1110111011011

1001100

110011001100

10101010101010

00011001001

Ekspert Wiresharka

Analiza ruchu sieciowego

Hacking i Cyberbezpieczeństwo | Giganci Programowania

Opracowanie: Michał Suchoń

Przypomnienie

1. Do czego służy Keylogger?
2. Jak się nazywa system operacyjny (distro Linuxa), posiadający narzędzia do hackingu?
3. Co to SSH?
4. Do czego służy DeepWeb?
5. Czym jest Phishing?

Przypomnienie

1. Do czego służy Keylogger?
   oprogramowanie bądź urządzenie (także jako wirus), służące do rejestrowania klawiszy bądź kliknięć myszki, np. celem kradzieży danych bądź badania zachowań użytkowników
2. Jak się nazywa system operacyjny (distro Linuxa), posiadający narzędzia do hackingu?
3. Co to SSH?
4. Do czego służy DeepWeb?
5. Czym jest Phishing?

Przypomnienie

1. Do czego służy Keylogger?
   oprogramowanie bądź urządzenie (także jako wirus), służące do rejestrowania klawiszy bądź kliknięć myszki, np. celem kradzieży danych bądź badania zachowań użytkowników

2. Jak się nazywa system operacyjny (distro Linuxa), posiadający narzędzia do hackingu?
   Kali Linux

3. Co to SSH?

4. Do czego służy DeepWeb?

5. Czym jest Phishing?

Przypomnienie

1. Do czego służy Keylogger?
   oprogramowanie bądź urządzenie (także jako wirus), służące do rejestrowania klawiszy bądź kliknięć myszki, np. celem kradzieży danych bądź badania zachowań użytkowników

2. Jak się nazywa system operacyjny (distro Linuxa), posiadający narzędzia do hackingu?
   Kali Linux

3. Co to SSH?
   ang. Secure Shell; protokół komunikacyjny, umożliwiający zdalne połączenie z innym komputerem (serwerem) z możliwością wydawania poleceń i konfigurowania. Protokół SSH (w odróżnieniu od przodka – Telnetu) jest zabezpieczony szyfrowanym połączeniem dwustronnym

4. Do czego służy DeepWeb?

5. Czym jest Phishing?

Przypomnienie

1. Do czego służy Keylogger?
   oprogramowanie bądź urządzenie (także jako wirus), służące do rejestrowania klawiszy bądź kliknięć myszki, np. celem kradzieży danych bądź badania zachowań użytkowników

2. Jak się nazywa system operacyjny (distro Linuxa), posiadający narzędzia do hackingu?
   Kali Linux

3. Co to SSH?
   ang. Secure Shell; protokół komunikacyjny, umożliwiający zdalne połączenie z innym komputerem (serwerem) z możliwością wydawania poleceń i konfigurowania. Protokół SSH (w odróżnieniu od przodka – Telnetu) jest zabezpieczony szyfrowanym połączeniem dwustronnym

4. Do czego służy DeepWeb?
   rodzaj sieci, która jest niedostępna poprzez klasyczną przeglądarkę, a wymaga podłączenia do sieci Tor, np. przez Tor Browser

5. Czym jest Phishing?

Przypomnienie

1. Do czego służy Keylogger?
   oprogramowanie bądź urządzenie (także jako wirus), służące do rejestrowania klawiszy bądź kliknięć myszki, np. celem kradzieży danych bądź badania zachowań użytkowników

2. Jak się nazywa system operacyjny (distro Linuxa), posiadający narzędzia do hackingu?
   Kali Linux

3. Co to SSH?
   ang. Secure Shell; protokół komunikacyjny, umożliwiający zdalne połączenie z innym komputerem (serwerem) z możliwością wydawania poleceń i konfigurowania. Protokół SSH (w odróżnieniu od przodka – Telnetu) jest zabezpieczony szyfrowanym połączeniem dwustronnym

