Lab 4

Aim :- To analyze network traffic using TCP Dump and Wireshark to identify and examine different links accessed by a victim on a network.

# Theory:

**TCP Dump:** TCP Dump is a command-line packet analyzer that allows users to capture and analyze network traffic. It can capture packets at the packet level, providing detailed information about the

data exchanged over a network.

**Wireshark:** Wireshark is a graphical user interface (GUI) network protocol analyzer. It allows for the real-time inspection and analysis of the data being exchanged on a network. Wireshark supports a wide range of protocols and provides a user-friendly interface for packet analysis.

# Procedure:

**Install TCP Dump and Wireshark:**

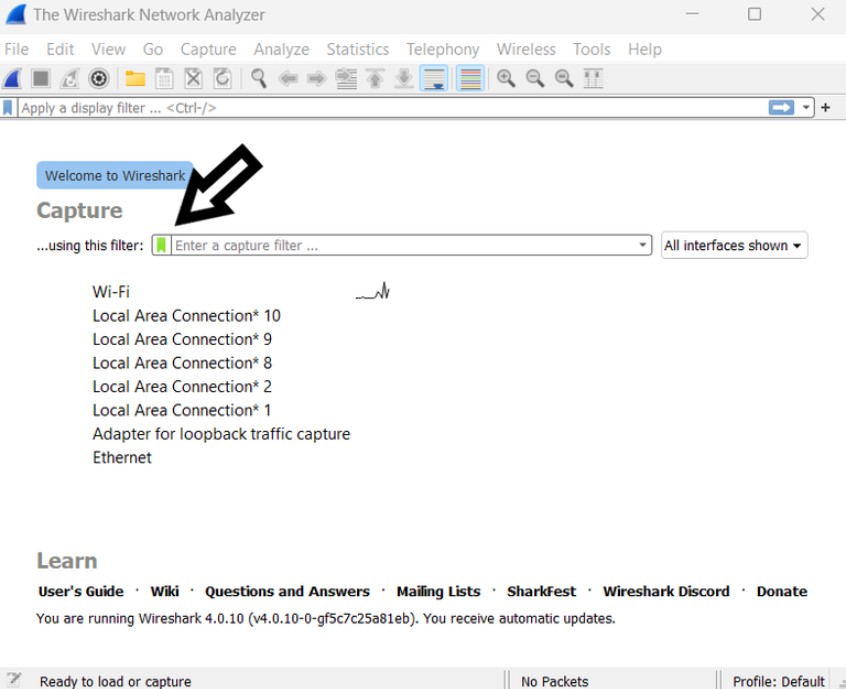
**For Linux**: Use package managers like **apt** or **yum** (e.g**., sudo apt-get install tcpdump wireshark**).

**For Windows:** Download and install the executable files from the official websites (https://[www.tcpdump.org/](http://www.tcpdump.org/) and <https://www.wireshark.org/>).

