## **Final: Malware Analysis Report**

**Submitted by**

**Chakresh Singh**

**UC 6+2: singhch**

**-----------------------------------------------------------------------------------------------------------------------------**

### **PDF Static Analysis:**

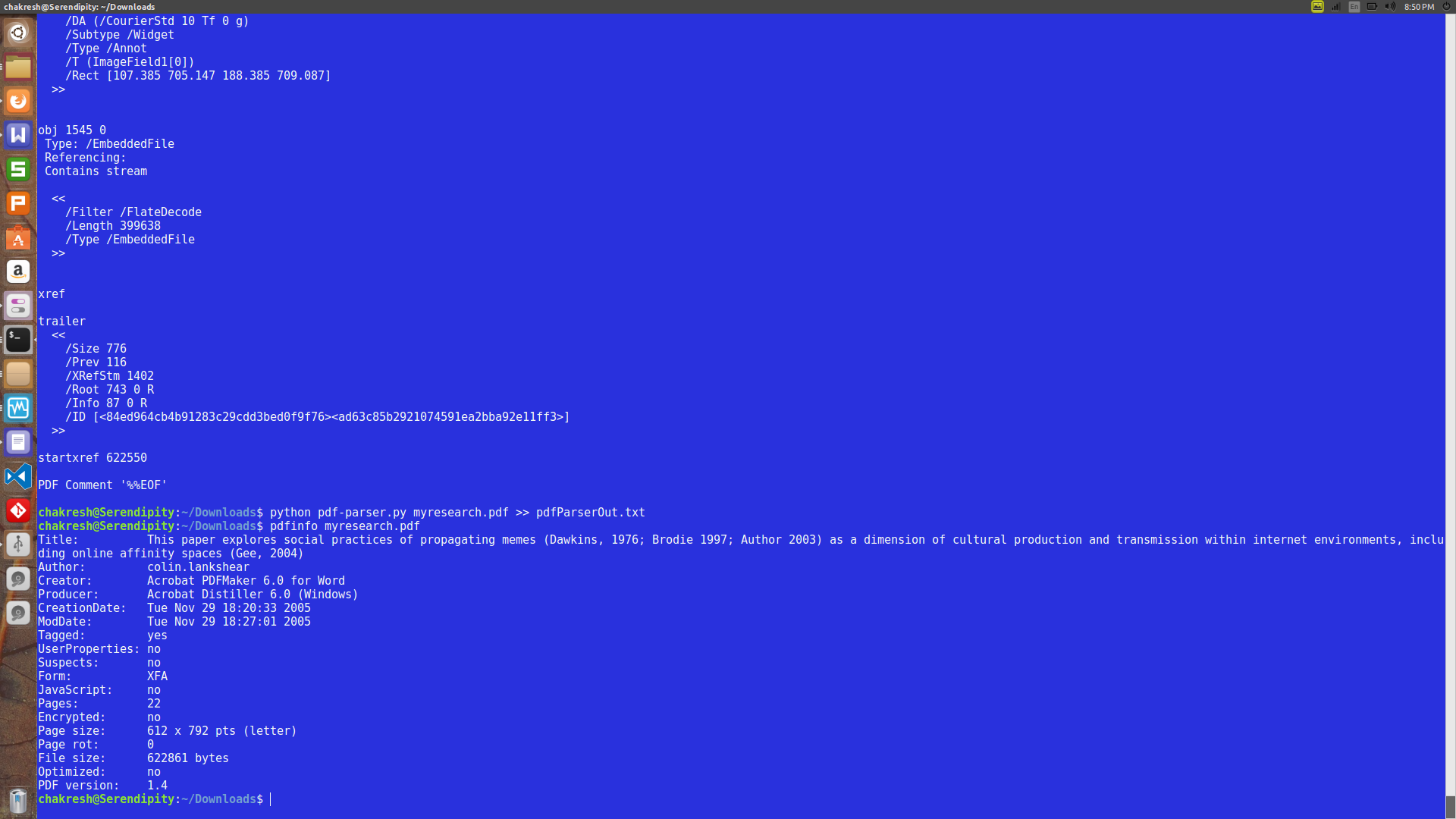
  
Illustration 1: pdfinfo command on malicious pdf

  
Illustration 2: MD5 and SHA1 hash for the pdf file

MD5sum: b55ed5064182f29ca55ce70c3b14bf3d -

SHA1Sum**:** 27493cc2859b765c366b6780cfd5226c79c0ce05

* **PDF File Name:** myresearch.pdf
* **PDF MD5 Hash:** b55ed5064182f29ca55ce70c3b14bf3d -
* **PDF SHA-1 Hash:** 27493cc2859b765c366b6780cfd5226c79c0ce05
* **PDF Creation Date:** 2005:11:29 18:20:33+11:00
* **PDF Modification Date:** 2005:11:29 18:27:01+11:00
* **PDF Title:** This paper explores social practices of propagating memes (Dawkins, 1976; Brodie 1997; Author 2003) as a dimension of cultural production and transmission within internet environments, including online affinity spaces (Gee, 2004)
* **PDF Author:** colin.lankshear
* **PDF Creator:** Acrobat PDFMaker 6.0 for Word
* **PDF Producer:** Acrobat Distiller 6.0 (Windows)
* **Number of named PDF objects:** 776
* **List of PDF object numbers that contain streams:** S

Streams (47): [744, 770, 759, 760, 761, 762, 763, 764, 768, 769, 2, 4, 6, 8, 10, 12, 13, 15, 17, 19, 21, 23, 24, 25, 27, 29, 37, 39, 41, 43, 45, 47, 49, 52, 54, 57, 62, 63, 66, 73, 74, 75, 76, 77, 78, 79, 86]

Streams (1): [1545]

* **List the object number (or numbers) that contain streams that causes the exploit:**

