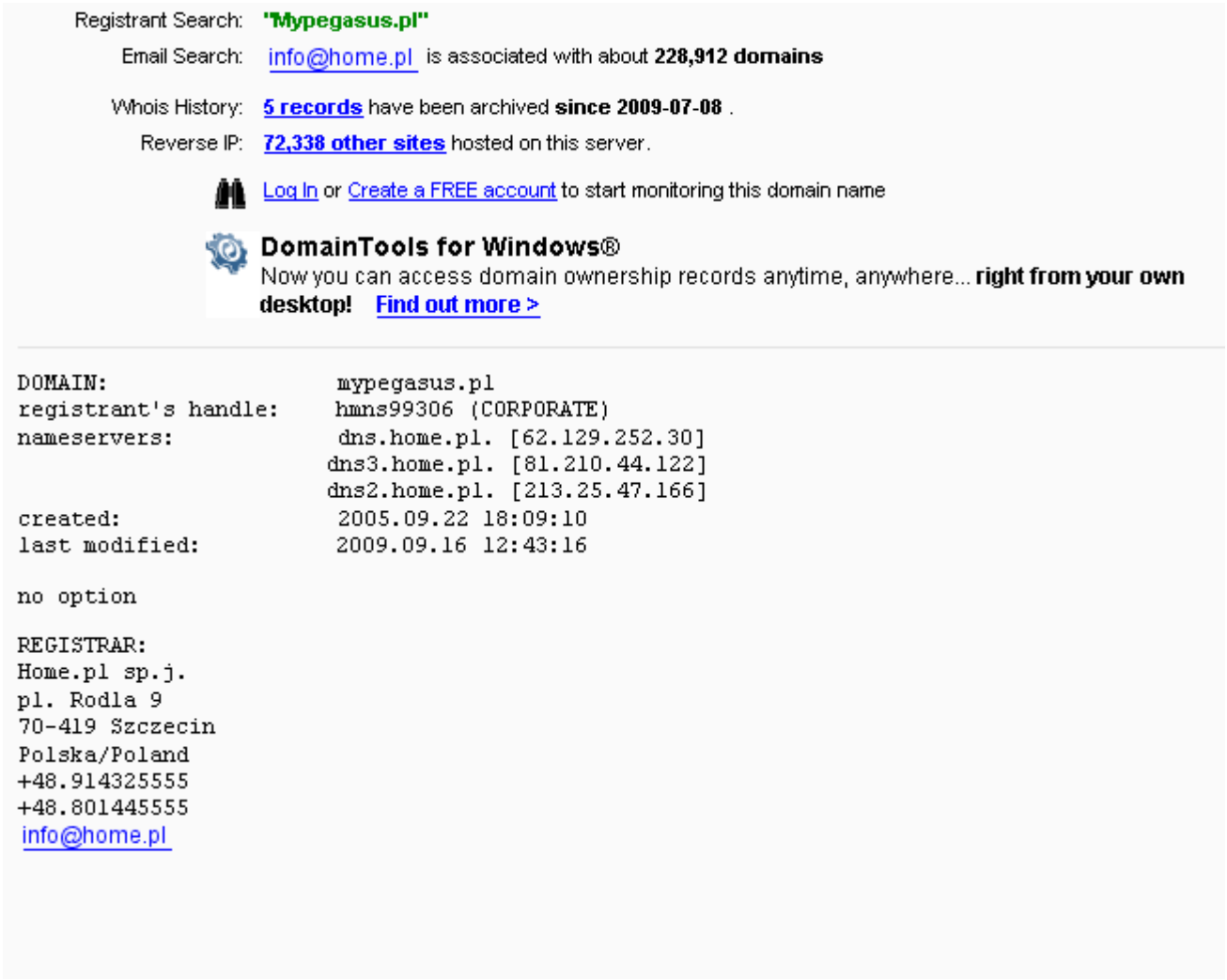
Ćwiczenie 3. Testy penetracyjne - rekonesans

Wykonał: Grzegorz Pol
Komputer: 237-16
Przedmiotem mojego zainteresowania była domena: www.mypegasus.pl

Rys. 1 (poniżej) Obrazy okien przeglądarki WWW zawierające dane uzyskane z serwera WHOIS: https://hrd.pl/pcenter/partner_frame/whois.php

