Comments and Understanding:

ApateDNS allows us to manipulate DNS responses. If there is malware on a computer which is then called a victim computer, the malware can send requests to the server. With ApateDNS, we can manipulate the response coming from the server that can confuse malware and it will behave in different ways.

Remnux Linux is acting as a DNS server. Through INetSim it can be used to simulate responses such as DNS, HTTP, FTP and many other network services. So when a query is sent from Windows XP, the INetSim provides a fake or controlled response. This can help analyze malware response.
The Remnux server actually intercepts the request and sends back a simulated response. So in this case the response on every http request is a static fake page (apparently) but actually Windows XP thinks of it as the request being served and the server has responded to the query. So If an image file is requested a fake image file is returned as response.

The NXDomain(domain does not exist) values 0,1,2,3 are actually used to trick the malware. When it gets a non-existent domain response, it might try a new domain/url whereas ApateDNS keeps recording the domains requested. This can help identify all the domains that are associated with a malware.

With IP settings, we have set up a controlled environment to analyze malware.

Activities

On opening the browser after running ApateDNS on Windows XP VM, I see this in internet explorer.

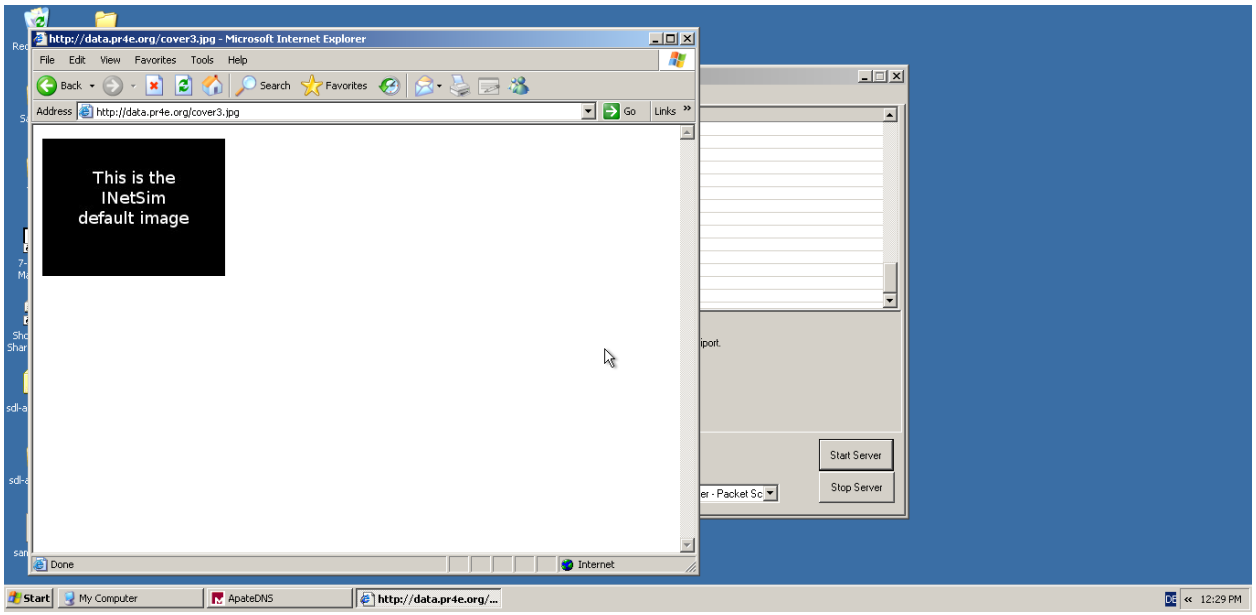
This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document

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?

I sent a request to http://data.pr4e.org/cover3.jpg

One record was captured in ApateDNS and dns returned: found.



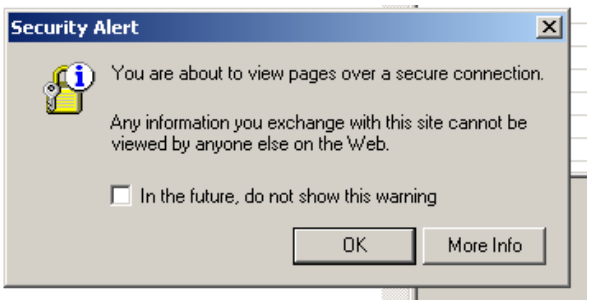
12:28:55	data.pr4e.org	FOUND

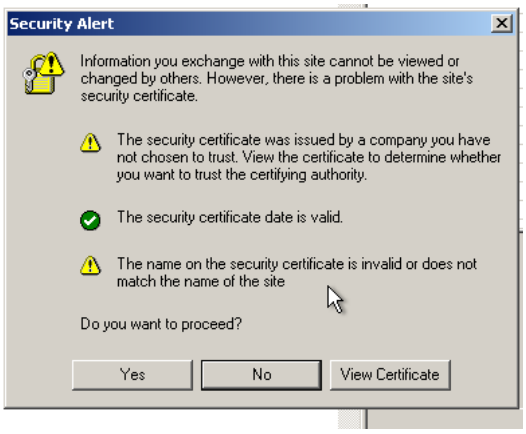
2. Send another request for a web page through HTTPS. What do you notice?

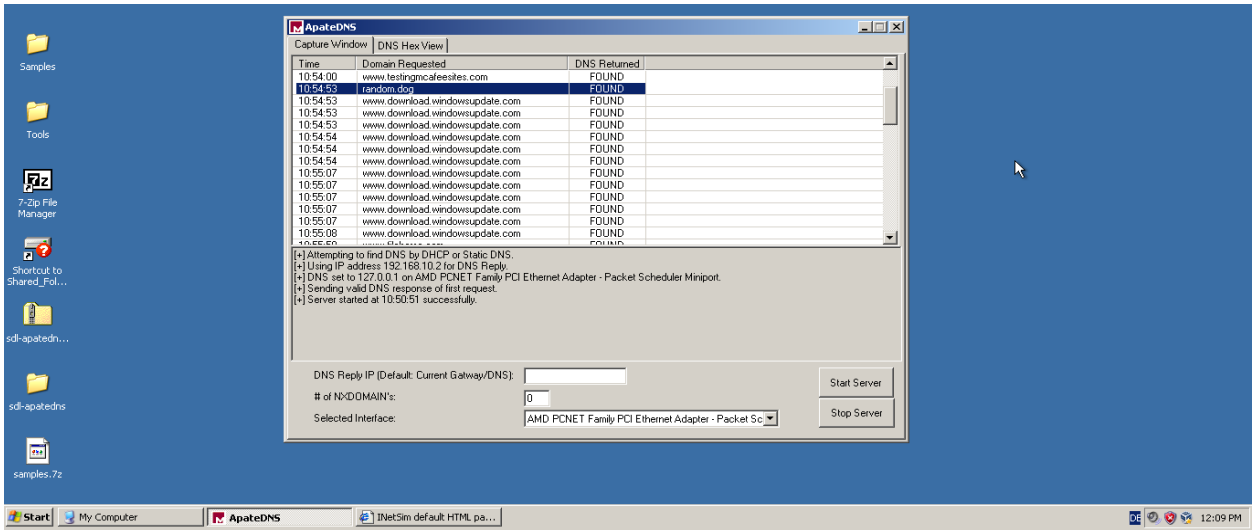
I sent a request to https://random.dog

It was captured in ApateDNS and dns returned: found.

These two popups appeared first.





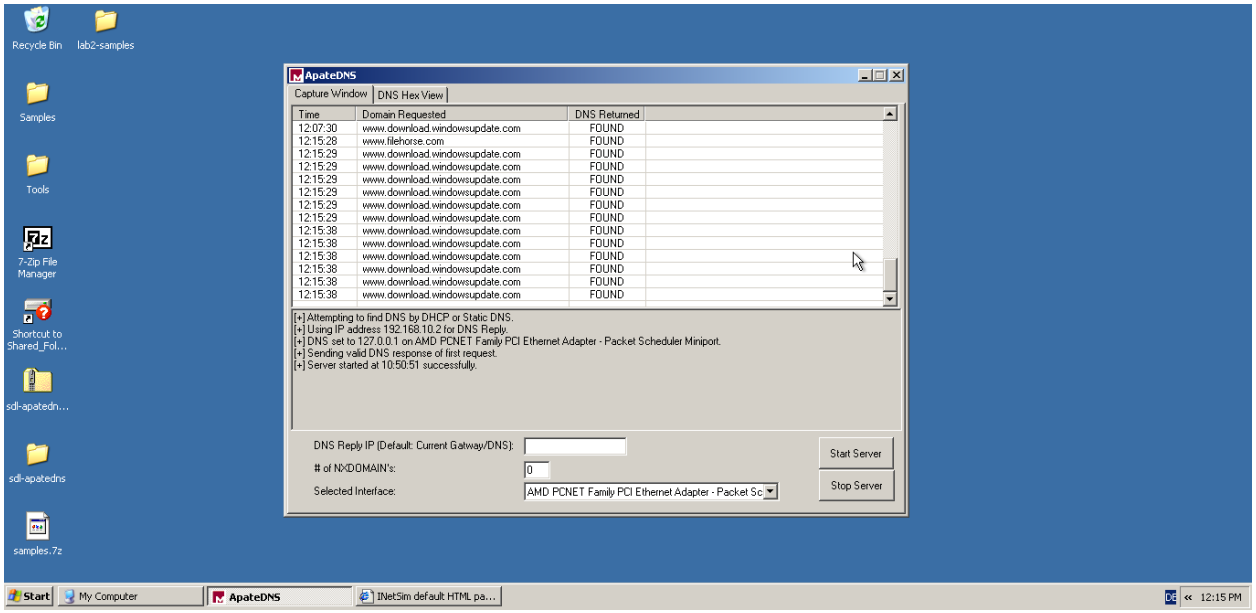


On visiting this website random.dog(https request), 12 further requests can be observed.

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

I sent a request to
https://www.filehorse.com/download-123-photo-viewer/download/

It was captured in ApateDNS as www.filehorse.com and dns returned: found.



A response similar to the https request made earlier can be observed, that is, afterwards 12 further requests were made for www.download.windowsupdate.com.
.