***1545***

* ***Please find attached yara rule in file named:*** singhch-pdf.yar

### Creating Yara Rule:

### Analyze Strings from Malware:

1545: Imagefield

yara a dummy rule for one object:

rule dummy{

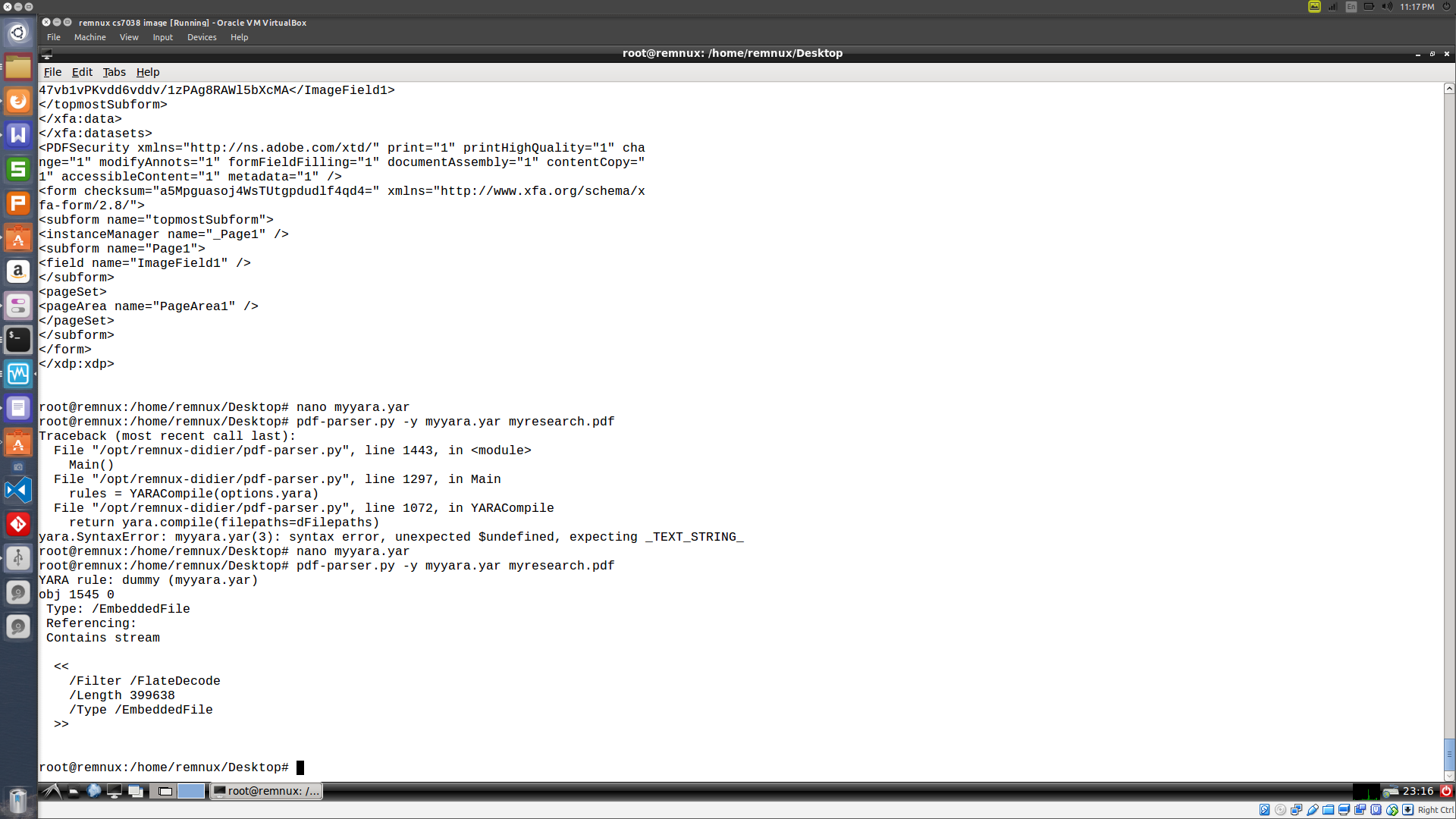
strings:

$s1 = "a5Mpguasoj4WsTUtgpdudlf4qd4"

condition:

