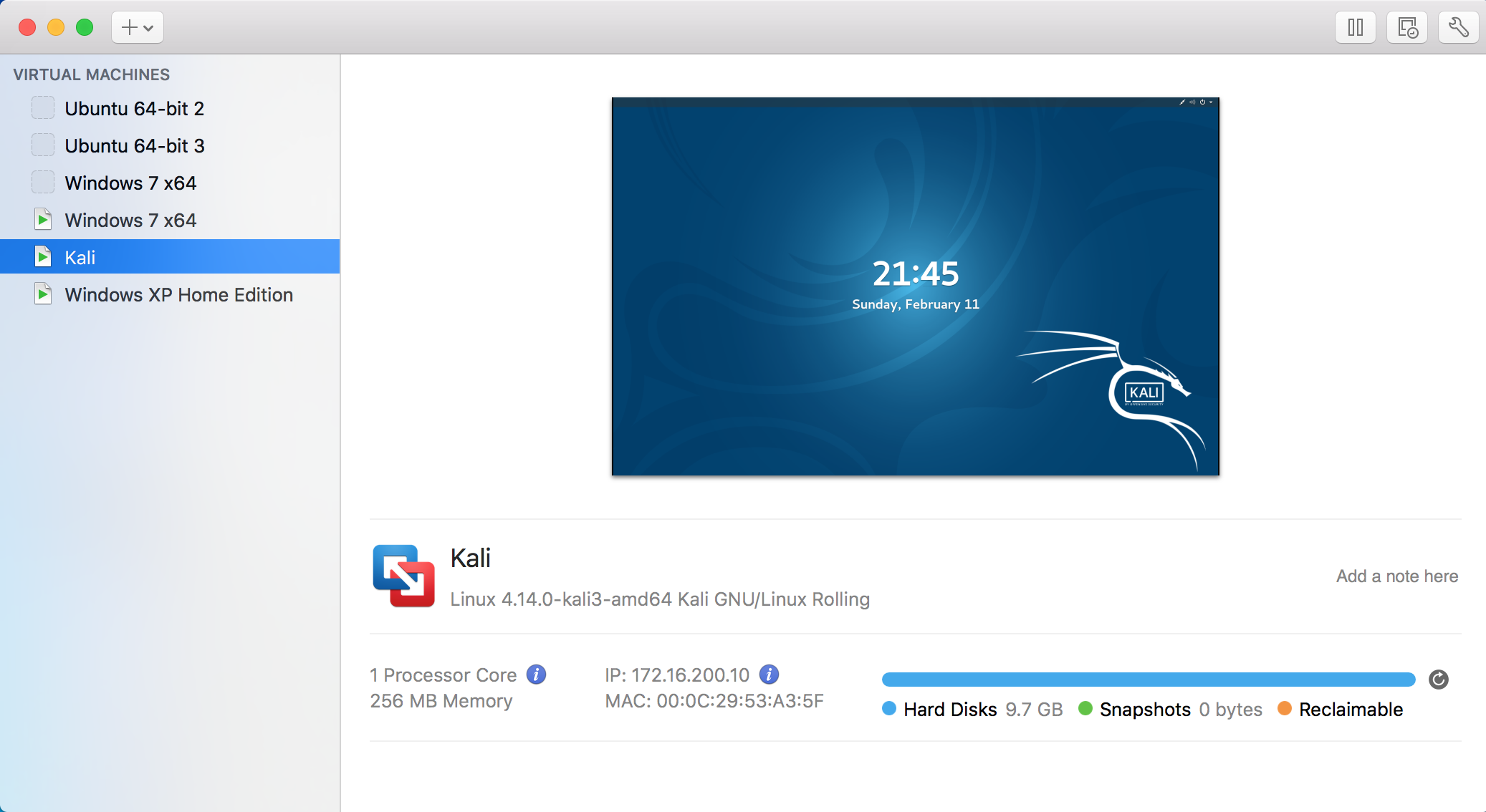
**Dynamic Analysis Environment Setup**

