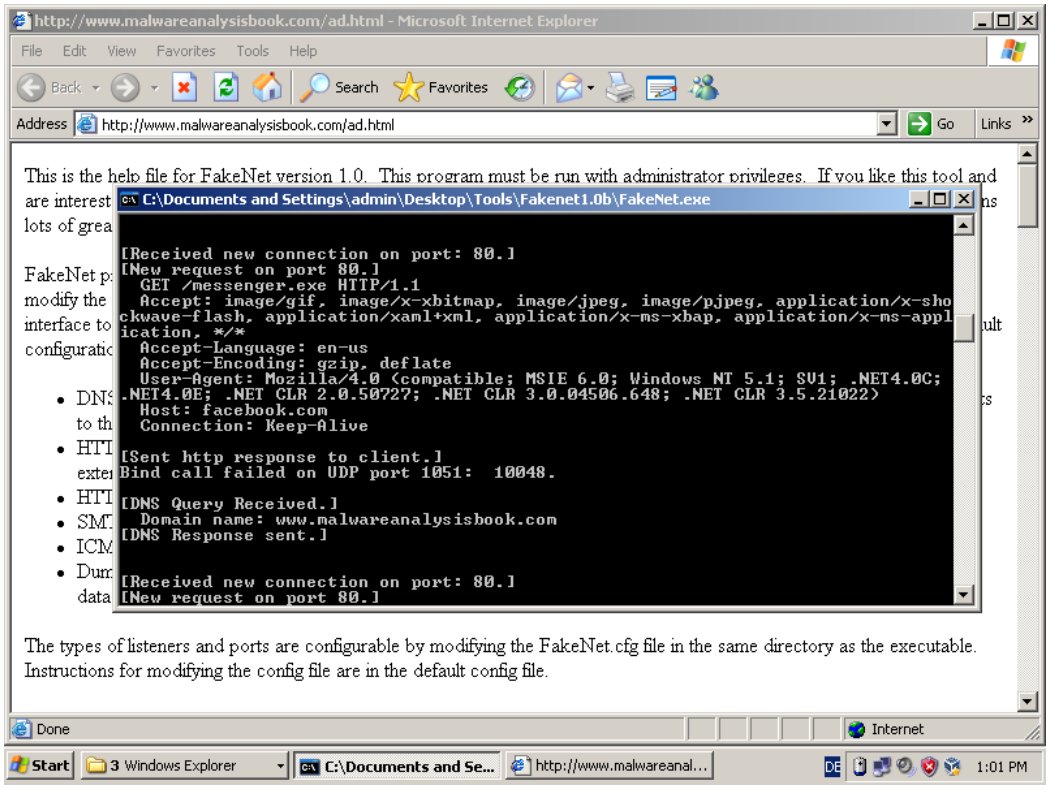
3.


http://google.com/image.jpeg - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address facebook.com/messenger.exe
Go Links
Practical Malware Analysis
The Hands-On Guide to Dissecting Malicious Software
Michael Sikorski and Andrew Honig
Foreword by Richard Bejtlich
File Download - Security Warning
Do you want to run or save this file?
Name: messenger.exe
Type: Application, 32.0 KB
From: facebook.com
Run
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?
Done
Internet
Start
3 Windows Explorer
C:\Documents and S...
http://google.com/i...
File Download
12:58 PM

