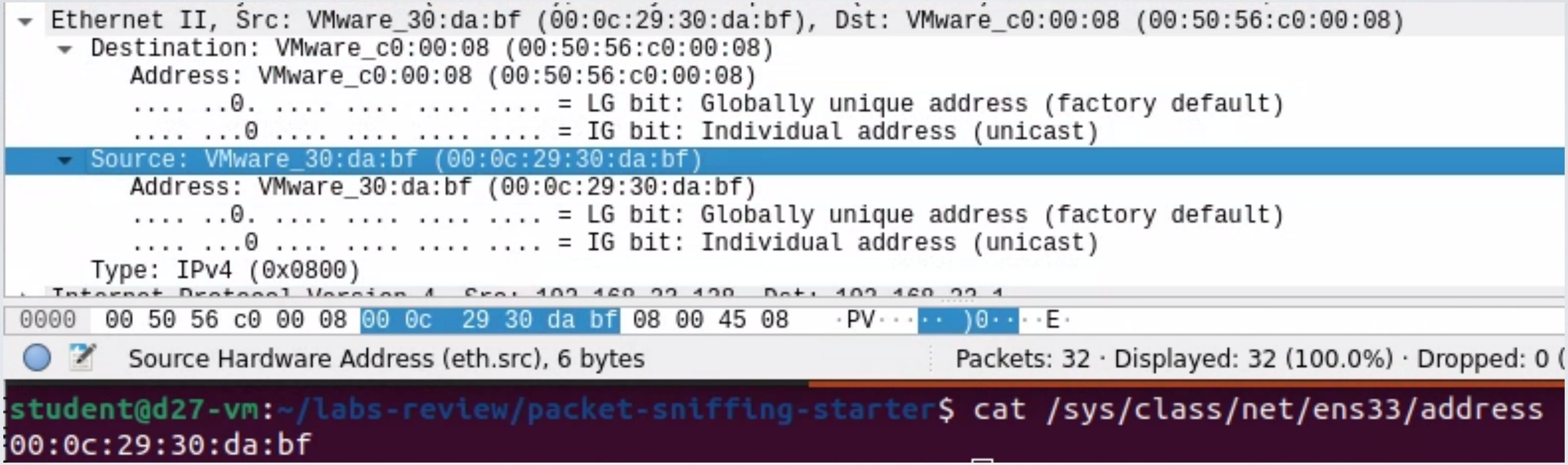

```
▾ Ethernet II, Src: VMware_30:da:bf (00:0c:29:30:da:bf), Dst: VMware_c0:00:08 (00:50:56:c0:00:08)
  ▾ Destination: VMware_c0:00:08 (00:50:56:c0:00:08)
      Address: VMware_c0:00:08 (00:50:56:c0:00:08)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: VMware_30:da:bf (00:0c:29:30:da:bf)
      Address: VMware_30:da:bf (00:0c:29:30:da:bf)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 192.168.22.128, Dst: 192.168.22.1
```

```
0000  00 50 56 c0 00 08 00 0c  29 30 da bf 08 00 45 08    ·PV··· ·· )0·· ··E·
```

```
Source Hardware Address (eth.src), 6 bytes        Packets: 32 · Displayed: 32 (100.0%) · Dropped: 0 (
```

```
student@d27-vm:~/labs-review/packet-sniffing-starter$ cat /sys/class/net/ens33/address
00:0c:29:30:da:bf
```

confidentiality

Packet Sniffing over Ethernet or WiFi

- All messages are transmitted on the medium with the MAC address of the recipient

- Each network interface only picks messages that correspond to its MAC address

➡ An attacker can set its network interface in ***promiscuous mode*** to capture (sniff) all traffic

e.g. Wireshark