

# LAB 6: NETWORK FORENSICS TECHNIQUES

## INTRODUCTION

In this lab, we will examine a malware generation toolkit called “DarkComet-RAT”. We will infect a virtual machine with the malware, and examine the network traffic generated by the malware to identify the source of the attack.

In this lab we'll act as the hacker, victim and then the forensic investigator. Once we have had fun playing with the malware we will then conduct a live forensic investigation. Your final report will purely be from the point of view of the investigator and the findings from your analysis.



**Note:** The malware toolkit we are using in this lab is real. While it can be used for legitimate purposes (such as infecting our own machine in the lab for testing purposes, or remote administration of your own computers), it should not be used outside this environment, and should *definitely* not be used on any computer you do not own.

## RESOURCES AND LINKS

- Wireshark - <http://www.wireshark.org>
- DarkComet Remote Administration Tool (*development discontinued by Author*)
- TinyWeb <http://www.ritlabs.com/en/products/tinyweb/download.php>

## LAB OUTLINE

1. Configure Hacker's Computer (Role: Hacker) .....	2
Configure Hacker's Network Settings .....	2
Generate Malware .....	3
2. Configure Victim's Machine (Role: Victim) .....	6
3. Take Control of the Victim's PC (Role: Hacker) .....	9
3. Live Forensic Investigation (Role: Investigator) .....	11
Scenario .....	11
Report .....	12
Live Forensic Triage .....	13
Locate Malware, and Source of Attack .....	14
Determine Timeline of Infection .....	15
Saving Data for Report .....	17
Appendix 1: Wireshark Interface Explanation .....	18

# LAB 6: NETWORK FORENSICS TECHNIQUES

## 1. CONFIGURE HACKER'S COMPUTER (ROLE: HACKER)


In this exercise, we'll be using two VMs:


ICT30010-Lab6-Hacker will be our hacker's computer and will also be used to generate the malware.

ICT30010-Lab6-Victim will be our "victim" machine. We'll be infecting it with our malware and using the tools in the VM to monitor the network traffic generated by the malware.

### CONFIGURE HACKER'S NETWORK SETTINGS

First, let's set up the hacker's PC, and generate our malware.

1. Start the ICT30010-Lab6-Hacker VM, and configure the network settings
  - a. Locate the "ICT30010-Lab6-Hacker.zip" file on T: and extract the ZIP file to your desktop.
  - b. Start the VM by running the "Windows XP Professional.vmx" file (the  icon)
  - c. You'll note that the Tinyweb web server program starts automatically. We'll be using TinyWeb to serve up our malware. All we need to do is get our victim to download and run a program.


Make a note of the "Root directory" in tinyweb, before clicking the "hide button" (you can also access this window by right-clicking on the tinyweb icon in the system tray () and selecting Options.

TinyWeb Root Directory: .....

- d. change the IP address of the "Local Area Connection" on the Hackers virtual machine
  - i. IP Address: 192.168.x.1  
(replace "x" with the last 2 digits of your student ID number)
  - ii. Subnet Mask: 255.255.255.0
  - iii. Gateway: Leave the gateway blank.

To get to the network connections in XP, click "Start", "Network Connections", and right-click the network adapter you wish to change, then select properties.

## LAB 6: NETWORK FORENSICS TECHNIQUES

- e. Check that you've set the IP address properly by opening a command shell (click  in the taskbar) and run "ipconfig".

```
Ethernet adapter Local Area Connection:  
  
    Connection-specific DNS Suffix  . :  
    IP Address. . . . . : 192.168.x.1  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . :
```

Figure 1. Example Output from ipconfig

### GENERATE MALWARE

2. Let's run the DarkComet Client program. This program allows you to generate the malware application that we will get the "victim" to run. It is also the tool you use to remotely control the victim's computer.
  - a. Launch the DarkComet client program from the icon on the desktop.
  - b. Click "I Accept" if you agree to the Terms and conditions.

You'll now be presented with the DarkComet Client screen. The default view is the "Connections" screen. This will show you any available "servers" (infected clients) which you can connect to, including details about the user and Operating System.

