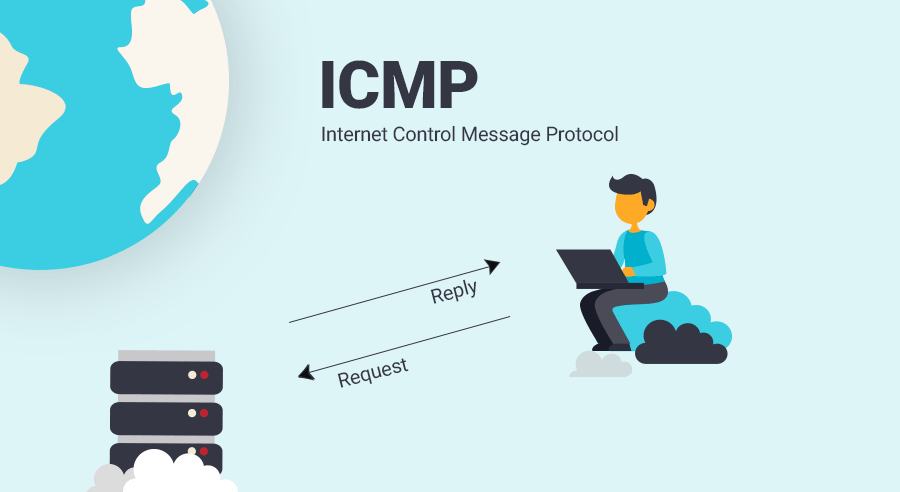
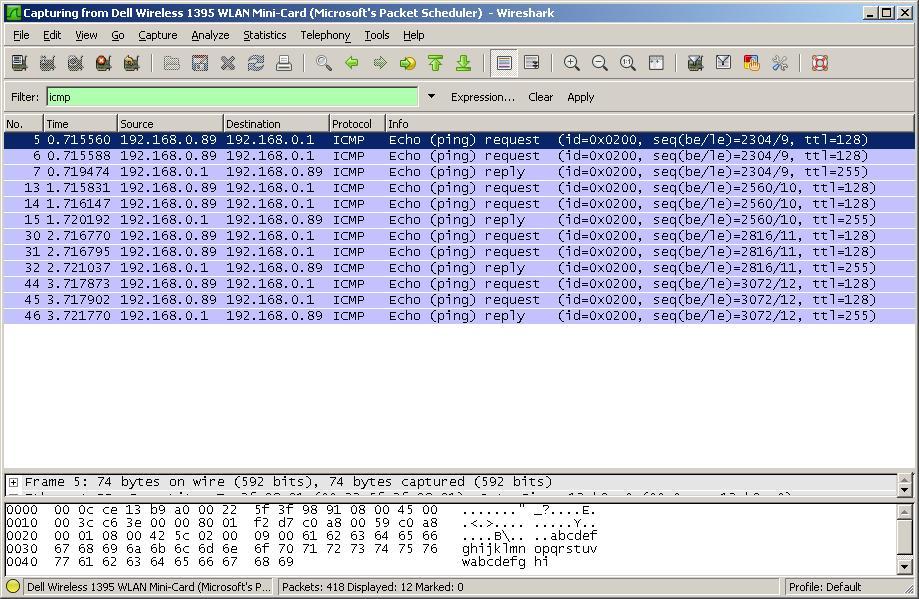
**CTF Topic: ICMP packet capture**