all of them

}

  
Illustration 3: Running pdf-parser with yara rule

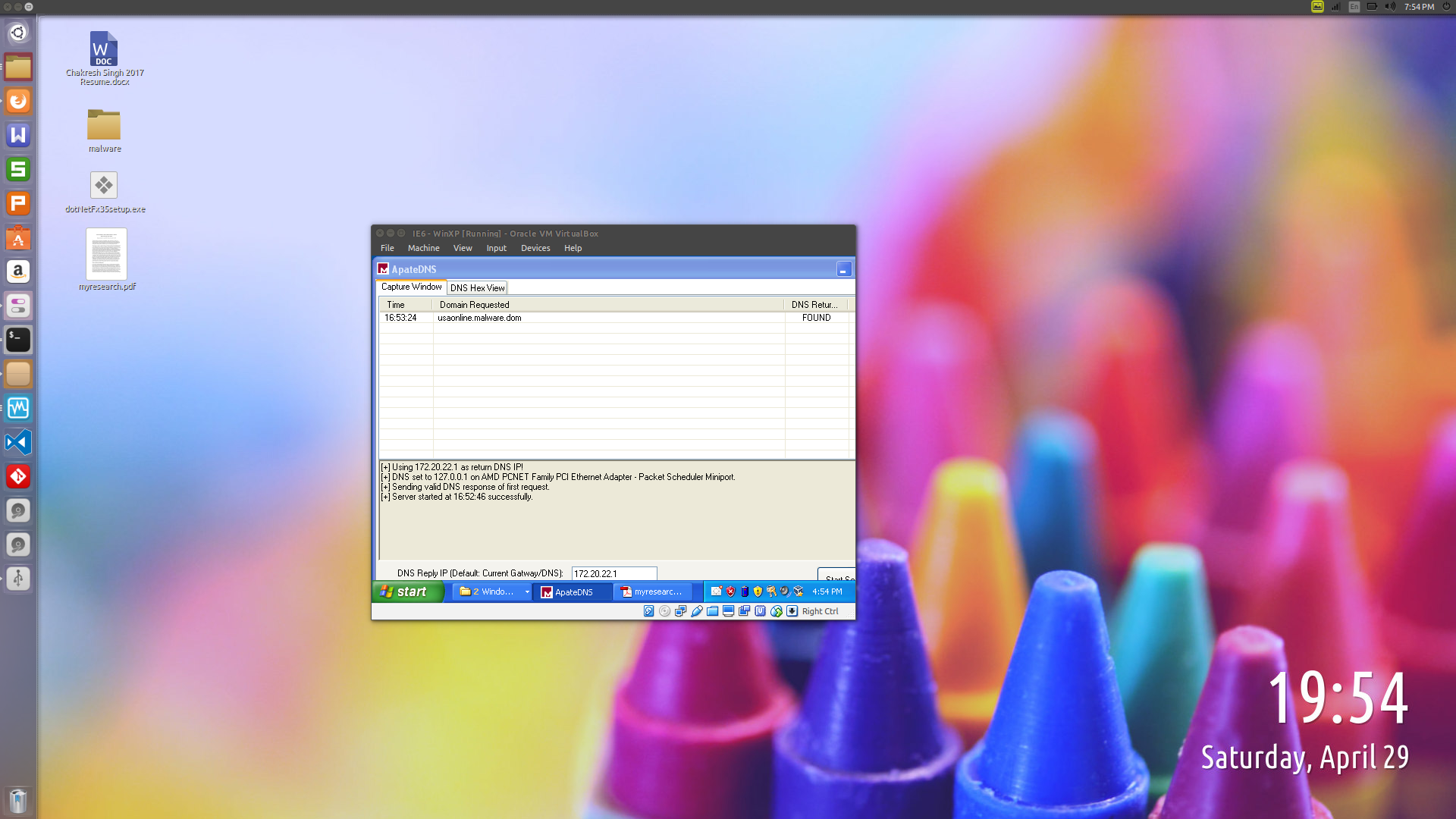
### **PDF Dynamic Analysis**

*What system-level effects does the PDF cause Acrobat Reader to take in order to get the backdoor onto the system (writes files to disk, deletes files, etc…)?*

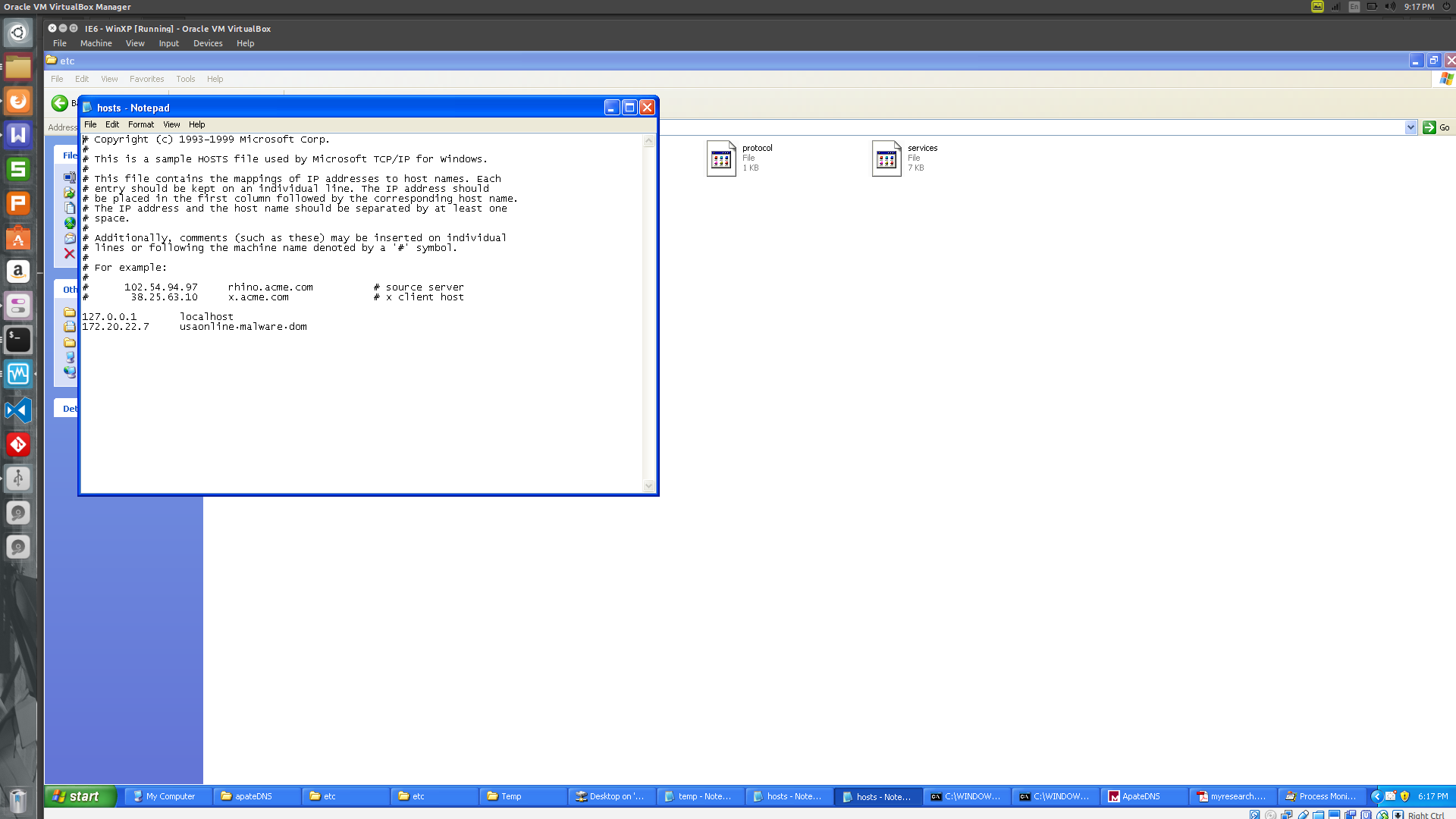
The pdf causes an exe to get executed (cvs.exe). This exe file loads a number of dlls. It tries to connect to usaonline.malware.dom. The related details are attached elsewhere in this report.