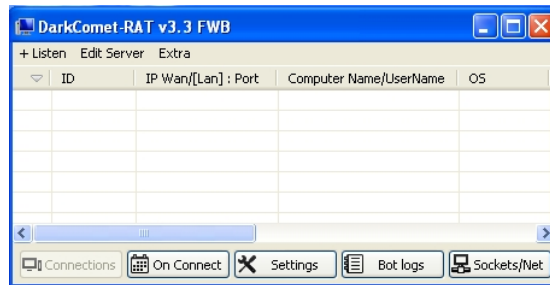


Figure 2. DarkComet-RAT Connections Window

The buttons on the bottom of the window allow you to select between the different views ("Connections", "On Connect", etc.). The "+ Listen" menu item tells DarkComet to listen out for incoming connections from infected machines. The "Edit Server" menu lets us create our malware (server module) or a small program to download our malware from a web server (server downloader).

## LAB 6: NETWORK FORENSICS TECHNIQUES

3. Let's create our malware.
  - a. Select "server module" from the "Edit Server" menu

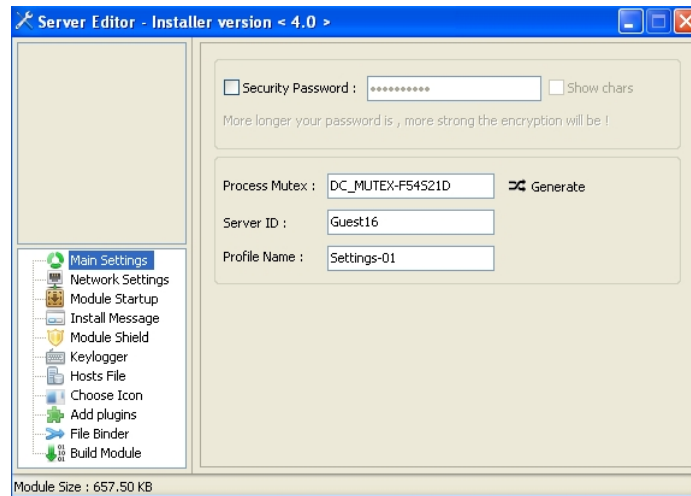


Figure 3. DarkComet Server Editor Window

The Server Editor window lets you choose various options for your malware. We'll only configure a few options in this case, but you may want to take a look at the range of features in the malware generator (including the ability to run at every startup, disable certain windows security features, and log the user's keystrokes).

4. First, we need to tell our malware where to connect back to.
  - a. Under the "Network Settings" in the server editor, enter the IP address of our Hacker's computer (192.168.x.1). Leave the port as "1604", and then click the "Add this configuration" button.  
  
If you can't remember the IP address of the hacker's computer, it is shown in the top section of the network settings window.
5. Let's also disable some of the stealthier functions of the malware, so we can locate it more easily - Under "Module Shield", disable "Active FWB (Explorer injection)"
6. Just so we don't accidentally start our malware without knowing, make it show a message when it runs.
  - a. Under "Install Message", tick the checkbox "Display a message box on first module load"
  - b. Pick an icon to display in the message window, and enter a message (something like "you've just been infected", or if you wanted to be more discrete something like "Error 24533")

## LAB 6: NETWORK FORENSICS TECHNIQUES

- c. You can see what your message will look like by clicking “Test Message Box”