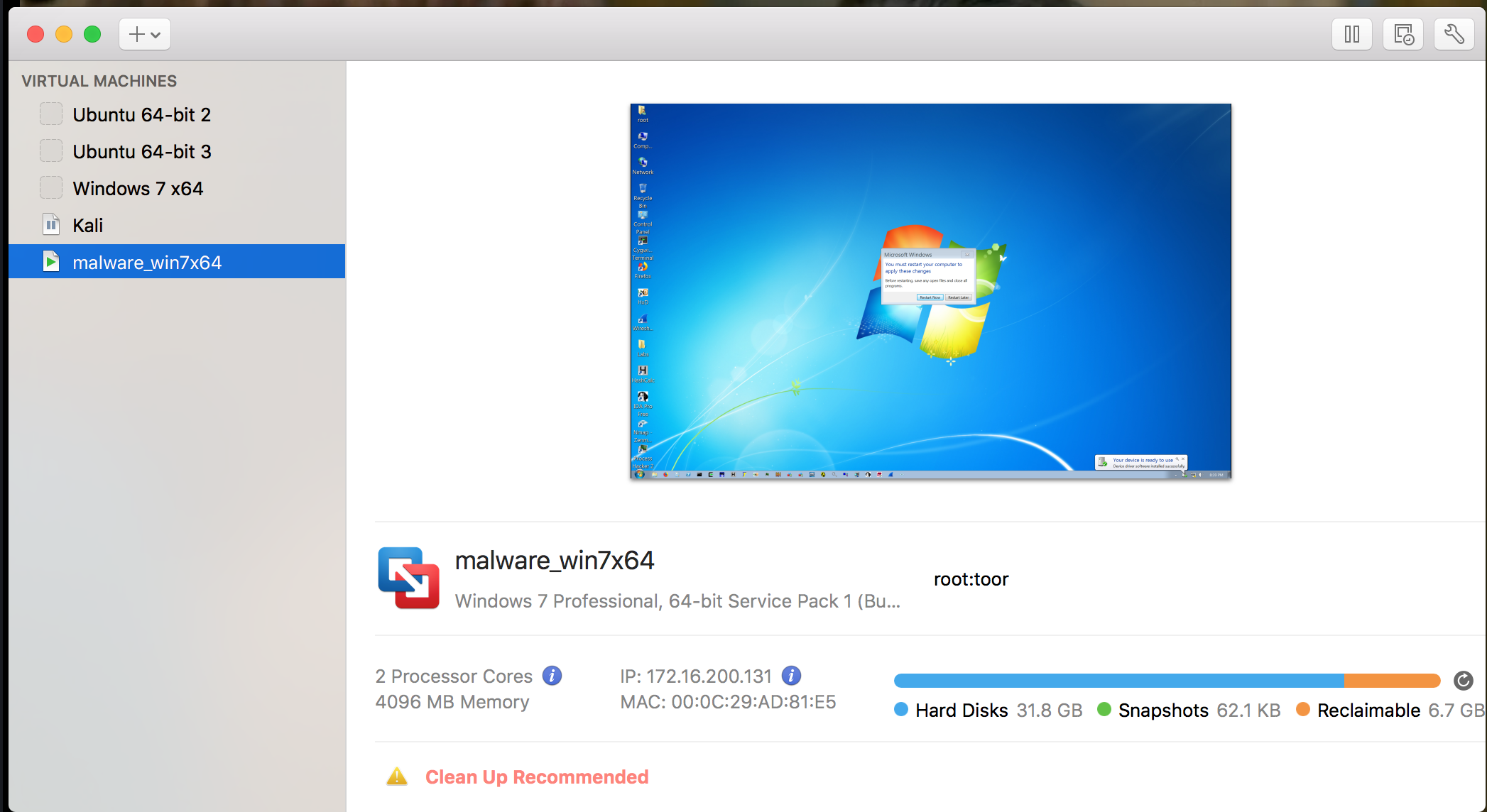
1. The following are the IP addresses of the virtual machines setup