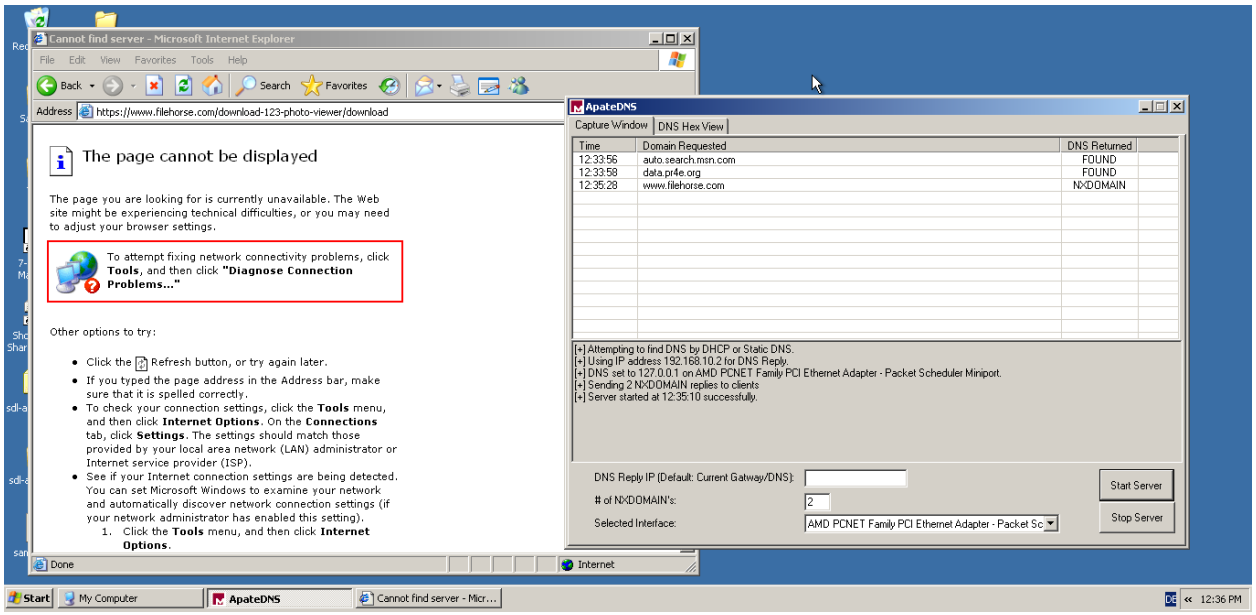
NX Domain Values 0,1,2,3 :

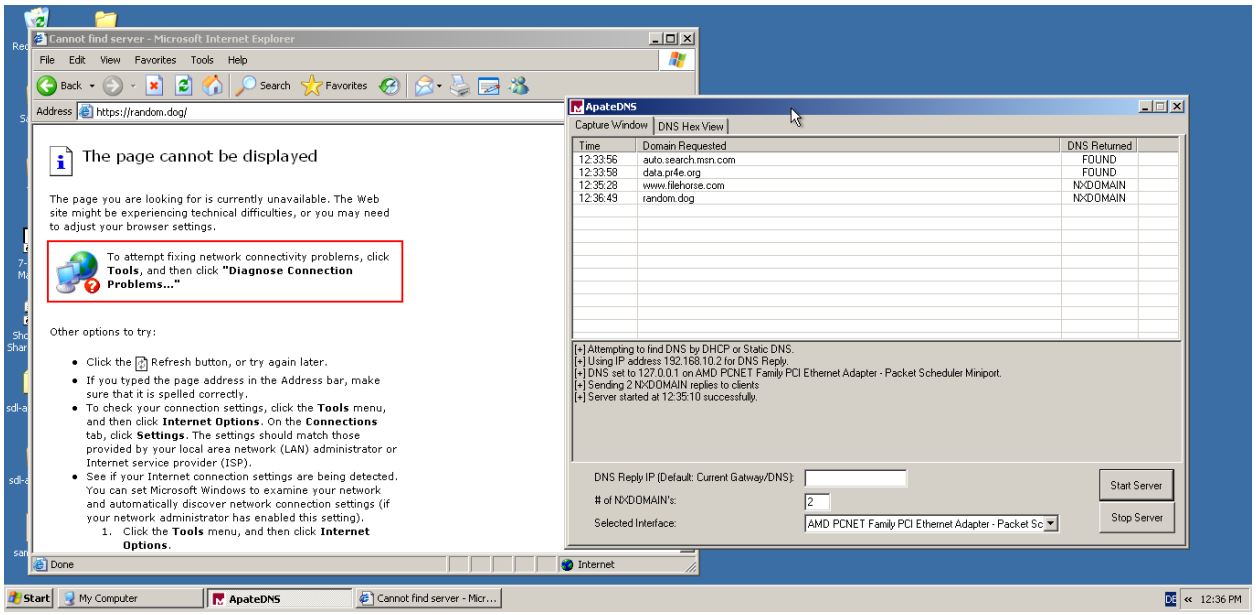
On changing NX Domain values, the web pages were not displayed and problems described here are:

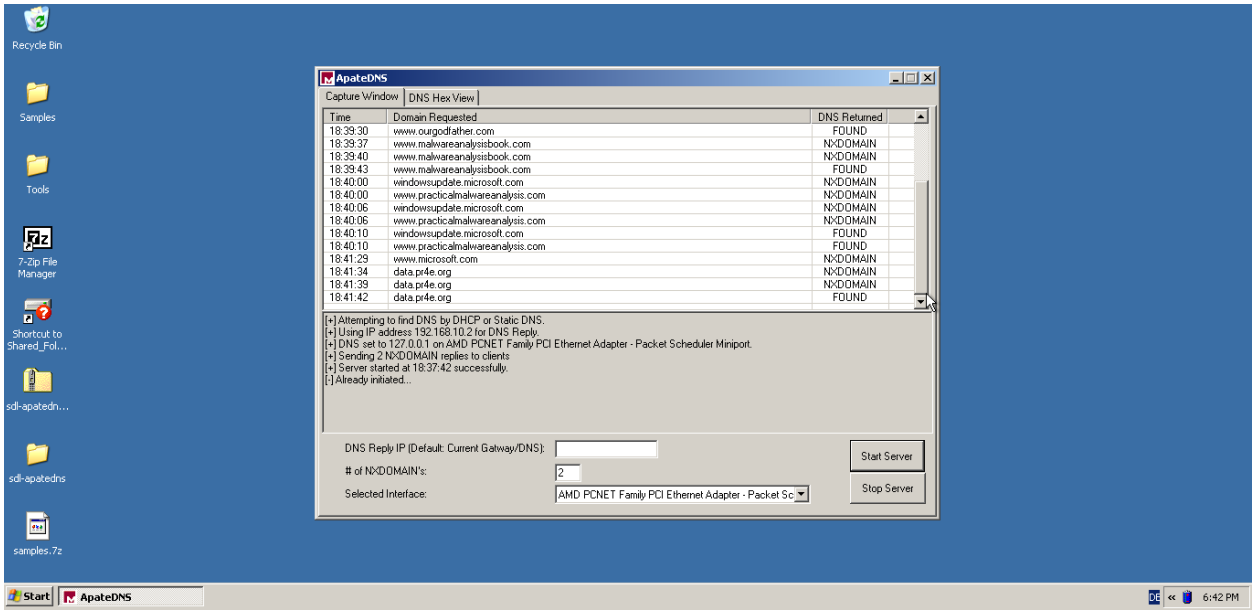
- Internet connection problem
- Security issues
- DNS server error

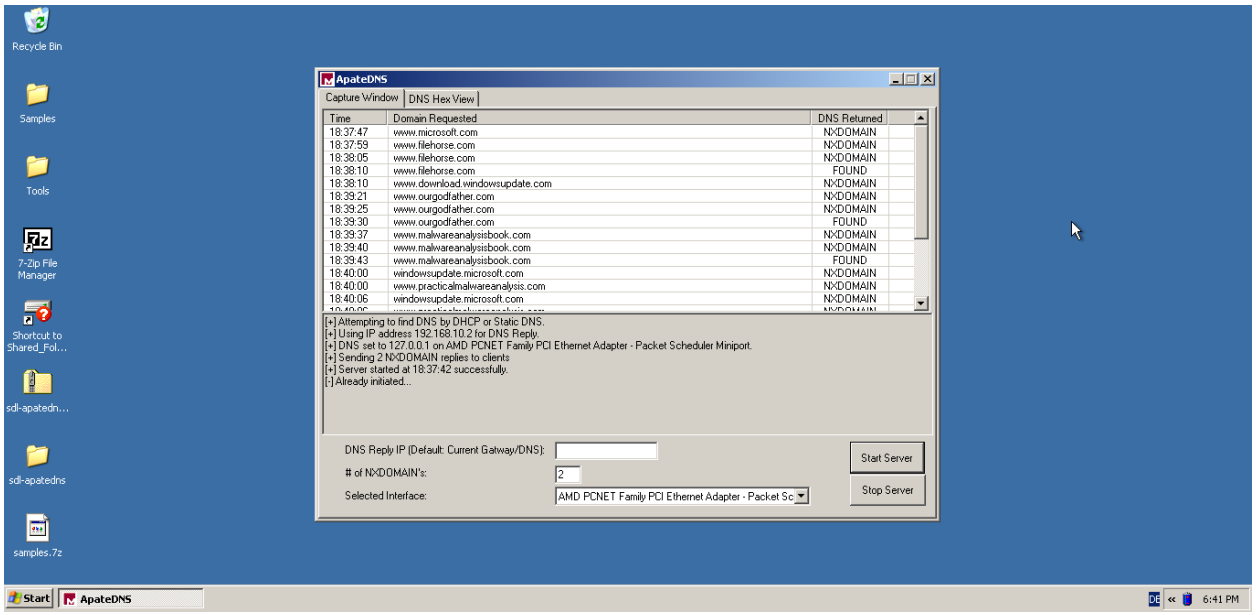
Actually, by setting the NX domain value we are telling ApateDNS to manipulate the response from the server. So according to the value of NXDomain, the response to the request is that the domain is non-existent.

