„Podsłuchiwanie” komunikacji z kartą – usbpcap i wireshark

126432

Agenda

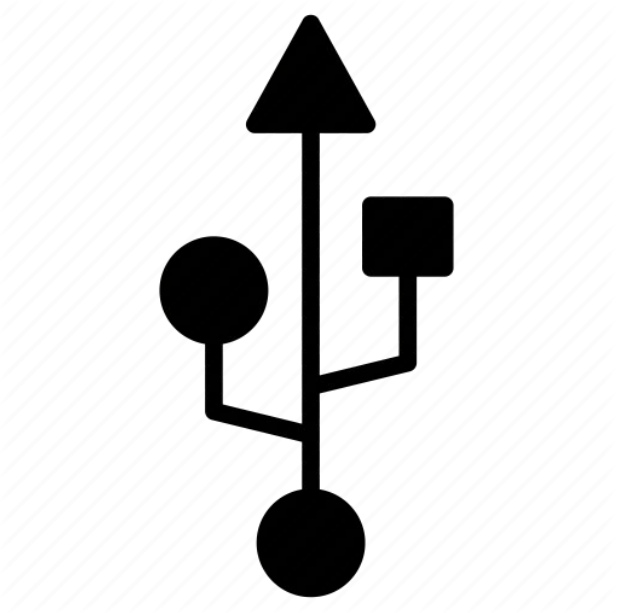
- Instalacja Środowiska
- Konfiguracja
- Odczytanie przechwyconej komunikacji
- Analiza komunikatów
- Możliwości wykorzystania przechwyconych informacji