4. Do czego służy DeepWeb?
   rodzaj sieci, która jest niedostępna poprzez klasyczną przeglądarkę, a wymaga podłączenia do sieci Tor, np. przez Tor Browser

5. Czym jest Phishing?
   rodzaj ataku, w którym wykorzystuje się elementy socjotechniki po to, aby uzyskać poufne dane

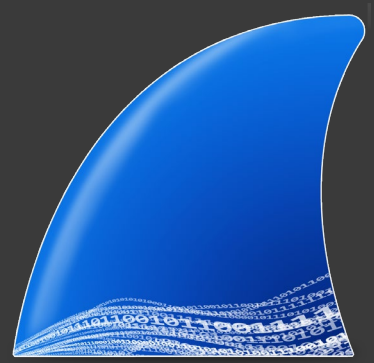
Do czego używa się Wiresharka?

WIRESHARK

Wireshark

wire – drut / przewód; shark - rekin

program przeznaczony do analizowania ruchu sieciowego

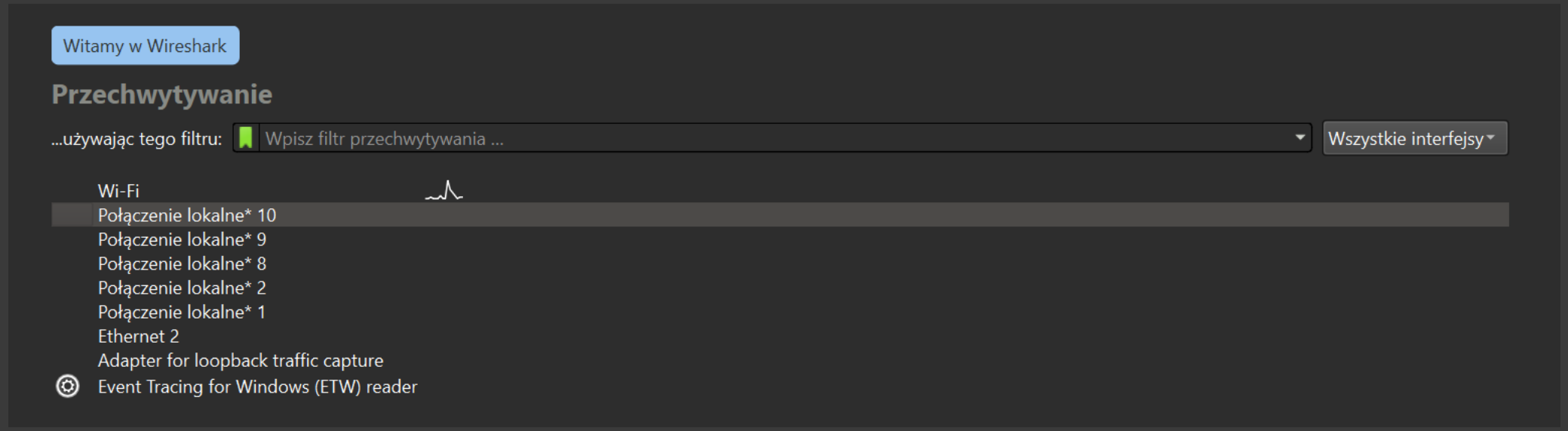


Co można zrobić za pomocą Wiresharka?

- Wireshark analizuje i wyświetla ruch sieciowy w czasie rzeczywistym.
- Pozwala na zapis i odczyt zebranego ruchu sieciowego tak, aby można było zabezpieczyć dane.
- Jest dostępny na wszystkie platformy (Windows, Linux, MacOS)
- Ma dużo wbudowanych funkcji np. do wydobywania plików z ruchu sieciowego czy przeglądania pakietów pojedynczych w prosty sposób.
- Pozwala na deszyfrowanie ruchu sieciowego.
- pierwotnie był tylko do analizy ruchu sieciowego przewodowego, jednak nie straszne mu są sieci wifi.
- Pozwala na dodawanie pluginów oficjalnych i mniej oficjalnych, które łamią prawo), dzięki czemu potrafi wspierać bluetooth, sieci LoraWan, GSM - Wymaga to dodatkowych modułów.
- Jest rozwijany na licencji open source