Domena	
Domena	mypegasus.pl
Id abonenta	hmns99306 (FIRMOWA)
Serwery nazw	dns.home.pl. [62.129.252.30] dns3.home.pl. [81.210.44.122] dns2.home.pl. [213.25.47.166]
Utworzona	2005.09.22 18:09:10
Ostatnia modyfikacja	2009.09.16 12:43:16
Opcja	brak
Registrar	Home.pl sp.j. pl. Rodła 9 70-419 Szczecin Polska/Poland +48.914325555 +48.801445555 info@home.pl
Abonent	
Firma	Floors Tomasz Pol
Ulica	Listopadowa 1
Miasto	02-496 Warszawa
Lokalizacja	PL
Ostatnia modyfikacja	2010.03.02

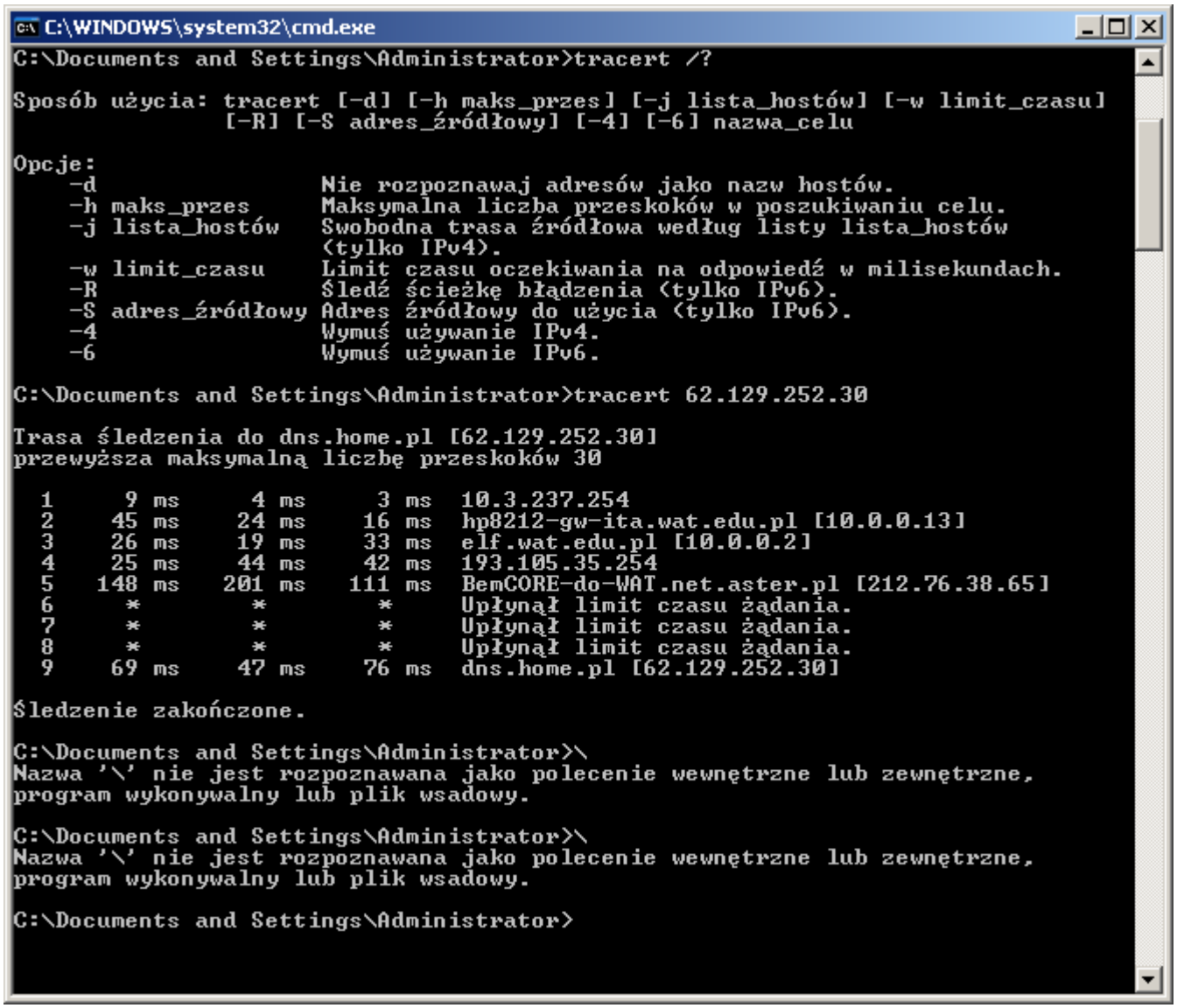
Rys. 2 (poniżej) Obrazy okien przeglądarki WWW zawierające dane uzyskane z serwera WHOIS: http://whois.domaintools.com/