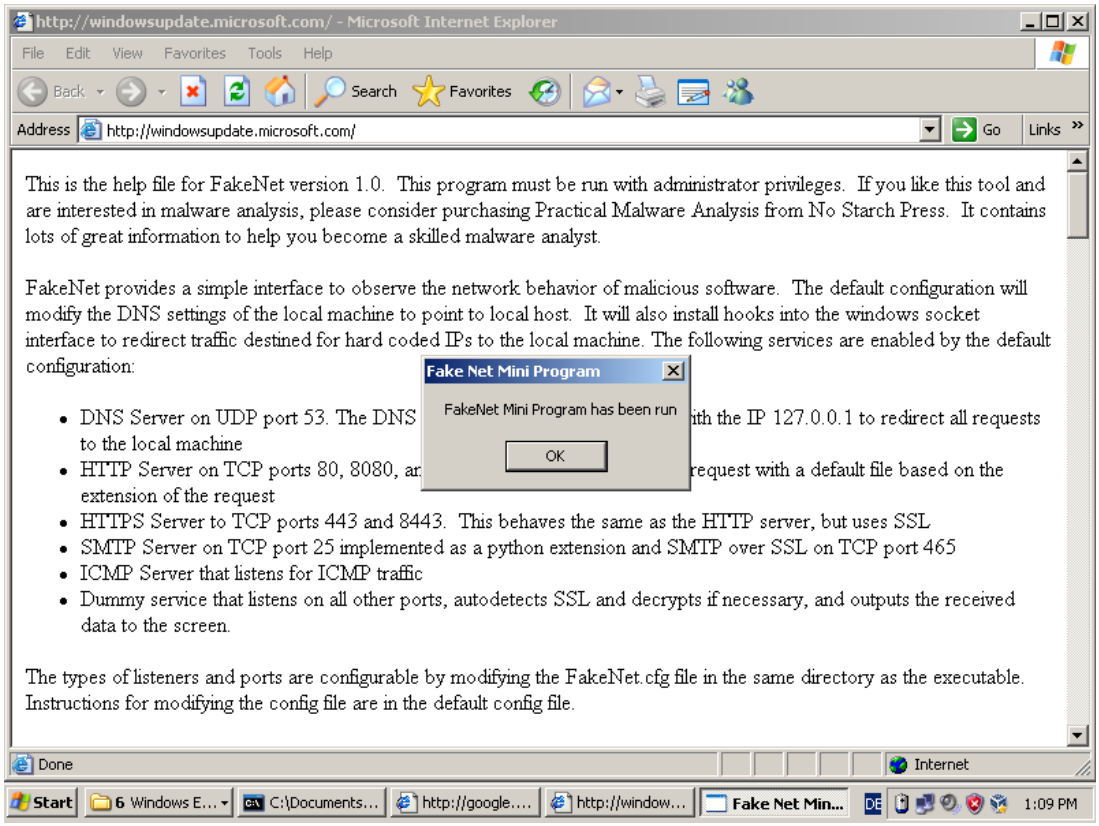

http://google.com/image.jpeg - Microsoft Internet Explorer
C:\Documents and Settings\admin\Local Settings\Temporary Internet Files\Content.IE5\4DM94PUR\...
Go Links
Fake Net Mini Program
FakeNet Mini Program has been run
OK
Michael Sikorski and Andrew Honig
Foreword by Richard Bejtlich
Done
Internet
Start
3 Windows E...
C:\Documents...
http://google....
C:\Documents...
Fake Net Min...
12:59 PM