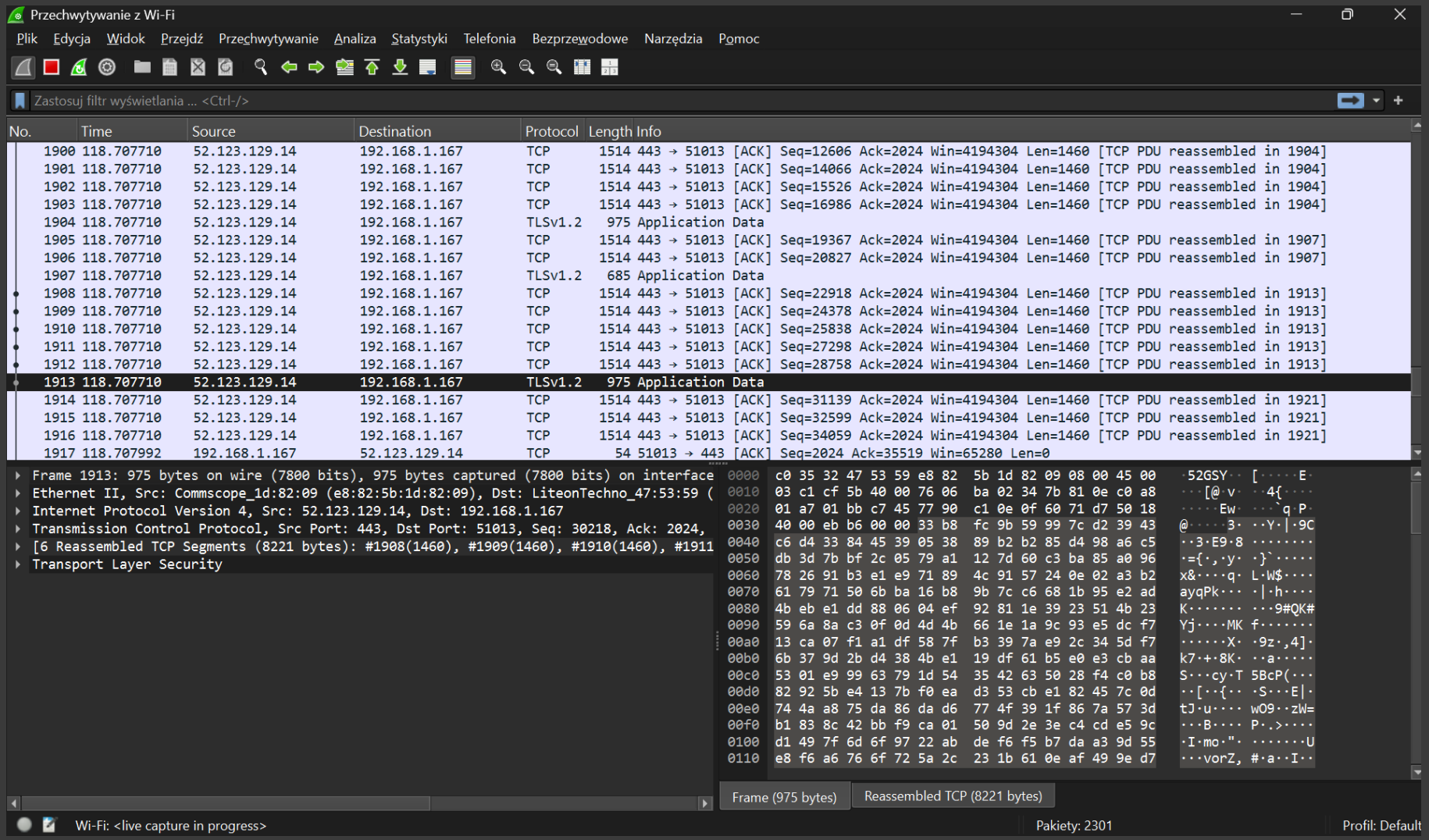
Interfejs Wiresharka

Ekran startowy - interfejsy

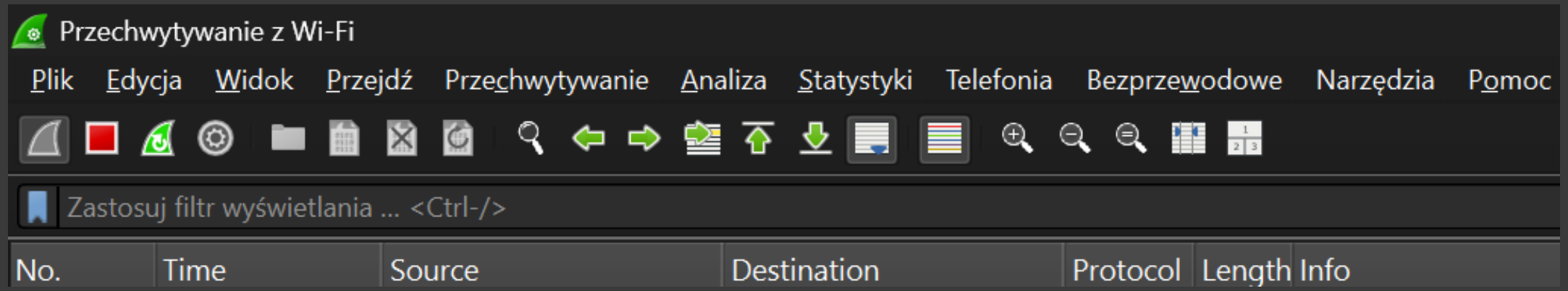


Umożliwia prześledzenie ruchu sieciowego na interfejsach (kartach sieciowych), dostępnych w komputerze oraz ewentualnych maszynach wirtualnych

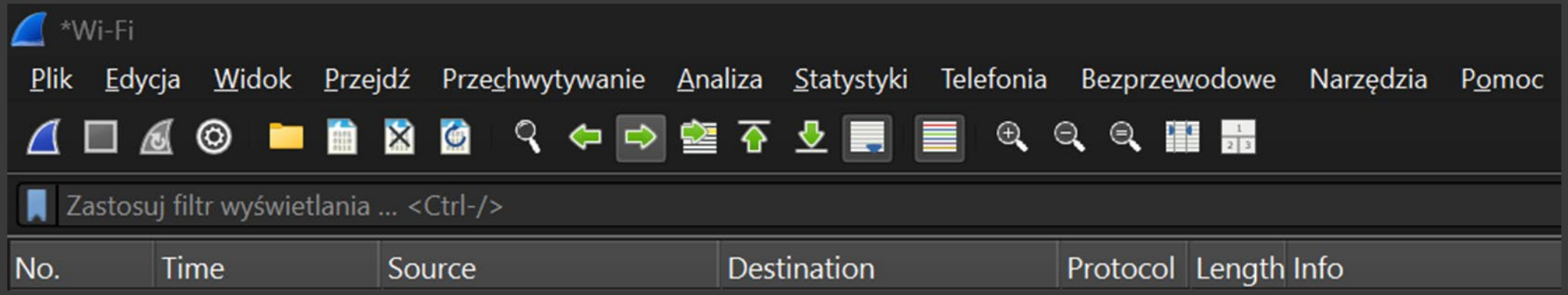
Ruch sieciowy na interfejsie



Statusy nasłuchiwania (on/off)