- If the value is 1, the first time when something is requested, response will be non-existent. Second time there will be a valid response.
- If the value is 2, the first and second time when something is requested, response will be non-existent. Third time there will be a valid response.
- If the value is 3, for the first three requests, the response will be non-existent. Fourth time there will be a valid response.


Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://www.filehorse.com/download-123-photo-viewer/download
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).
1. Click the Tools menu, and then click Internet Options.
Done
Internet
ApateDNS
Capture Window
DNS Hex View
Time
Domain Requested
DNS Returned
12:33:56 auto.search.msn.com FOUND
12:33:58 data.pr4e.org FOUND
12:35:28 www.filehorse.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 2 NXDOMAIN replies to clients
[+] Server started at 12:35:10 successfully.
DNS Reply IP (Default: Current Gatway/DNS):
# of NXDOMAIN's:
2
Selected Interface:
AMD PCNET Family PCI Ethernet Adapter - Packet Sc
Start Server
Stop Server
Start
My Computer
ApateDNS
Cannot find server - Micr...
12:36 PM


Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://random.dog/
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).
1. Click the Tools menu, and then click Internet Options.
Done
Internet
ApateDNS
Capture Window
DNS Hex View
Time
Domain Requested
DNS Returned
12:33:56 auto.search.msn.com FOUND
12:33:58 data.pr4e.org FOUND
12:35:28 www.filehorse.com NXDOMAIN
12:36:49 random.dog 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 2 NXDOMAIN replies to clients
[+] Server started at 12:35:10 successfully.
DNS Reply IP (Default: Current Gatway/DNS):
# of NXDOMAIN's:
2
Selected Interface:
AMD PCNET Family PCI Ethernet Adapter - Packet Sc
Start Server
Stop Server
Start
My Computer
ApateDNS
Cannot find server - Micr...
12:36 PM


Recycle Bin
Samples
Tools
7-Zip File Manager
Shortcut to Shared_Fol...
sdl-apatedn...
sdl-apatedns
samples.7z
ApateDNS
Capture Window
DNS Hex View
Time
Domain Requested
DNS Returned
18:39:30 www.ourgodfather.com FOUND
18:39:37 www.malwareanalysisbook.com NXDOMAIN
18:39:40 www.malwareanalysisbook.com NXDOMAIN
18:39:43 www.malwareanalysisbook.com FOUND
18:40:00 windowsupdate.microsoft.com NXDOMAIN
18:40:00 www.practicalmalwareanalysis.com NXDOMAIN
18:40:06 windowsupdate.microsoft.com NXDOMAIN
18:40:06 www.practicalmalwareanalysis.com NXDOMAIN
18:40:10 windowsupdate.microsoft.com FOUND
18:40:10 www.practicalmalwareanalysis.com FOUND
18:41:29 www.microsoft.com NXDOMAIN
18:41:34 data.pr4e.org NXDOMAIN
18:41:39 data.pr4e.org NXDOMAIN
18:41:42 data.pr4e.org 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 2 NXDOMAIN replies to clients
[+] Server started at 18:37:42 successfully.
[-] Already initiated...
DNS Reply IP (Default: Current Gatway/DNS):
# of NXDOMAIN's:
2
Selected Interface:
AMD PCNET Family PCI Ethernet Adapter - Packet Sc
Start Server
Stop Server
Start
ApateDNS
6:42 PM


Recycle Bin
Samples
Tools
7-Zip File Manager
Shortcut to Shared_Fol...
sdl-apatedn...
sdl-apatedns
samples.7z
ApateDNS
Capture Window
DNS Hex View
Time
Domain Requested
DNS Returned
18:37:47 www.microsoft.com NXDOMAIN
18:37:59 www.filehorse.com NXDOMAIN
18:38:05 www.filehorse.com NXDOMAIN
18:38:10 www.filehorse.com FOUND
18:38:10 www.download.windowsupdate.com NXDOMAIN
18:39:21 www.ourgodfather.com NXDOMAIN
18:39:25 www.ourgodfather.com NXDOMAIN
18:39:30 www.ourgodfather.com FOUND
18:39:37 www.malwareanalysisbook.com NXDOMAIN
18:39:40 www.malwareanalysisbook.com NXDOMAIN
18:39:43 www.malwareanalysisbook.com FOUND
18:40:00 windowsupdate.microsoft.com NXDOMAIN
18:40:00 www.practicalmalwareanalysis.com NXDOMAIN
18:40:06 windowsupdate.microsoft.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 2 NXDOMAIN replies to clients
[+] Server started at 18:37:42 successfully.
[-] Already initiated...
DNS Reply IP (Default: Current Gatway/DNS):
# of NXDOMAIN's:
2
Selected Interface:
AMD PCNET Family PCI Ethernet Adapter - Packet Sc
Start Server
Stop Server
Start
ApateDNS
6:41 PM

4. Unzip the file containing the three malware samples (password: infected). Execute each of them and note/record their network behavior as observed by you and/or logged with the tools.

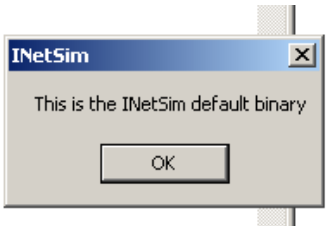
Which domains are the samples trying to contact?

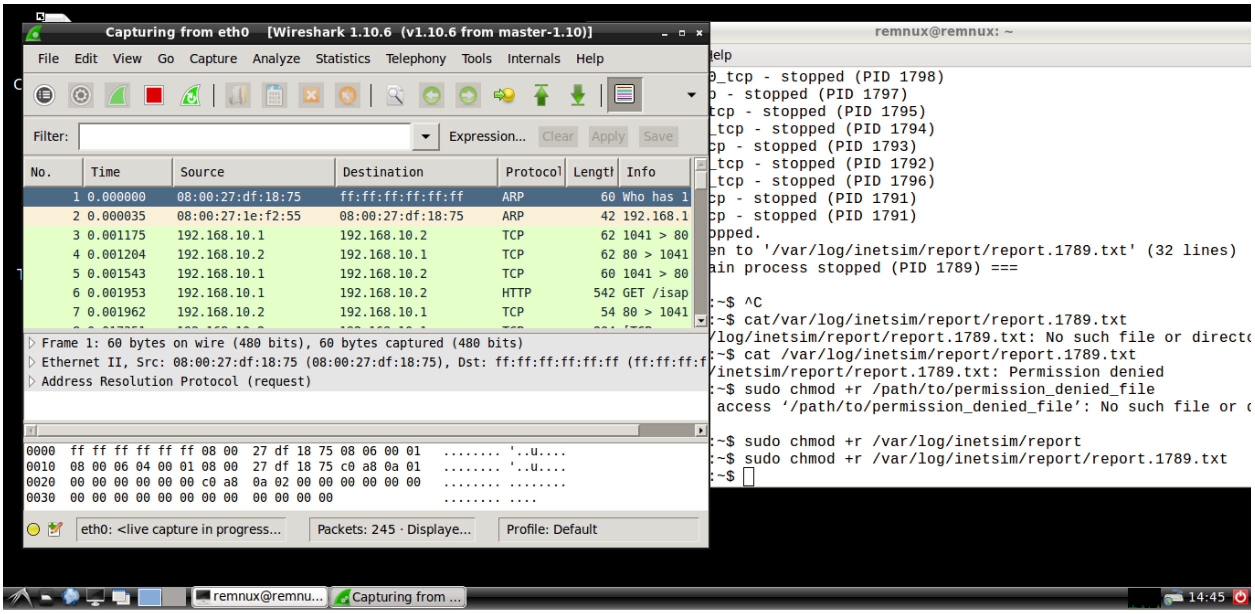
www.ourgodfather.com
www.malwareanalysisbook.com
windowsupdate.microsoft.com
www.practicalmalwareanalysis.com

What http requests (if any) are being made and when do these requests occur?

http://www.ourgodfather.com/
http://www.malwareanalysisbook.com/ad.html
http://windowsupdate.microsoft.com/

All are http requests. Last one also displays a pop up saying "This is the INetSim default binary"





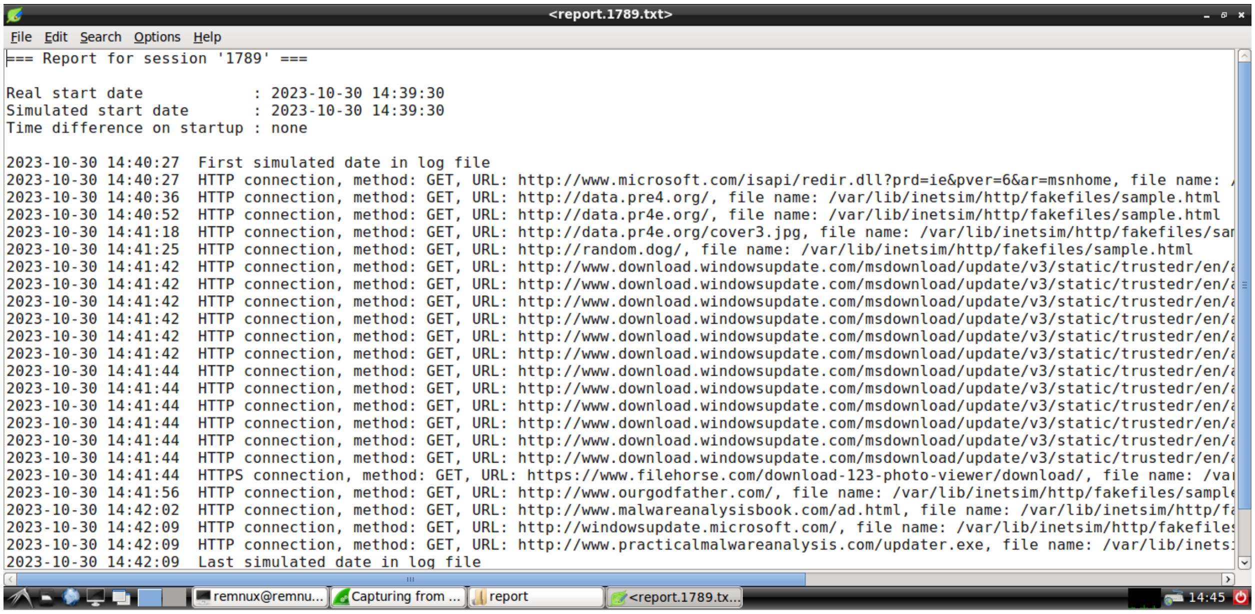
```
No.    Time      Source             Destination        Protocol Length Info
     1 0.000000  08:00:27:df:18:75  ff:ff:ff:ff:ff:ff  ARP          60 Who has 1
     2 0.000035  08:00:27:1e:f2:55  08:00:27:df:18:75  ARP          42 192.168.1
     3 0.001175  192.168.10.1       192.168.10.2       TCP          62 1041 > 80
     4 0.001204  192.168.10.2       192.168.10.1       TCP          62 80 > 1041
     5 0.001543  192.168.10.1       192.168.10.2       TCP          60 1041 > 80
     6 0.001953  192.168.10.1       192.168.10.2       HTTP        542 GET /isap
     7 0.001962  192.168.10.2       192.168.10.1       TCP          54 80 > 1041
```

```
▷ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▷ Ethernet II, Src: 08:00:27:df:18:75 (08:00:27:df:18:75), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:f
▷ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 08 00  27 df 18 75 08 06 00 01   ........ '..u....
0010  08 00 06 04 00 01 08 00  27 df 18 75 c0 a8 0a 01   ........ '..u....
0020  00 00 00 00 00 00 c0 a8  0a 02 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

eth0: <live capture in progress... | Packets: 245 · Displaye... | Profile: Default

