**LAB ASSIGNMENT 1**

**AIM**:

**To make students familiar with packet capturing concepts, use of various capturing tools and analysis of various protocols involved in communication between client and server**

**THEORY:**

**What does Packet Capture mean?**

Packet capture is a computer networking term for intercepting a data packet that is crossing or moving over a specific computer network. Once a packet is captured, it is stored temporarily so that it can be analyzed. The packet is inspected to help diagnose and solve network problems and determine whether network security policies are being followed.

Hackers can also use packet capturing techniques to steal data that is being transmitted over a network.

**Network managers analyze and manage overall network traffic and performance**. To examine and capture real-time running packets over a network, different packet capturing techniques are used.

One type of packet capturing is filtering, in which filters are applied over network nodes or devices where data is captured. Conditional statements determine which data is captured. For example, a filter might capture data coming from ABC route and having W.X.Y.Z IP address. Instead of filtering a specific portion of a packet, complete packets can also be captured.

**The full packet includes two things: a payload and a header. The payload is the actual contents of the packet, while the header contains extra information, including the packet's source and destination address**.

The different applications and uses of data capturing include the following:

* **Security**: Data capturing is used to identify security flaws and breaches by determining the point of intrusion.
* **Identification of Data Leakage**: Content analysis and monitoring helps to ascertain the leakage point and its sources.
* **Troubleshooting**: Managed through data capturing, troubleshooting detects the occurrence of undesired events over a network and helps solve them. If the network administrator has full access to a network resource, he can access it remotely and troubleshoot any issues.
* **Identifying Data/Packet Loss**: When data is stolen, the network administrator can retrieve the stolen or lost information easily using data capturing techniques.
* **Forensics**: Whenever viruses, worms or other intrusions are detected in computers, the network administrator determines the extent of the problem. After initial analysis, she may block some segments and network traffic in order to save historical information and network data.

**What are the advantages and disadvantages of Packet Capturing Tools?**

**ADVANTAGES:**

* It is used to debug communication between a client and a server.
* With packet capturing tools network is more secure so, network problems can be identified before they become serious
* Network administrator can monitor network users.
* Network administrator can monitor traffic and troubleshoot problems.

**DISADVANTAGES:**

* It is extremely time consuming to capture every packet and examine them
* Read all network packets that arrive which may contain Trojan horses

