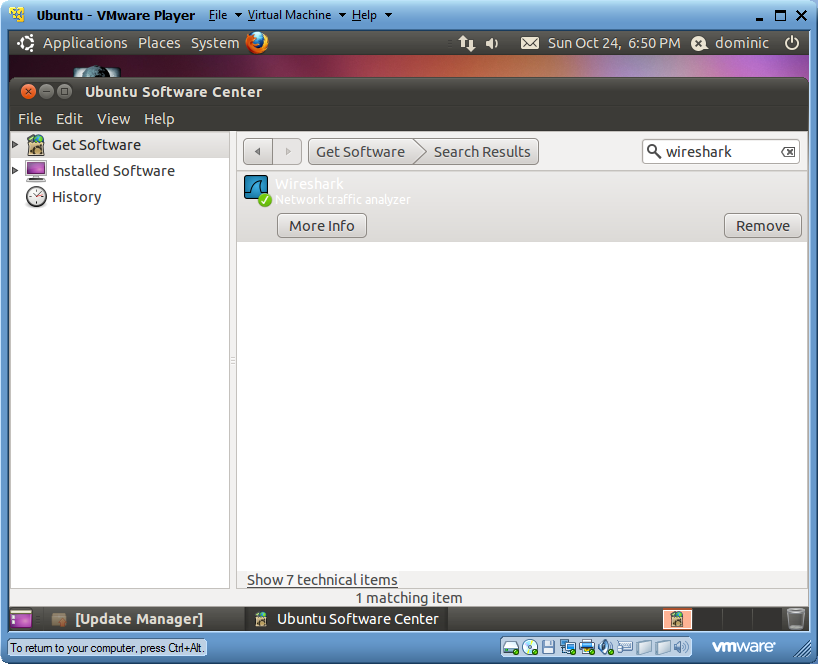
# Task 3 – Capture and analyze network traffic:

1. Boot Ubuntu using VMPlayer. Login as the user you created in Task 1 (dominic).
2. Install Wireshark traffic capture utility:
   1. Click the Applications menu option from the taskbar at the top of the screen
   2. Select the “Ubuntu Software Center” from the list of available choices. Different versions of Ubuntu may say different things.
   3. In the search bar, enter “Wireshark”. When the results come up, click “Install” next to the Wireshark result. Wait for it to download and install.



1. Install Apache Tomcat Web Server:
   1. Open a new shell window by clicking Applications menu option from the taskbar at the top of the screen, navigating to the “Accessories” item, and clicking “Terminal”
   2. Once the shell window has started, execute these commands:
      1. sudo apt-get update
      2. sudo apt-get install apache2

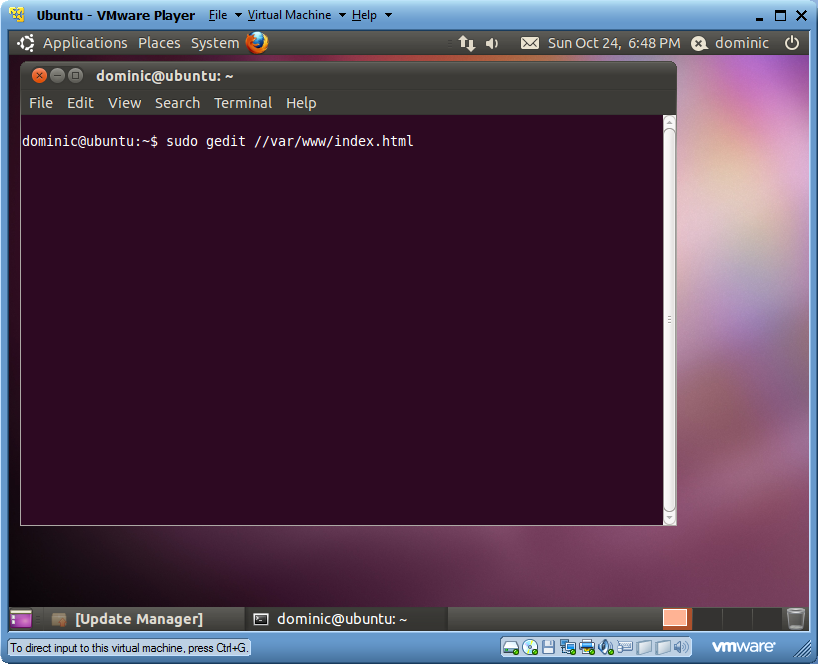
The first command updates the apt programs local database with the server’s pkglist files (in this case the default Ubuntu repository)