```
0_tcp - stopped (PID 1798)
o - stopped (PID 1797)
tcp - stopped (PID 1795)
_tcp - stopped (PID 1794)
cp - stopped (PID 1793)
_tcp - stopped (PID 1792)
_tcp - stopped (PID 1796)
cp - stopped (PID 1791)
cp - stopped (PID 1791)
opped.
en to '/var/log/inetsim/report/report.1789.txt' (32 lines)
ain process stopped (PID 1789) ===

:~$ ^C
:~$ cat/var/log/inetsim/report/report.1789.txt
/log/inetsim/report/report.1789.txt: No such file or directo
:~$ cat /var/log/inetsim/report/report.1789.txt
/inetsim/report/report.1789.txt: Permission denied
:~$ sudo chmod +r /path/to/permission_denied_file
 access ‘/path/to/permission_denied_file’: No such file or c

:~$ sudo chmod +r /var/log/inetsim/report
:~$ sudo chmod +r /var/log/inetsim/report/report.1789.txt
:~$ 
```



```
=== Report for session '1789' ===

Real start date            : 2023-10-30 14:39:30
Simulated start date       : 2023-10-30 14:39:30
Time difference on startup : none

2023-10-30 14:40:27  First simulated date in log file
2023-10-30 14:40:27  HTTP connection, method: GET, URL: http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome, file name: /
2023-10-30 14:40:36  HTTP connection, method: GET, URL: http://data.pre4.org/, file name: /var/lib/inetsim/http/fakefiles/sample.html
2023-10-30 14:40:52  HTTP connection, method: GET, URL: http://data.pr4e.org/, file name: /var/lib/inetsim/http/fakefiles/sample.html
2023-10-30 14:41:18  HTTP connection, method: GET, URL: http://data.pr4e.org/cover3.jpg, file name: /var/lib/inetsim/http/fakefiles/sar
2023-10-30 14:41:25  HTTP connection, method: GET, URL: http://random.dog/, file name: /var/lib/inetsim/http/fakefiles/sample.html
2023-10-30 14:41:42  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/a
2023-10-30 14:41:42  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/a
2023-10-30 14:41:42  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/a
2023-10-30 14:41:42  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/a
2023-10-30 14:41:42  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/a
2023-10-30 14:41:42  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/a
2023-10-30 14:41:44  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/a
2023-10-30 14:41:44  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/a
2023-10-30 14:41:44  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/a
2023-10-30 14:41:44  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/a
2023-10-30 14:41:44  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/a
2023-10-30 14:41:44  HTTP connection, method: GET, URL: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/a
2023-10-30 14:41:44  HTTPS connection, method: GET, URL: https://www.filehorse.com/download-123-photo-viewer/download/, file name: /var
2023-10-30 14:41:56  HTTP connection, method: GET, URL: http://www.ourgodfather.com/, file name: /var/lib/inetsim/http/fakefiles/sample
2023-10-30 14:42:02  HTTP connection, method: GET, URL: http://www.malwareanalysisbook.com/ad.html, file name: /var/lib/inetsim/http/fa
2023-10-30 14:42:09  HTTP connection, method: GET, URL: http://windowsupdate.microsoft.com/, file name: /var/lib/inetsim/http/fakefiles
2023-10-30 14:42:09  HTTP connection, method: GET, URL: http://www.practicalmalwareanalysis.com/updater.exe, file name: /var/lib/inets
2023-10-30 14:42:09  Last simulated date in log file
```

2nd part: Network services with FakeNet

Initial State

```
C:\Documents and Settings\admin\Desktop\Tools\Fakenet1.0b\FakeNet.exe
FakeNet Version 1.0
[Starting program, for help open a web browser and surf to any URL.]
[Press CTRL-C to exit.]
[Modifying local DNS Settings.]
Error installing provider. 11003
Install my provider error 0.
[Listening for traffic on port 80.]
[Listening for SSL traffic on port 443.]
[Listening for SSL traffic on port 8443.]
[Listening for traffic on port 8080.]
[Listening for traffic on port 8000.]
[Listening for traffic on port 1337.]
[Listening for SSL traffic on port 31337.]
[Listening for ICMP traffic.]
[Listening for traffic on port 25.]
[Listening for SSL traffic on port 465.]
[Listening for DNS traffic on port: 53.]
Bind call failed on UDP port 1031:  10048.

[DNS Query Received.]
  Domain name: www.microsoft.com
[DNS Response sent.]


[Received new connection on port: 80.]
[New request on port 80.]
  GET /isapi/redir.dll?prd=ie&pver=6&ar=msnhome HTTP/1.1
  Accept: */*
  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.microsoft.com
  Connection: Keep-Alive

[Sent http response to client.]

[DNS Query Received.]
  Domain name: javadl-esd-secure.oracle.com
[DNS Response sent.]


[Received new connection on port: 443.]
[New request on port 443 with SSL.]
  [Received unsupported HTTP request.]


[Received new connection on port: 443.]
[New request on port 443 with SSL.]
  [Received unsupported HTTP request.]
Start   C:\Documents and Se...   https://random.dog/ - Mi...
```

Image Request(http) and Download File request(https)

```
C:\Documents and Settings\admin\Desktop\Tools\Fakenet1.0b\FakeNet.exe

[Received new connection on port: 443.]
[New request on port 443 with SSL.]
  [Received unsupported HTTP request.]

[DNS Query Received.]
  Domain name: data.pr4e.org
[DNS Response sent.]


[Received new connection on port: 80.]
[New request on port 80.]
  GET /cover3.jpg 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; SV1; .NET4.0C;
.NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
  Host: data.pr4e.org
  Connection: Keep-Alive

[Sent http response to client.]

[DNS Query Received.]
  Domain name: www.filehorse.com
[DNS Response sent.]


[Received new connection on port: 443.]
[New request on port 443 with SSL.]
  [Received unsupported HTTP request.]


[Received new connection on port: 443.]
[New request on port 443 with SSL.]
  GET /download-123-photo-viewer/download/ 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; SV1; .NET4.0C;
.NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
  Host: www.filehorse.com
  Connection: Keep-Alive

[Sent http response to client.]

Start   C:\Documents and Se...   https://random.dog/ - Mi...
```

Https request

```
C:\Documents and Settings\admin\Desktop\Tools\Fakenet1.0b\FakeNet.exe
[Sent http response to client.]

[DNS Query Received.]
  Domain name: random.dog
[DNS Response sent.]


[Received new connection on port: 443.]
[New request on port 443 with SSL.]
  [Received unsupported HTTP request.]


[Received new connection on port: 443.]
[New request on port 443 with SSL.]
  GET / 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; SV1; .NET4.0C;
.NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
  Host: random.dog
  Connection: Keep-Alive

[Sent http response to client.]
_
```

Start | C:\Documents and Se... | https://random.dog/ - Mi...

Malware 1

```
C:\Documents and Settings\admin\Desktop\Tools\Fakenet1.0b\FakeNet.exe
FakeNet Version 1.0
[Starting program, for help open a web browser and surf to any URL.]
[Press CTRL-C to exit.]
[Modifying local DNS Settings.]
Scanning Installed Providers
Installing Layered Providers
Preparing To Reoder Installed Chains
Reodering Installed Chains
Saving New Protocol Order
[Listening for traffic on port 80.]
[Listening for SSL traffic on port 443.]
[Listening for SSL traffic on port 8443.]
[Listening for traffic on port 8080.]
[Listening for traffic on port 8000.]
[Listening for traffic on port 1337.]
[Listening for SSL traffic on port 31337.]
[Listening for traffic on port 25.]
[Listening for SSL traffic on port 465.]
[Listening for ICMP traffic.]
[Listening for DNS traffic on port: 53.]
Bind call failed on UDP port 1038:  10048.

[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: */*
  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.]
```

DE 8:06 AM

Malware 2

```
C:\Documents and Settings\admin\Desktop\Tools\Fakenet1.0b\FakeNet.exe
FakeNet Version 1.0
[Starting program, for help open a web browser and surf to any URL.]
[Press CTRL-C to exit.]
[Modifying local DNS Settings.]
Scanning Installed Providers
Installing Layered Providers
Preparing To Reoder Installed Chains
Reodering Installed Chains
Saving New Protocol Order
[Listening for traffic on port 80.]
[Listening for SSL traffic on port 443.]
[Listening for SSL traffic on port 8443.]
[Listening for traffic on port 8080.]
[Listening for traffic on port 8000.]
[Listening for traffic on port 1337.]
[Listening for SSL traffic on port 31337.]
[Listening for traffic on port 25.]
[Listening for SSL traffic on port 465.]
[Listening for ICMP traffic.]
[Listening for DNS traffic on port: 53.]
Bind call failed on UDP port 1040:  10048.

