Describe las funcionalidades de la biblioteca pcap.
La biblioteca de pcap es utilizada para poder capturar los paquetes que se transmiten dentro de una red, para conseguir una lista de las interfaces de red y para transmitir paquetes en la capa de enlace de una red. La biblioteca pcap se usa para la captura de paquetes, con este se pueden crear programas de captura de las tramas de red (packet sniffers), generadores de tráfico y puesta a punto de la red.

¿Cuáles son las principales vulnerabilidades de seguridad del protocolo http?
Las principales vulnerabilidad de http provienen del hecho que los mensajes se envían sin ser cifrados, lo cual la hace vulnerable a muchos ataques. La información es fácil de interceptar y no se encuentra protegida de ninguna forma. También http no requiere ninguna validación para el dominio, pero eso es más desde otro enfoque
.
Principales ataques informáticos que explotan el protocolo http. Da una breve descripción de cada uno.
Man-in-the-middle: En este ataque se interceptan mensajes entre una pareja para poderlos leer, modificar e insertar otros que los remplacen, de tal manera que ninguno sepa que el enlace fue roto y remplazado. El atacante se hace pasar por alguna de las partes para poder obtener acceso o información.
Eavesdropping: Es cuando se interceptan mensajes y estos se leen en busca de información. El objetivo es tomar la mayor cantidad de información al interceptar e interpretar paquetes de tal manera que no se de cuenta los contricantes. Es mucho más fácil hacerlo si los mensajes no son cifrados.
Sniffeo y modificación de paquetes: Se interceptan paquetes dentro de la red y como el http esta en texto plano, se interpretan estos y luego se les modifica el header y se remplaza en el flujo.

Flujo del programa:
El programa tiene un menú principal que hace que el usuario elija dos opciones. Estar escuchando indefinidamente o cargar una captura pcap desde un archivo. En ambos casos se pide al usuario que seleccione especificaciones. Por un lado se pide al usuario que seleccione el dispositivo especifico y por el otro se le pide que seleccione la captura específica. En ambos casos se hace captura de datos y se despliegan los headers para que se pueda analizar los paquetes que se están transmitiendo.

Principales problemas que se encontraron y cómo los solucionaron:
Para hacer el sniffer lo más difícil fue poder tomar de manera adecuado lo recibido para poder formar el header adecuadamente,porque realmente las cosas no están en la forma deseada. Un dificultad para mi fue después de hacer el sniffer ponerlo en la forma pedida, pero creo que fue más por poca comprensión de lo que se solicitaba. Para lograr hacer adecuadamente uso de pcap y formar los headers leí documentación y cheque archivos en internet donde se usaba la biblioteca. Para el formato pedido consulte con compañeros de la clase del método usado.