Technologie Informatyczne 1

Zadanie: Podstawy sieci i bezpieczeństwa w Internecie

Autor (imię, nazwisko, numer indeksu): Mateusz Kmieć 228409

# Zasady zaliczania

Zadanie składa się z części oznaczonych jako (3), (4) oraz (5).

Zaliczenie danej części zadania wymaga wykonania czynności, udokumentowania wyników w niniejszym sprawozdaniu oraz poddaniu się weryfikacji kompetencji przez prowadzącego laboratorium (tzw. odpowiedź / dyskusja).

Zaliczenie zadania na daną ocenę (3, 4, 5) wymaga poprawnego zrealizowania wszystkich części oznaczonych daną oceną. W szczególności brak poprawnej realizacji wszystkich części oznaczonych (3) oznacza brak zaliczenia zadania i w konsekwencji brak zaliczenia laboratorium.

W przypadku realizacji części zadania oznaczonych (4) lub (5) uzyskana ocena może być obniżona decyzją prowadzącego laboratorium, ze względu na niepełną realizację, nieterminową realizację lub stwierdzone braki w kompetencjach autora.

# Część 1: Bezpieczne WWW

(3) Otwórz stronę logowania portalu Wikamp (kliknij trzymając wciśnięty klawisz CTRL): [https://ftims.edu.p.lodz.pl/login/index.php](http://skl.it.p.lodz.pl/~mak/ftims/login.html) i zaloguj się. Nie przechodź do dalszej treści zadania zanim się nie zalogujesz!

-

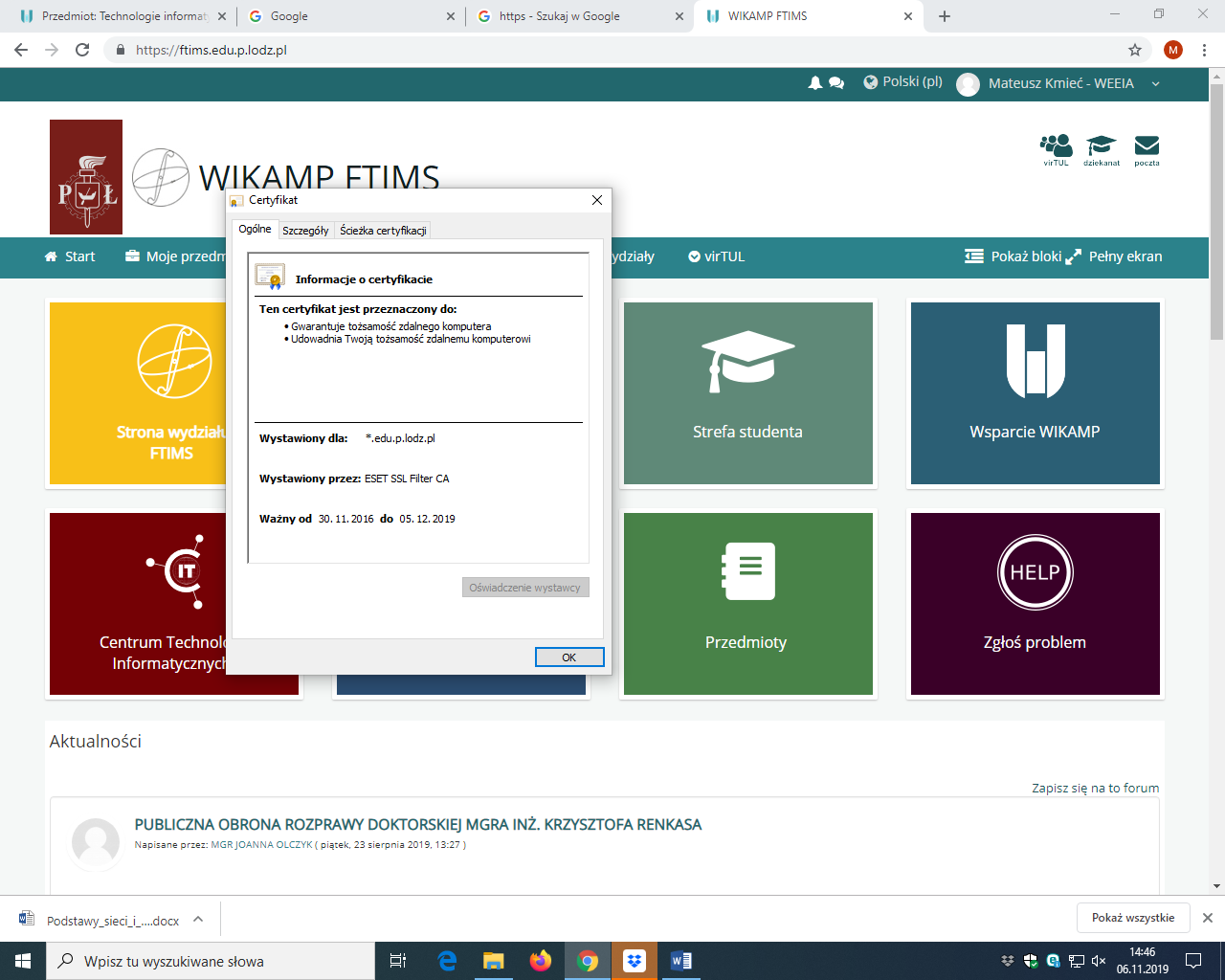
Bez obaw - Twoje konto jest bezpieczne. Porównaj URL otwartej strony z treścią odnośnika otwartego przed chwilą oraz z URL prawdziwej strony portalu Wikamp (tej na której właśnie czytasz zadanie). Czy widzisz różnicę? Dowiedz się co oznacza określenie phishing i do jakich celów ta technika jest wykorzystywana. Poniżej zamieść krótką wypowiedź na ten temat.