[DNS Query Received.]
  Domain name: www.malwareanalysisbook.com
[DNS Response sent.]


[Received new connection on port: 80.]
[New request on port 80.]
  GET /ad.html HTTP/1.1
  Accept: */*
  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.malwareanalysisbook.com
  Connection: Keep-Alive

[Sent http response to client.]
```

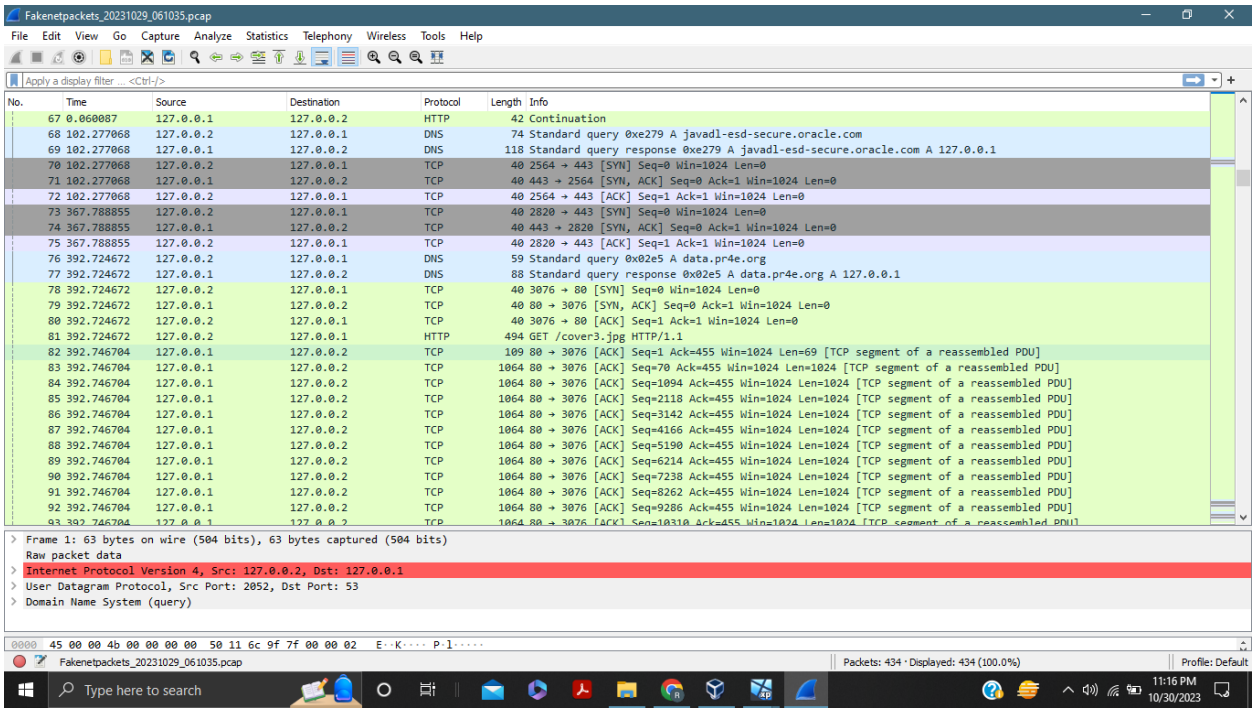
8:10 AM

Malware 3

```
C:\Documents and Settings\admin\Desktop\Tools\Fakenet1.0b\FakeNet.exe
Reodering Installed Chains
Saving New Protocol Order
[Listening for traffic on port 80.]
[Listening for SSL traffic on port 443.]
[Listening for SSL traffic on port 8443.]
[Listening for traffic on port 8080.]
[Listening for traffic on port 8000.]
[Listening for traffic on port 1337.]
[Listening for SSL traffic on port 31337.]
[Listening for traffic on port 25.]
[Listening for SSL traffic on port 465.]
[Listening for ICMP traffic.]
[Listening for DNS traffic on port: 53.]
Bind call failed on UDP port 1040:  10048.

[DNS Query Received.]
  Domain name: windowsupdate.microsoft.com
Bind call failed on UDP port 1041:  10048.
[DNS Response sent.]

[DNS Query Received.]
  Domain name: www.practicalmalwareanalysis.com
[DNS Response sent.]


[Received new connection on port: 80.]
[New request on port 80.]
  GET / HTTP/1.1
  Accept: */*
  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: windowsupdate.microsoft.com


[Received new connection on port: 80.]
  Connection: Keep-Alive

[Sent http response to client.]
[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.]
```

DE 8:11 AM

Image Http/Https/Exe Requests



Fakenetpackets_20231029_061035.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.2	127.0.0.1	DNS	63	Standard query 0x25ea A www.microsoft.com
2	0.050072	127.0.0.1	127.0.0.2	DNS	96	Standard query response 0x25ea A www.microsoft.com A 127.0.0.1
3	0.050072	127.0.0.2	127.0.0.1	TCP	40	2308 → 80 [SYN] Seq=0 Win=1024 Len=0
4	0.050072	127.0.0.1	127.0.0.2	TCP	40	80 → 2308 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
5	0.050072	127.0.0.2	127.0.0.1	TCP	40	2308 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
6	0.050072	127.0.0.2	127.0.0.1	HTTP	369	GET /isapi/redir.dll?prd=ie&pver=6&ar=msnhome HTTP/1.1
7	0.050072	127.0.0.1	127.0.0.2	TCP	107	80 → 2308 [ACK] Seq=1 Ack=330 Win=1024 Len=67 [TCP segment of a reassembled PDU]
8	0.050072	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=68 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
9	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=1092 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
10	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=2116 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
11	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=3140 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
12	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=4164 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
13	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=5188 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
14	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=6212 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
15	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=7236 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
16	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=8260 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
17	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=9284 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
18	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=10308 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
19	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=11332 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
20	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=12356 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
21	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=13380 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
22	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=14404 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
23	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=15428 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
24	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=16452 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
25	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=17476 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
26	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=18500 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
27	0.060087	127.0.0.1	127.0.0.2	TCP	1064	80 → 2308 [ACK] Seq=19524 Ack=330 Win=1024 Len=1024 [TCP segment of a reassembled PDU]

```
> Frame 1: 63 bytes on wire (504 bits), 63 bytes captured (504 bits)
  Raw packet data
> Internet Protocol Version 4, Src: 127.0.0.2, Dst: 127.0.0.1
> User Datagram Protocol, Src Port: 2052, Dst Port: 53
> Domain Name System (query)