The second command gets and installs the apache2 tomcat module.

Both of these commands are executed with super user privileges.

* 1. Keep the terminal window open

1. Start Apache Tomcat using the following command:
   1. sudo apache2ctl start
2. Open the \*.html file that Apache Tomcat points to by default using the following command:
   1. sudo gedit //var/www/index.html



1. Once the index.html file is open in gedit, proceed to add a heading with your first and last name. Also add your date of birth using a heading 2 tag. The html file should look like:

<html>

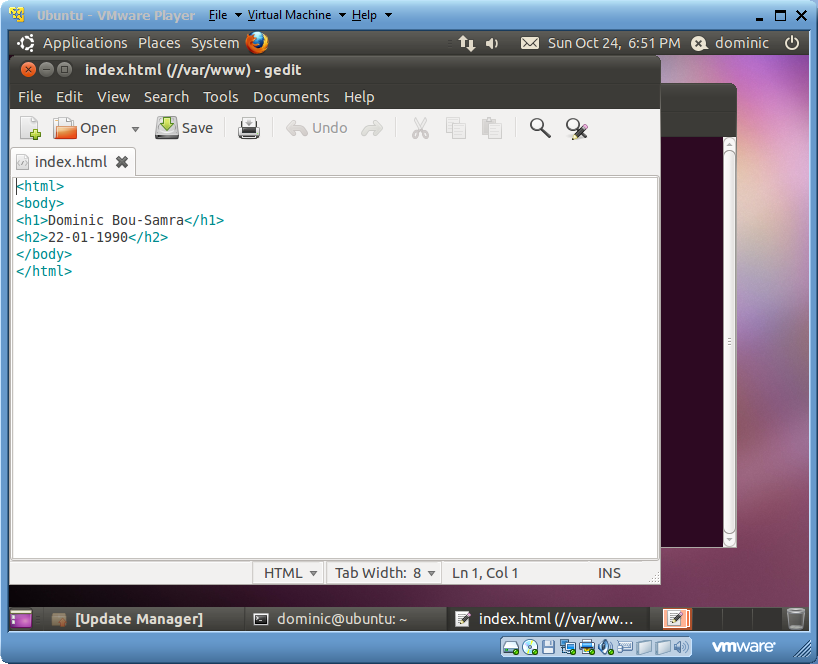
<body>

<h1>Dominic Bou-Samra</h1>

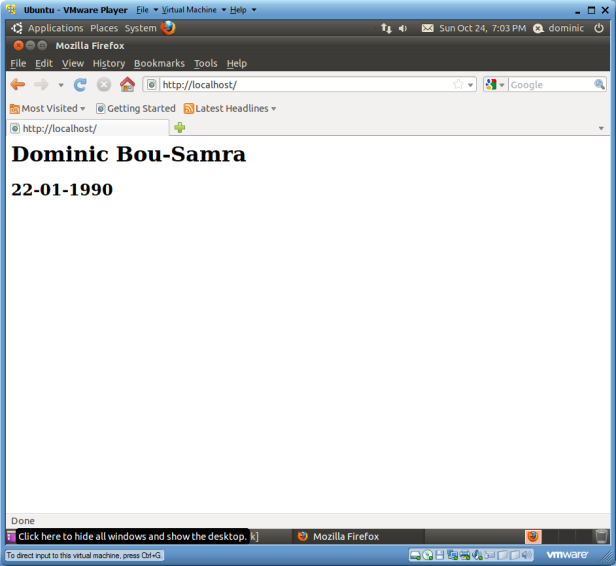
<h2>22-01-1990</h2>

</body>

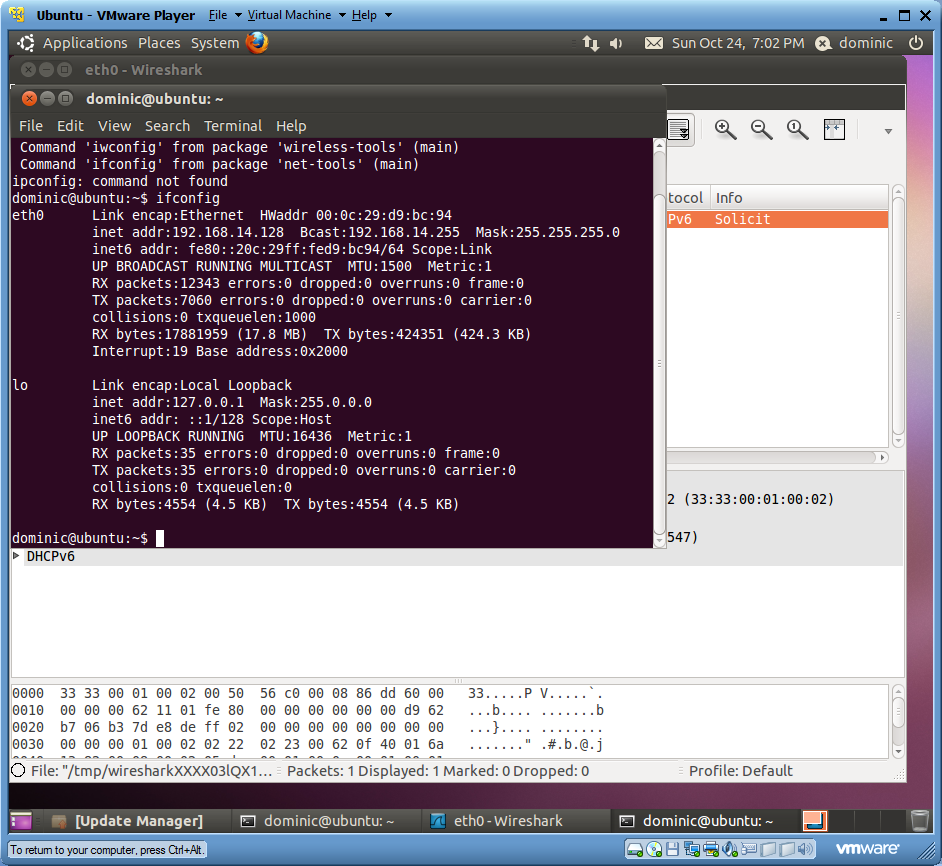
</html>



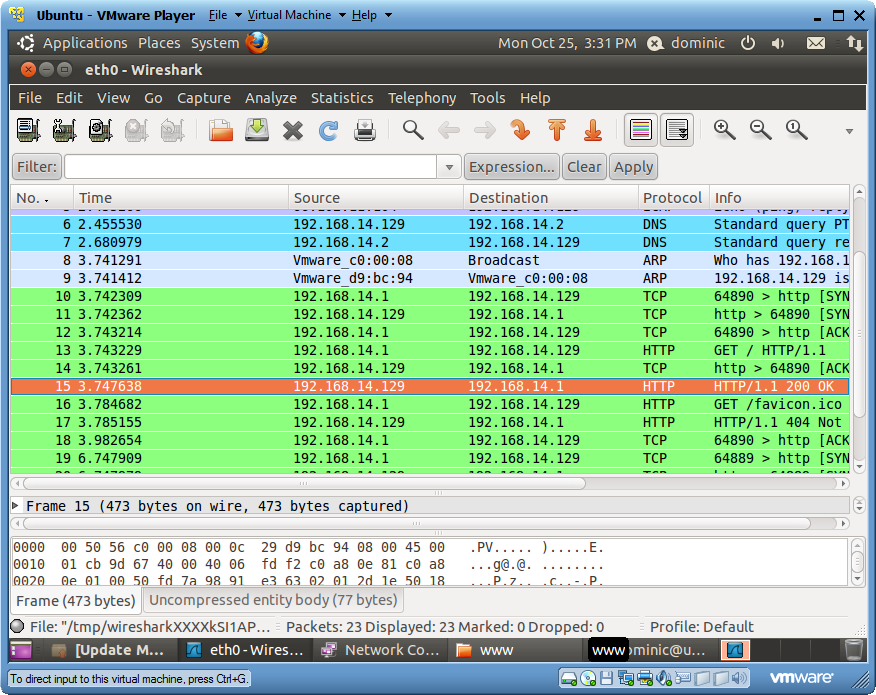
1. Verify Apache Tomcat is installed, running and is pointing to the index.html we just edited, by opening Firefox and accessing the localhost address (simply enter localhost). It should have the name and date of birth in large headings.



1. Capture Traffic to Localhost:
   1. Start Wireshark using the “Applications” menu button in the taskbar at the top of the screen. It is located under “Internet”.
   2. Obtain the virtual machines IP address by running the ifconfig command from the terminal. It will be something like 192.168.14.128.



* 1. To start capturing traffic click “eth0” under the Interface list.