### **Backdoor Dynamic Analysis:**

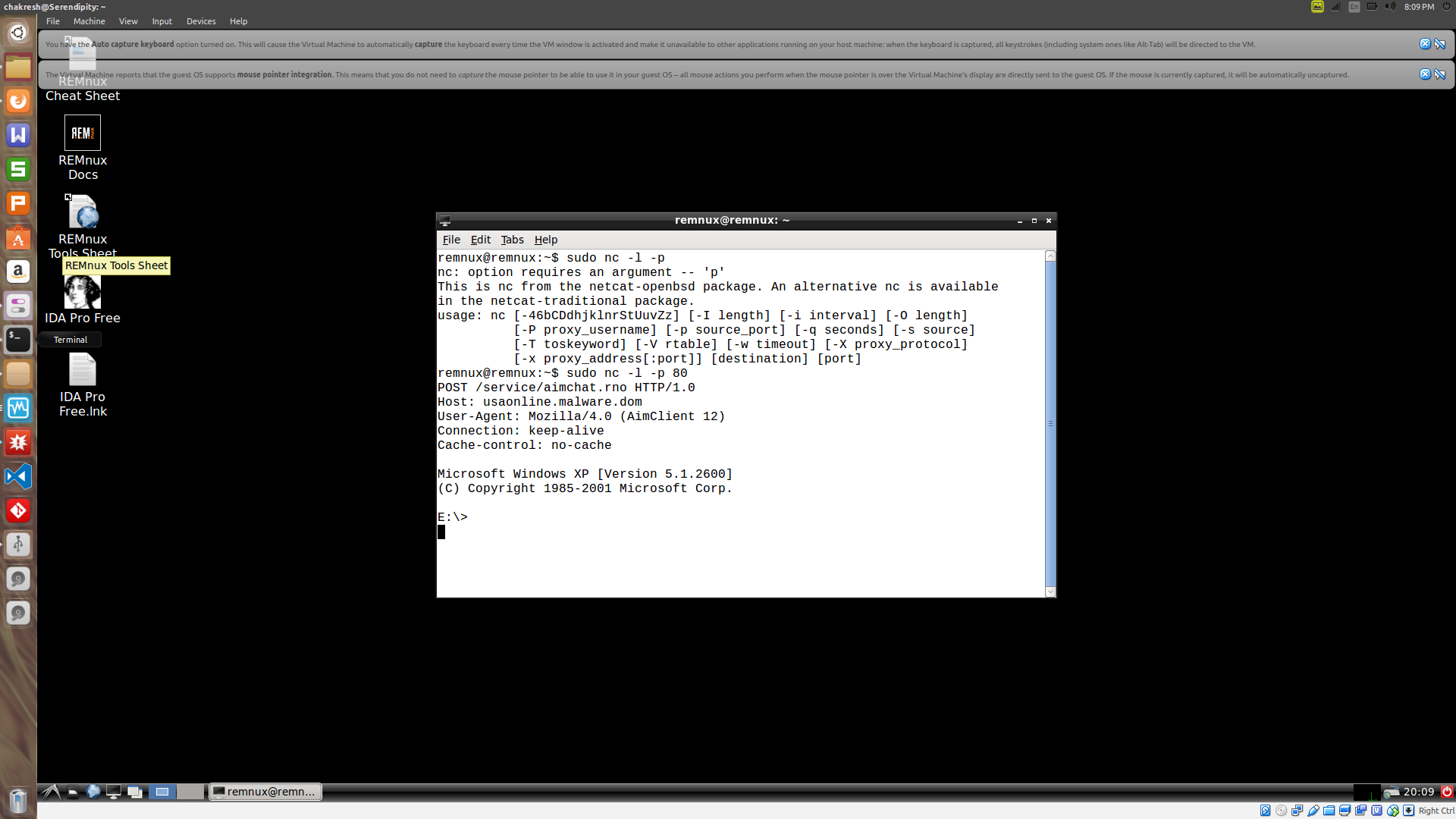
After setting up the lap environment, when I opened the “myresearch.pdf” folder on Acrobat Reader in Windows XP VM, I could see it connecting to **unsaonline.malware.dom** in ApateDNS.

