Name: .....

Student ID: .....

LAB 5: INTRODUCTION TO NETWORKS

INTRODUCTION

The purpose of this lab is to investigate some common network protocols using Wireshark, and to understand some of the types of information we can obtain from monitoring network traffic.

We'll monitor some website traffic, and determine the MAC address of the machine that's communicating with us.

We will then explore the use of various command line tools that may assist with a live forensic investigation

RESOURCES AND LINKS

- Wireshark
  http://www.wireshark.org
- Web Server Log Files (Apache specific)
  http://httpd.apache.org/docs/2.0/logs.html

LAB OUTLINE

Name: .....

Student ID: .....

LAB 5: INTRODUCTION TO NETWORKS

1. CONFIGURE SERVER RUNNING TINYBOX WEB SERVER

For this exercise, we'll need to have two VMs. We'll use one to generate network traffic (the client) and one which will be serving up content for us to view (server) and monitoring the traffic using Wireshark.

First, let's set up the server.

1. Start the Server VM, and configure the network settings

    a. Locate the "ICT30010-Lab5-Server.zip" file on T: and extract the ZIP file to your desktop.

    b. Start the VM by double clicking on the "Windows XP Professional.vmx" file (the  icon) – ensure that it opened in VMWare or VMWare Player

    c. Ensure the VM network connection is set to "Host-Only" in the virtual machine settings

    d. Once the machine restarts, change the IP address of the "Local Area Connection"

        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.

    e. Check that you've set the IP address properly by opening a command shell "Start", "All Programs", "Accessories" and run "`ipconfig`".

```
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.xx.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
```

    f. Note your IP address: .....

2. While we're at the command prompt, let's take a look at what network services are currently running on the VM. Knowing how to acquire this information could be useful if you're conducting an investigation of a live computer, since it is unlikely we'll be able to recover it from the hard disk alone.

Name: .....

Student ID: .....

LAB 5: INTRODUCTION TO NETWORKS

We'll use the "netstat" command to determine all the ports in the "LISTENING" state, but running "netstat" without any other options won't provide us this.

a. Get help on the netstat command by running "`netstat -?`".

b. We want to find the options to list "all" connections and listening ports, and to make sure the ports are listed in numerical form.

c. Re-run the netstat command with the required options. You should see it return a screen similar to the following:

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:xxx            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:xxx            0.0.0.0:0              LISTENING
  TCP    127.0.0.1:xxxx         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 1. Example Output from Netstat

A single TCP connection consists of a source and a destination, each with its own port number. Port numbers are typically associated with particular network services or applications (e.g. 80 is usually for HTTP/web traffic, 25 is for SMTP/email). Netstat lists the local machine's address and port number (address:port) in the left column.

Note that "0.0.0.0" means all IP addresses, so that a line which read "TCP 0.0.0.0:123 0.0.0.0:0 LISTENING", would mean that *all* network interfaces on the computer will respond to incoming traffic on port 123 from *any* computer.

d. What port numbers are currently open on the server (i.e. port number of local addresses in the listening state)? (some port numbers may be listed more than once, but just list unique numbers)

Listening Port 1: .....

Listening Port 2: .....

Listening Port 3: .....

Listening Port 4: .....

Listening Port 5: .....

LAB 5: INTRODUCTION TO NETWORKS

3. Let's run a web server on this VM.

   Open "Tinybox" from the Windows Start menu (inside the VM), and note the "root" directory (this is where HTML pages and other resources can be stored, and will then be made available over HTTP):

   .....

   a. Click "Start" to start the web server, the "Hide" to close the window.

4. Re-run the netstat command as you ran earlier. Do you see any additional ports listed as "LISTENING"

   What port: .....

5. Open up web browser from within the VM and see the homepage of your web server by simply entering the IP address of your VM (which you configured and noted earlier).

6. Now we have the server up and running, let's start monitoring the network traffic (we'll examine the captured traffic later).