0000  45 00 00 4b 00 00 00 00  50 11 6c 9f 7f 00 00 02   E··K···· P·l·····
```

Fakenetpackets_20231029_061035.pcap Packets: 434 · Displayed: 434 (100.0%) Profile: Default

Type here to search 11:16 PM 10/30/2023

Fakenetpackets_20231029_061035.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

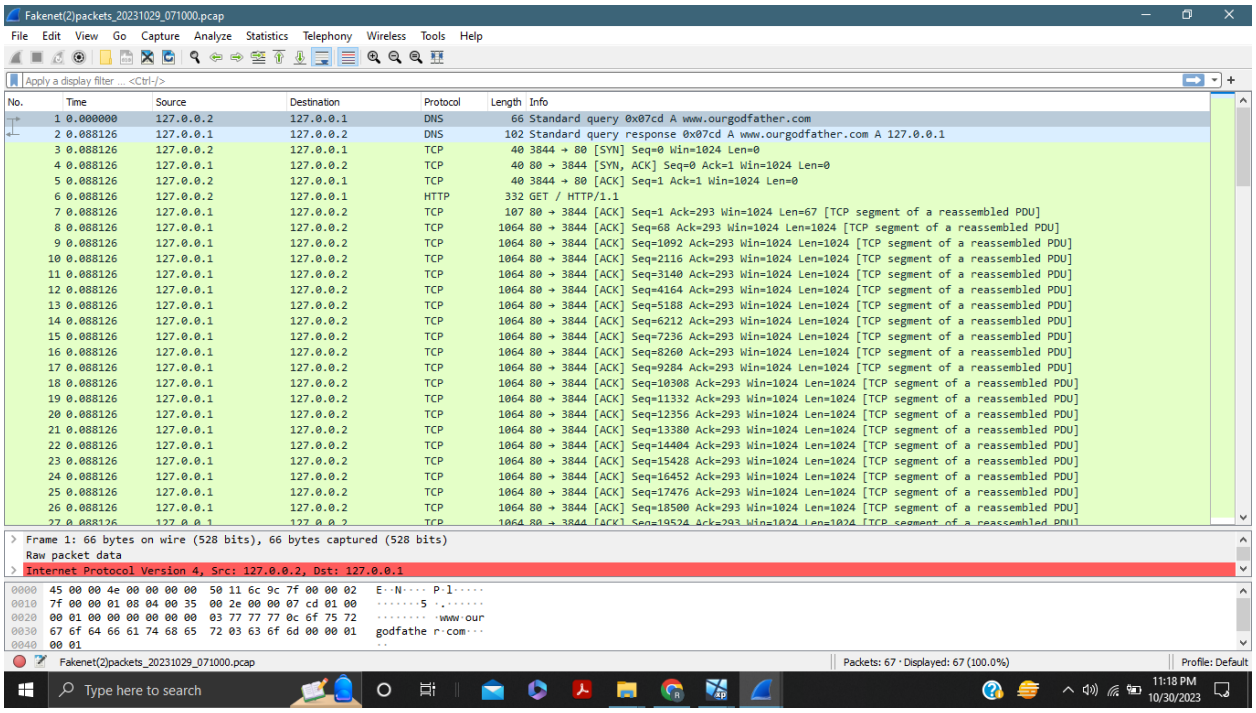
No.	Time	Source	Destination	Protocol	Length	Info
409	392.768735	127.0.0.1	127.0.0.2	HTTP	223	HTTP/1.1 200 OK (JPEG JFIF image)
410	392.768735	127.0.0.1	127.0.0.2	HTTP	42	Continuation
411	428.124573	127.0.0.2	127.0.0.1	DNS	63	Standard query 0x42d3 A www.filehorse.com
412	428.124573	127.0.0.1	127.0.0.2	DNS	96	Standard query response 0x42d3 A www.filehorse.com A 127.0.0.1
413	428.124573	127.0.0.2	127.0.0.1	TCP	40	3332 → 443 [SYN] Seq=0 Win=1024 Len=0
414	428.124573	127.0.0.1	127.0.0.2	TCP	40	443 → 3332 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
415	428.124573	127.0.0.2	127.0.0.1	TCP	40	3332 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=0
416	433.912897	127.0.0.2	127.0.0.1	TCP	40	3588 → 443 [SYN] Seq=0 Win=1024 Len=0
417	433.912897	127.0.0.1	127.0.0.2	TCP	40	443 → 3588 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
418	433.912897	127.0.0.2	127.0.0.1	TCP	40	3588 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=0
419	433.942940	127.0.0.2	127.0.0.1	HTTP	523	GET /download-123-photo-viewer/download/ HTTP/1.1
420	433.942940	127.0.0.1	127.0.0.2	TCP	107	443 → 3588 [ACK] Seq=1 Ack=484 Win=1024 Len=67 [TCP segment of a reassembled PDU]
421	433.942940	127.0.0.1	127.0.0.2	HTTP	59785	HTTP/1.1 200 OK (text/html)
422	433.952954	127.0.0.1	127.0.0.2	HTTP	42	Continuation
423	449.134785	127.0.0.2	127.0.0.1	DNS	56	Standard query 0x1faa A random.dog
424	449.134785	127.0.0.1	127.0.0.2	DNS	82	Standard query response 0x1faa A random.dog A 127.0.0.1
425	449.134785	127.0.0.2	127.0.0.1	TCP	40	3844 → 443 [SYN] Seq=0 Win=1024 Len=0
426	449.134785	127.0.0.1	127.0.0.2	TCP	40	443 → 3844 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
427	449.134785	127.0.0.2	127.0.0.1	TCP	40	3844 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=0
428	450.626930	127.0.0.2	127.0.0.1	TCP	40	4100 → 443 [SYN] Seq=0 Win=1024 Len=0
429	450.626930	127.0.0.1	127.0.0.2	TCP	40	443 → 4100 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
430	450.626930	127.0.0.2	127.0.0.1	TCP	40	4100 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=0
431	450.646959	127.0.0.2	127.0.0.1	HTTP	481	GET / HTTP/1.1
432	450.656973	127.0.0.1	127.0.0.2	TCP	107	443 → 4100 [ACK] Seq=1 Ack=442 Win=1024 Len=67 [TCP segment of a reassembled PDU]
433	450.656973	127.0.0.1	127.0.0.2	HTTP	59785	HTTP/1.1 200 OK (text/html)
434	450.656973	127.0.0.1	127.0.0.2	HTTP	42	Continuation

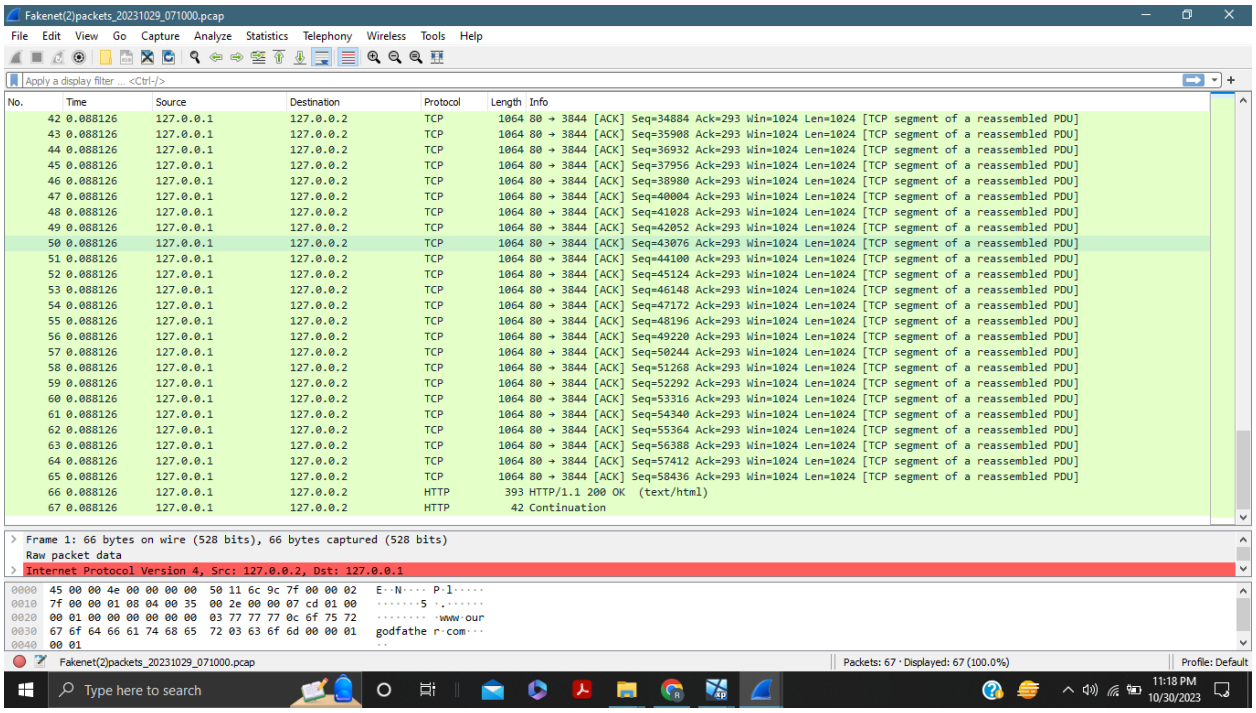

```
> Frame 1: 63 bytes on wire (504 bits), 63 bytes captured (504 bits)
  Raw packet data
> Internet Protocol Version 4, Src: 127.0.0.2, Dst: 127.0.0.1
> User Datagram Protocol, Src Port: 2052, Dst Port: 53
> Domain Name System (query)