WireShark

- Sniffer
- OpenSource
- Dawniej “Etherea”
- GUI

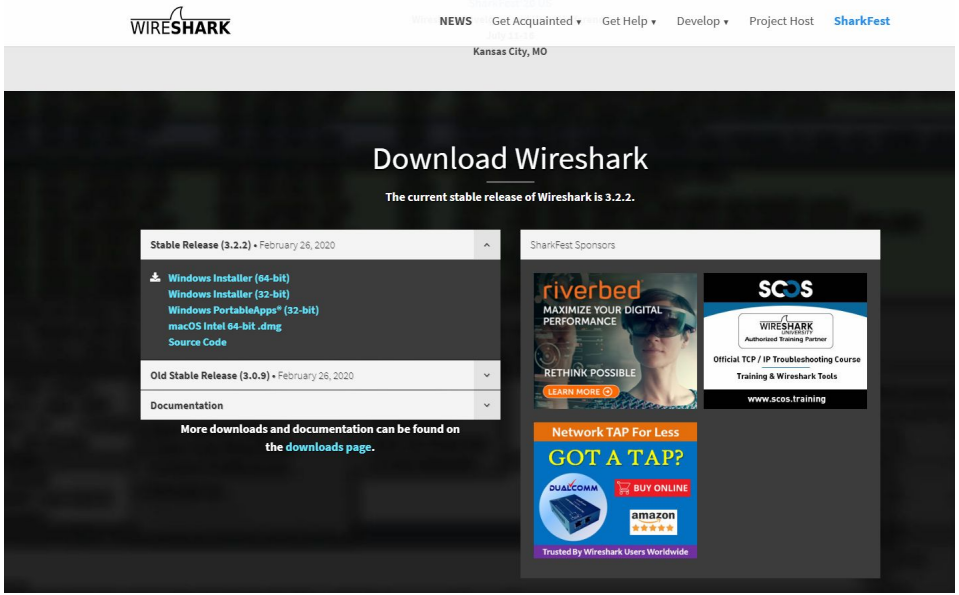
USBpCap

- OpenSource
- USB sniffer
- Windows

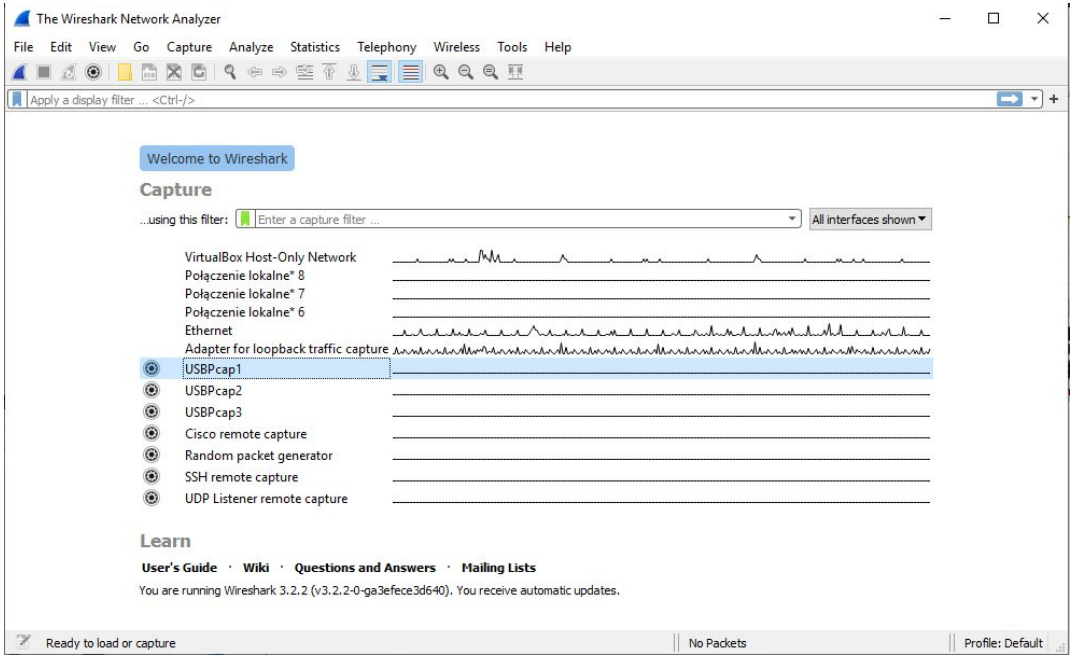


Instalacja

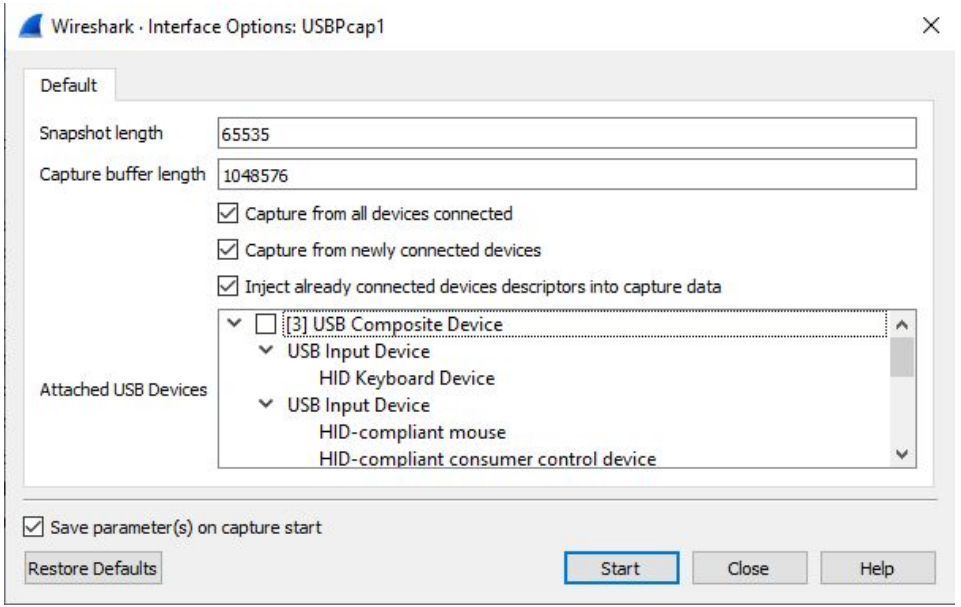
- https://www.wireshark.org/#download
- Możliwość automatycznej instalacji pakietu USBpCap
- Wymagany restart