Adres URL otwartej strony, treść odnośnika otwartego przed chwilą i prawdziwa strona różnią się od siebie.Phishing jest metodą oszustwa w której osoba podszywa się pod inną osobę lub instytucję w celu wyłudzenia informacji, zainfekowania komputera wirusem lub nakłonienia użytkownika do określonych działań.

(3) W innej niż obecnie przeglądarce otwórz prawdziwą stronę logowania do portalu Wikamp (w przypadku niedostępności innej przeglądarki będzie trzeba wylogować się z portalu Wikamp). Zwróć uwagę na słowo https rozpoczynające URL tej strony. Dowiedz się co ono oznacza. Poniżej zamieść krótką wypowiedź na ten temat.

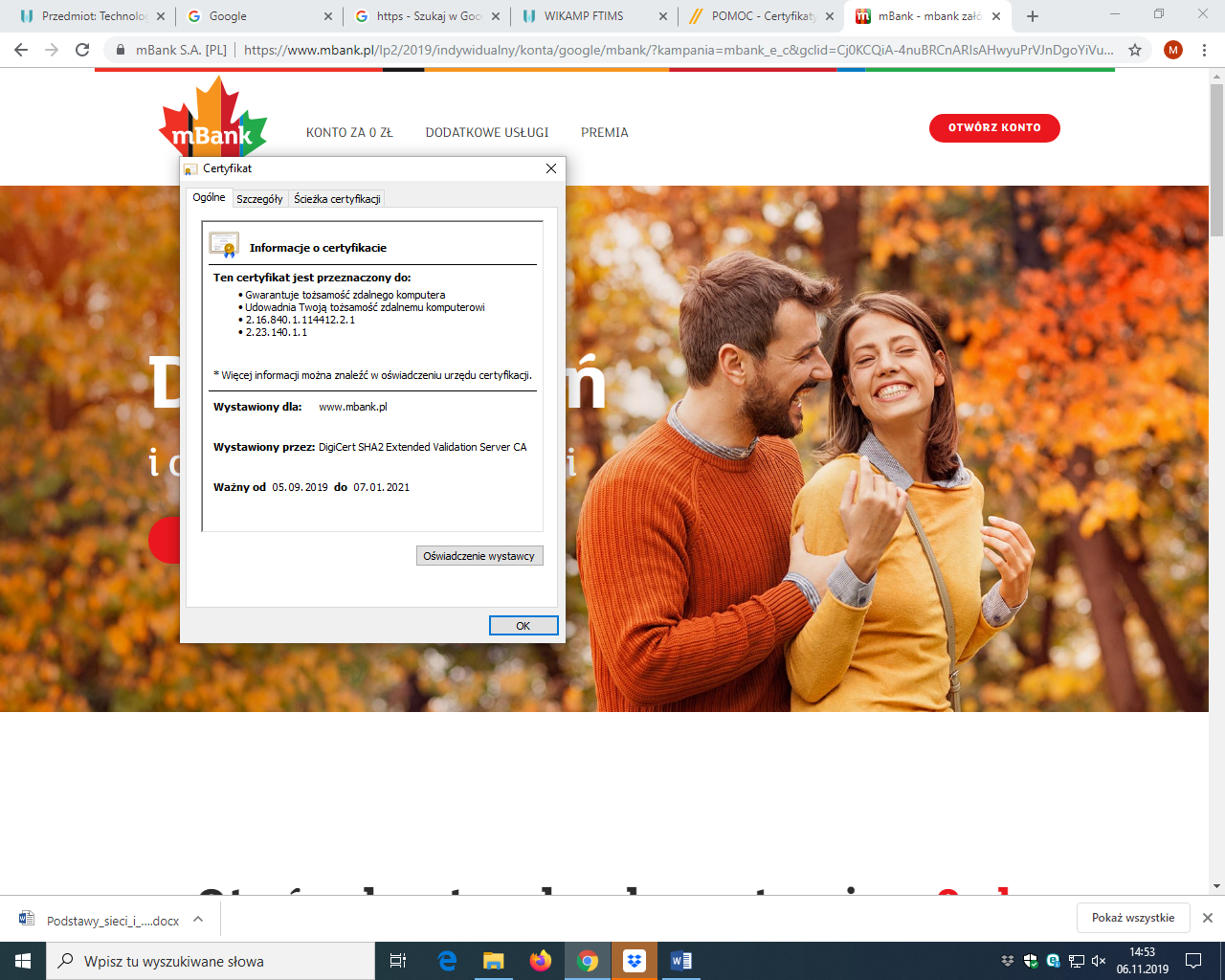
Skrót http oznacza, że dana strona ma wykupiony i skonfigurowany certyfikat SSL. Przesyłane dane są zaszyfrowane. Loginy, hasła i inne dane osobowe są bezpieczniejsze