0000  45 00 00 4b 00 00 00 00  50 11 6c 9f 7f 00 00 02   E··K···· P·l·····
```

Fakenetpackets_20231029_061035.pcap Packets: 434 · Displayed: 434 (100.0%) Profile: Default

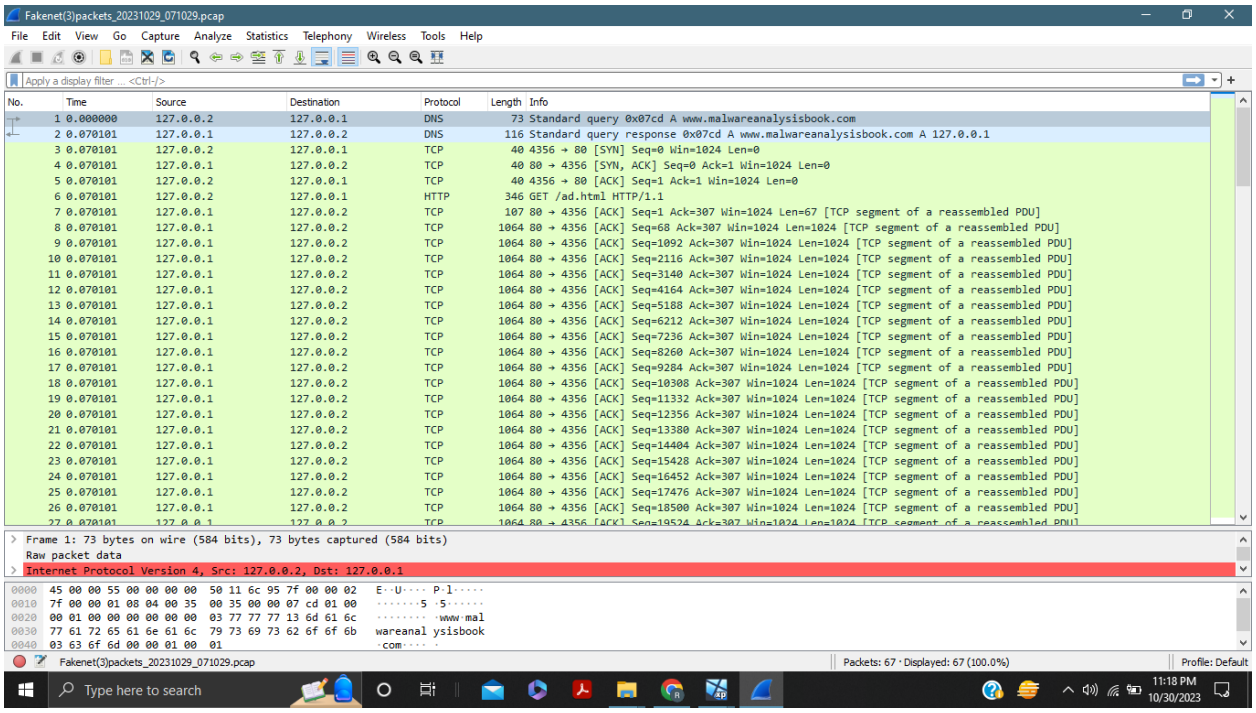
Type here to search 11:16 PM 10/30/2023

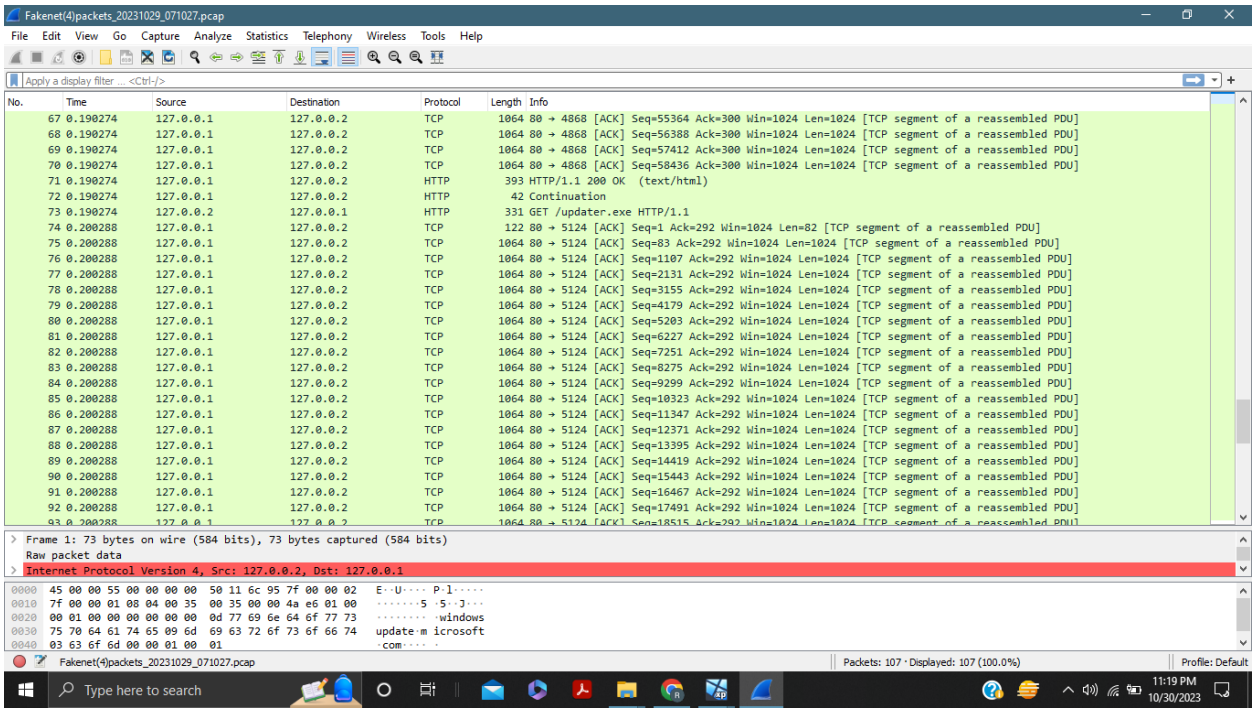
Malware 1


Fakenet(2)packets_20231029_071000.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 127.0.0.2 127.0.0.1 DNS 66 Standard query 0x07cd A www.ourgodfather.com
2 0.088126 127.0.0.1 127.0.0.2 DNS 102 Standard query response 0x07cd A www.ourgodfather.com A 127.0.0.1
3 0.088126 127.0.0.2 127.0.0.1 TCP 40 3844 → 80 [SYN] Seq=0 Win=1024 Len=0
4 0.088126 127.0.0.1 127.0.0.2 TCP 40 80 → 3844 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
5 0.088126 127.0.0.2 127.0.0.1 TCP 40 3844 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
6 0.088126 127.0.0.2 127.0.0.1 HTTP 332 GET / HTTP/1.1
7 0.088126 127.0.0.1 127.0.0.2 TCP 107 80 → 3844 [ACK] Seq=1 Ack=293 Win=1024 Len=67 [TCP segment of a reassembled PDU]
8 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=68 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
9 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=1092 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
10 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=2116 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
11 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=3140 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
12 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=4164 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
13 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=5188 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
14 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=6212 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
15 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=7236 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
16 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=8260 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
17 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=9284 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
18 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=10308 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
19 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=11332 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
20 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=12356 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
21 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=13380 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
22 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=14404 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
23 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=15428 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
24 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=16452 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
25 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=17476 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
26 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=18500 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Raw packet data
Internet Protocol Version 4, Src: 127.0.0.2, Dst: 127.0.0.1
0000 45 00 00 4e 00 00 00 00 50 11 6c 9c 7f 00 00 02 E··N···· P·l·····
0010 7f 00 00 01 08 04 00 35 00 2e 00 00 07 cd 01 00 ·····5 ·.·····
0020 00 01 00 00 00 00 00 00 03 77 77 77 0c 6f 75 72 ····· ·www·our
0030 67 6f 64 66 61 74 68 65 72 03 63 6f 6d 00 00 01 godfathe r·com···
0040 00 01 ··
Fakenet(2)packets_20231029_071000.pcap
Packets: 67 · Displayed: 67 (100.0%)
Profile: Default
Type here to search
11:18 PM
10/30/2023

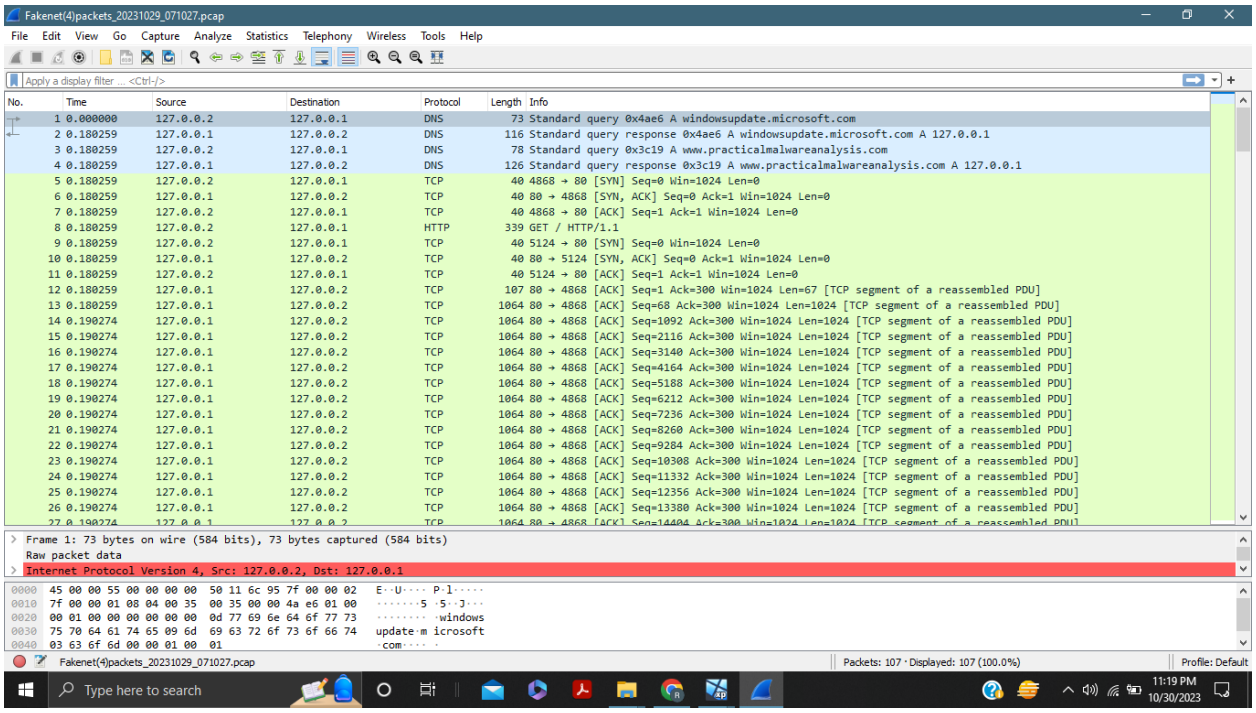

Fakenet(2)packets_20231029_071000.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
42 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=34884 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
43 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=35908 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
44 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=36932 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
45 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=37956 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
46 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=38980 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
47 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=40004 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
48 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=41028 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
49 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=42052 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
50 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=43076 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
51 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=44100 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
52 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=45124 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
53 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=46148 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
54 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=47172 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
55 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=48196 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
56 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=49220 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
57 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=50244 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
58 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=51268 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
59 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=52292 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
60 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=53316 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
61 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=54340 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
62 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=55364 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
63 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=56388 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
64 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=57412 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
65 0.088126 127.0.0.1 127.0.0.2 TCP 1064 80 → 3844 [ACK] Seq=58436 Ack=293 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
66 0.088126 127.0.0.1 127.0.0.2 HTTP 393 HTTP/1.1 200 OK (text/html)
67 0.088126 127.0.0.1 127.0.0.2 HTTP 42 Continuation
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Raw packet data
Internet Protocol Version 4, Src: 127.0.0.2, Dst: 127.0.0.1
0000 45 00 00 4e 00 00 00 00 50 11 6c 9c 7f 00 00 02 E··N···· P·l·····
0010 7f 00 00 01 08 04 00 35 00 2e 00 00 07 cd 01 00 ·····5 ·.·····
0020 00 01 00 00 00 00 00 00 03 77 77 77 0c 6f 75 72 ····· ·www·our
0030 67 6f 64 66 61 74 68 65 72 03 63 6f 6d 00 00 01 godfathe r·com···
0040 00 01 ··
Fakenet(2)packets_20231029_071000.pcap
Packets: 67 · Displayed: 67 (100.0%)
Profile: Default
Type here to search
11:18 PM
10/30/2023

Malware 2


Fakenet(3)packets_20231029_071029.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 127.0.0.2 127.0.0.1 DNS 73 Standard query 0x07cd A www.malwareanalysisbook.com
2 0.070101 127.0.0.1 127.0.0.2 DNS 116 Standard query response 0x07cd A www.malwareanalysisbook.com A 127.0.0.1
3 0.070101 127.0.0.2 127.0.0.1 TCP 40 4356 → 80 [SYN] Seq=0 Win=1024 Len=0
4 0.070101 127.0.0.1 127.0.0.2 TCP 40 80 → 4356 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
5 0.070101 127.0.0.2 127.0.0.1 TCP 40 4356 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
6 0.070101 127.0.0.2 127.0.0.1 HTTP 346 GET /ad.html HTTP/1.1
7 0.070101 127.0.0.1 127.0.0.2 TCP 107 80 → 4356 [ACK] Seq=1 Ack=307 Win=1024 Len=67 [TCP segment of a reassembled PDU]
8 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=68 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
9 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=1092 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
10 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=2116 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
11 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=3140 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
12 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=4164 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
13 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=5188 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
14 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=6212 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
15 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=7236 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
16 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=8260 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
17 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=9284 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
18 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=10308 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
19 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=11332 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
20 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=12356 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
21 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=13380 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
22 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=14404 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
23 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=15428 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
24 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=16452 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
25 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=17476 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
26 0.070101 127.0.0.1 127.0.0.2 TCP 1064 80 → 4356 [ACK] Seq=18500 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
Raw packet data
Internet Protocol Version 4, Src: 127.0.0.2, Dst: 127.0.0.1
0000 45 00 00 55 00 00 00 00 50 11 6c 95 7f 00 00 02 E··U···· P·l·····
0010 7f 00 00 01 08 04 00 35 00 35 00 00 07 cd 01 00 ·····5 ·5·····
0020 00 01 00 00 00 00 00 00 03 77 77 77 13 6d 61 6c ····· ·www·mal
0030 77 61 72 65 61 6e 61 6c 79 73 69 73 62 6f 6f 6b wareanal ysisbook
0040 03 63 6f 6d 00 00 01 00 01 ·com···· ·
Fakenet(3)packets_20231029_071029.pcap
Packets: 67 · Displayed: 67 (100.0%)
Profile: Default
Type here to search
11:18 PM
10/30/2023


Fakenet(4)packets_20231029_071027.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
67 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=55364 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
68 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=56388 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
69 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=57412 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
70 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=58436 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
71 0.190274 127.0.0.1 127.0.0.2 HTTP 393 HTTP/1.1 200 OK (text/html)
72 0.190274 127.0.0.1 127.0.0.2 HTTP 42 Continuation
73 0.190274 127.0.0.2 127.0.0.1 HTTP 331 GET /updater.exe HTTP/1.1
74 0.200288 127.0.0.1 127.0.0.2 TCP 122 80 → 5124 [ACK] Seq=1 Ack=292 Win=1024 Len=82 [TCP segment of a reassembled PDU]
75 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=83 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
76 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=1107 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
77 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=2131 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
78 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=3155 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
79 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=4179 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
80 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=5203 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
81 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=6227 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
82 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=7251 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
83 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=8275 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
84 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=9299 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
85 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=10323 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
86 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=11347 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
87 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=12371 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
88 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=13395 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
89 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=14419 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
90 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=15443 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
91 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=16467 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
92 0.200288 127.0.0.1 127.0.0.2 TCP 1064 80 → 5124 [ACK] Seq=17491 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
Raw packet data
Internet Protocol Version 4, Src: 127.0.0.2, Dst: 127.0.0.1
0000 45 00 00 55 00 00 00 00 50 11 6c 95 7f 00 00 02 E··U···· P·l·····
0010 7f 00 00 01 08 04 00 35 00 35 00 00 4a e6 01 00 ·····5 ·5··J···
0020 00 01 00 00 00 00 00 00 0d 77 69 6e 64 6f 77 73 ····· ·windows
0030 75 70 64 61 74 65 09 6d 69 63 72 6f 73 6f 66 74 update·m icrosoft
0040 03 63 6f 6d 00 00 01 00 01 ·com···· ·
Fakenet(4)packets_20231029_071027.pcap
Packets: 107 · Displayed: 107 (100.0%)
Profile: Default
Type here to search
11:19 PM
10/30/2023

Malware 3


Fakenet(4)packets_20231029_071027.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 127.0.0.2 127.0.0.1 DNS 73 Standard query 0x4ae6 A windowsupdate.microsoft.com
2 0.180259 127.0.0.1 127.0.0.2 DNS 116 Standard query response 0x4ae6 A windowsupdate.microsoft.com A 127.0.0.1
3 0.180259 127.0.0.2 127.0.0.1 DNS 78 Standard query 0x3c19 A www.practicalmalwareanalysis.com
4 0.180259 127.0.0.1 127.0.0.2 DNS 126 Standard query response 0x3c19 A www.practicalmalwareanalysis.com A 127.0.0.1
5 0.180259 127.0.0.2 127.0.0.1 TCP 40 4868 → 80 [SYN] Seq=0 Win=1024 Len=0
6 0.180259 127.0.0.1 127.0.0.2 TCP 40 80 → 4868 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
7 0.180259 127.0.0.2 127.0.0.1 TCP 40 4868 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
8 0.180259 127.0.0.2 127.0.0.1 HTTP 339 GET / HTTP/1.1
9 0.180259 127.0.0.2 127.0.0.1 TCP 40 5124 → 80 [SYN] Seq=0 Win=1024 Len=0
10 0.180259 127.0.0.1 127.0.0.2 TCP 40 80 → 5124 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
11 0.180259 127.0.0.2 127.0.0.1 TCP 40 5124 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
12 0.180259 127.0.0.1 127.0.0.2 TCP 107 80 → 4868 [ACK] Seq=1 Ack=300 Win=1024 Len=67 [TCP segment of a reassembled PDU]
13 0.180259 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=68 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
14 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=1092 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
15 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=2116 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
16 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=3140 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
17 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=4164 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
18 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=5188 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
19 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=6212 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
20 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=7236 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
21 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=8260 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
22 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=9284 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
23 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=10308 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
24 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=11332 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
25 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=12356 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
26 0.190274 127.0.0.1 127.0.0.2 TCP 1064 80 → 4868 [ACK] Seq=13380 Ack=300 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
Raw packet data
Internet Protocol Version 4, Src: 127.0.0.2, Dst: 127.0.0.1
0000 45 00 00 55 00 00 00 00 50 11 6c 95 7f 00 00 02 E··U···· P·l·····
0010 7f 00 00 01 08 04 00 35 00 35 00 00 4a e6 01 00 ·····5 ·5··J···
0020 00 01 00 00 00 00 00 00 0d 77 69 6e 64 6f 77 73 ····· ·windows
0030 75 70 64 61 74 65 09 6d 69 63 72 6f 73 6f 66 74 update·m icrosoft
0040 03 63 6f 6d 00 00 01 00 01 ·com···· ·
Fakenet(4)packets_20231029_071027.pcap
Packets: 107 · Displayed: 107 (100.0%)
Profile: Default
Type here to search
11:19 PM
10/30/2023

Fakenet(4)packets_20231029_071027.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
82	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=7251 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
83	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=8275 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
84	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=9299 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
85	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=10323 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
86	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=11347 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
87	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=12371 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
88	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=13395 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
89	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=14419 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
90	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=15443 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
91	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=16467 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
92	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=17491 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
93	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=18515 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
94	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=19539 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
95	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=20563 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
96	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=21587 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
97	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=22611 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
98	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=23635 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
99	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=24659 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
100	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=25683 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
101	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=26707 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
102	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=27731 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
103	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=28755 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
104	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=29779 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
105	0.200288	127.0.0.1	127.0.0.2	TCP	1064	80 → 5124 [ACK] Seq=30803 Ack=292 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
106	0.200288	127.0.0.1	127.0.0.2	HTTP	1064	HTTP/1.1 200 OK
107	0.200288	127.0.0.1	127.0.0.2	HTTP	42	Continuation