Figure 2. Tiny Box Web Server Default Homepage

   a. Open "Wireshark" from the start menu of the server, and then click the "Interface list" to list the networking interfaces available in the VM. Identify the interface that you set the IP address for earlier (192.168.x.1), and click the "Start" button for that interface.

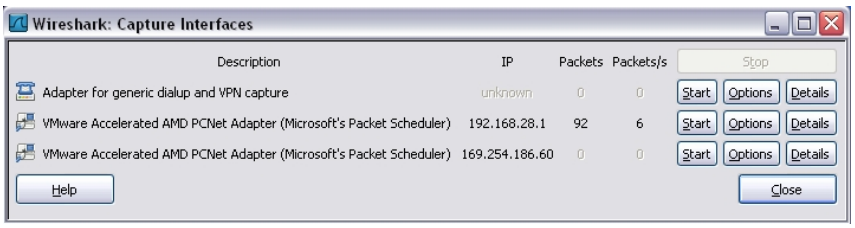


Figure 3. Interface List in Wireshark

7. Keep the Server VM (and Wireshark) running. Minimise it if you like.

Name: .....

Student ID: .....

LAB 5: INTRODUCTION TO NETWORKS

2. LIVE FORENSIC INVESTIGATION

When undertaking a live forensic investigation, we often rely on built in command line tools along with 3rd party tools such as the Sysinternals Suite to collect information relating to the operating system. We have already used the command line determine the IP address and open ports on the server. We will now explore some additional tools of interest.

8. Go back to the server VM.
9. Open the command prompt (click in the taskbar), we will explore some built-in tools
10. Type the command "`date /t`" followed by the command "`time /t`"
    a. System Date: .....
    b. System Time: .....
    c. Current Date: .....
    d. Current Time: .....
11. Type the command "`systeminfo`"
    e. OS Name: .....
    f. OS Version: .....
12. To make finding information easier, we can leverage the "findstr" command type the command "`systeminfo | findstr /B /C:"OS Name" /C:"OS Version"`"
13. Open the command prompt (click in the taskbar) and run "`cd c:\SysinternalsSuite`".
14. Type the command "`psinfo`"
    g. Uptime: .....
    h. Registered Owner: .....
    i. Registered Organisation: .....
15. Type the command "`PsLoggedOn`"
    j. Logon Time: .....
    k. Logged on User: .....
16. This is not a definitive list of all the tools available but will give you an idea of what can be achieved via the command line. The Sysinternals Suite is full of useful command line and GUI based applications.

LAB 5: INTRODUCTION TO NETWORKS

17. Consider a live incident response investigation, you will want to have an extensive set of tools that can capture relevant information from a running computer system. Explore the tools in the Sysinternals Suite and document 5 tool that may be useful for this task.

Tool Name	Purpose	Expected Results	Relevance

Name: .....

Student ID: .....

LAB 5: INTRODUCTION TO NETWORKS

3. START UP XP CLIENT, GENERATE NETWORK TRAFFIC

Our second VM is just a basic windows XP machine. We'll use it to generate some network traffic, and examine the traffic back on the server.

18. Start the Windows XP Client VM, and configure the network settings

    a. Locate the "ICT30010-Lab5-Client.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) – ensure that it opened in VMWare or VMWare Player

    c. Ensure the VM network connection is set to "Host-Only" in the virtual machine settings

    d. Change the network settings in the Client VM to:

        i. IP Address: 192.168.x.2 (use the same subnet as before, last 2 digits of your student ID number)

        ii. Subnet Mask: 255.255.255.0

        iii. Gateway: 192.168.x.1 (IP of the server)

        iv. Preferred DNS: 192.168.x.1 (IP of the server)

19. Check that you've set the network settings correctly by attempting to connect to the web server.

    a. Open Internet explorer on the Client VM, and enter the IP address of the server

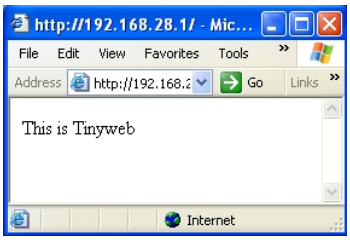


Figure 4. Tinyweb Server Accsesed from Client

Name: .....