(3) Po lewej stronie URL powinien widnieć symbol kłódki - kliknij na nią. Znajdź komunikaty mówiące o tym, że tożsamość strony jest zweryfikowana/potwierdzona i kto jest potwierdzającym, poniżej wstaw zrzut ekranu zawierający te informacje. Dowiedz się co to jest certyfikat SSL/TLS i do czego służy oraz jakie instytucje wystawiają certyfikaty. Poniżej zamieść krótką wypowiedź na ten temat.



Certyfikat SSL jest narzędziem poświadczającym wiarygodność domeny i właściciela. Certyfikat ten gwarantuje poufność danych oraz całej komunikacji. Instytucjami wystawiającymi certyfikaty cyfrowe są Urzędy Certyfikacji (CA).

(4) W podobny sposób sprawdź, czy wiarygodne są witryny: wybranego banku internetowego, wybranego portalu społecznościowego. W przypadku wybranej z nich wstaw zrzut ekranu z widocznymi informacjami jak w poprzednim punkcie.



(4) Wróć do fałszywej strony logowania i dopisz https:// na początku jej URL. Przeczytaj uważnie komunikat przeglądarki i zorientuj się, z jakiej przyczyny certyfikat nie został uznany za wiarygodny. Czy bezpieczne jest podawanie swoich poufnych danych na takiej stronie? Poniżej zamieść krótką wypowiedź na oba tematy.

Podawanie poufnych danych na takiej stronie nie jest bezpiecznie ponieważ dane mogą być niezaszyfrowane a także przechwycone. Certyfikat nie został uznany za wiarygodny ponieważ nie został wystawiony przez Urząd Certyfikacji.

# Część 2: Mój system w sieci

(3) Uruchom wiersz poleceń (program *cmd*) i wydaj polecenie *ipconfig /all*. Zanotuj parametry, które uda Ci się odnaleźć: adres IPv4, maska podsieci, brama domyślna, serwer[y] DNS, serwer[y] DHCP. Jakie znaczenie mają poszczególne z tych pojęć? Porównaj te parametry z analogicznymi ustawieniami sąsiedniego stanowiska - które się różnią, a które są identyczne? Porównaj wartość maski podsieci z różnicami w adresach IPv4 w dwóch wybranych stanowiskach i wyciągnij wniosek co do interpretowania maski podsieci.