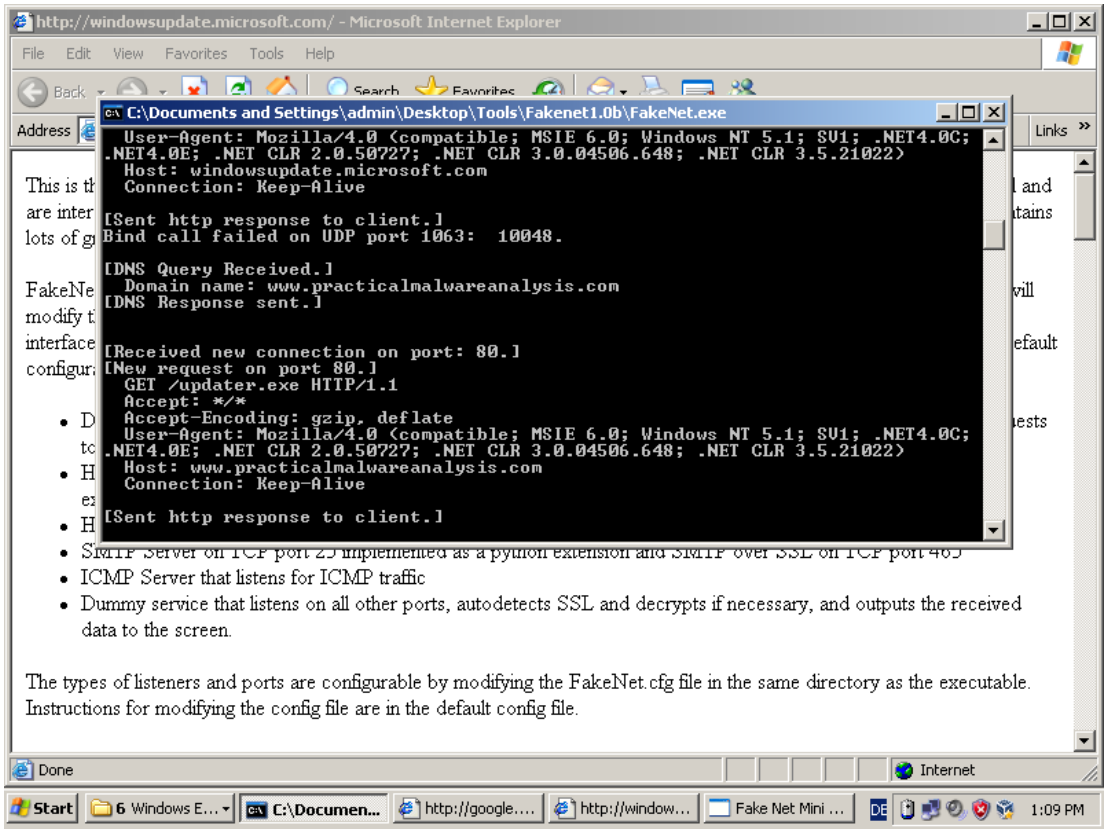
Sample 1


http://www.malwareanalysisbook.com/ad.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.malwareanalysisbook.com/ad.html
Go Links
This is the help file for FakeNet version 1.0. This program must be run with administrator privileges. If you like this tool and are interested in malware analysis, please consider purchasing Practical Malware Analysis from No Starch Press. It contains lots of great information to help you become a skilled malware analyst.
FakeNet provides a simple interface to observe the network behavior of malicious software. The default configuration will modify the DNS settings of the local machine to point to local host. It will also install hooks into the windows socket interface to redirect traffic destined for hard coded IPs to the local machine. The following services are enabled by the default configuration:
DNS Server on UDP port 53. The DNS server responds to all requests with the IP 127.0.0.1 to redirect all requests to the local machine
HTTP Server on TCP ports 80, 8080, and 8000. This responds to all get request with a default file based on the extension of the request
HTTPS Server to TCP ports 443 and 8443. This behaves the same as the HTTP server, but uses SSL
SMTP Server on TCP port 25 implemented as a python extension and SMTP over SSL on TCP port 465
ICMP Server that listens for ICMP traffic
Dummy service that listens on all other ports, autodetects SSL and decrypts if necessary, and outputs the received data to the screen.
The types of listeners and ports are configurable by modifying the FakeNet.cfg file in the same directory as the executable. Instructions for modifying the config file are in the default config file.
Done
Internet
Start
3 Windows Explorer
C:\Documents and Settin...
http://www.malware...
1:00 PM