****

**Introduction**

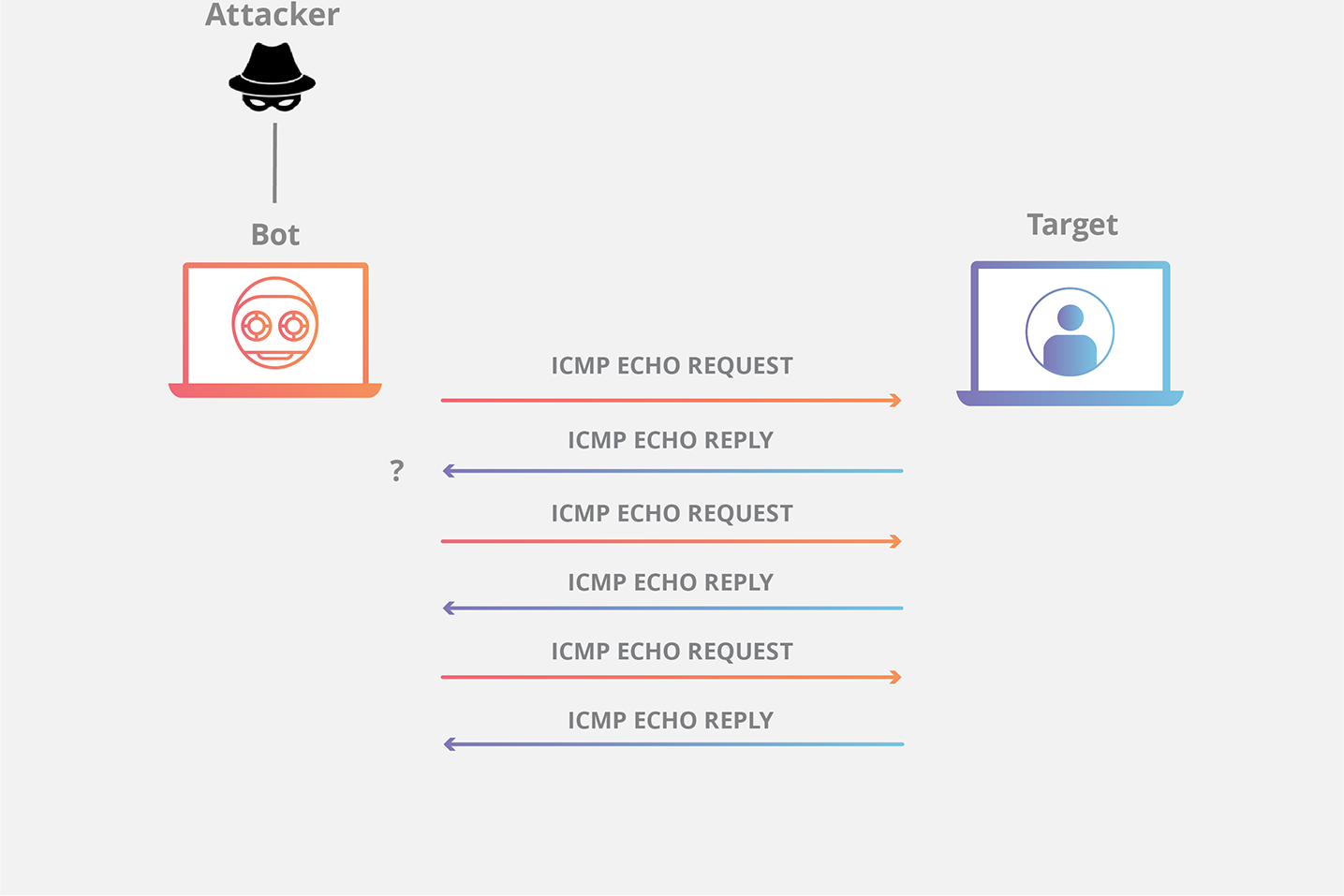
****

Packet capture is a networking practice involving the interception of data packets travelling over a network. These packets are then stored by IT teams for further analysis. The inspection of these packets allows IT teams to identify issues and solve network problems affecting daily operations.

**Tools and Requirements**

Wireshark

**Scenario**

****

An evil group is coordinating with each other and doing some malicious activities with a low security transfer protocol i.e ICMP. A Cyber Security team catches the packet and analyses the packet and finds out what they are going to do.

**Process**

Step 1: To complete this you have to download the wireshark from the Link\_1 below and the file packet.pcapng given in the Link\_2.

Step 2: Thereafter open the file and it will open in the wireshark automatically or you should select the wireshark option.

Step 3: Search ICMP on the search bar which will be located on the top.

Step 4: Click on the 1st and a popup window will appear and tick on the show packet bytes options which was located on the bottom left corner.

Link\_1: <https://www.wireshark.org/download.html>

Link\_2: <https://www.mediafire.com/file/nhq9f5mpyii9wk0/Packet.pcapng/file>

**Questions**

**Flag 1: What was the message Captured?**

**Answer: Kill\_Hari\_Bahadur/Amount=1crore**

**Flag Captured.**

**Flag 2: Which Internet protocol did it use to transfer messages?**

**Answer:4**

**Flag Captured.**

**Hint**