Konfiguracja

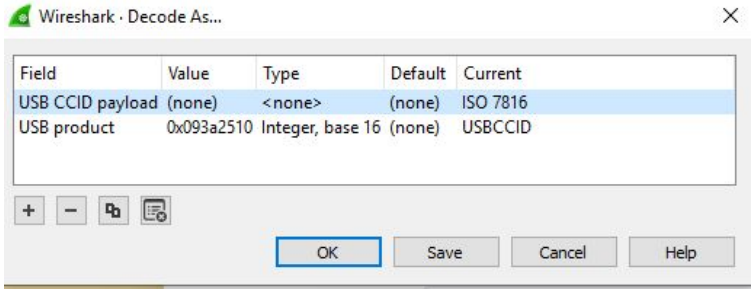


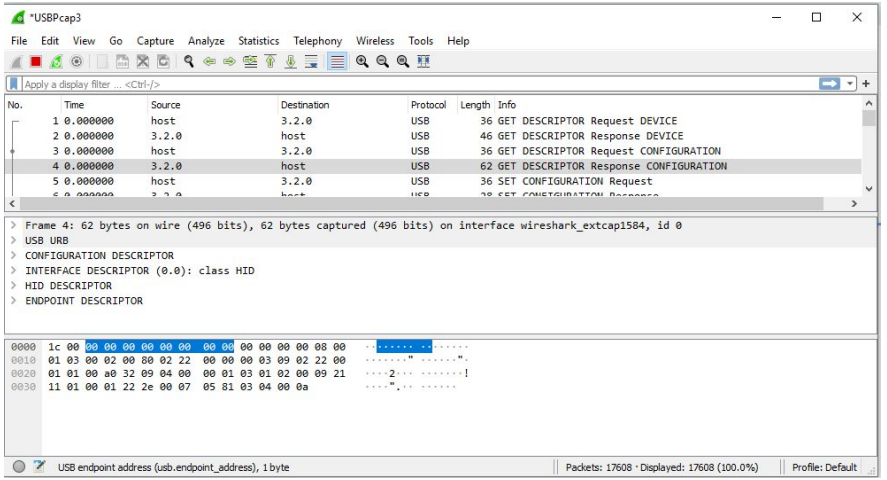
Konfiguracja



Odczytywanie przechwyconej komunikacji

- Analyze -> Decode As





CCID (ang. Chip card interface device)

- Wspólny protokół komunikacyjny USB do komunikacji między czytnikiem kart a komputerem
- Ułatwienie dla producentów
- 14 komand

ISO/IEC 7816

- Międzynarodowy standard określający normy dla kart elektronicznych
- Definicja poleceń APDU

Analiza komunikatów - polecenie APDU

Pole	Długość (w bajtach)	Opis
CLA	1	określa klasę instrukcji, do której należy polecenie
INS	1	określa konkretną instrukcję do wykonania na karcie, np.: „zapisz dane”
P1-P2	2	określa parametry instrukcji, np. offset w pliku, do którego mają być zapisane dane
L_c	0, 1 lub 3	określa liczbę (N_c) bajtów z danymi
Dane instrukcji	N_c	N_c bajtów z danymi
L_e	0, 1, 2 or 3	określa maksymalną liczbę (N_e) bajtów spodziewanych w odpowiedzi

Analiza komunikatów - odpowiedź APDU

Odpowiedź APDU		
Dane odpowiedzi.	N_r (max. N_e)	Dane zwrócone przez kartę na zadaną instrukcję z parametrami.
SW1-SW2[2]	2	Kody statusu odpowiedzi, np 90 00 (szesnastkowo) oznacza prawidłową odpowiedź

Analiza Komunikatów - instrukcje

- READ BINARY command
- WRITE BINARY command
- UPDATE BINARY command
- ERASE BINARY command
- READ RECORD(S) command
- WRITE RECORD command
- APPEND RECORD command
- UPDATE RECORD command
- GET DATA command
- PUT DATA command
- SELECT FILE command
- VERIFY command
- INTERNAL AUTHENTICATE command
- EXTERNAL AUTHENTICATE command
- GET CHALLENGE command
- MANAGE CHANNEL command

Możliwość wykorzystania przechwyconych komunikatów

- Analiza prawidłowego działania urządzenia
- Odtworzenie wykonywanych działań
- Przeprowadzanie ataków

Źródła

https://cardwerk.com/smart-card-standard-iso7816-4-section-6-basic-interindustry-commands/

https://ludovicrousseau.blogspot.com/2014/10/ccid-usb-spy-using-wireshark.html

https://ludovicrousseau.blogspot.com/2019/08/iso-7816-4-spy-using-wireshark.html

https://pl.wikipedia.org/wiki/Application_Protocol_Data_Unit


Dziękuje za uwagę