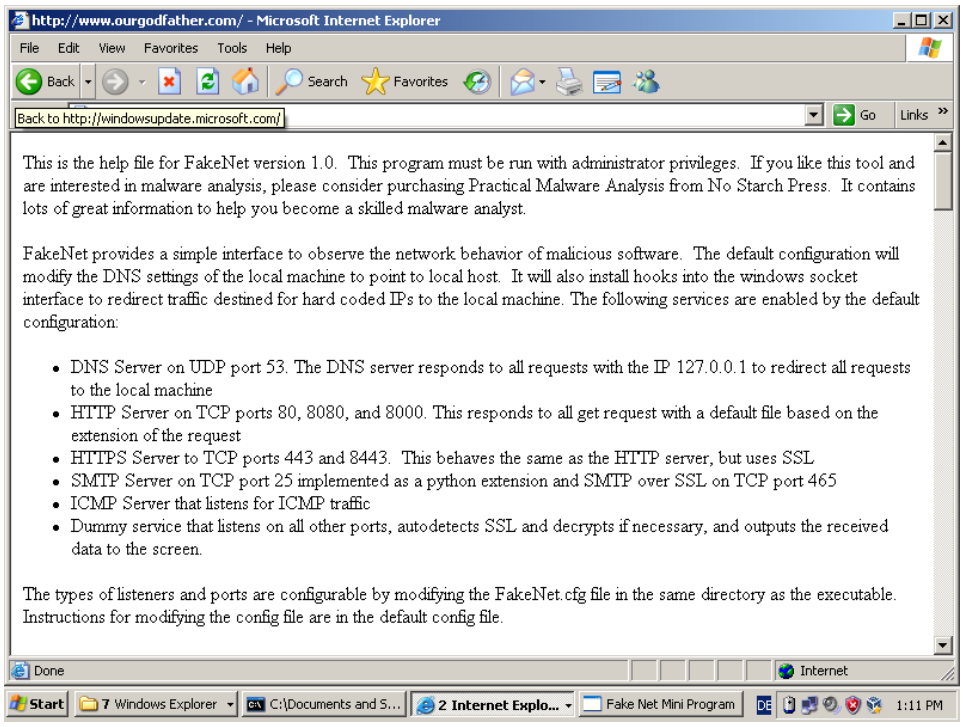

http://www.malwareanalysisbook.com/ad.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.malwareanalysisbook.com/ad.html
Go Links
C:\Documents and Settings\admin\Desktop\Tools\Fakenet1.0b\FakeNet.exe
[Received new connection on port: 80.]
[New request on port 80.]
GET /messenger.exe HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/xaml+xml, application/x-ms-xbap, application/x-ms-application, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: facebook.com
Connection: Keep-Alive
[Sent http response to client.]
Bind call failed on UDP port 1051: 10048.
[DNS Query Received.]
Domain name: www.malwareanalysisbook.com
[DNS Response sent.]
[Received new connection on port: 80.]
[New request on port 80.]
The types of listeners and ports are configurable by modifying the FakeNet.cfg file in the same directory as the executable. Instructions for modifying the config file are in the default config file.
Done
Internet
Start
3 Windows Explorer
C:\Documents and Se...
http://www.malwareanal...
1:01 PM