Adres IPv4: 192.168.1.100,

Maska podsieci: 255.255.255.0

Brama domyślna: 192.168.1.1

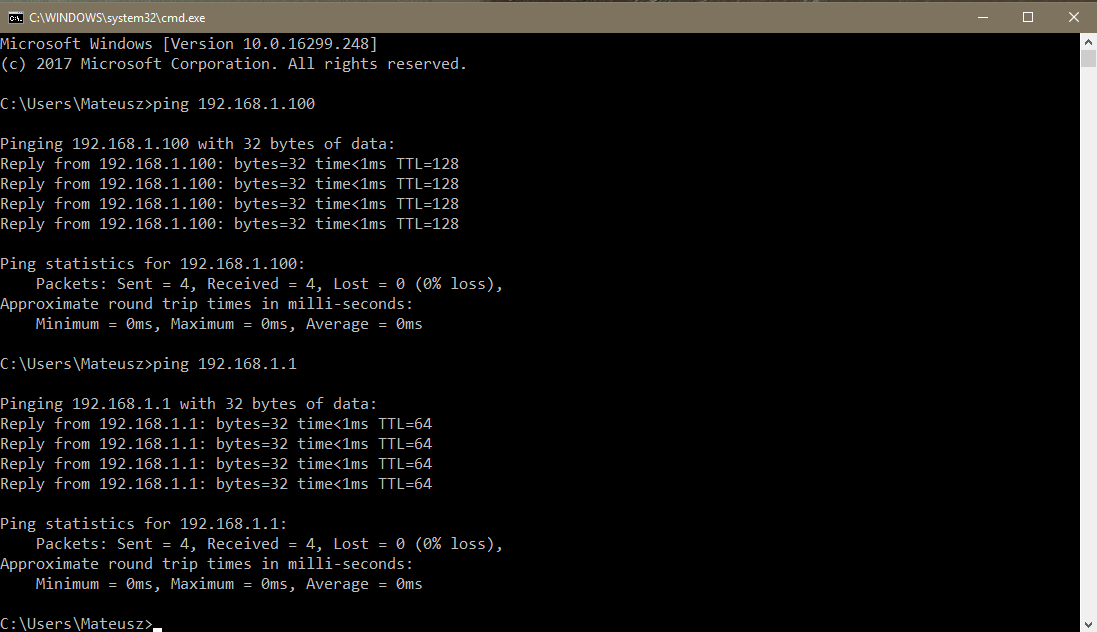
Serwer DHCP: 192.168.1.1

Serwer DNS: 8.8.8.8

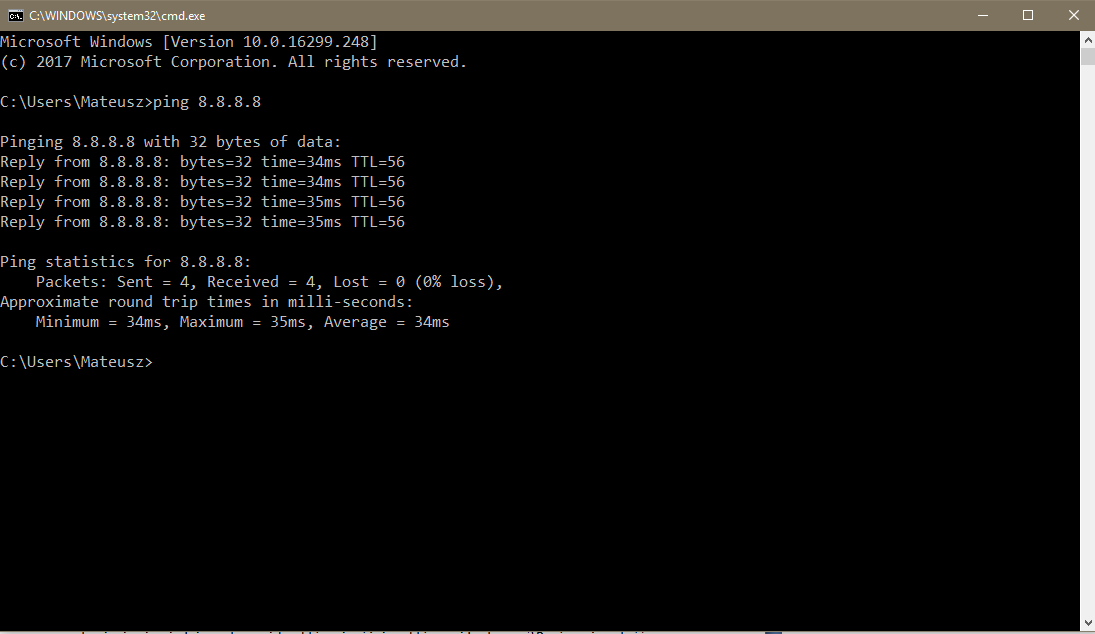
Adres IP jest unikatowy dla komputera w danej podsieci. Maska podsieci jest taka sama dla każdego komputera w danej podsieci. Brama domyślna jest adresem routera do którego komputery mają wysyłać pakiety. Serwer DNS służy do tłumaczenia nazwy domenowej na przypisany do niej adres IP. Serwer DHCP służy do przydzielania adresów IP poszczególnym komputerom w podsieci. Identyczne są brama domyślna, maska podsieci, serwer dns oraz serwer dhcp. Adres IP się różni. Maska podsieci określa zakres adresów IP, które należą do danej sieci.