Student ID: .....

LAB 5: INTRODUCTION TO NETWORKS

4. EXAMINE NETWORK TRAFFIC / WIRESHARK INTRO

WIRESHARK INTERFACE EXAPLAINATION

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" 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**).

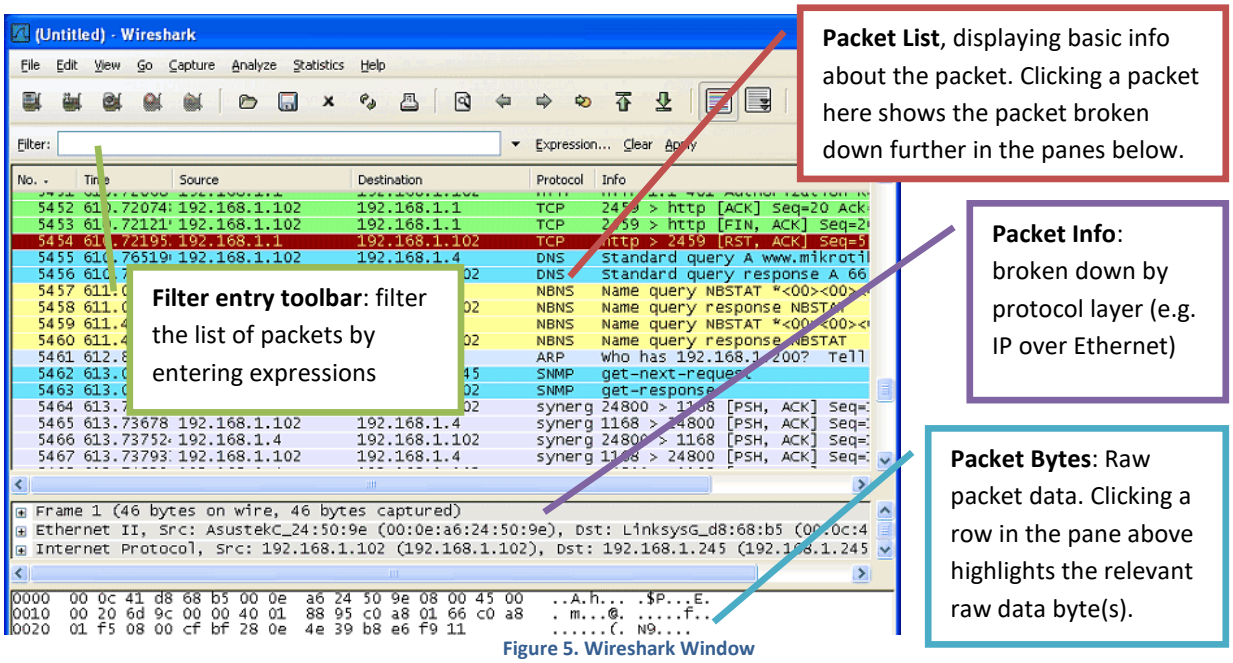
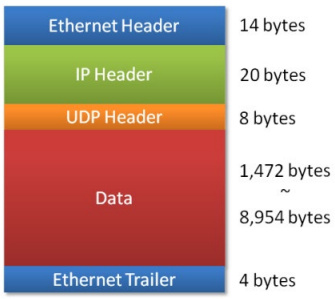


Figure 5. Wireshark Window

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.

Name: .....

Student ID: .....

LAB 5: INTRODUCTION TO NETWORKS

EXAMINE HTTP TRAFFIC

20. Go back to the Server VM, and let's take a look at what Wireshark.

21. By default Wireshark shows the timestamp as the seconds since the capture started, for investigation purposes we will find the date/time beneficial

    a. Within wireshark click View -> Time Display Format -> Date and Time of Day

22. Let's find the HTTP traffic we generated by accessing the web server

    a. Locate the web request and reply packets in Wireshark. They will be highlighted in Green near the bottom of the Packet List pane, and will be listed as "HTTP" protocol packets.