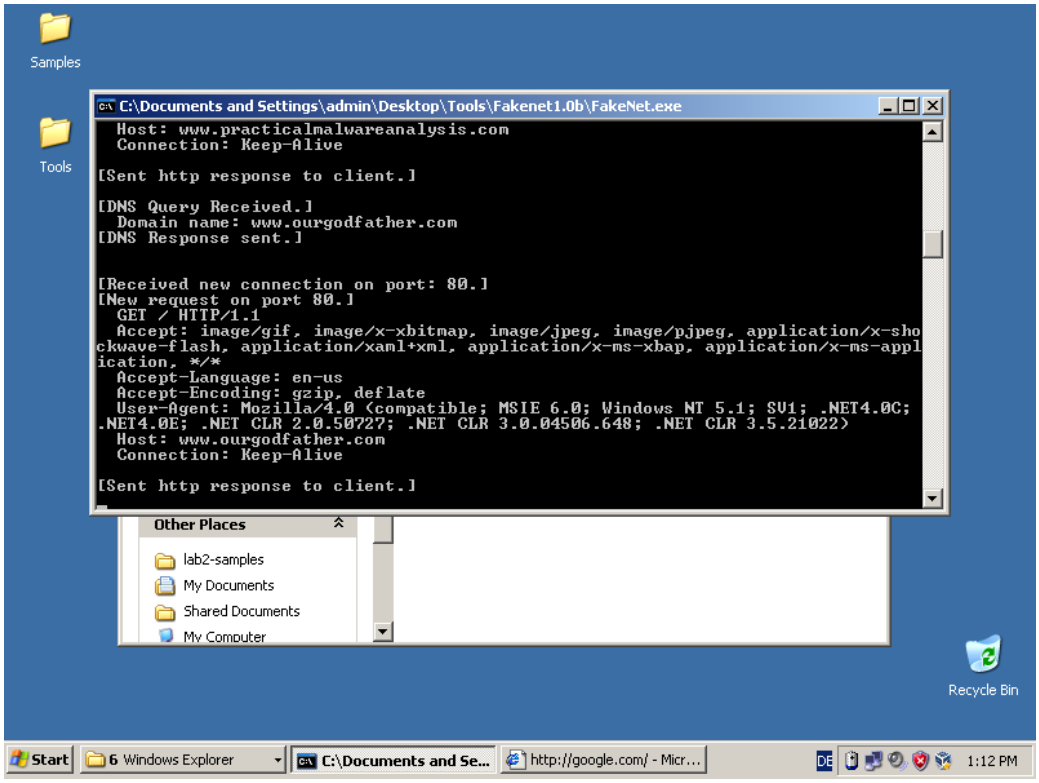
Sample 2


http://windowsupdate.microsoft.com/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://windowsupdate.microsoft.com/
Go Links
This is the help file for FakeNet version 1.0. This program must be run with administrator privileges. If you like this tool and are interested in malware analysis, please consider purchasing Practical Malware Analysis from No Starch Press. It contains lots of great information to help you become a skilled malware analyst.
FakeNet provides a simple interface to observe the network behavior of malicious software. The default configuration will modify the DNS settings of the local machine to point to local host. It will also install hooks into the windows socket interface to redirect traffic destined for hard coded IPs to the local machine. The following services are enabled by the default configuration:
Fake Net Mini Program
FakeNet Mini Program has been run
OK
DNS Server on UDP port 53. The DNS
ith the IP 127.0.0.1 to redirect all requests to the local machine
HTTP Server on TCP ports 80, 8080, ar
request with a default file based on the extension of the request
HTTPS Server to TCP ports 443 and 8443. This behaves the same as the HTTP server, but uses SSL
SMTP Server on TCP port 25 implemented as a python extension and SMTP over SSL on TCP port 465
ICMP Server that listens for ICMP traffic
Dummy service that listens on all other ports, autodetects SSL and decrypts if necessary, and outputs the received data to the screen.
The types of listeners and ports are configurable by modifying the FakeNet.cfg file in the same directory as the executable. Instructions for modifying the config file are in the default config file.
Done
Internet
Start
6 Windows E...
C:\Documents...
http://google....
http://window...
Fake Net Min...
1:09 PM

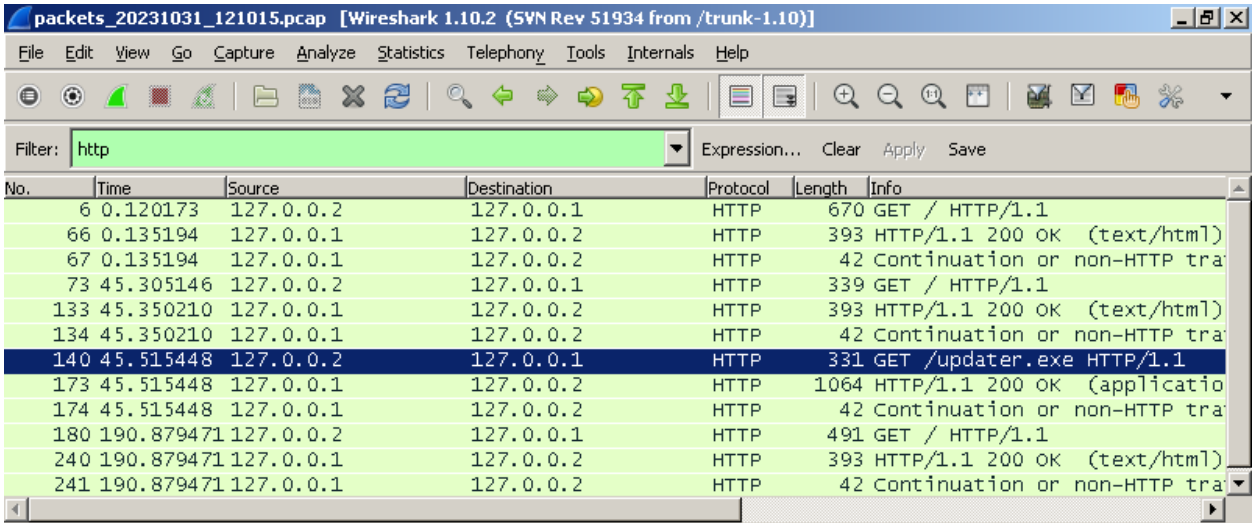

http://windowsupdate.microsoft.com/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
C:\Documents and Settings\admin\Desktop\Tools\Fakenet1.0b\FakeNet.exe
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: windowsupdate.microsoft.com
Connection: Keep-Alive
[Sent http response to client.]
Bind call failed on UDP port 1063: 10048.
[DNS Query Received.]
Domain name: www.practicalmalwareanalysis.com
[DNS Response sent.]
[Received new connection on port: 80.]
[New request on port 80.]
GET /updater.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: www.practicalmalwareanalysis.com
Connection: Keep-Alive
[Sent http response to client.]
ICMP Server that listens for ICMP traffic
Dummy service that listens on all other ports, autodetects SSL and decrypts if necessary, and outputs the received data to the screen.
The types of listeners and ports are configurable by modifying the FakeNet.cfg file in the same directory as the executable. Instructions for modifying the config file are in the default config file.
Done
Internet
Start
6 Windows E...
C:\Documen...
http://google....
http://window...
Fake Net Mini ...
1:09 PM