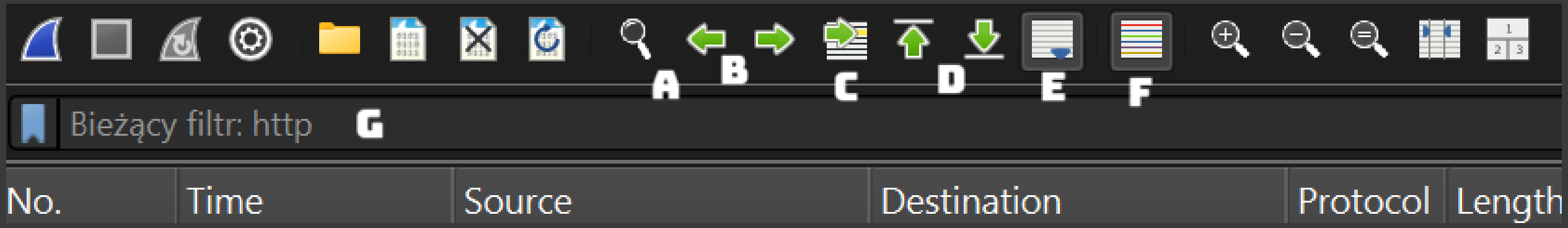


AKTYWNE NASŁUCHIWANIE (CZERWONY KWADRAT „STOP” PODŚWIETLONY)



WYŁĄCZONE NASŁUCHIWANIE
(CZERWONY KWADRAT „STOP” SZARY, START – NIEBIESKA PŁETWA)

Narzędzia filtrowania



- **A –** wyszukiwanie konkretnego rodzaju pakietów
- **B –** przełączanie następny/poprzedni pakiet
- **C –** przejście do wybranego pakietu
- **D –** przejście do pierwszego/ostatniego pakietu
- **E –** automatyczne przewijanie, gdy nasłuchiwanie jest aktywne
- **F –** przełączanie formatowania pakietów (kolorowanie wybranych danego rodzaju)
- **G –** tożsame z A

HTTP filtruje pakiety nieszyfrowane. W jaki sposób więc można wyszukać szyfrowane pakiety HTTPS?

(wyszukanie https nie działa!)

HTTP filtruje pakiety nieszyfrowane. W jaki sposób więc można wyszukać szyfrowane pakiety HTTPS?

Podpowiedź: protokół, dzięki któremu połączenia są szyfrowane (certyfikaty)

HTTP filtruje pakiety nieszyfrowane. W jaki sposób więc można wyszukać szyfrowane pakiety HTTPS?

ROZWIĄZANIE:

Należy zastosować protokół SSL (lub następca: TLS)

