Instrukcja:

1. Instalacja wtyczki USBCap

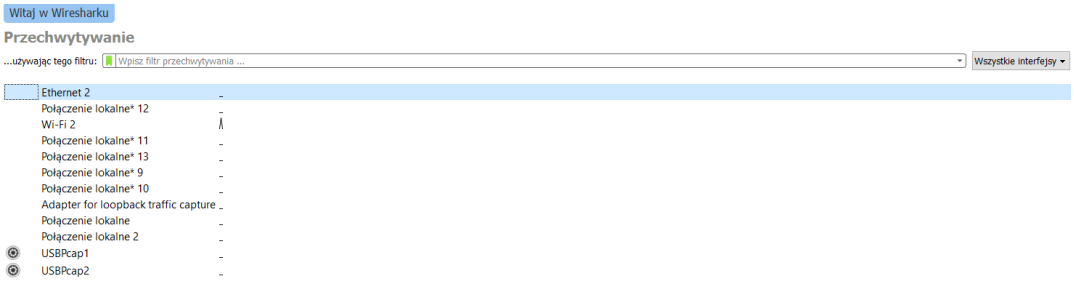
a) Wchodzimy na stronę https://desowin.org/usbpcap/ i pobieramy instalator **USBPcapSetup-1.5.4.0.exe**.

b) Następnie instalujemy z zachowaniem domyślnych ustawień i resetujemy komputer.

c) Po resecie odnajdujemy folder z rozszerzeniami Wireshark-a:
uruchamiamy Wireshark-> Pomoc-> O programie Wireshark -> Foldery -> odnajdujemy Global Extcap path i klikamy dwukrotnie, otworzy się folder

d) Z folderu gdzie zainstalowaliśmy uprzednio wtyczkę USBCap (u mnie C:\Program Files\USBPcap) kopiujemy plik USBPcapCMD.exe i wklejamy do folderu Global Extcap path.

Teraz po ponownym uruchomieniu Wiresharka powinniśmy zobaczyć możliwość sniffowania urządzeń USB:



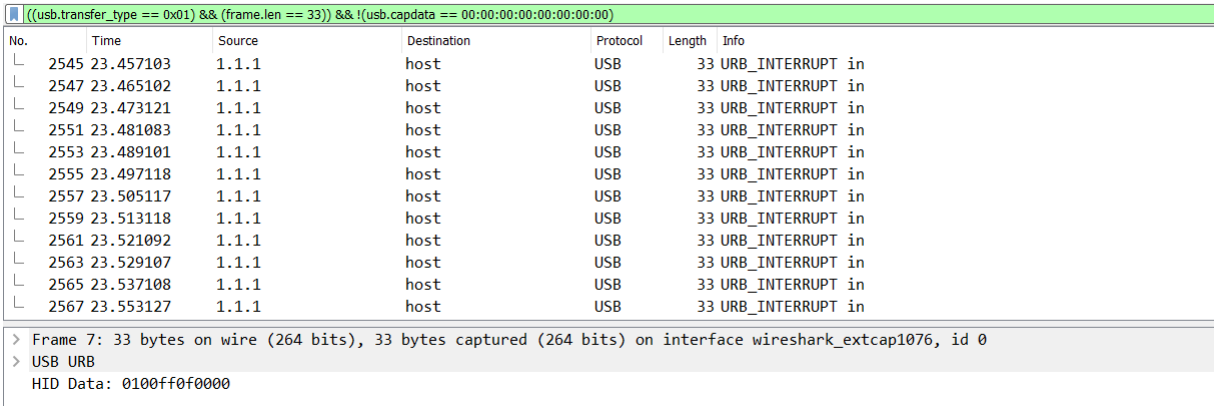
2. Sniffowanie pakietów USB

a) Klikamy USBPcap1 i obserwujemy czy po poruszaniu myszką uzyskujemy pakiety, jeśli nie uruchamiamy USBPcap2.

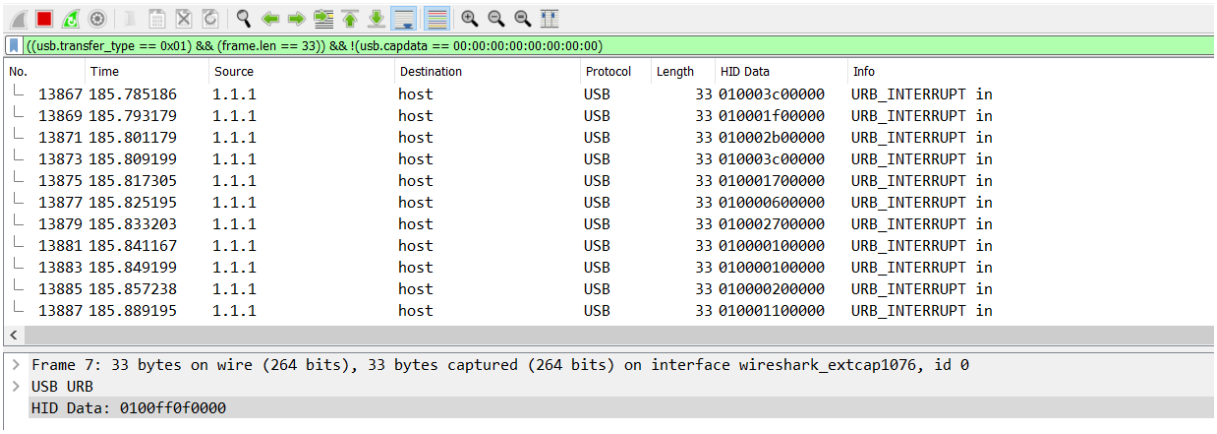
b) Jako filtr wklejamy:

