Demonstration of packet capturing in a Wireless network using Wireshark's Promiscuous mode and Monitoring mode.

1. Experimental set up

Mode	Promiscuous		Monitoring	
Network	Acer router (I)	Smart Remote (SR) (II)	Acer router (III)	Smart Remote (SR) (IV)
Infrastructure	**Access point:** Acer router WiFi network **Client(s):** ThinkPad 1, ThinkPad 2, ThinkPad 3. All three are connected to the AP.	**Access point:** The AP which gets created when the Smart Remote is switched on. **Client(s):** 2 GoPro's and my computer.	**Access point:** Acer router WiFi network. **Client(s):** ThinkPad 1, ThinkPad 2, ThinkPad 3 (this is the attacker and not on the network).	**Access point:** The AP which gets created when the Smart Remote is switched on. **Client(s):** 2 GoPro's and my computer.
How we create the experimental set up.	Connect all the ThinkPad's to the Acer router WiFi network and then start Wireshark in Promiscuous mode for the wireless interface on the ThinkPad which is designated as the attacker.	The internal mechanism of the GoPro is used to connect to the SR. Since we know the name of the hidden WiFi which the SR creates, we connect the computer to this WiFi (authentication is not required). Then start Wireshark in promiscuous mode for the wireless interface on my computer.	Type 1 - Connect all three ThinkPad's to the Acer router WiFi and then start Wireshark on the attacking computer and enable monitor mode. Type 2 – Connect 2 ThinkPad's to the AP. Start monitor mode on the attacking ThinkPad using Airmon-ng.	The SR access point is started. The GoPros are connected to it. A monitoring interface is set up on the computer for the wireless interface. Assuming that the Acer router WiFi is active in the area, we start Wireshark for the monitoring interface that was just created.
What we expect to see	If I send a message like ping from one of the ThinkPads to the other, the attacking ThinkPad's wireshark should be able to observe these messages.	Messages sent to and from the SR to the GoPros.	If I send a message like ping from one of the ThinkPads to the other, the attacking ThinkPad's wireshark should be able to observe these messages.	Messages sent to and from the SR to the GoPros along with messages from other WiFi networks like the Acer router.