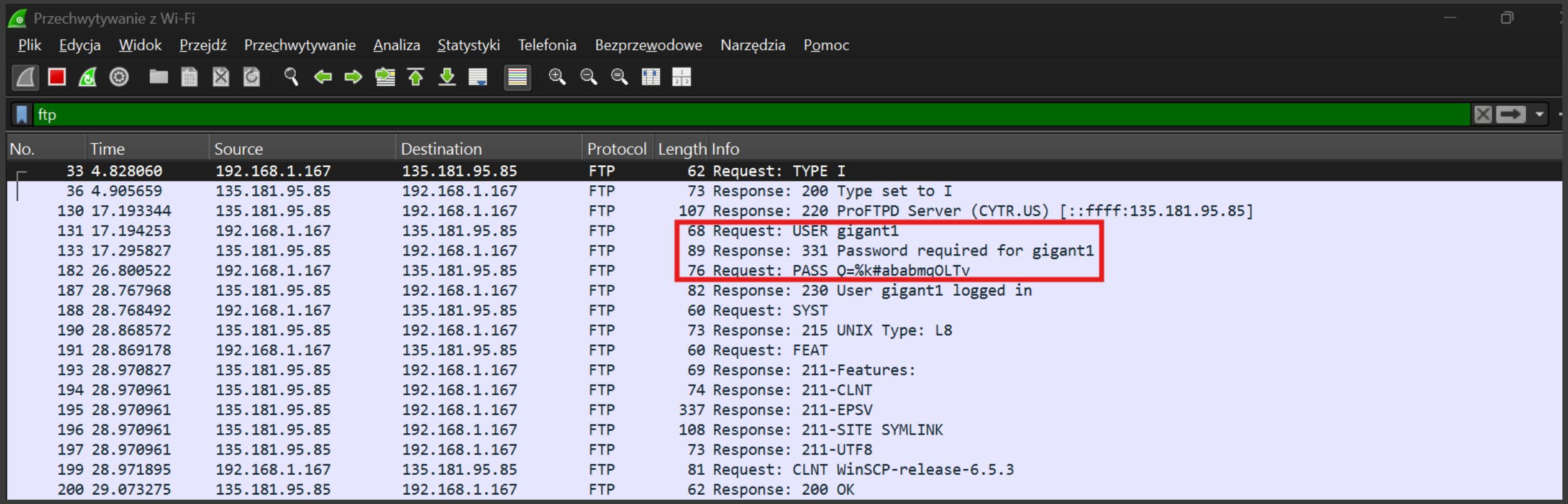
ĆWICZENIE 1 | Przejmowanie danych przez FTP

1. Uruchamiamy Filezillę i logujemy się do serwera FTP:

   adres serwera: **ftp.cytr.us**
   login: **gigant1** ... (do) **gigant15**
   hasło: **Q=%k#ababmqOLTv**

2. Przechodzimy do Wiresharka, resetujemy nasłuchiwanie i wyszukujemy pakiety, filtrując po **ftp**.

3. Szukamy informacji na temat hasła w szczegółach o pakiecie


Przechwytywanie z Wi-Fi
Plik Edycja Widok Przejdź Przechwytywanie Analiza Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc
ftp
No. Time Source Destination Protocol Length Info
33 4.828060 192.168.1.167 135.181.95.85 FTP 62 Request: TYPE I
36 4.905659 135.181.95.85 192.168.1.167 FTP 73 Response: 200 Type set to I
130 17.193344 135.181.95.85 192.168.1.167 FTP 107 Response: 220 ProFTPD Server (CYTR.US) [::ffff:135.181.95.85]
131 17.194253 192.168.1.167 135.181.95.85 FTP 68 Request: USER gigant1
133 17.295827 135.181.95.85 192.168.1.167 FTP 89 Response: 331 Password required for gigant1
182 26.800522 192.168.1.167 135.181.95.85 FTP 76 Request: PASS Q=%k#ababmqOLTv
187 28.767968 135.181.95.85 192.168.1.167 FTP 82 Response: 230 User gigant1 logged in
188 28.768492 192.168.1.167 135.181.95.85 FTP 60 Request: SYST
190 28.868572 135.181.95.85 192.168.1.167 FTP 73 Response: 215 UNIX Type: L8
191 28.869178 192.168.1.167 135.181.95.85 FTP 60 Request: FEAT
193 28.970827 135.181.95.85 192.168.1.167 FTP 69 Response: 211-Features:
194 28.970961 135.181.95.85 192.168.1.167 FTP 74 Response: 211-CLNT
195 28.970961 135.181.95.85 192.168.1.167 FTP 337 Response: 211-EPSV
196 28.970961 135.181.95.85 192.168.1.167 FTP 108 Response: 211-SITE SYMLINK
197 28.970961 135.181.95.85 192.168.1.167 FTP 73 Response: 211-UTF8
199 28.971895 192.168.1.167 135.181.95.85 FTP 81 Request: CLNT WinSCP-release-6.5.3
200 29.073275 135.181.95.85 192.168.1.167 FTP 62 Response: 200 OK

ĆWICZENIE 2 | Pliki *.pcap

Spróbuj przechwycić dowolne pakiety ze swojej karty sieciowej (możesz np. wejść na jakąś stronę i spróbować się zalogować bądź wrzucić plik, np. na chmurze Dysk Google lub podobnej). Następnie, przefiltruj po wybranym protokole, np. http/ssl lub ftp / ssh (w zależności od tego, jakiego rodzaju połączenia nawiązujesz).