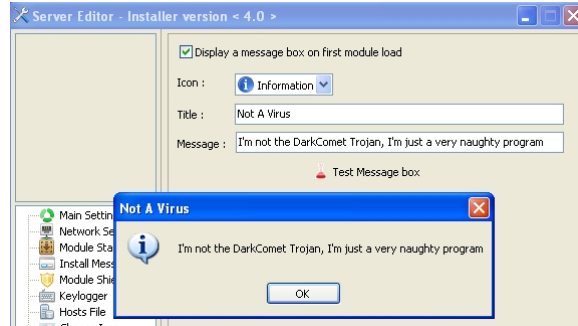


Figure 4. Example DarkComet Startup Message

7. Choose a custom icon for your malware.
  - a. Under the “Choose Icon” section, select “Custom Icon”, and choose an icon
8. Now let’s create the .exe file which will be our malware.
  - a. Under “Build Module” section, leave the default options, and click “Build Server”
    - i. Path: tiny web root directory you noted earlier.
    - ii. File name: server **(do not include an extension or any other values, windows will automatically add the “.exe”)**
  - b. Browse to the tiny web root directory and confirm that your malware is there (but don’t run it!)
9. We’re nearly done. Now we have the malware accessible to anyone that can connect to our web server. We just need to start the DarkComet program’s listening service to allow infected computers to announce themselves.
  - a. Close the DarkComet Server Editor window if you haven’t already.
  - b. Click the “+ Listen” button in DarkComet, leave the listening port as 1604 and click “Listen”. When prompted, select “Unblock” to let the program through the Windows firewall
  - c. If you now check the “Sockets/Net” window (click the button at the bottom of DarkComet’s client interface), you should now see one open socket listed.

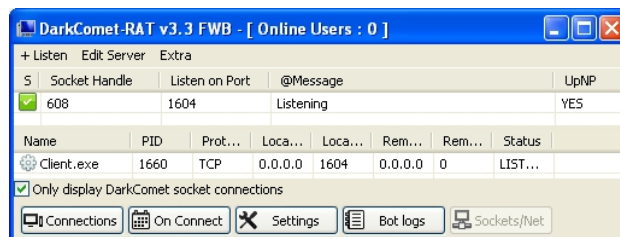



Figure 5. DarkComet Sockets/Net Window

## LAB 6: NETWORK FORENSICS TECHNIQUES


### 2. CONFIGURE VICTIM'S MACHINE (ROLE: VICTIM)

First, let's set up the victim's PC, and generate our malware.

10. Start the ICT30010-Lab6-Hacker VM, and configure the network settings

- a. Locate the "ICT30010-Lab6-Victim.zip" file on T: and extract the ZIP file to your desktop.
- b. Start the VM by running the "Windows XP Professional.vmx" file (the  icon)
- c. Change the network settings in the Victims's VM to:
  - i. IP Address: 192.168.x. 2 (use the same subnet as before - replace "x" with the last 2 digits of your student ID number)
  - ii. Subnet Mask: 255.255.255.0
  - iii. Gateway: Leave the gateway blank.

To get to the network connections in XP, click "Start", "Network Connections", and right-click the network adapter you wish to change, then select properties.