✓ While it may not be necessary in this exercise, if you start to deal with large amounts of data in Wireshark, you'll need to learn to use filters. You can click the "expression" button in the filter toolbar to help you generate filter expressions, or you can type them manually.

The Wireshark help file (Help | Manual Pages | Wireshark Filter), or the online documentation at http://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html should help you learn how to build filter expressions.

Expression	Meaning
tcp	List all packets using the Transport Control Protocol
udp.dstport == 63	List all UDP packets with a destination port of 63 (DNS traffic)
tcp.port == 80 and ip.src == 192.168.2.1	Just show packets from 192.168.2.1 on TCP port 80 (HTTP traffic)
ip.src == 192.168.1.1 or ip.dst 192.168.1.1	Show packets to or from 192.168.1.1

Figure 6. Wireshark Filter Expression Examples

    b. Locate the HTTP "GET" request packet (the HTTP layer), and answer the following questions:

        i. What is the "Request version" for this request? .....
        (you'll need to expand the items under "Hypertext Transfer Protocol" in the Packet Details pane)

        ii. What was the User-Agent of the client? (the user agent string identifies the internet browser that was used to request the page)

        .....

    c. Locate the HTTP reply packet (the HTTP layer), and answer the following:

        i. What version is the TinyWeb server reporting? .....

        ii. When was the page last modified? .....

LAB 5: INTRODUCTION TO NETWORKS

iii. Right click on one of the packets, and select "Follow TCP Stream". This view shows you the textual representation of the messages back and forward. This can be particularly useful when some of the messages/content may be broken up across multiple packets.

You'll also notice that the full HTML source code of the home page "<html><body>This is Tinyweb</body></html>" is available – we could save whole web pages from within Wireshark if we needed to.

In the HTTP reply packet, examine the Ethernet layer.

iv. What is the MAC address of the server? .....

v. What is the MAC address of the client? .....

vi. Verify these values by running "`ipconfig /all`" on both virtual machines (click in the taskbar, or find the "Command Prompt" under Start | Programs | Accessories)

EXAMINE ARP TRAFFIC

While we requested the web server using its IP address (OSI Network Layer), devices that communicate other over Ethernet actually identify each other by MAC address (OSI Data Link Layer). You're probably familiar with the protocol that converts domain names (such as google.com) to IP addresses – that's DNS (Domain Name Service). The protocol which helps convert IP addresses to MAC addresses is called ARP (Address Resolution Protocol).

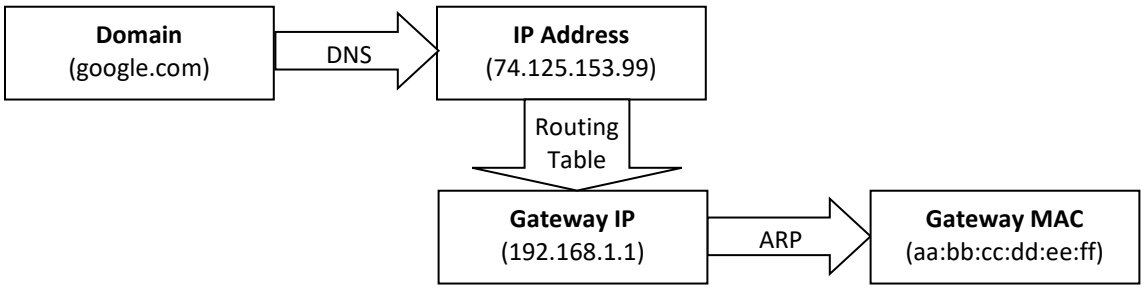


Figure 7. DNS, Routing Tables and ARP Explanation

When connecting to a website, our computer first looks up the IP address of the server we're trying to connect to using **DNS**. If the IP address is not on our local network (as determined by the **routing table**), we can't talk directly to the web server using Ethernet, so we need to talk to the gateway first. Our computer then converts the gateway's IP address to a MAC address using **ARP**.