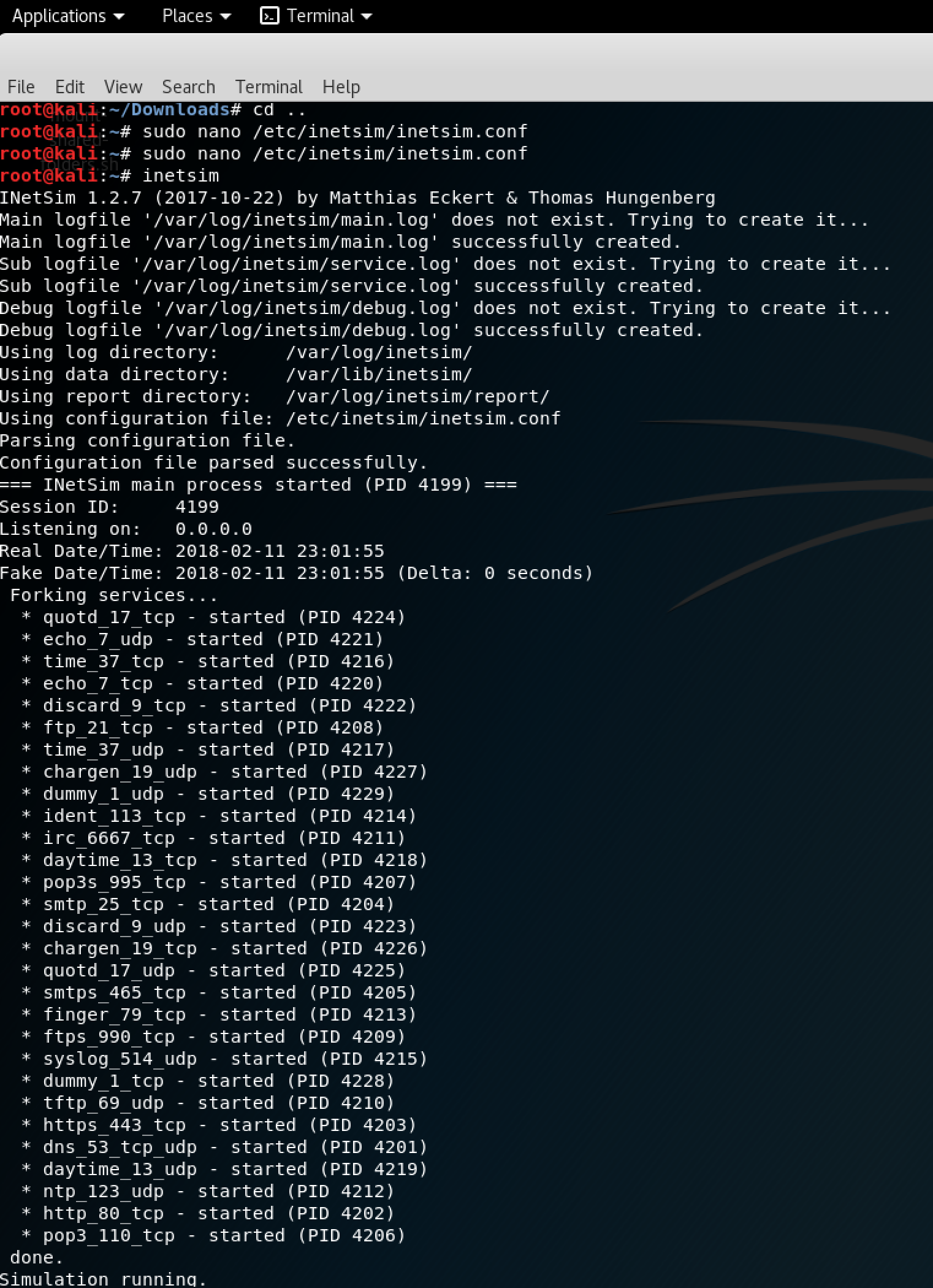
Windows 7 VM: 172:16:200:131

Kali VM: 172:16:200:10

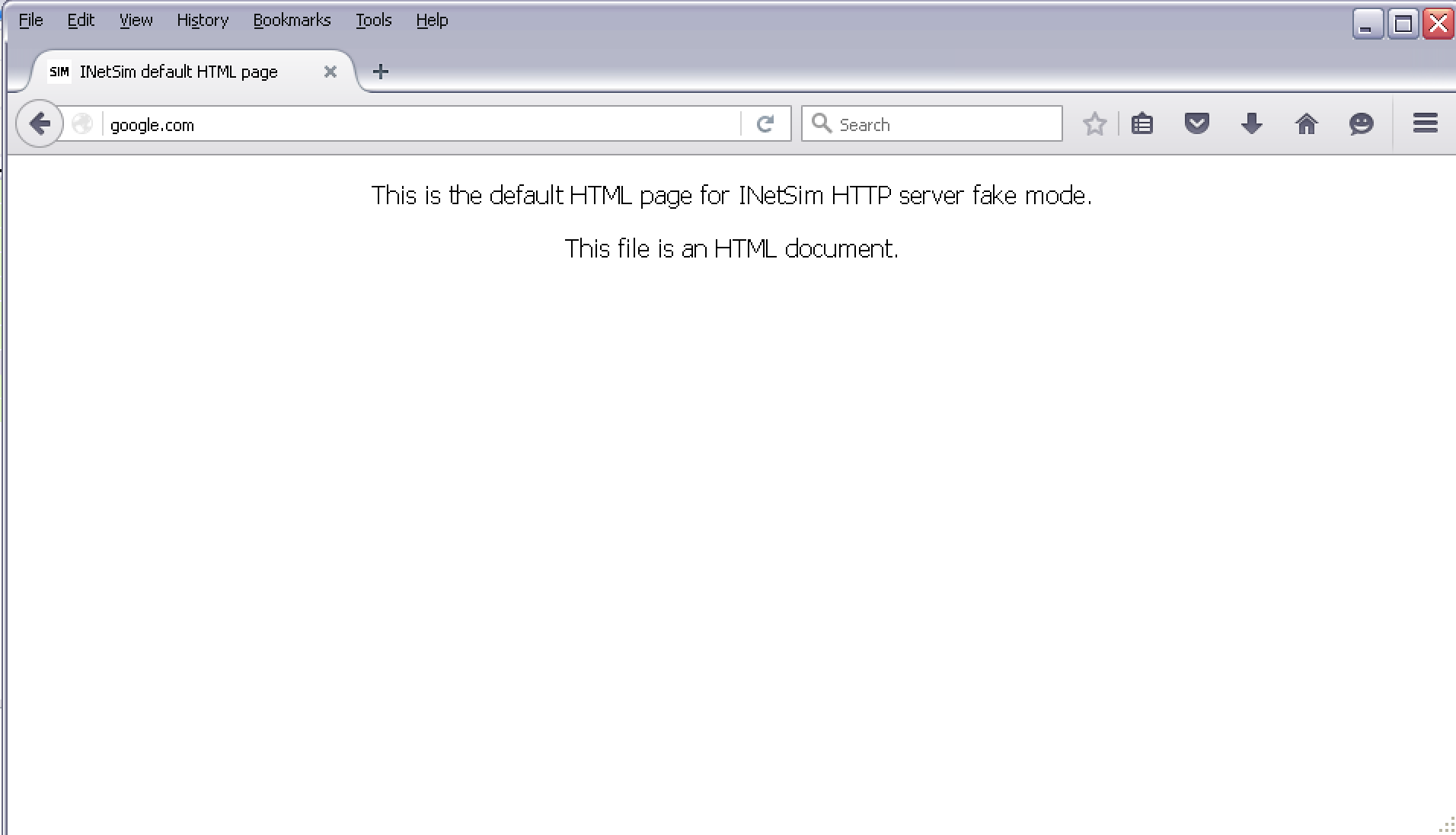
Host only adapter: 172:16:200:1

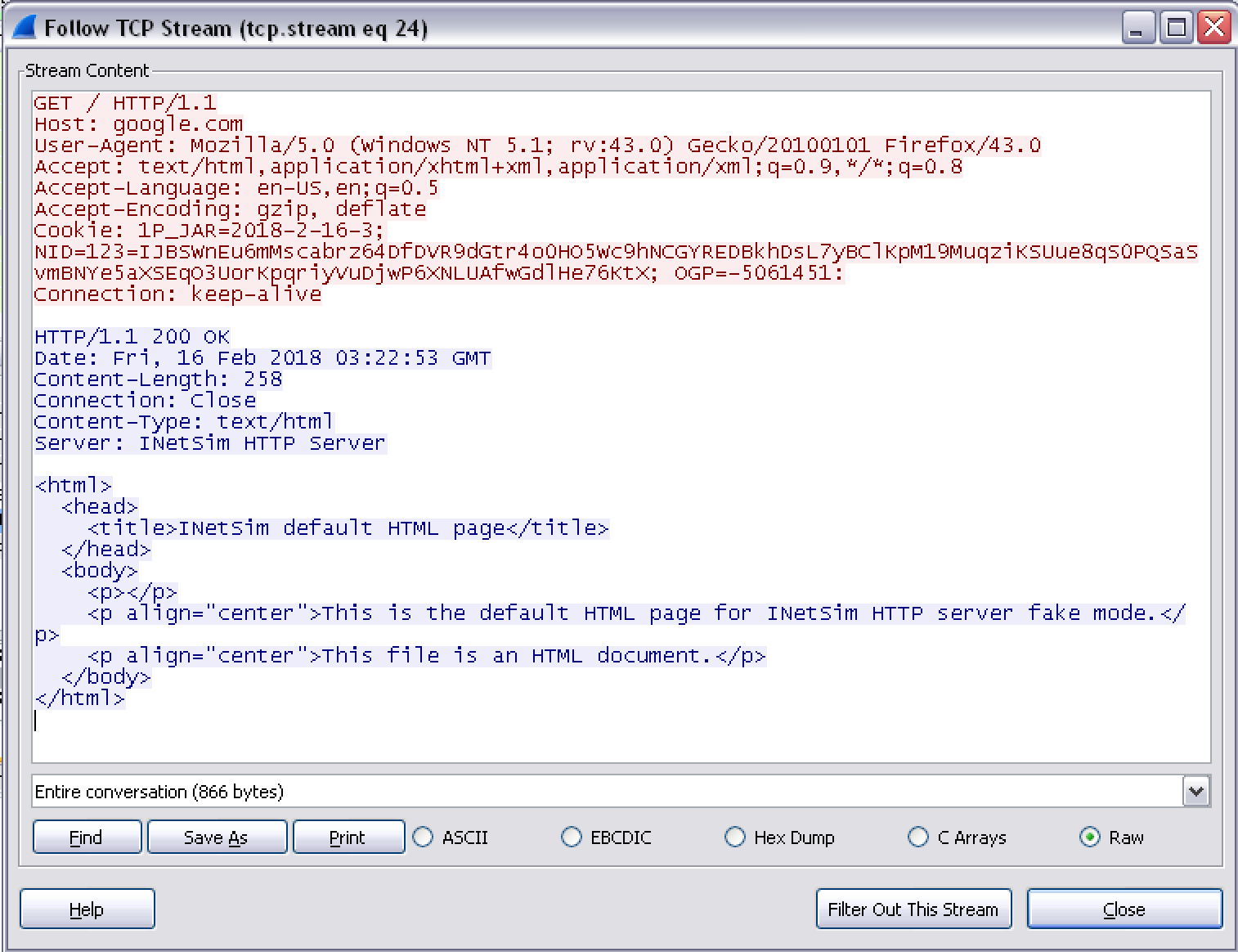






1. I performed this question on Windows XP



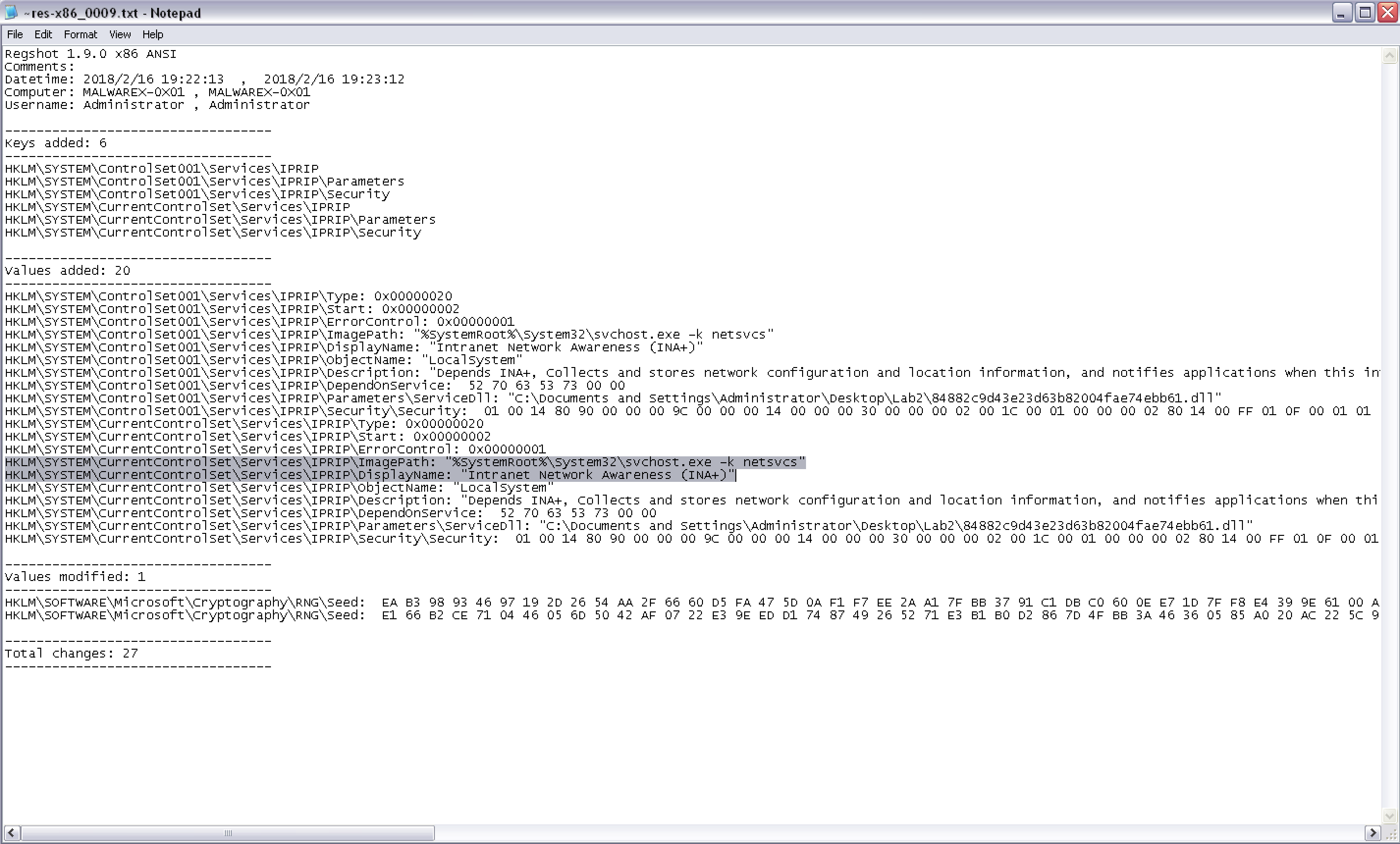
****

**84882c9d43e23d63b82004fae74ebb61**

1. This is an unpacked DLL file. This needs to be executed with the command prompt. We first need to install it and then execute it. So, we must check the functions in the dll file to understand the command it needs to be installed. Therefore, I ran the DLL file thru IDA Pro to check for the functions and I found install and installA.
2. To install the malware, we need to run the command as below:

*rundll32 84882c9d43e23d63b82004fae74ebb61.dll, installA*