(3) Użyj polecenia *ping* podając adres IPv4 innego komputera w pracowni, adres IPv4 bramy domyślnej, adres 8.8.8.8. Treść poleceń wraz z ich wynikami wklej poniżej. Do czego można wykorzystać polecenie *ping*?

ping 192.168.1.100 oraz ping 192.168.1.1

**

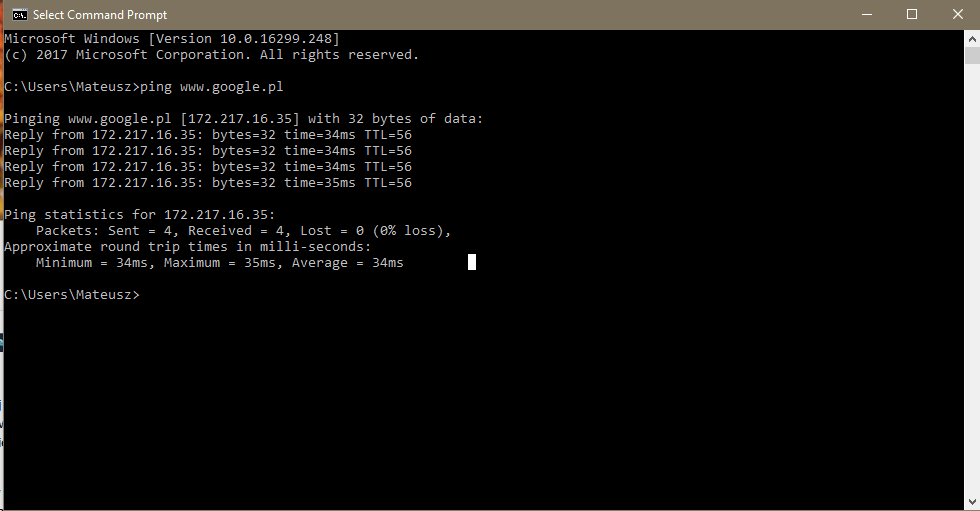
ping 8.8.8.8



Polecenie ping służy do diagnozowania połączeń sieciowych. Można sprawdzić czy istnieje połączenie pomiędzy hostami a także zbadać opóźnienia transmisji i utratę pakietów.

(3) Użyj polecenia *ping* podając *nazwę* wybranej witryny internetowej. Treść polecenia wraz z wynikiem wklej poniżej. Zwróć uwagę na udzielane odpowiedzi - podawany jest adres IPv4. Spróbuj użyć tego adresu jako witryny w przeglądarce. Który parametr jest rzeczywiście używany w komunikacji z witryną - nazwa czy adres? Poniżej zamieść krótką wypowiedź na ten temat.