((usb.transfer_type == 0x01) && (frame.len == 33)) && !(usb.capdata == 00:00:00:00:00:00:00:00)

Powinniśmy otrzymać podobny efekt:



c) Teraz klikamy prawym przyciskiem myszy na HID Data lub Leftover Capture Data i wybieramy Utwórz kolumnę z pola.



Po uzyskaniu tego kroku możemy już zdekodować otrzymywane dane.

3. Dekodowanie ruchów myszki

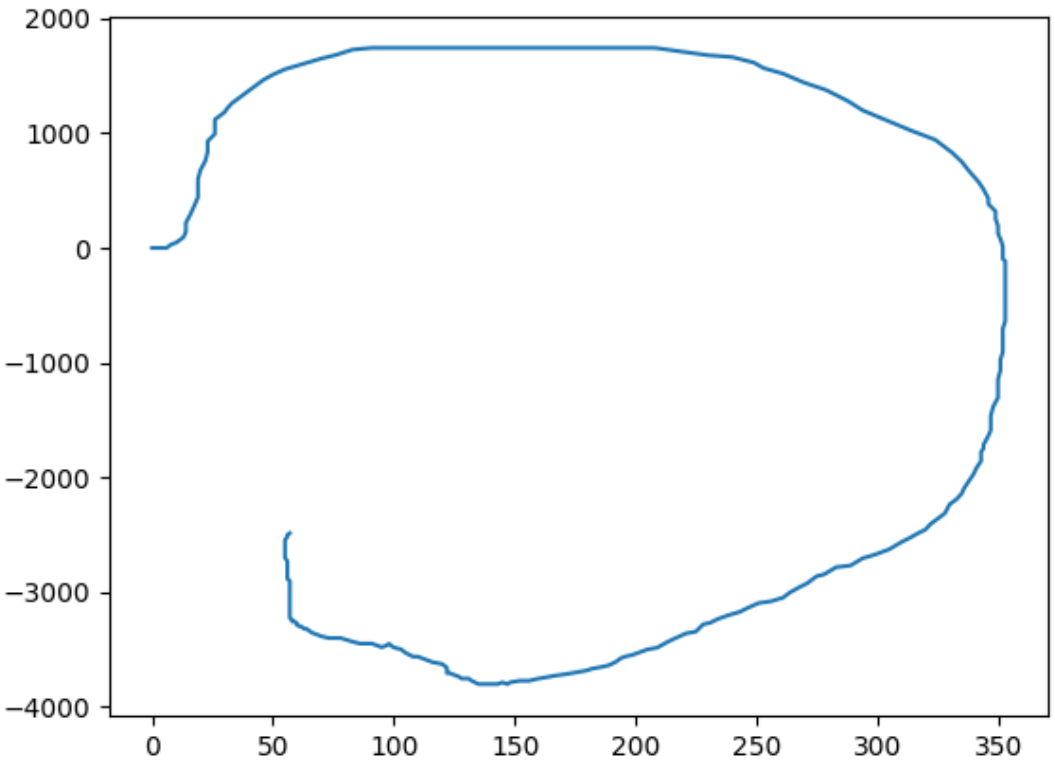
a) Z repozytorium: kopiujemy kod do VS Code i zapisujemy, najlepiej w nowym folderze na pulpicie.

b) Wracamy do Wiresharka, uruchamiamy przechwytywanie pakietów i wykonujemy ruch myszką, na przykład poruszamy nią „rysując” koło.

c) Stopujemy przechwytywanie pakietów i wybieramy Plik -> Eksportuj prezentację pakietów -> jako CSV.

d) Zapisujemy plik csv pod nazwą sisk(można użyć oczywiście innej, wiąże się to tylko ze zmianą nazwy w kodzie) w folderze, gdzie wcześniej zapisaliśmy kod pythona.

e) Uruchamiamy kod w VS Code, powinniśmy otrzymać zdekodowane ruchy myszki:



Dodatkowo jeśli w trakcie rysowania trzymaliśmy jakiś przycisk myszy, to pojawi się to w logach.