**Which are the different tools used for Packet Capturing?**

* **Wireshark or Ethereal**
* **Ksniffe**
* **Snort**
* **IpGrab**
* **Capsa**

**WIRESHARK:**

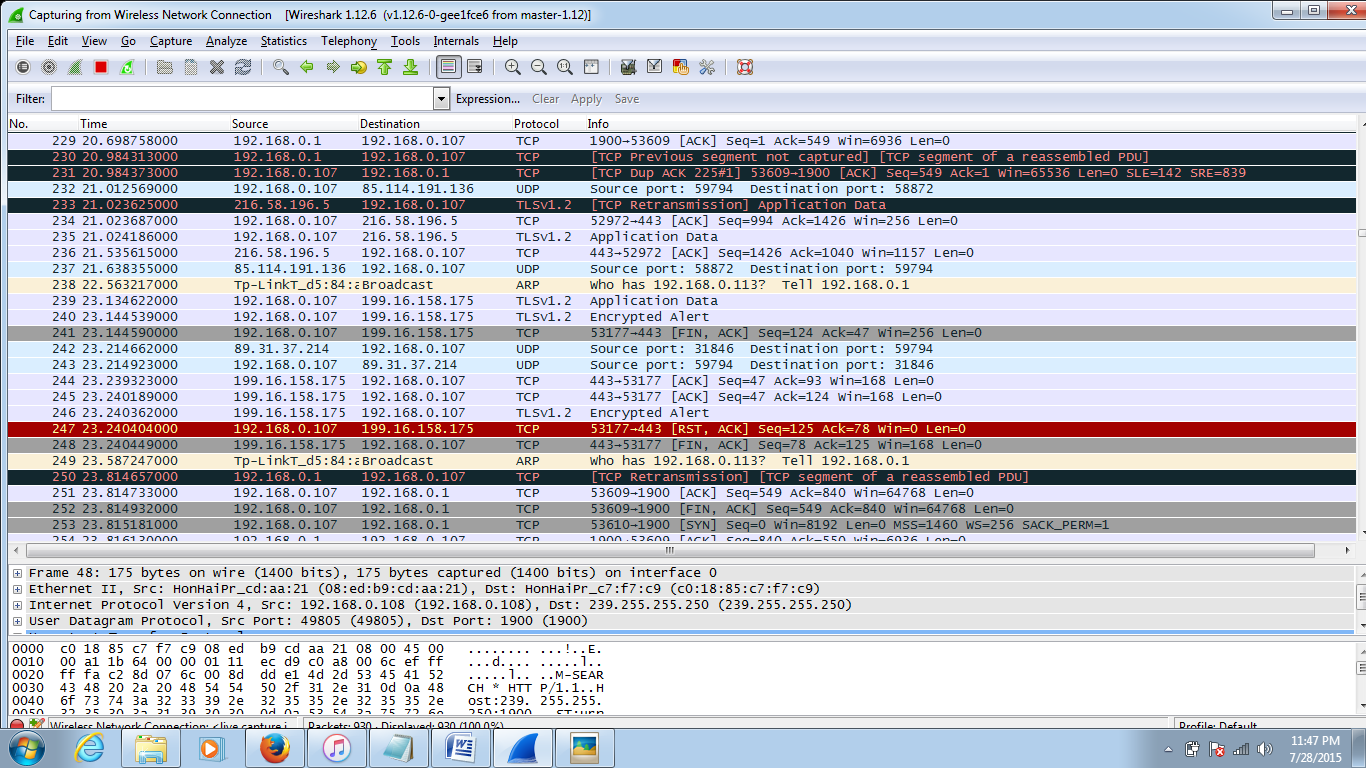
Wireshark is the world’s foremost network protocol analyzer. It lets you capture the traffic and browse it on a network

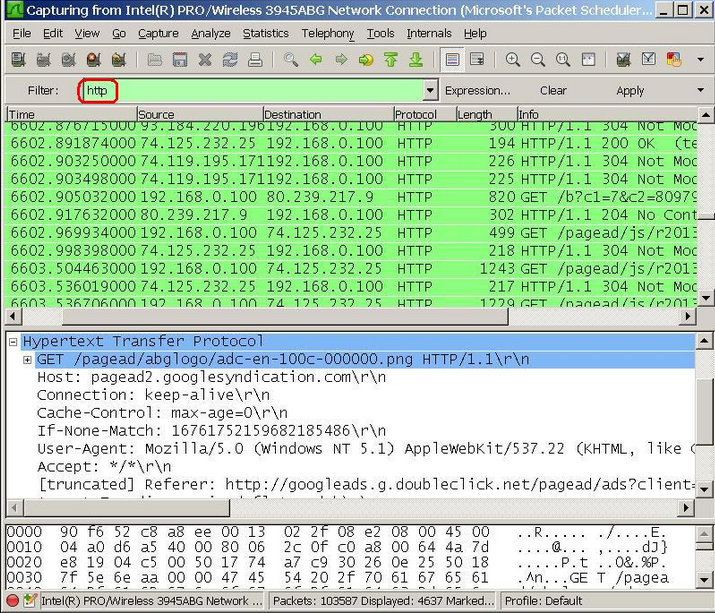
It is available for UNIX and WINDOWS

Capture live packet data from a network interface

Displays packet with very detailed protocol information

Filters **packet and colorize the filtered packet**

****

****

**What are the pros and cons of Wireshark?**

**Pros:**

* Open Source
* Support on Windows, Linux, MAC, Solaris
* Presence of both command shell and graphical user interface
* Port Mirroring

**Cons:**

* Running Wireshark through an admin account for multiple exploits, is unsecured
* Cannot manipulate things on the network
* Cannot be used for MIDM attacks
* Lack of modules for ARP poisoning and caching

**What are the pros and cons of Capsa?**

**Pros:**

* Well-organized interface.
* Easy-to-use.
* Provides information about a large number of network characteristics.

**Cons:**

* Quite high system requirements

**CONCLUSION:**

In this experiment, we studied and implemented Packet Capturing Tools **(WIRESHARK)**