Rezultaty zapisz do pliku: File/Plik -> Export Specified Packets/Zapisz wybrane pakiety

1. *Jakie protokoły zostały użyte podczas komunikacji?*
2. *Z jakich adresów komunikacja się odbywała?*
3. *Co to jest za adres 127.0.0.1?*
4. *Jeżeli podczas komunikacji http była próba przesłania plików, w jaki sposób możemy je odszukać i wyciągnąć?*

ĆWICZENIE 3 | Przesyłanie pliku i wyciąganie go z komunikacji FTP

Ponownie łączymy się z serwerem FTP za pomocą danych z ćwiczenia 1. Przesyłamy plik, np. obrazek przy uruchomionym nasłuchiwaniu w Wireshark'u. **Filtrujemy po FTP.**

Jakie są rezultaty? Czy udało się odnaleźć przesyłany plik?

ĆWICZENIE 3 | Przesyłanie pliku i wyciąganie go z komunikacji FTP

Ponownie łączymy się z serwerem FTP za pomocą danych z ćwiczenia 1. Przesyłamy plik, np. obrazek przy uruchomionym nasłuchiwaniu w Wireshark'u. **Filtrujemy po FTP.**

Jakie są rezultaty? Czy udało się odnaleźć przesyłany plik?

Podpowiedź: **Musimy połączyć dwa różne filtry: ftp oraz ftp-data. W celu zastosowania wspólnego filtra dla dwóch rodzajów, musimy zastosować operację logiczną (AND / OR).**

Którą z nich zastosujemy i dlaczego? Jak to zapisać, jeśli jest to analogiczne do języków programowania?

ĆWICZENIE 3 | Przesyłanie pliku i wyciąganie go z komunikacji FTP

Ponownie łączymy się z serwerem FTP za pomocą danych z ćwiczenia 1. Przesyłamy plik, np. obrazek przy uruchomionym nasłuchiwaniu w Wireshark'u. **Filtrujemy po FTP.**

Jakie są rezultaty? Czy udało się odnaleźć przesyłany plik?

Rozwiązanie: **Stosujemy operację LUB (OR) – AND spowodowałby, że oczekiwalibyśmy dwóch osobnych rodzajów pakietów jednocześnie!**

Zapisujemy więc:

ftp || ftp-data

Na koniec, eksportujemy:
Plik > Eksportuj obiekty > FTP-DATA
Wybieramy plik i zapisujemy na naszym komputerze.

Podsumowanie

1. Jakiego znaku trzeba użyć w filtrze wiresharka aby 2 różne filtry zastosować?
2. Co się nam wyświetli jeżeli użyjemy filtru ftp-data?
3. Co to jest plik o rozszerzeniu PCAP?

ZADANIE EXTRA | Własna analiza

Sprawdź swoje ulubione strony internetowe, jak wygląda ruch sieciowy i czy da się coś z nich wyciągnąć stosując filtr **ip.addr = ip strony ulubionej**

- Zobacz jak wygląda ruch sieciowy podczas grania w grę sieciową.
- Połącz się z kimś przez komunikator głosowy i zobacz jak wygląda takie połączenie.
- Spróbuj tak ustawić wiresharak aby przechwytywał ruch sieciowy tylko z maszyny wirtualnej np z kali linuxa, bez ruchu sieciowego z windowsa.

Polecam!

ŹRÓDŁO:
https://www.youtube.com/watch?v=5qecyZHL-GU

Polecam!

ŹRÓDŁO:
https://www.youtube.com/watch?v=C4Gtq5anlyc