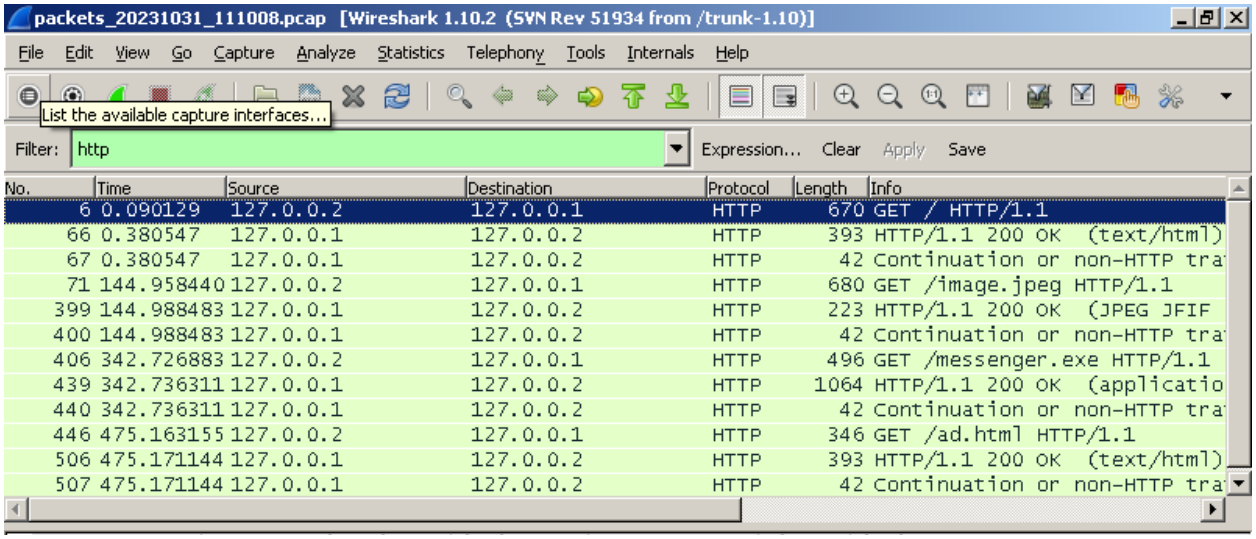
Messenger


http://www.ourgodfather.com/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Back to http://windowsupdate.microsoft.com/
Go Links
This is the help file for FakeNet version 1.0. This program must be run with administrator privileges. If you like this tool and are interested in malware analysis, please consider purchasing Practical Malware Analysis from No Starch Press. It contains lots of great information to help you become a skilled malware analyst.
FakeNet provides a simple interface to observe the network behavior of malicious software. The default configuration will modify the DNS settings of the local machine to point to local host. It will also install hooks into the windows socket interface to redirect traffic destined for hard coded IPs to the local machine. The following services are enabled by the default configuration:
DNS Server on UDP port 53. The DNS server responds to all requests with the IP 127.0.0.1 to redirect all requests to the local machine
HTTP Server on TCP ports 80, 8080, and 8000. This responds to all get request with a default file based on the extension of the request
HTTPS Server to TCP ports 443 and 8443. This behaves the same as the HTTP server, but uses SSL
SMTP Server on TCP port 25 implemented as a python extension and SMTP over SSL on TCP port 465
ICMP Server that listens for ICMP traffic
Dummy service that listens on all other ports, autodetects SSL and decrypts if necessary, and outputs the received data to the screen.
The types of listeners and ports are configurable by modifying the FakeNet.cfg file in the same directory as the executable. Instructions for modifying the config file are in the default config file.
Done
Internet
Start
7 Windows Explorer
C:\Documents and S...
2 Internet Explo...
Fake Net Mini Program
1:11 PM


Samples
Tools
C:\Documents and Settings\admin\Desktop\Tools\Fakenet1.0b\FakeNet.exe
Host: www.practicalmalwareanalysis.com
Connection: Keep-Alive
[Sent http response to client.]
[DNS Query Received.]
Domain name: www.ourgodfather.com
[DNS Response sent.]
[Received new connection on port: 80.]
[New request on port 80.]
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/xaml+xml, application/x-ms-xbap, application/x-ms-application, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: www.ourgodfather.com
Connection: Keep-Alive
[Sent http response to client.]
Other Places
lab2-samples
My Documents
Shared Documents
My Computer
Recycle Bin
Start
6 Windows Explorer
C:\Documents and Se...
http://google.com/ - Micr...
1:12 PM

PCB file in Wireshark





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.