- d. Check that you've set the IP address properly by opening a command shell (click  in the taskbar) and run "ipconfig".

```
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix  . : 
IP Address. . . . . : 192.168.x.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Figure 6. Example Output from ipconfig

## LAB 6: NETWORK FORENSICS TECHNIQUES

11. While we're at the command prompt, let's take a look at what network services are currently running on the VM.
  - a. Run "netstat" with the same options you used last week. Remember we want to list "all" connections and listening ports, and to make sure the ports are listed in numerical form (run "netstat -an")

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1206	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1038	127.0.0.1:1039	ESTABLISHED
TCP	127.0.0.1:1039	127.0.0.1:1038	ESTABLISHED
TCP	127.0.0.1:1041	127.0.0.1:1042	ESTABLISHED
TCP	127.0.0.1:1042	127.0.0.1:1041	ESTABLISHED

Figure 7. Example Output from Netstat

- b. Observe the listed connections. Observe the foreign addresses column it should only list 0.0.0.0:0 (all IP addresses) or \*, if a remote computer is connected to this computer it will be listed as a foreign IP, make note of them here (there shouldn't be any at this stage, so leave this section blank if that is the case):

Connection 1 – Foreign Address: ..... State: .....

Connection 2 – Foreign Address: ..... State: .....

Connection 3 – Foreign Address: ..... State: .....

12. Now we have the malware configured and ready for use, let's start monitoring the network traffic (we'll examine the captured traffic later). A victim wouldn't typically have Wireshark going during a hacking attempt, but for the purposes of this lab, let's just assume that the victim's network is being monitored.
  - a. Open "Wireshark" from the start menu of the victim's computer, and then click the "Interface list" to list the networking interfaces available in the VM. Identify the interface which you set the IP address for earlier (192.168.x.2), and click the "Start" button for that interface.

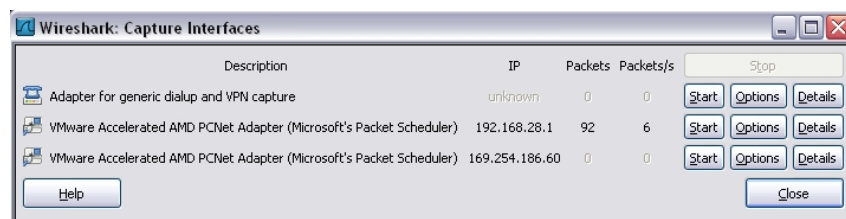


Figure 8. Interface List in Wireshark

## LAB 6: NETWORK FORENSICS TECHNIQUES

13. Now we want to infect our victim's computer. Normally, a hacker might entice a victim to click a link or download a program by sending an email to them (e.g. "Your \$200 order from Amazon has just been shipped. Open the attached document for more details.") or via a 0-Day exploit without the victims consent

In this case, we'll simply visit the hacker's website and infect ourselves this will also help to generate some additional traffic that we can investigate.

- a. Open Internet Explorer from within the Victims VM.
- b. Type the address "http://192.168.x.1/server.exe" (replacing the x with the IP address you set for the hacker's server).
  - i. If you've entered the correct URL, you should be prompted with what you would like to do, click "Save".
- c. Once the file has downloaded click "Run" to execute the malware
  - i. Windows also warns you that the file does not contain a valid digital signature. Software manufacturers like Microsoft will "sign" their applications so that users know that the software came from them. Click "Run" on the windows Security Warning dialog.
  - ii. You should now see the message box you configured earlier – we've now infected the victim's computer, click OK on the message box.
  - iii. You can close internet explorer if you wish but ensure Wireshark is still running.



## LAB 6: NETWORK FORENSICS TECHNIQUES

### 3. TAKE CONTROL OF THE VICTIM'S PC (ROLE: HACKER)

Let's now use the DarkComet client program to take control of the victim's computer, and generate some traffic that we can investigate.

14. Back on the Hacker's PC, let's see if DarkComet has recognised our newly infected computer.
  - a. In the DarkComet "Connections" window you should now see one entry listed. Note the Operating System version of the infected computer:  
.....
15. Double click on the victim's entry in the connections window to open the DarkComet control window. Here you can see a number of in-built functions that the DarkComet malware has to control a remote computer.
  - a. Send the victim a message, by using the "MessageBox" function (located under "Fun Functions"). Choose an icon, title and message, then click "Send" to send this message to your victim. Jump back to the Victim's VM to see your message
  - b. From the Hacker's PC, capture the victim's keystrokes:
    - i. Double click on "Keylogger" (found under the "Spy Functions" section)
    - ii. Click "Activate Keylogger"