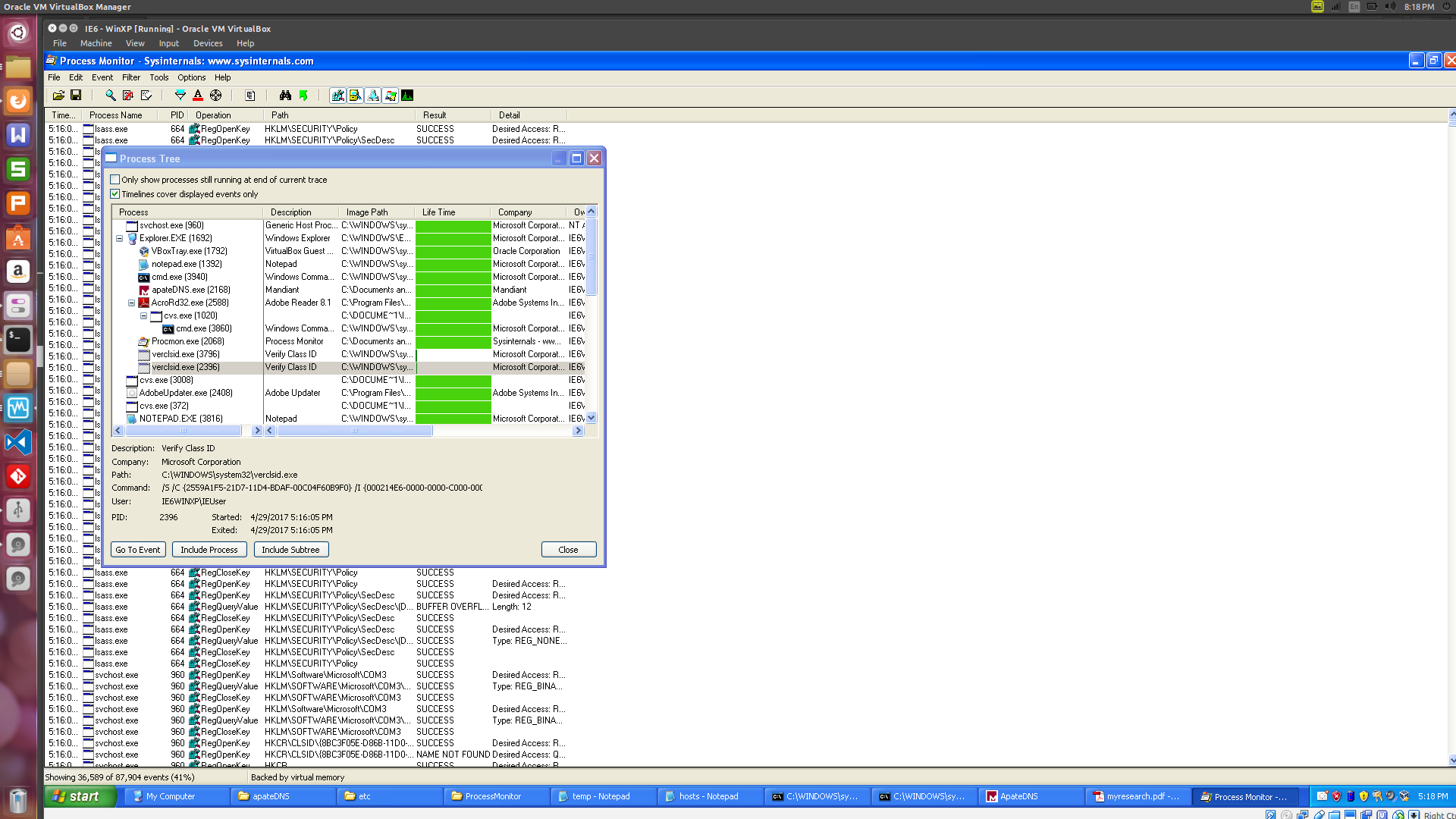
  
Illustration 4: Viewing the URL hit by the malicious PDF

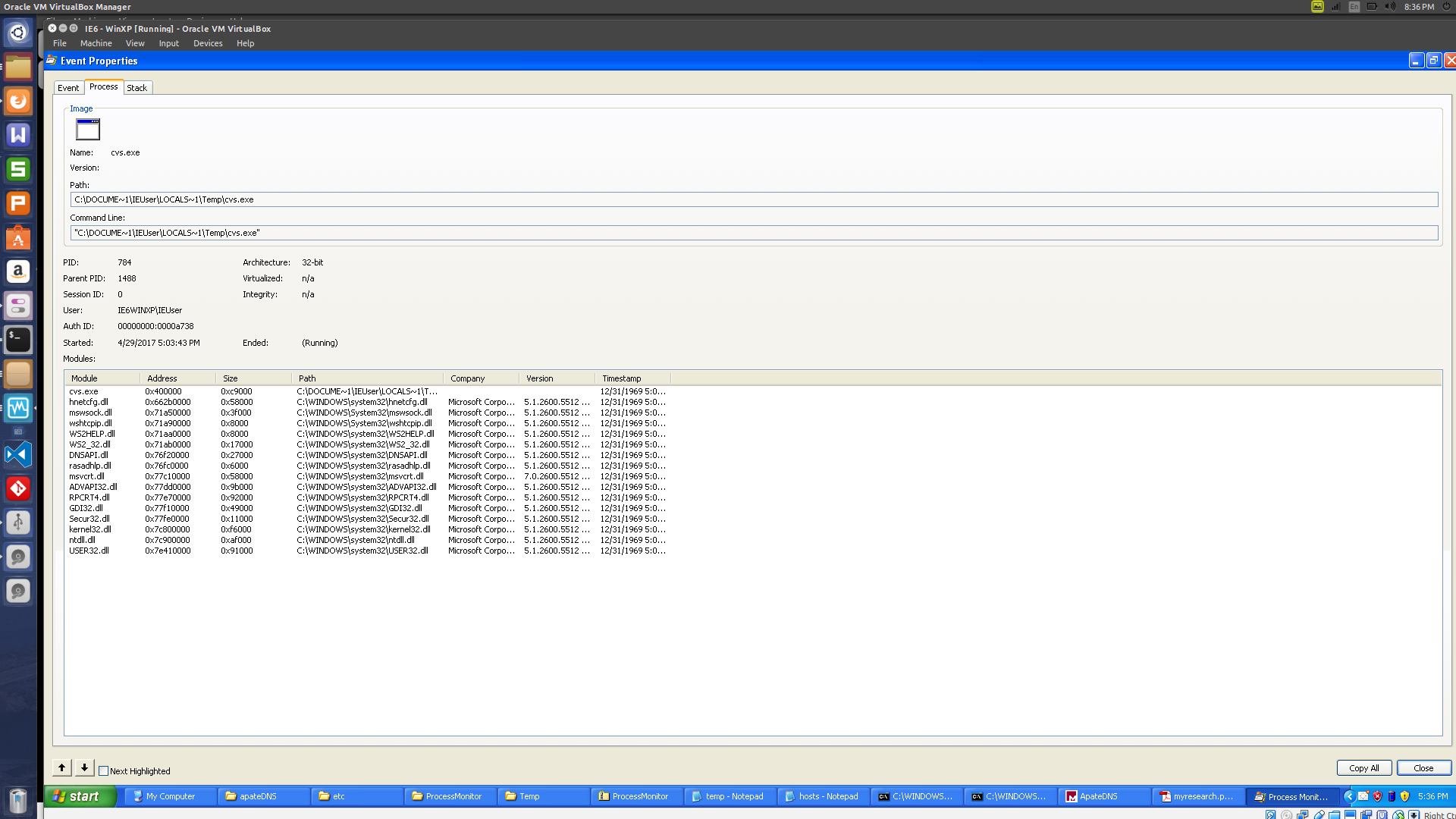
Next, I made changes to the hosts file at the location: C:\WINDOWS\systems32\drivers\etc and redirected the URL to the IP of another VM (REMNux).

