



„Podstuchiwanie” komunikacji z kartą – usbpcap i wireshark



Agenda

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

WireShark

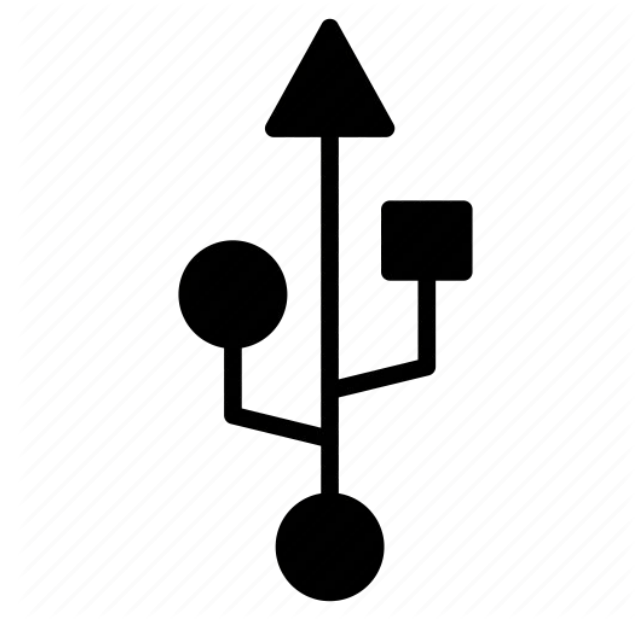
- Sniffer
- OpenSource
- Dawniej "Etherea"
- GUI