    - iii. Go back to the Victim's computer, open Notepad (start -> run -> notepad <enter>), and type "I'm typing out a really sensitive document. I hope no-one is watching me." Its best to use English words instead of garbage characters as this will make locating the evidence easier.
    - iv. Back on the Hacker's computer, click the "Get the Logs" button to see what was captured (do not use the option "Online Keylogging" as the logs will not be visible in wireshark).

**The logs will not come through immediately keep typing in your notepad document on the victim and pressing the "Get the Logs" button on the Hacker, the logs will come through eventually as there is a timed delay.**

Name: .....

Student ID: .....

## LAB 6: NETWORK FORENSICS TECHNIQUES

- c. Open a web browser on the victim's computer
  - v. Double click the "Browse Page" item under "Network Functions" in the DarkComet Control panel, and enter the URL of your tiny web server - i.e. <http://192.168.x.1/index.html> (if you forget the /index.html, Internet explorer may have already cached the homepage, and it won't show up in Wireshark)
  - vi. Check that the web browser opened on the victim's computer (i.e. see what the victim would have seen)
- d. We are now finished with the hackers virtual machine you can shut it down if you wish.

**End of Lab Setup Phase**

## LAB 6: NETWORK FORENSICS TECHNIQUES

### 3. LIVE FORENSIC INVESTIGATION (ROLE: INVESTIGATOR)

From this point on, let's approach the victim's computer as if we were conducting a live forensic investigation.

**It's your actions from here on that will form the basis for your written report for the assignment.**

**All of the previous steps are only relevant to the setup and preparation of the lab for you to now commence your forensic investigation and report. Do not include any of the previous steps in your report**

To assist with the completion of this lab refer to the following material:

- Lecture 03 - Computer Forensics
- Lecture 04 - Forensic Report Writing
- Lab 05 - Introduction to Networks

#### SCENARIO

You have been asked to investigate a potential malware attack by a Mr ImaVictim. You arrive at his house where you find his computer still running, with Wireshark capturing data. He advises you that he browsing the web when he downloaded a program called "server.exe". When he ran the program, a message popped up then nothing else seemed to happen. A short while later, his internet browser opened (without him clicking anything).

Mr ImaVictim states that he regularly monitors his network traffic with Wireshark, and is concerned that his activities may have been monitored by a third party, as he was writing a rather sensitive business proposal at the time.

You've been asked to locate any evidence that he can take to the police to help identify and prosecute the potential offender.

## LAB 6: NETWORK FORENSICS TECHNIQUES

### REPORT

For this lab, you'll need to write up a report for Mr ImaVictim outlining your observations of their computer, the process you followed and the findings of your live forensic analysis.

This report may be used by the police or in court if Mr ImaVictim decides to take further action.

Your report should be factual and include enough information for another forensic examiner to replicate or validate your results and findings. The language use in the report needs to be suitable for the intended audience.

The audience for your report will be Mr ImaVictim, police, lawyers, judges and other non-technical people.

It is important that opinions and other suppositions are not part of your report.

All work presented in the final report must be your own, do not screenshot the lab sheet and include it in your report.

You will be marked on:

1. System Triage - An explanation of how you dealt with the live running system upon arrival including the process undertaken, tools used and the documentation of the critical system information (3 marks)
2. Live Forensic Analysis - The content of your report including the steps undertaken as a part of your analysis and the location and presentation of the evidence relating to the malware compromise (5 marks)
3. Presentation - Your overall presentation of the report and your ability to stick to the facts while presenting an accurate report that is appropriate to the target audience (2 marks)

## LAB 6: NETWORK FORENSICS TECHNIQUES

### LIVE FORENSIC TRIAGE

As this is a live forensic investigation we should collect as much information about the running system as possible prior to the system shutdown. How you approach this step of the investigation is entirely up to you, you may choose to navigate via the GUI, use command line tools (Sysinternals Suite is in the C:\) or a combination of both. What is important is the documentation of the steps you followed and the results produced.