* 1. Go to your host machine, and start your web browser. Attempt to access the IP address recorded above.

## *Analyzing the captured traffic:*

* DNS Traffic:
  + The Domain Name System is used to retrieve the literal address of a domain name. For example, when one wants to ping/whois a domain name like [www.google.com](http://www.google.com), the computer has no way to know it’s IPV4/IPV6 address, and needs to look it up. A DNS server will be queried and the Google’s IP address sent back. Once the name has been resolved to an address, communication can continue.
  + The biggest advantage to using the DNS protocol is that users are not required to remember difficult numerical addresses for websites and email addresses. This system was key in allowing the masses to unleash the power on the Internet.
  + Examining the DNS packets just prior to my ICMP ping request shows the virtual machine NIC sent a query for [www.google.com.au](http://www.google.com.au), and immediately after, a DNS query response was sent with the corresponding with the resolved IP address 66.102.11.104.
* ARP Traffic:
  + Address Resolution Protocol is a method for resolving a logical address (an IP address for example) against an absolute address (a MAC address). A table, usually called the “ARP cache” is used to maintain a correlation between logical and absolute addresses. It provides the rules (depending on the implementation) for making this match, and providing address conversion in both ways.
  + When a packet meant for a host machine arrives at the gateway (a router for instance), the gateway will attempt to match the IP address contained within the packet, to the absolute addresses stored in the ARP cache. If a match IS found, the packet is converted to the right length/format and sent along to the recipient.
  + In the event the ARP cache does not contain the IP address listed (out of date for example), the ARP program will broadcast a request packet to all machines on the network to see if a machines corresponding IP address matches. The cache will be updated, and the original packet is sent along to that MAC address.
* HTTP Traffic
  + Hypertext Transfer Protocol is the underlying protocol used by the worldwide web. It defines how Web Browsers should interpret information, and what actions should be taken in response to various commands.
  + Examining the packets sent and received when my host machine attempted to access the webpage hosted within the virtual machine, it can be seen that several HTTP requests were made by the host machine:
    - GET: The initial request asking for the web page located at 192.168.14.129.
    - OK: The web page text contents is sent. In this case, HTML

<html>

<body>

<h1>Dominic Bou-Samra</h1>

<h2>1990-01-22</h2>

</body>

</html>

* + - GET: The second get request looking for a favorite icon. None can be found, so Apache formulates a 404 webpage, and a response packet is sent. Whether to display this page or not is the browsers choice.