# Wireshark - ćwiczenie

**Zadania do wykonania**

Zapoznać się z instrukcją programu Wireshark oraz jego działaniem.

Z pomocą programu Wireshark wykonać następujące zadania:

1. Uruchomić program ping podając adres domenowy. Przeanalizować w pliku przechwyconych danych – protokoły ARP, ICMP, DNS. (ARP jest dla przykładu przeanalizowany)
2. Uruchomić program tracert dla różnych stacji podając adres domenowy. Przeanalizować w pliku przechwyconych danych – protokoły ARP, ICMP, DNS .
3. Uruchomić przeglądarkę WWW dla wybranych adresów sieciowych i przeanalizować w pliku przechwyconych danych – protokoły HTTP, DNS .
4. Uruchomić wybraną stronę https i przeanalizować przechwycone dane.
5. Wejść na wybraną stronę gdzie jest panel logowania (nie zabezpieczoną https) wpisać hasło i przechwycić to hasło w wiresharku. Proces ten pokazać na printscreenach.

W formie pisemnego sprawozdania przygotować dokładną analizę wykonanych zadań. Sprawozdanie należy zrealizować według następującego planu:

1. Wprowadzenie, cel ćwiczenia.
2. Opis najważniejszych cech wybranych protokółów sieciowych (wymiana informacji, format pakietów, itp.).
3. Analiza otrzymanych logów z programu Wireshark (dla danego protokołu, po wcześniejszym przefiltrowaniu).
4. Wnioski.

*Przykład analizy otrzymanego logu dla protokołu ARP:*

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 15 | 6.481702 | 156.17.43.50 | Broadcast | ARP | Who has 156.17.43.62? Tell 156.17.43.50 |
| 16 | 6.481937 | 156.17.43.62 | 156.17.43.50 | ARP | 156.17.43.62 is at 00:02:bb:55:45:56 |

***Opis*** *Protokół ARP (Adress Resolution Protocol) służy do uzyskania przez stację A adresu MAC(czyli adresu Ethernet) stacji, która jest bramą dla stacji A.*
*No. 15. Stacja o adresie IP 156.17.43.50 potrzebuje adresu MAC stacji o adresie156.17.43.62, która jest bramą (gateway) dla stacji 156.17.43.50. Dlatego wysyła ramkę rozgłoszeniową (broadcast) o adresie docelowymMAC w postaci ff:ff:ff:ff:ff:ff .*
*No. 16. Z definicji bramy wynika, że musi się znajdować w tej samej podsieci co stacja, dla której jest bramą. Dlatego otrzyma ramkę rozgłoszeniową i odpowie na nią przesyłając swój adres MAC. W tym momencie stacja o adresie IP 156.17.43.50 zna adres MAC swojej bramy, więc może zacząć wysyłać pakiety IP do stacji znajdujących się w innych podsieciach.*

**Ocena**

Na ocenę z tego ćwiczenia będzie wpływać: praca w czasie realizacji zadań w laboratorium oraz sprawozdanie oddane na następnych (po wykonaniu zadania) zajęciach.

Sprawozdania proszę przesłać w pliku pdf w ciągu 7 dni od ćwiczeń na adres k.serkowska@zsl.gda.pl