#### 16. Time details:

- a. System Date: .....
- b. System Time: .....
- c. System Timezone: .....
- d. Current Date: .....
- e. Current Time: .....
- f. Time Variation (+/-): .....

#### 17. Operating System Details

- a. OS Name: .....
- b. OS Version: .....
- c. System Uptime: .....

#### 18. User Account Details

- a. Logon Time: .....
- b. Logged on User: .....

#### 19. IP Address Details

- a. IP Address: .....
- b. Subnet Mask: .....
- c. MAC Address: .....

## LAB 6: NETWORK FORENSICS TECHNIQUES

### LOCATE MALWARE, AND SOURCE OF ATTACK

20. Let's check the task manager to see if we recognise any suspicious processes (in this case, we have a head start – we know the executable file was called "server.exe")

- Open the windows task manager by right clicking the taskbar and selecting "Task Manager"
- Click on the "Processes" tab and sort by "Image Name".
- Show the Process ID column by selecting "Select Columns" from the "View" menu.
- Locate the "server.exe" in the Image Name. Note the PID of the malware:

PID: .....

21. If we weren't able to locate the malware so easily by knowing its name, we might try locating it by checking for processes with currently open network connections. In this case, let's verify that the PID we just located is our malware by checking for open network connections.

- Let's re-run netstat to see what network connections are open. This time, though, let's add another option to display the Process ID (PID) of the program making the connection, and see if we can find anything associated with the "server.exe" process.. So run "**netstat -ano**" from a command line window (open a new one if you need to).
- Locate the entry for our malware. Remember the hacker's machine is listening on port 1604.

Foreign Address: ..... State: ..... PID: .....

22. With the information we now know about the malware executable locate where it is stored on the Victims computer and document the following information

- File Name: .....
- Path: .....
- Size: .....
- Created: .....
- Modified: .....
- Accessed: .....

## LAB 6: NETWORK FORENSICS TECHNIQUES

### DETERMINE TIMELINE OF INFECTION

We'd also like to locate evidence to determine a timeline of events. This could be useful to later match up with the suspect's computer, to help build the case that it was, in fact, them who distributed the malware. In this case, we were lucky enough to also have a full packet capture of the internet traffic that occurred while the victim was infected, and during the time the attacker was controlling the computer. Normally, we'd examine this packet capture from our forensic workstation, to minimise changes to the machine we're investigating, but in this case, we'll just review the packet capture on the live machine.

23. In Wireshark, change the Time Display format to show you the time packets were capture.
  - a. Under the "View" menu, select "Time Display Format", then "Date and Time of Day"
24. Locate the initial HTTP request that prompted the malware download.
  - a. What time was the malware downloaded? .....
  - b. What was the Full Request URI for the malware? .....  
(this is under the HTTP layer of the packet details section)
  - c. Copy the summary details as "CSV" by right-clicking on the packet and selecting "Copy", then "Summary (CSV)".
  - d. Open notepad (start -> run -> notepad <enter>), and paste this copied data in. We'll collect details of a few packets, so leave notepad open.
25. Locate the HTTP reply packet which contained the data from the executable.
  - e. Select the "Media Type" header from the packet details window, then right click and select "Export Selected Packet Bytes...". Save a copy of the file.

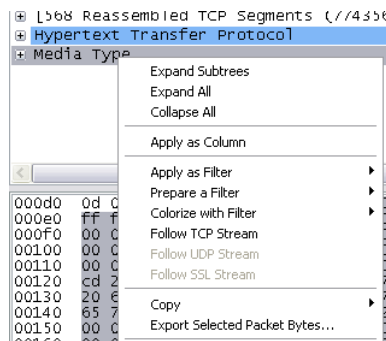


Figure 9. Wireshark Menu Showing "Export Selected Packet Bytes" Option

Obtaining a copy of the malware could be very important to our investigation. When we locate the suspect, we could then examine their computer and attempt to locate an identical file.

Name: .....

Student ID: .....

## LAB 6: NETWORK FORENSICS TECHNIQUES

- f. Right click on the saved file and select properties. Note the file size:

server.exe File Size: .....

26. Back in Wireshark, locate the HTTP request that was generated by Firefox when the hacker was remotely controlling the machine.

g. What time was the webpage opened? .....

h. What was the Full Request URI for the web page? .....