  
Illustration 5: Directing the cvs.exe network call to REMNux IP

On REMNux, I started netcat and then I re-opened the malicious pdf on the XP VM.

  
Illustration 6: Netcat coomand on REMnux

  
Illustration 7: Process Monitor in XP VM showing the exe running with the PDF

  
Illustration 8: Details of all DLLs loaded by the executable

**EXE Filename:**

* EXE File Name:

***cvs.exe***

* EXE Comiple Time:

***Time/Date Wed Dec 31 19:00:00 1969***

* + ***(refer objdumpcvs.txt file)***
* EXE Type (.NET or Normal WinAPI executable? 32-bit? 64-bit?):

***32-bit***

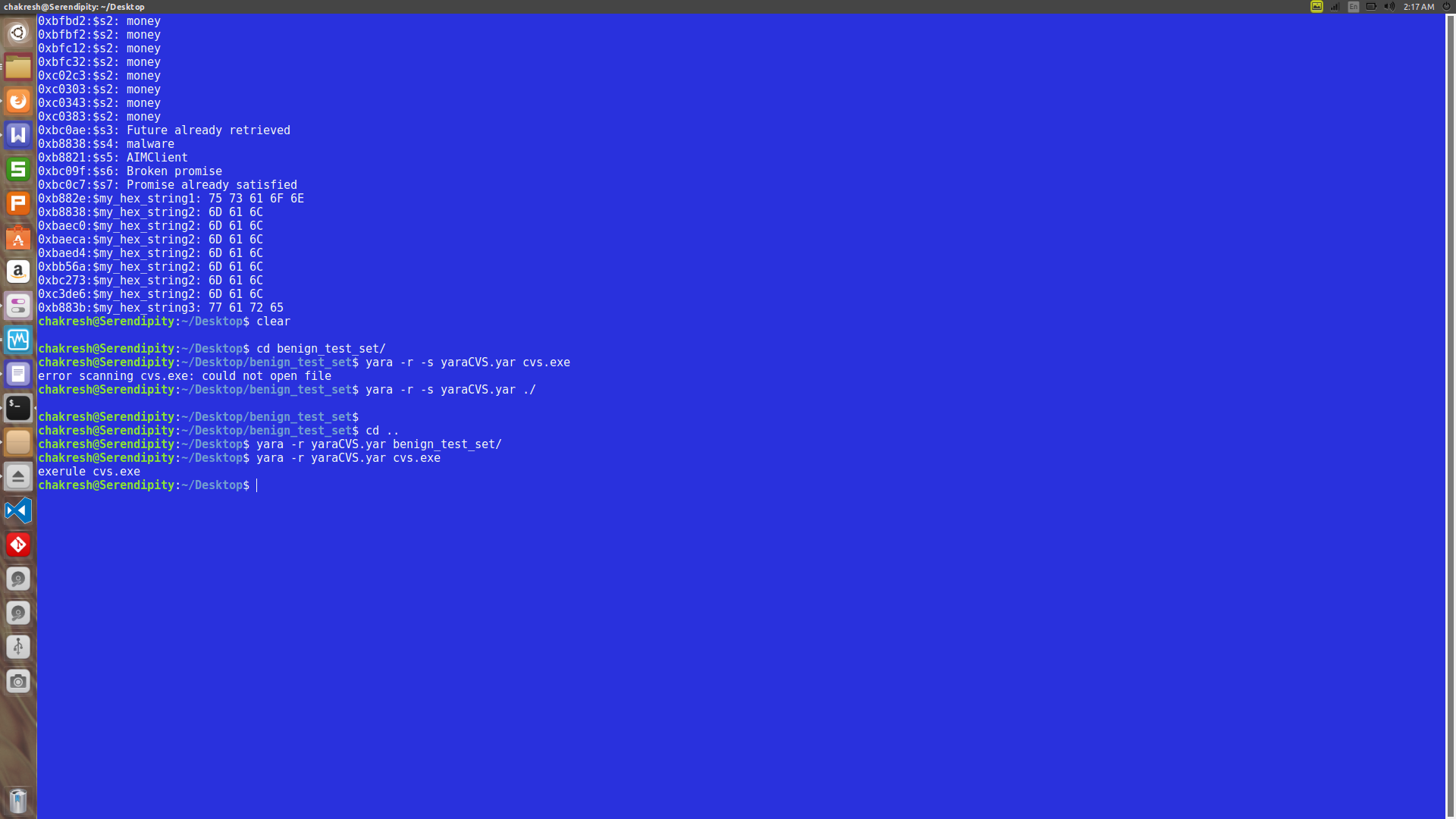
* DLL Imports (DLL filename, Symbol name):

***please see the illustration 8 above***

* How does the EXE achieve persistence (Registry Run? Start Menu? Service?):