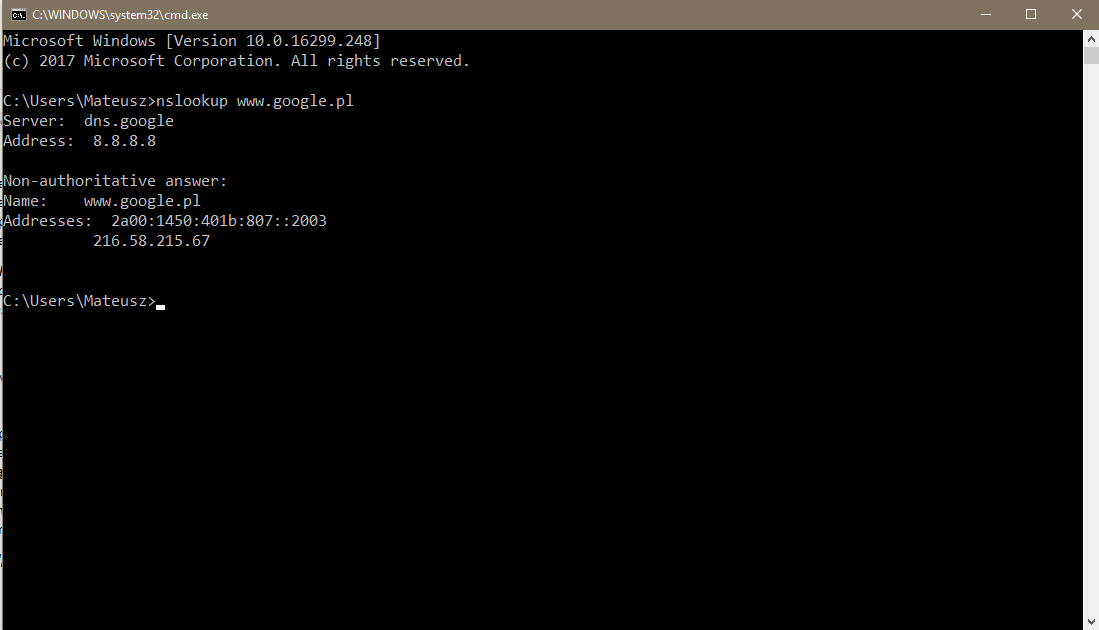
ping www.google.pl



Można użyć zarówno nazwy jak i adresu. Ludzie korzystają z nazwy ponieważ jest wygodniejsza do użycia i zapamiętania.

(4) Dowiedz się czym jest usługa DNS. Użyj polecenia *nslookup* podając jeszcze raz nazwę wybranej witryny. Treść polecenia wraz z wynikiem wklej poniżej. Czy umiesz zidentyfikować serwer DNS, który udzielił odpowiedzi? Porównaj jego adres z ustawieniami serwerów DNS zanotowanymi w pierwszym etapie. Poniżej zamieść krótką wypowiedź na ten temat.

nslookup www.google.pl



DNS pozwala tłumaczyć nazwę na odpowiadający jej adres IP. Serwer DNS który udzielił odpowiedzi to google. Adres serwera odpowiada temu adresowi, który został sprawdzony przez polecenie ipconfig /all

(4) Znajdź i otwórz dowolną witrynę na której można odczytać swój adres IPv4. Czy podany adres jest taki sam jak adres zanotowany na etapie 1? Porównaj swój wynik z wynikami innych. Poniżej zamieść krótką wypowiedź na ten temat. Dowiedz się, czym są adresy (podsieci) prywatne i publiczne oraz co to jest NAT lub maskarada IPv4.

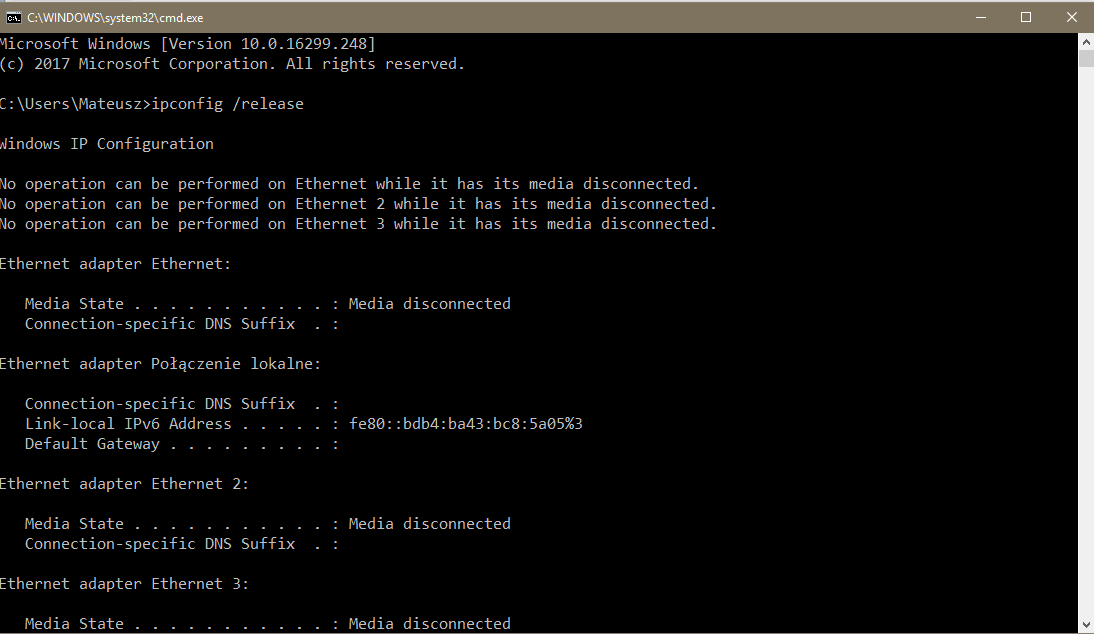
Adresy różnią się od siebie. Adres odczytany w etapie pierwszym jest adresem prywatnym a adres odczytany na stronie to adres publiczny. Adresy publiczne są unikalne na skalę światową natomiast adresy prywatne są unikalne tylko w obrębie danej podsieci. NAT pozwala spowolnić wyczerpywanie puli publicznych adresów dzięki używaniu jednego adresu publicznego przez komputery w obrębie danej sieci prywatnej.