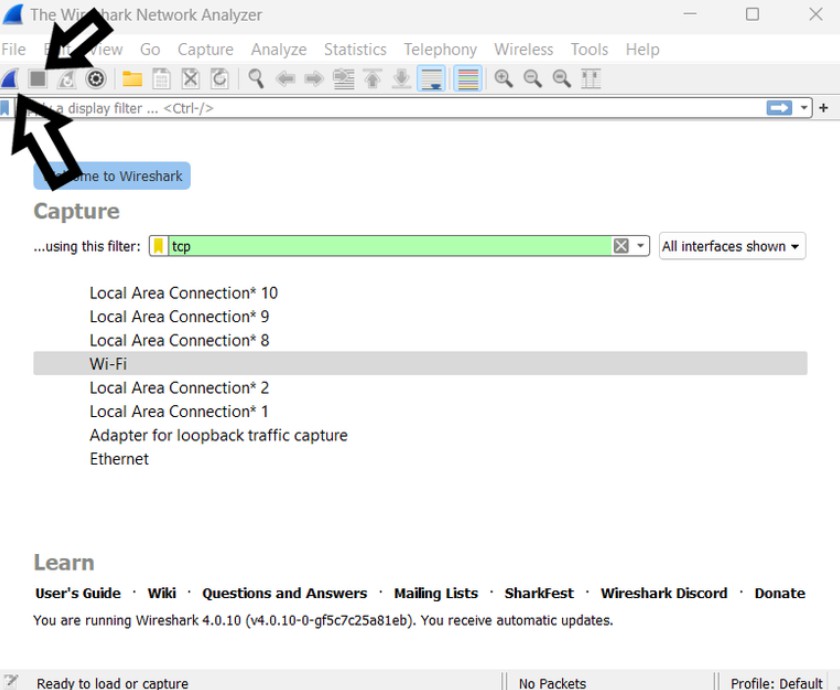
**Using Wireshark:**

**Begin Packet Capturing:**

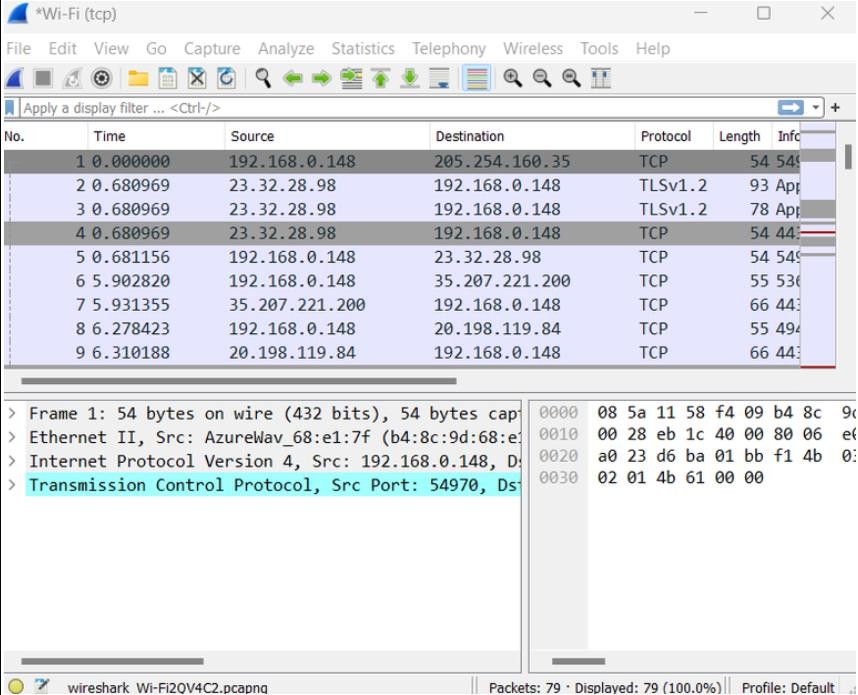
Open Wireshark and choose the network interface from which to begin collecting packets.



There are several local interfaces available; please choose one.

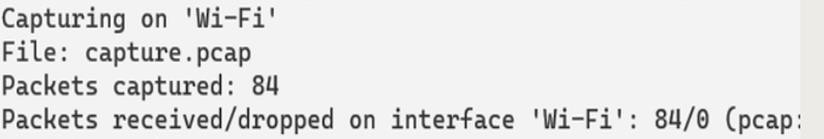


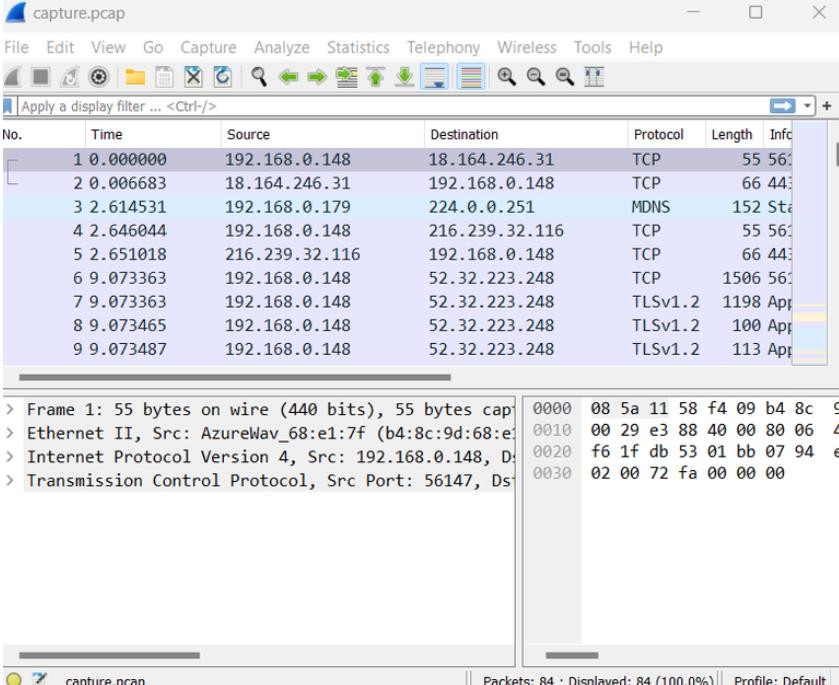
Press the Start button.