USBpCap

- OpenSource
- USB sniffer
- Windows

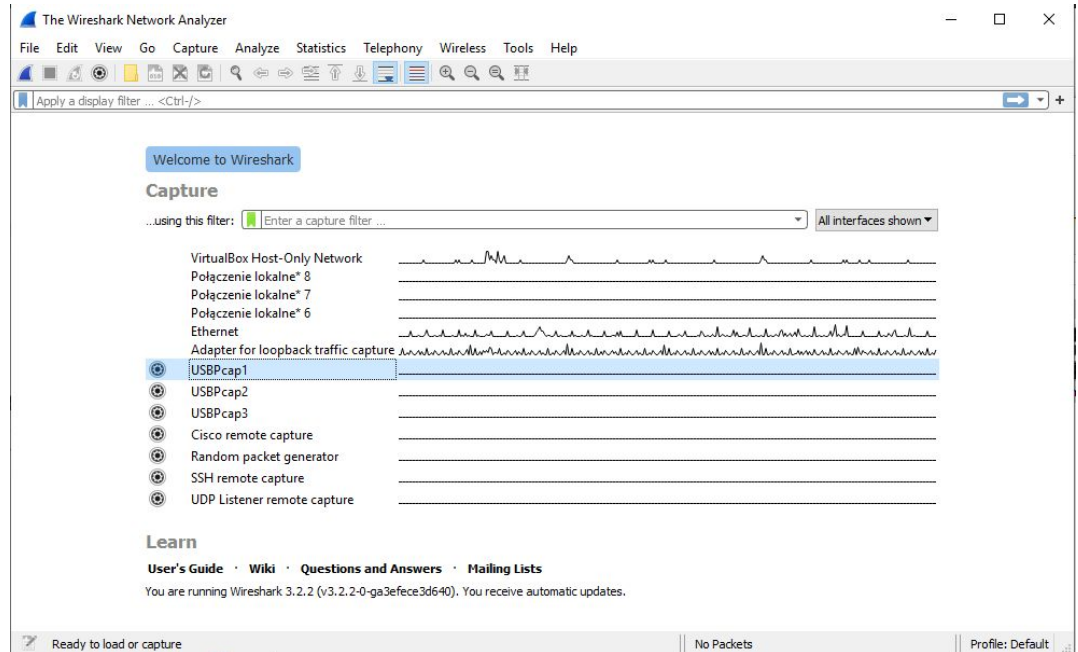


Instalacja

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

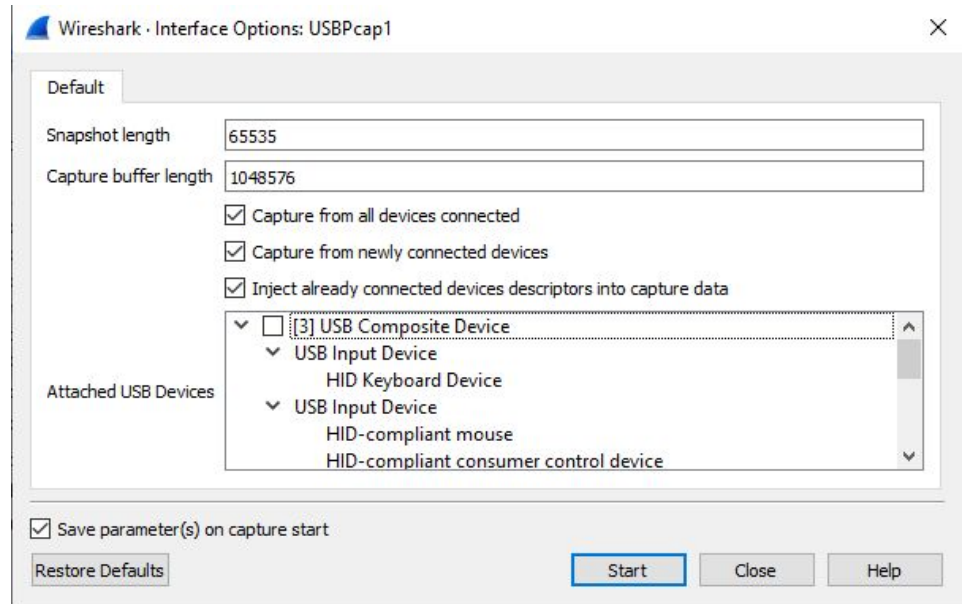
The screenshot shows the Wireshark website's download page. At the top, the Wireshark logo is on the left, and navigation links for NEWS, Get Acquainted, Get Help, Develop, Project Host, and SharkFest are on the right. Below the navigation, the location "Kansas City, MO" is displayed. The main heading is "Download Wireshark" with the subtext "The current stable release of Wireshark is 3.2.2." Below this, there are two main content areas. The left area is a dropdown menu for "Stable Release (3.2.2) • February 26, 2020" which lists: Windows Installer (64-bit), Windows Installer (32-bit), Windows PortableApps® (32-bit), macOS Intel 64-bit .dmg, and Source Code. Below this is a section for "Old Stable Release (3.0.9) • February 26, 2020" and a link to "Documentation". A note states: "More downloads and documentation can be found on the downloads page." The right area is titled "SharkFest Sponsors" and features three advertisements: "riverbed" (Maximize Your Digital Performance), "SCOS" (Official TCP/IP Troubleshooting Course), and "Network TAP For Less GOT A TAP?" (featuring Qualcomm and Amazon logos).