23. Let's examine the ARP traffic that we generated while connecting to the Web server.

    a. Filter data in Wireshark to only that using the "arp" protocol. Remember our client and server was "192.168.x.1" "192.168.x.2"and, so find an ARP request that is asking "Who has 192.168.x.2?". This is an "ARP request". The reply should follow immediately after (e.g. "192.168.x.2 is at aa:bb:cc:dd:ee:ff").

Name: .....

Student ID: .....

LAB 5: INTRODUCTION TO NETWORKS

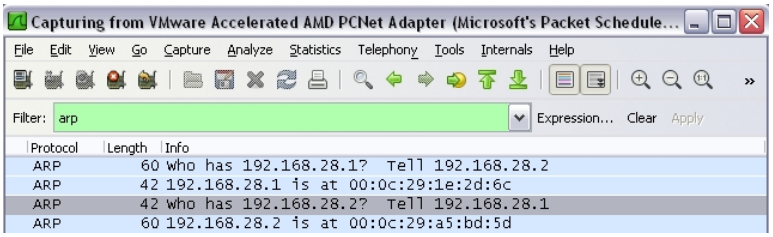


Figure 8. Wireshark ARP Packets

b. Answer the following questions about the ARP request (you'll need to be looking at data in the Packet Details and the Packet Bytes panes):

   i. At what offset (in hex) is the target MAC address? .....

   ii. What is the target MAC address? .....

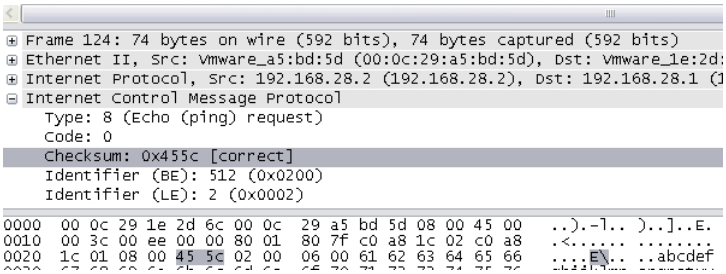


Figure 9. ICMP Ping packet shown in Wireshark.
Note the ICMP Checksum is selected in the Packet Details pane, highlighting the relevant data in byte view (hex offset 24)

c. Now take a look at the ARP reply packet (the one that says "192.168.x.2 is at ...."), and answer the following:

   i. What is the MAC address for the sender? .....

   ii. At what offset (in hex) is this located? .....

Name: .....

Student ID: .....

LAB 5: INTRODUCTION TO NETWORKS

5. EXAMINE LOG FILES

While the live packet capture can provide huge amounts of information, including the ability to view downloaded web pages, as forensic examiners we will rarely have access to this amount of information (unless we have a lawful data interception order, or are monitoring traffic on our own network).

Typically in network forensics, we'll only be provided with log files. Let's finish up by quickly examining the log files generated by TinyWeb.

24. Open the TinyWeb Log files.

    a. Locate the TinyWeb icon in the system tray on the server (), right click it and select "Logs".

    b. Take a look at the "Access", "Agent", "Error" and "Referer" logs by clicking the appropriate buttons.

        i. The **Access log** should show you each request that is made of the server, including the IP address the request came from, the date and time of the request, and exactly what was requested (e.g. "GET / HTTP/1.1" means get the page "/" using v1.1 of the HTTP)

        ii. The **Agent log** lists the User Agents (the string identifying a browser version) have been accessing the website.

        iii. The **Error** and **Referer** (sic.) logs will probably be empty. The Referrer can be useful sometimes, however, as it will tell you what page a user was on *before* they visited the web server (Did they type the link in manually, or did they come from a Google search, etc.).

    The exact format of these logs may differ from server to server, but they will usually contain at least this basic information.

    c. From examining the logs, what time did you first connect to the web server from the client?

    .....