## Using tcpdump

* 1. Launch a Terminal or Command Prompt:
     + On Unix-based systems, open a terminal window. As an administrator, run the Command Prompt on Windows.
  2. Begin Packet Capturing:
     + In the first case, run dumpcap -i <interface>-w<output\_file>, where <interface> is the network interface that you choose to start capturing from.
  3. View Captured Packets:
     + tcpdump will present captured packets in a readable format on the terminal window.





# Result:

The analysis using Wireshark will reveal a list of different links accessed by the victim.

URLs, along with associated protocols and data exchanged, will be visible in the captured packets.

This information can help in understanding the network activity and identifying potential security concerns or unauthorized access.

Lab 5

Aim :- To install SPAN for AVISPA tool and explore the features of AVISPA tool along with their architecture and component .

# Theory:

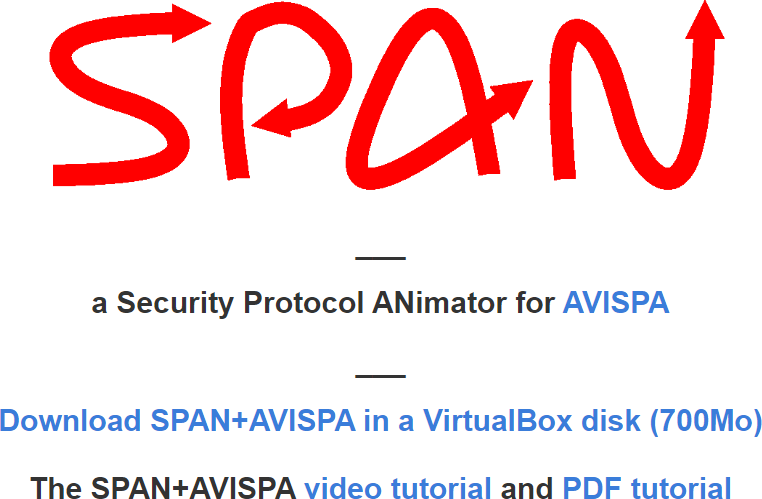
AVISPA is a tool designed for the formal verification of security protocols. It supports multiple back- ends, each using a different technique for protocol analysis. Some of its components include the

OFMC (the OFMC protocol analyzer), SATMC (the SATMC protocol analyzer), and CL-AtSe (the constraint logic-based attack search engine).

# Procedure:

**Download and Install AVISPA +SPAN:**

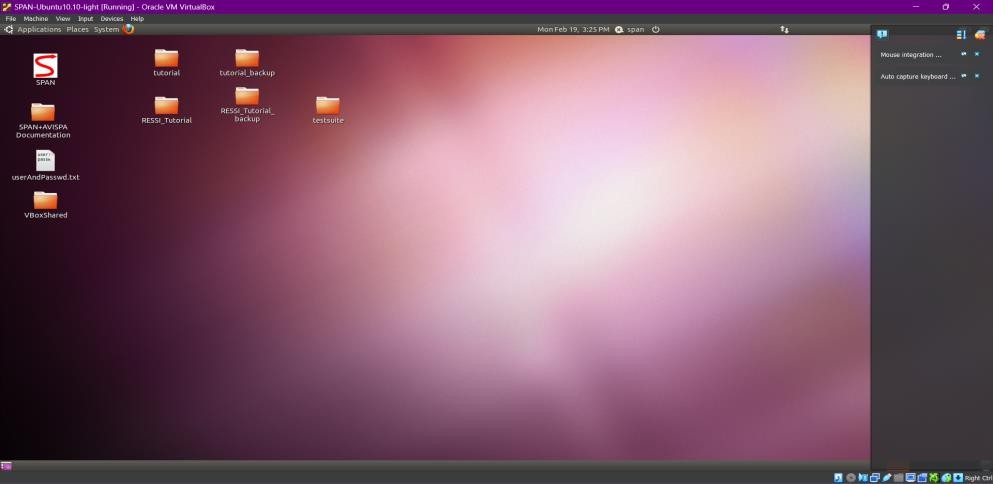
* Visit the official AVISPA website to download the tool.