Konfiguracja



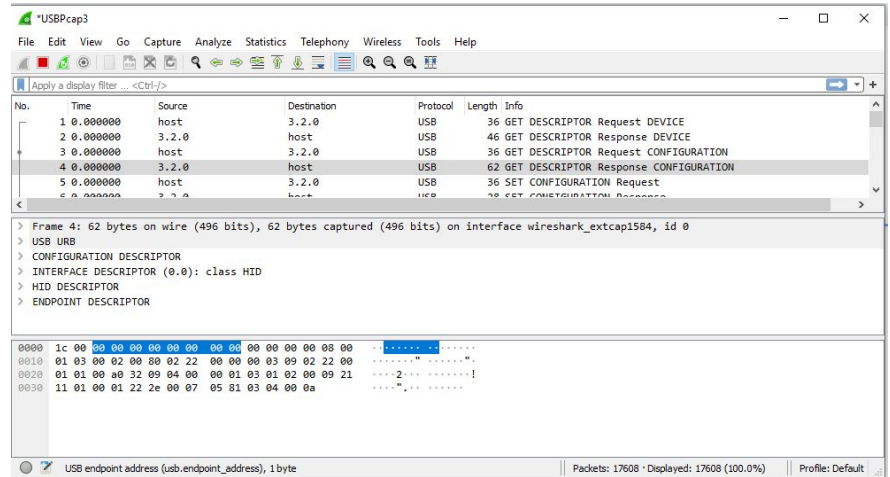
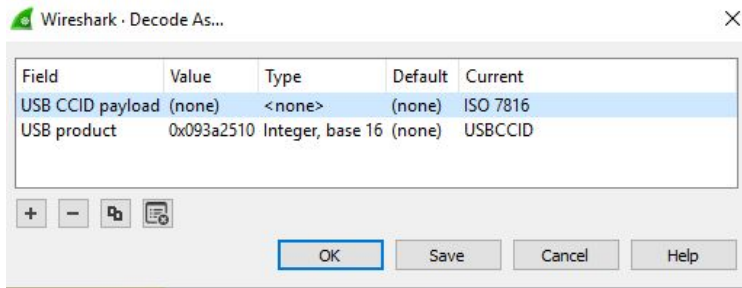


Konfiguracja



Odczytywanie przechwyczonej komunikacji

- Analyze -> Decode As



*USBpcap3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	host	3.2.0	USB	36	GET_DESCRIPTOR Request DEVICE
2	0.000000	3.2.0	host	USB	46	GET_DESCRIPTOR Response DEVICE
3	0.000000	host	3.2.0	USB	36	GET_DESCRIPTOR Request CONFIGURATION
4	0.000000	3.2.0	host	USB	62	GET_DESCRIPTOR Response CONFIGURATION
5	0.000000	host	3.2.0	USB	36	SET_CONFIGURATION Request
6	0.000000	3.2.0	host	USB	36	SET_CONFIGURATION Response

> Frame 4: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface wireshark_extcap1584, id 0
> USB URB
> CONFIGURATION_DESCRIPTOR
> INTERFACE_DESCRIPTOR (0.0): class HID
> HID_DESCRIPTOR
> ENDPOINT_DESCRIPTOR

```
0000 1c 00 03 03 00 00 00 00 00 00 00 00 00 00 00 .....
0010 01 03 00 02 00 00 02 22 00 00 00 03 00 02 22 00 .....
0020 01 01 00 a0 32 09 04 00 00 01 03 01 02 00 09 21 .....
0030 11 01 00 01 22 2e 00 07 05 81 03 04 00 0a .....

```

USB endpoint address (usb.endpoint_address), 1 byte

Packets: 17608 · Displayed: 17608 (100.0%) Profile: Default

CCID (ang. Chip card interface device)

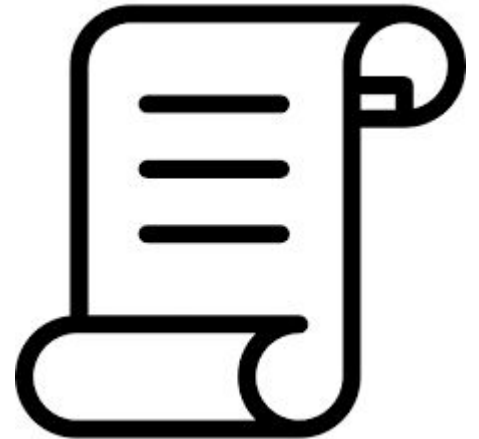
- Wspólny protokół komunikacyjny USB do komunikacji między czytnikiem kart a komputerem
- Ułatwienie dla producentów
- 14 komand





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

A scenic landscape featuring rolling green hills under a warm, golden sky. A paved road curves through the fields, leading towards a forested ridge in the distance. The foreground is filled with tall grasses and wildflowers. The overall atmosphere is peaceful and serene.

Dziękuję za uwagę