i. Copy the CSV summary of this packet, and paste it into notepad (make sure it's on a new line)

27. We earlier identified that the attacker was on the local network (since they shared a similar IP address), we should be able to identify the attacker's MAC address by examining the ARP traffic.

j. What is the MAC address of the Attacker? .....

k. Copy the CSV summary of this packet, and paste it into notepad (make sure it's on a new line)

28. If you were able to obtain the keylogging information, you should be able to identify the packet that contains the logged data. Since the DarkComet program doesn't use a specific known protocol (i.e. Wireshark can display, but cannot interpret, the messages going back and forward between the client and server), let's just look for large TCP packets going to the hacker's computer.

✓ If you weren't able to get DarkComet to retrieve any keylogging data, try again now. Repeat the steps under 15c. Ask for help if you still can't get the keylogger to work.

- a. Filter your Wireshark view using "tcp.len > 100 and ip.dst == 192.168.x.1" (using the full IP address of the hacker's computer)
- b. Browse the TCP packets manually, paying particular attention to the packet bytes section. You will hopefully find a packet that contains the text displayed by the keylogger

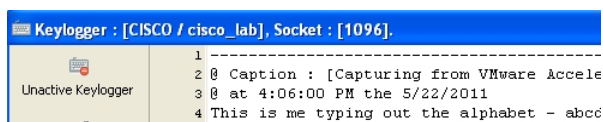


Figure 10. DarkComet Keylogger Window

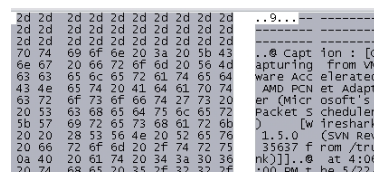


Figure 11. Wireshark Packet Bytes showing Keylogged Data

c. What time was the key logged data sent? .....

d. Copy the CSV summary of this packet, and paste it into notepad (make sure it's on a new line)



## LAB 6: NETWORK FORENSICS TECHNIQUES

### SAVING DATA FOR REPORT

As you'll need to produce a report for this lab, you may want to save the data you collected from the "victim's" computer.

29. To save the list of packets you copied from Wireshark
  - a. Save the Notepad file you created to the desktop as "packets.csv" (it will then open directly in Excel on another computer)
  - b. Copy the file to your main computer's desktop by dragging the file from the VM.
  - c. Email the file to yourself, or save it on a USB drive.
30. If you wish, you can save the entire packet capture (which you can later read in another version of Wireshark on your own PC)
  - a. First, click the "Stop the running live capture" button on the Wireshark toolbar
  - b. Select "File" then "Save As".
  - c. Make sure "All packets" and "Captured" are selected, otherwise you may only save a small subset of the total capture packets.
  - d. Move this file to your main desktop computer, then email it to yourself or save to a USB drive.

# LAB 6: NETWORK FORENSICS TECHNIQUES

## APPENDIX 1: WIRESHARK INTERFACE EXPLANATION

Each line in the **Packet List** pane represents a single packet. Listed with each packet is the time (in seconds since you began the capture), the source address (IP or MAC) and destination address of the packet, the protocol (e.g. TCP, DNS) and a basic description of the contents of the packet (e.g. DNS “Standard query A [www.google.com](http://www.google.com)” is a DNS lookup for the IP address of the Google web server).

You can also see the packet broken down further by clicking on the packet you are interested in the **Packet List** pane, and viewing the details in the bottom two panes (**Packet Info** and **Packet Bytes**).

**Filter entry toolbar:** filter the list of packets by entering expressions

**Packet List:** displaying basic info about the packet. Clicking a packet here shows the packet broken down further in the panes below.

**Packet Info:** broken down by protocol layer (e.g. IP over Ethernet)

**Packet Bytes:** Raw packet data. Clicking a row in the pane above highlights the relevant raw data byte(s).

Figure 12. Wireshark Window

Remember that data travelling across a network is encapsulated (or wrapped up) as it passes down from one network layer to the next (i.e. Application -> Presentation -> Session -> Transport -> Network -> Datalink -> Physical), before it travels across the physical medium (e.g. CAT5 cable). The data is then unwrapped as it traverses back up the layers. This means that each layer may add headers and/or footers to the data. A single captured packet may contain a number of these headers and footers surrounding the actual sent “data” (as shown to the right – a typical UDP packet).

Wireshark breaks down packets in the **Packet Info** pane, showing you as much detail as it can about the data in each layer.

Ethernet Header	14 bytes
IP Header	20 bytes
UDP Header	8 bytes
Data	1,472 bytes ~ 8,954 bytes
Ethernet Trailer	4 bytes