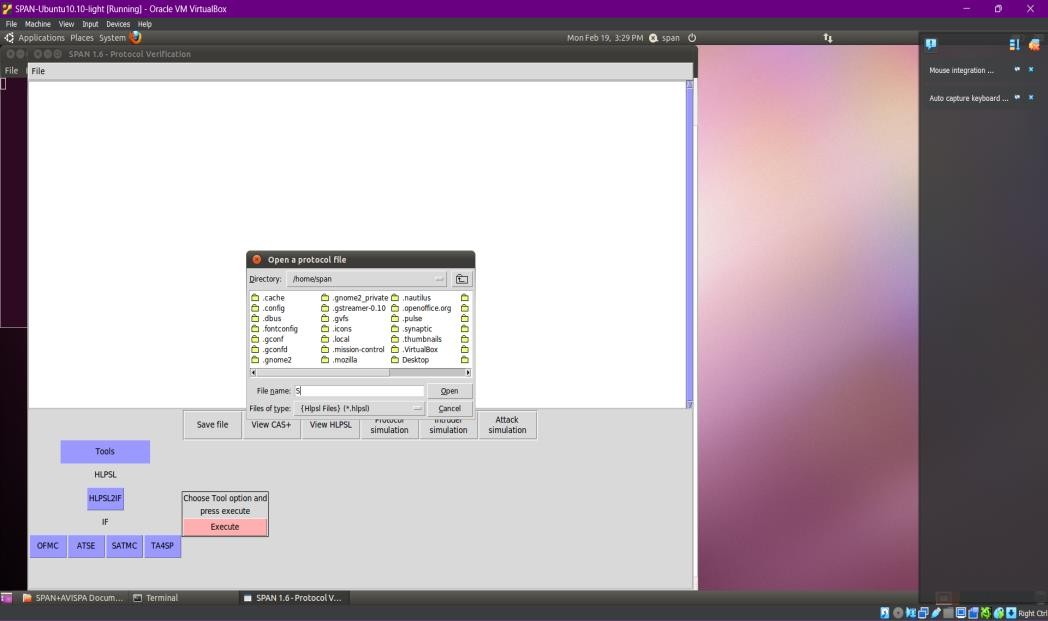
* Follow the installation instructions provided for your operating system.

**Explore AVISPA Features:**

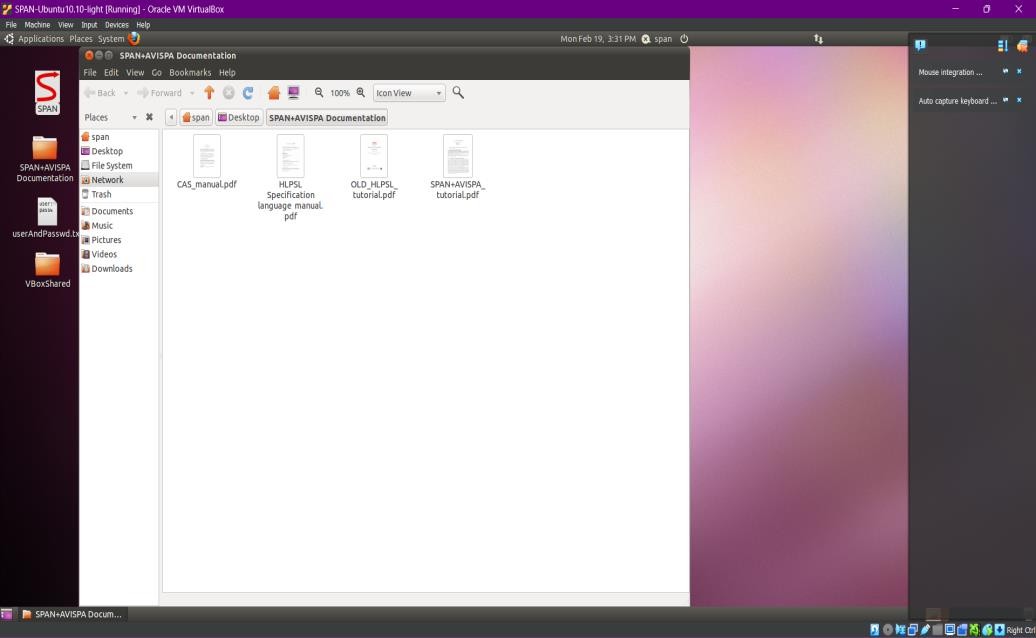
* Launch AVISPA and familiarize yourself with its user interface.



* Experiment with different security protocols and scenarios using the available analyzers.



**Understand AVISPA and SPAN Architecture:**

* Study the documentation to understand the architecture of AVISPA +SPAN.
* Learn about the different analyzers and their underlying techniques.

**Explore Components:**

* Understand the role of each component (OFMC, SATMC, CL-AtSe) in the analysis process.
* Experiment with each component to see how they handle different types of security protocols.

# Result:

* Successful installation and exploration of AVISPA+ SPAN, gaining insights into its user interface, features, and components.
* Understanding of how to use AVISPA +SPAN for the formal analysis of security protocols.
* Increased knowledge of the role of each component in the AVISPA tool.