```
> Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
  Raw packet data
> Internet Protocol Version 4, Src: 127.0.0.2, Dst: 127.0.0.1

0000  45 00 00 55 00 00 00 00  50 11 6c 95 7f 00 00 02   E··U···· P·l·····
0010  7f 00 00 01 08 04 00 35  00 35 00 00 4a e6 01 00   ·******5 ·5··J···
0020  00 01 00 00 00 00 00 00  0d 77 69 6e 64 6f 77 73   ******** ·windows
0030  75 70 64 61 74 65 09 6d  69 63 72 6f 73 6f 66 74   update·m icrosoft
0040  03 63 6f 6d 00 00 01 00  01                        ·com···· ·
```

Fakenet(4)packets_20231029_071027.pcap Packets: 107 · Displayed: 107 (100.0%) Profile: Default

Type here to search 11:19 PM 10/30/2023

Fakenet(3)packets_20231029_071029.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
42	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=34884 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
43	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=35908 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
44	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=36932 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
45	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=37956 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
46	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=38980 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
47	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=40004 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
48	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=41028 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
49	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=42052 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
50	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=43076 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
51	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=44100 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
52	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=45124 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
53	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=46148 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
54	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=47172 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
55	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=48196 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
56	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=49220 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
57	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=50244 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
58	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=51268 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
59	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=52292 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
60	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=53316 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
61	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=54340 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
62	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=55364 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
63	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=56388 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
64	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=57412 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
65	0.070101	127.0.0.1	127.0.0.2	TCP	1064	80 → 4356 [ACK] Seq=58436 Ack=307 Win=1024 Len=1024 [TCP segment of a reassembled PDU]
66	0.070101	127.0.0.1	127.0.0.2	HTTP	393	HTTP/1.1 200 OK (text/html)
67	0.070101	127.0.0.1	127.0.0.2	HTTP	42	Continuation

```
> Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
  Raw packet data
> Internet Protocol Version 4, Src: 127.0.0.2, Dst: 127.0.0.1

0000  45 00 00 55 00 00 00 00  50 11 6c 95 7f 00 00 02   E··U···· P·l·····
0010  7f 00 00 01 08 04 00 35  00 35 00 00 07 cd 01 00   ·******5 ·5******
0020  00 01 00 00 00 00 00 00  03 77 77 77 13 6d 61 6c   ******** ·www·mal
0030  77 61 72 65 61 6e 61 6c  79 73 69 73 62 6f 6f 6b   wareanal ysisbook
0040  03 63 6f 6d 00 00 01 00  01                        ·com···· ·
```

Fakenet(3)packets_20231029_071029.pcap Packets: 67 · Displayed: 67 (100.0%) Profile: Default

Type here to search 11:18 PM 10/30/2023

Analysis of Reports and Tools:

The Sequence of Requests are:

- ARP requests for DNS
- TCP Handshakes
- Then Http request
- Lastly, data transfer over TCP

InetSim with ApateDNS provides a more realistic simulated network environment. It provides more detailed analysis. However, FakeNet is more easy to use and an easy to set up tool. It provides a basic level analysis.
So the differences are in:

- Simulation Type
- Simulation Level
- Details in logs
- Responses

Whereas the comparison of two tools in analyzing malware behavior turns out quite useful.