(5) Otwórz także dowolną stronę oferującą [geo]lokalizację adresu IP i sprawdź, czy "twój" adres IPv4 można zlokalizować. Podobnie sprawdź za pomocą usługi whois kto jest zarządcą adresu. Poniżej zamieść krótką wypowiedź na ten temat.

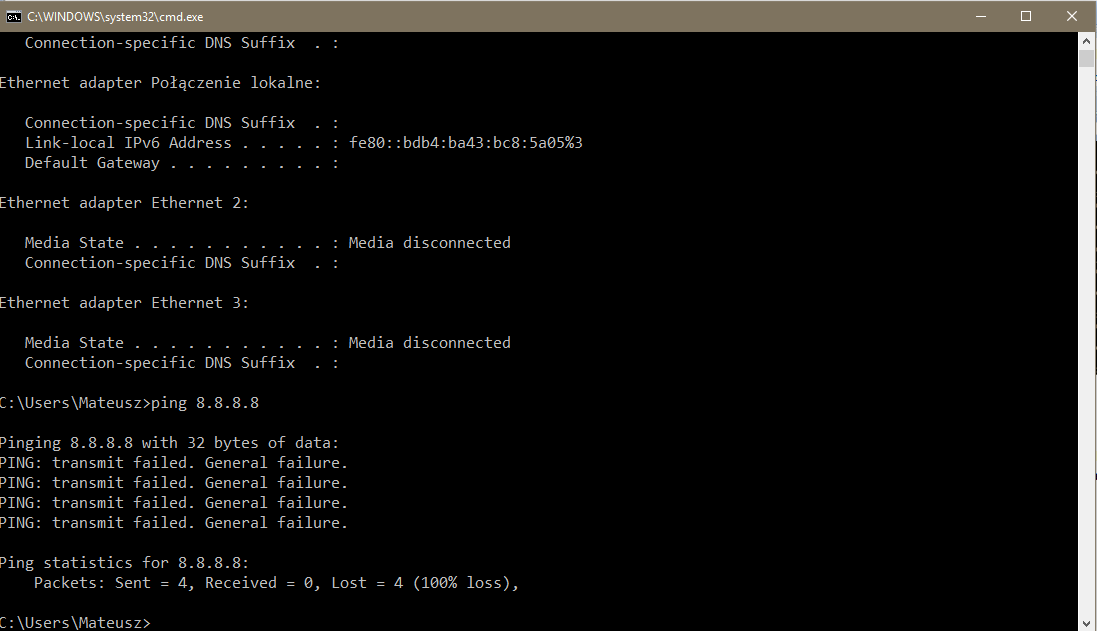
Dzięki geolokalizacji adresu IP możemy uzyskać przybliżoną lokalizację adresu IP z dużą dokładnością. Zarządcą adresu jest instytucja RIPE.

(5) Wydaj polecenie *ipconfig /release*. Treść polecenia wraz z wynikiem wklej poniżej. Powtórz badanie za pomocą polecenia *ping* adresu innego komputera w pracowni, zanotowanego wcześniej adresu IPv4 bramy domyślnej, adresu 8.8.8.8. Treść poleceń wraz z ich wynikami wklej poniżej. Jaki jest skutek wykonania tej czynności? Poniżej zamieść krótką wypowiedź na ten temat.

