

The screenshot displays a Windows 10 desktop environment with two network analysis tools open. The primary tool in the foreground is Wireshark, titled "Wireshark - Packet 18199 - Forensics.pcapng". It shows a packet capture of ICMP Echo (ping) requests. The packet list pane on the left shows 18199 frames, with the selected packet (18199) being an ICMP Echo (ping) request from 192.168.112.128 to 137.74.202.89. The packet details pane on the right shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The packet bytes pane at the bottom shows the raw data, with a red circle highlighting the 'n' field in the ICMP Echo (ping) request. The background tool, NetworkMiner, is also open, showing a similar packet capture of ICMP Echo (ping) requests from 192.168.112.128 to 137.74.202.89. The desktop includes a taskbar with various application icons and a system tray showing the date and time as 11:15 AM on 10/20/2023.

THE FLAG :
ROCSC{6cda4ec353b3a3838a5ac951b9499e693a11c32130f5ba7c744ee99940b10371}
~Z4que