**Start Menu (cmd.exe).**

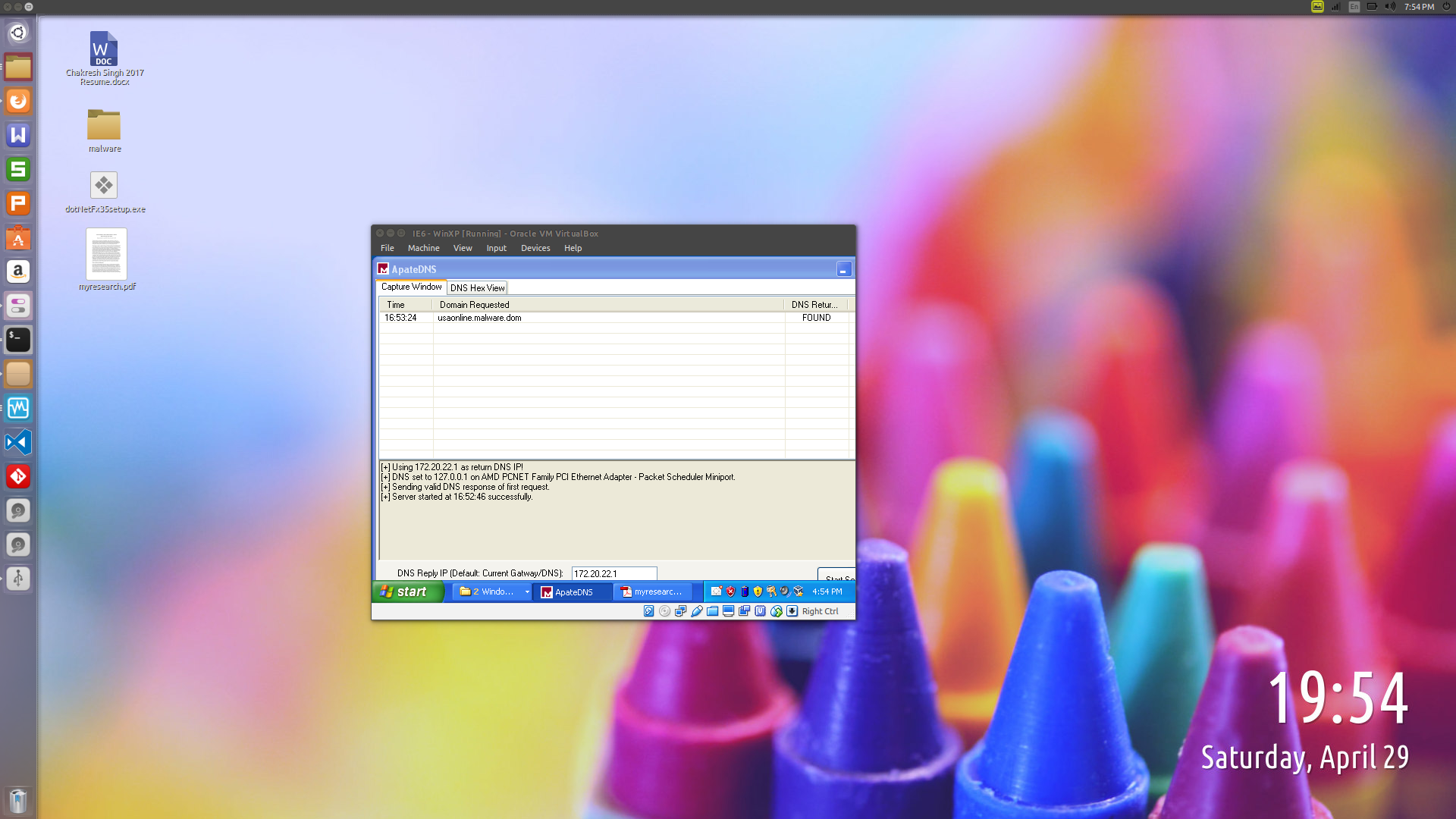
### **Analyze Strings from Malware:**

  
Illustration 9: Checking Yara

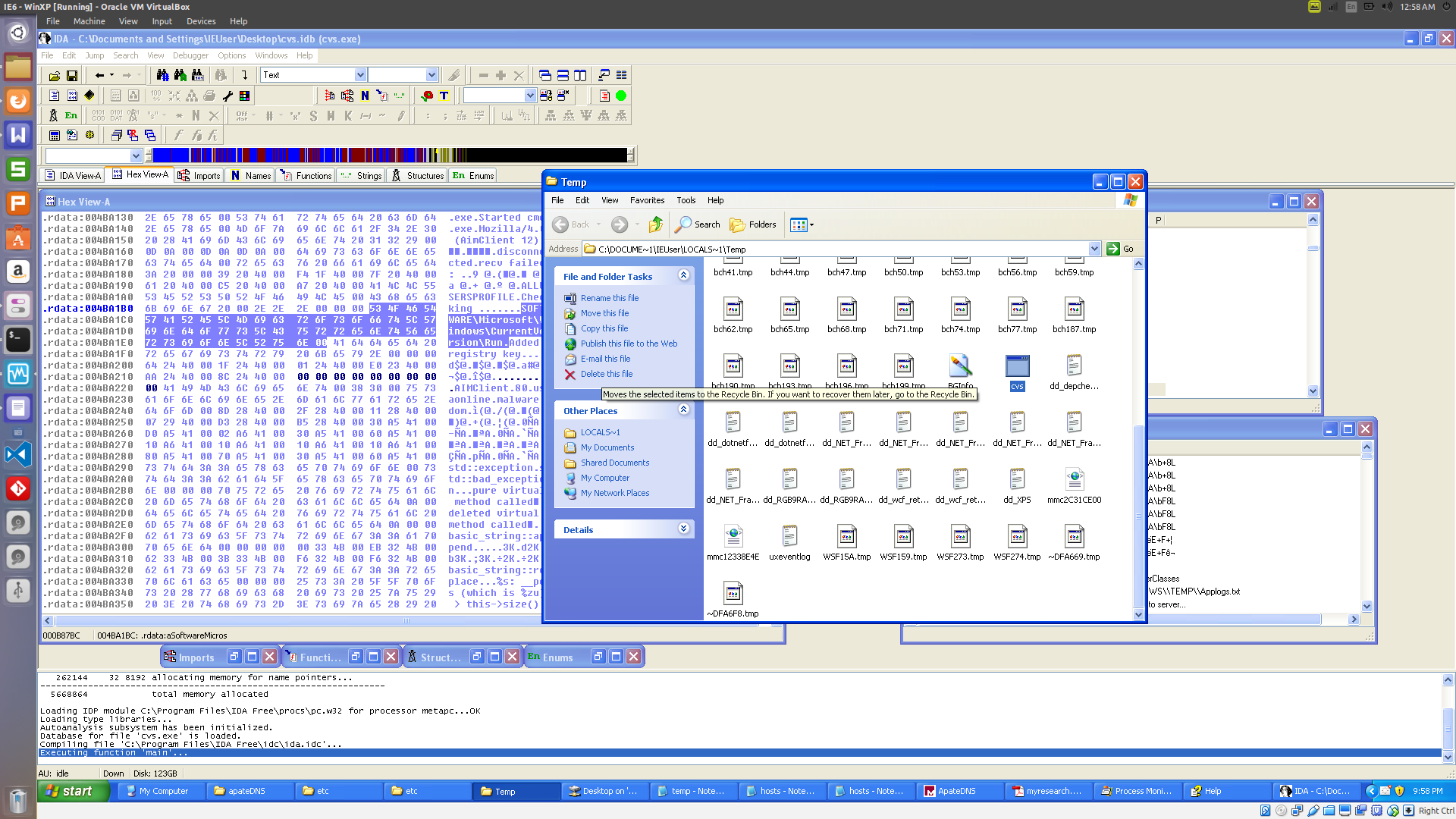
The yara rule for identify cvs.exe is included along (singhch-strings.yar) with the output of yara with -s argument (malwar\_exe\_yara\_s.yar). The Benign folder was also check for the same yara rule and it worked fine.