1. Before installing, I took a shot using Regshot. The comparisons of the shots before and after installation is shown below:



This shows us that s service IPRIP needs to be started to run the malware. Therefore, I used the command:

*net start IPRIP*

which is how the file runs.

1. I used two filters for:

* process name which contains “rundll32.exe”
* path which contains “IPRIP”

1. Host base signatures:

* IPRIP
* cmd.exe
* Windows XP 6.11

1. Network based signatures:

* practicalmalwareanalysis.com
* server.html
* GET
* HTTP/1.1

1. To inspecting this malware I used, Regshot, ApateDNS, Command Prompt, Process Explorer and Process Monitor. On ApateDNS we see that when we try to run the malware by starting the IPRIP service, it contacts practicalmalwareanalysis.com. Considering this and the fact that we see strings such as cmd.exe we can assume the malware is requesting the command prompt for the remote host: http://practicalmalwareanalysis.com

**e2bf42217a67e46433da8b6f4507219e**

* 1. When running the exe file, Process Monitor detects that it generates svchost.exe. This process runs in the background even though it shows an error to the user while opening the malware.
  2. There are live memory modifications. We know this because, when combing thru the properties of service svchost.exe, we look under strings tab and find that when toggling between Memory and Image there are differences in the strings. This means that there have been some modifications with the memory.
  3. Host base signatures:

