

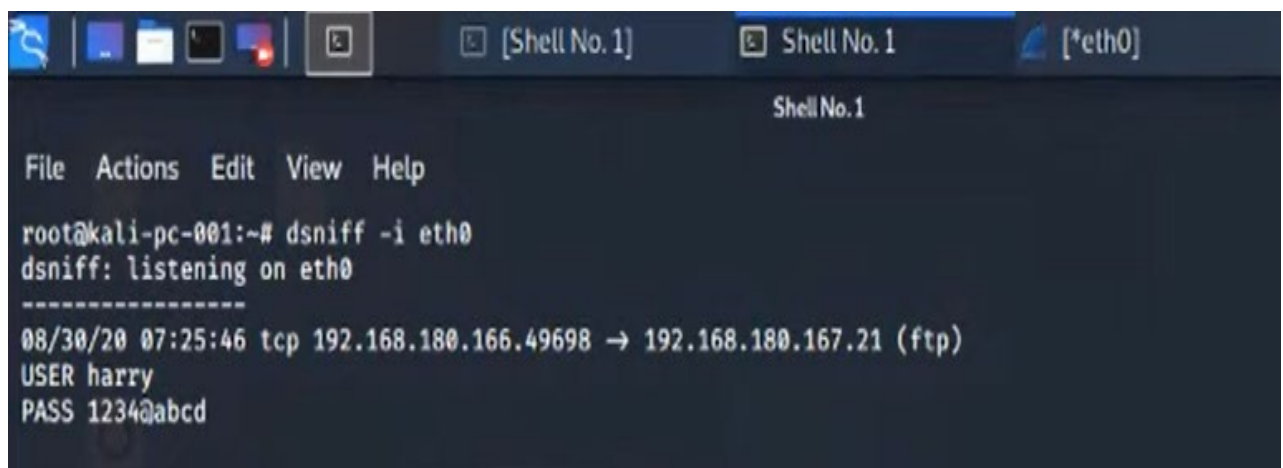
The screenshot displays the Wireshark network protocol analyzer interface. At the top, the menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The status bar at the top indicates the interface is 'eth0'.

The main window is divided into three panes:

- Packet List Pane:** Shows a list of captured packets. Packet 67 is selected, which is an ICMP Redirect (Type 3, Code 1) from 192.168.188.167 to 192.168.188.166. The length is 66 bytes.
- Packet Details Pane:** Provides a hierarchical view of the selected packet's structure. It shows:
  - Ethernet II, Src: VMware\_64:29:1c (08:0c:29:64:29:1c), Dst: VMware\_85:8a:32 (08:0c:29:85:8a:32)
  - Internet Protocol Version 4, Src: 192.168.188.166, Dst: 192.168.188.167
  - Transmission Control Protocol, Src Port: 49698, Dst Port: 21, Seq: 15, Ack: 86, Len: 12
  - File Transfer Protocol (FTP)
- Packet Bytes Pane:** Displays the raw data of the selected packet in hexadecimal and ASCII. The data starts with '0000 00 0c 29 85 6a 32 00 0c 29 64 29 1c 06 00 45 02' and ends with '0000 0d 0a'.

The packet capture filter is set to 'tcp.port == 21'. The packet list pane also shows other packets, including a TCP Reset (Seq=15, Win=0) and a TCP Reset (Seq=15, Win=0).

Question3 : mitm attack of ftp transaction with dsniff



The image shows a terminal window titled "Shell No. 1" with a tab labeled "[\*eth0]". The terminal displays the following text:

```
File Actions Edit View Help
root@kali-pc-001:~# dsniff -i eth0
dsniff: listening on eth0
-----
08/30/20 07:25:46 tcp 192.168.180.166.49698 → 192.168.180.167.21 (ftp)
USER harry
PASS 1234@abcd
```