### **Backdoor Dynamic Analysis**

### **URL hit:** usaonline.malware.dom

  
Illustration 10: ApateDNS

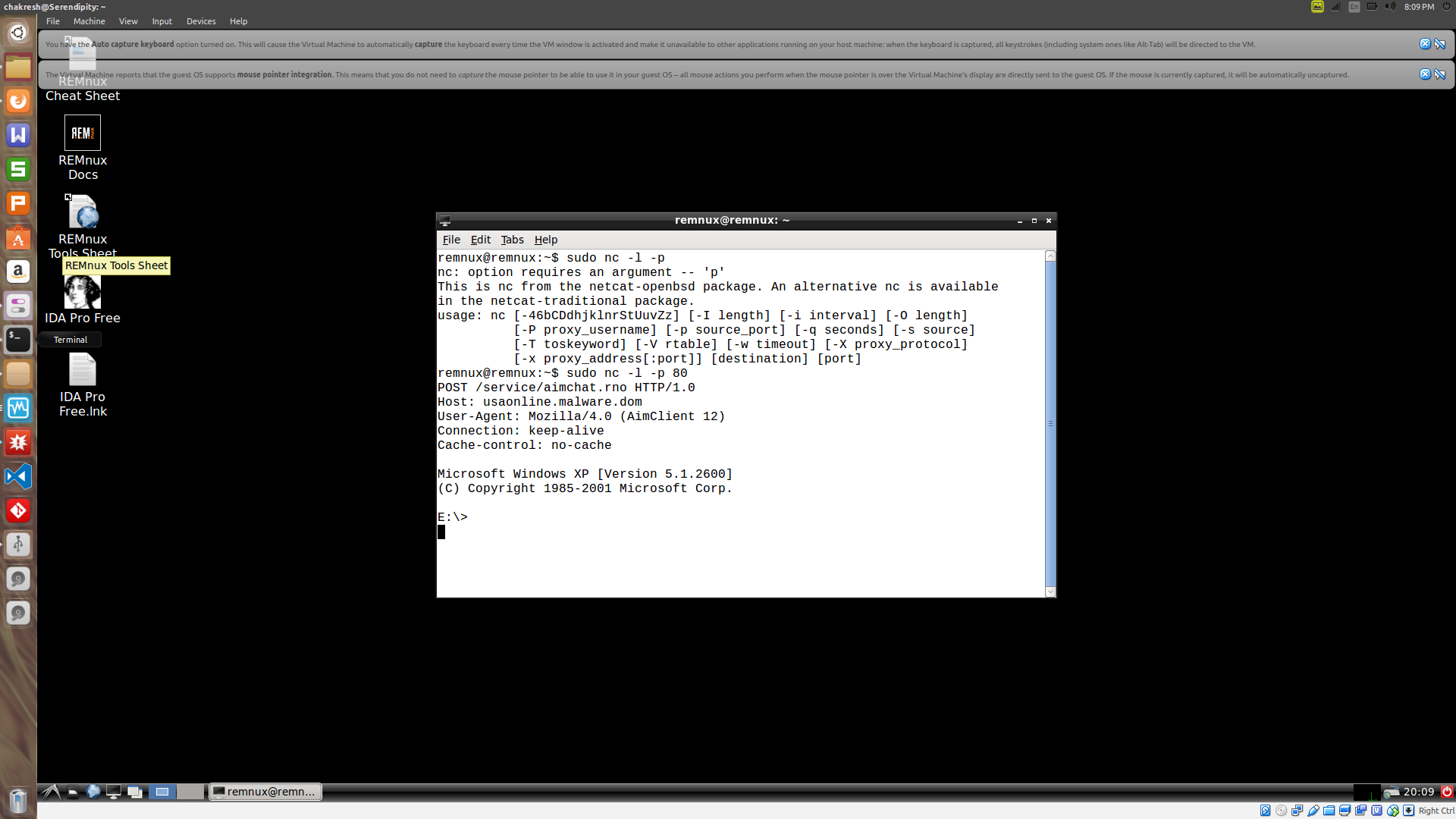
### **Analyze Strings from Malware:**

  
Illustration 11: cvs.exe in the temp folder

**Where was this EXE installed on the system?**

In the temp folder: can search %temp% in the run prompt.

### **Document the HTTP traffic:**

  
Illustration 12: running NETCAT on REMux to observe HTTP traffic

* What is the HTTP path requested?

**/service/aimchat.rno HTTP/1.0**

* What is the HTTP command/verb being used?

**POST**

* What is the User-Agent value being sent (one of the HTTP headers)?

**Mozilla/4.0**

--------------------------------------------------------------------------------------------------------------------------------------

This concludes my analysis of the malware pdf.

Regards,

Chakresh Singh