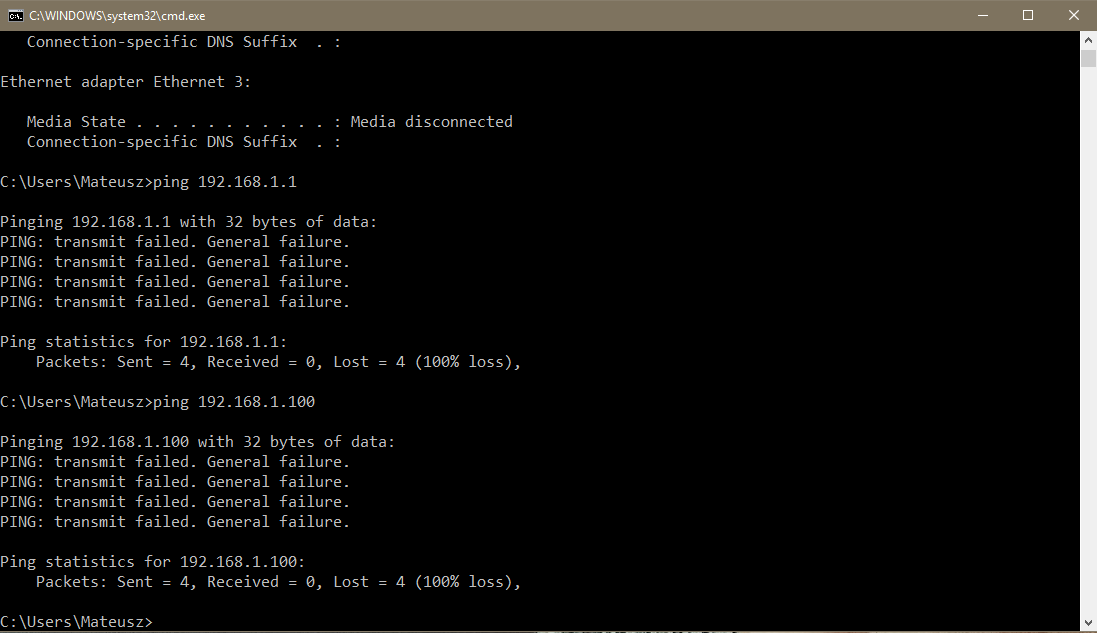
ipconfig /release

**

ping 8.8.8.8



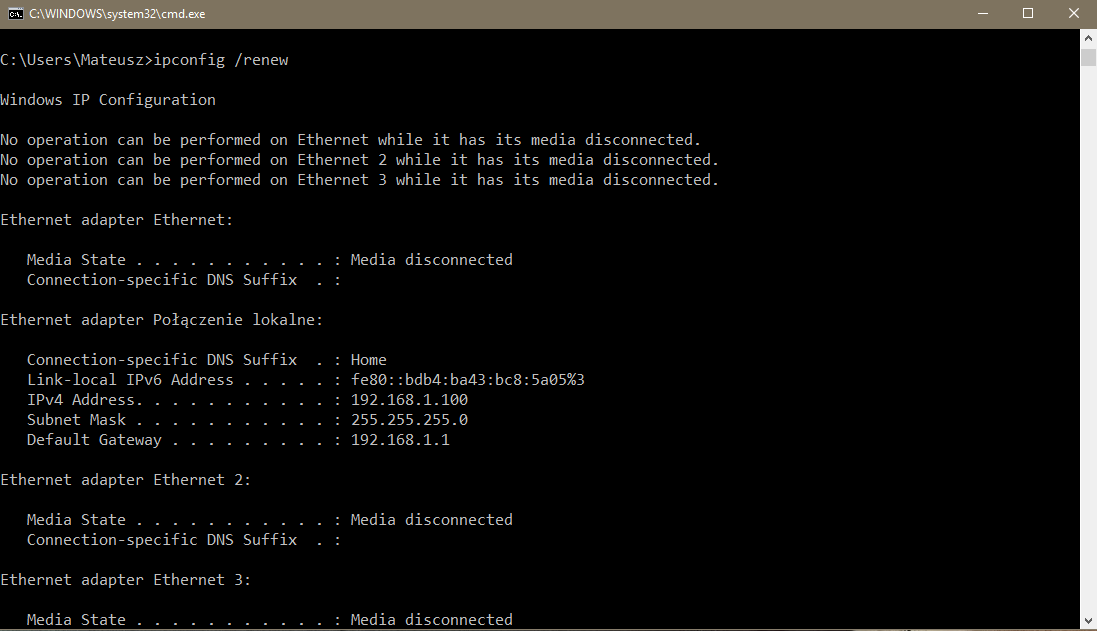
ping 192.168.1.1 oraz ping 192.168.1.100



Po wykonaniu tego polecenia (zwolnieniu adresu) tracimy możliwość połączenia z siecią i komputerami.

(5) Użyj polecenia *ipconfig /renew*. Treść polecenia wraz z wynikiem wklej poniżej. Jaki jest skutek wykonania tej czynności? Poniżej zamieść krótką wypowiedź na ten temat.

ipconfig /renew



Po wykonaniu tego polecenia (odnowieniu adresu) ponownie zyskujemy możliwość połączenia z siecią i komputerami.