practicalmalwareanalysis.log

* 1. When we open the malware, we see that it creates a file practicalmalwareanalysis.log next to the malware. When combing thru the strings in the memory section of “svchost.exe” we find strings such as
* practicalmalwareanalysis.log
* [ENTER]
* [CAPS LOCK]
* [SHIFT]
* [CTRL]
* [DELETE]

This mean that the malware is a keylogger. The file practicalmalwareanalysis.log, starts to build whenever a key is presses. This logs all the keys pushed and saves them on the .log file created.

**b94af4a4d4af6eac81fc135abda1c40c**

1. When I try to run the file, it disappears. When Going thru process monitor we find a process created to call cmd.exe and then and instruction to delete the malware from the c drive.

"C:\WINDOWS\system32\cmd.exe" /c del C:\DOCUME~1\ADMINI~1\Desktop\Lab2\B94AF4~1.EXE >> NUL”

1. The set back is that the program deletes itself from the hard drive.
2. Another way to run the malware is to debug it using IDA Pro and ollydbg. By locating the delete instruction, we can code to jump to the next instruction instead of executing the delete command.
3. There are several strings found in this malware:

* <http://www.practicalmalwareanalysis.com>
* command.com
* Manager Service.exe
* cmd.exe
* UPLOAD
* DOWNLOAD
* /c del

All these strings suggest that the malware is being used to remotely access the command prompt and possibly connect to <http://www.practicalmalwareanalysis.com> from where it can UPLOAD or DOWNLOAD malware. The remote attacker could also control the Service Manager and install services and or remove them.