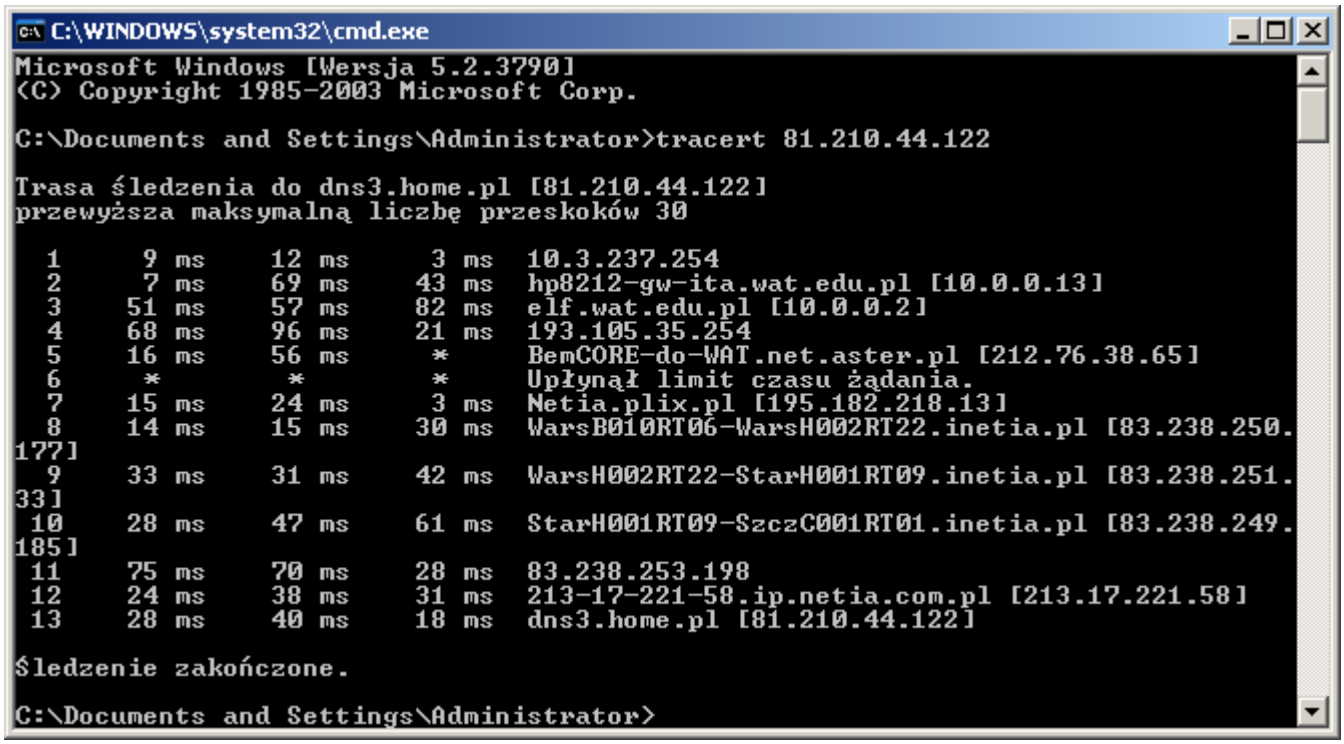
Rys. 3 (poniżej) Lista wszystkich autorytatywnych serwerów DNS badanej domeny
1. dns.home.pl. [62.129.252.30]
2. dns3.home.pl. [81.210.44.122]
3. dns2.home.pl. [213.25.47.166]

Rys. 4 (poniżej) Obrazy okien programu *tracert* uzyskane w czasie badania osiągalności wszystkich autorytatywnych serwerów DNS badanej domeny

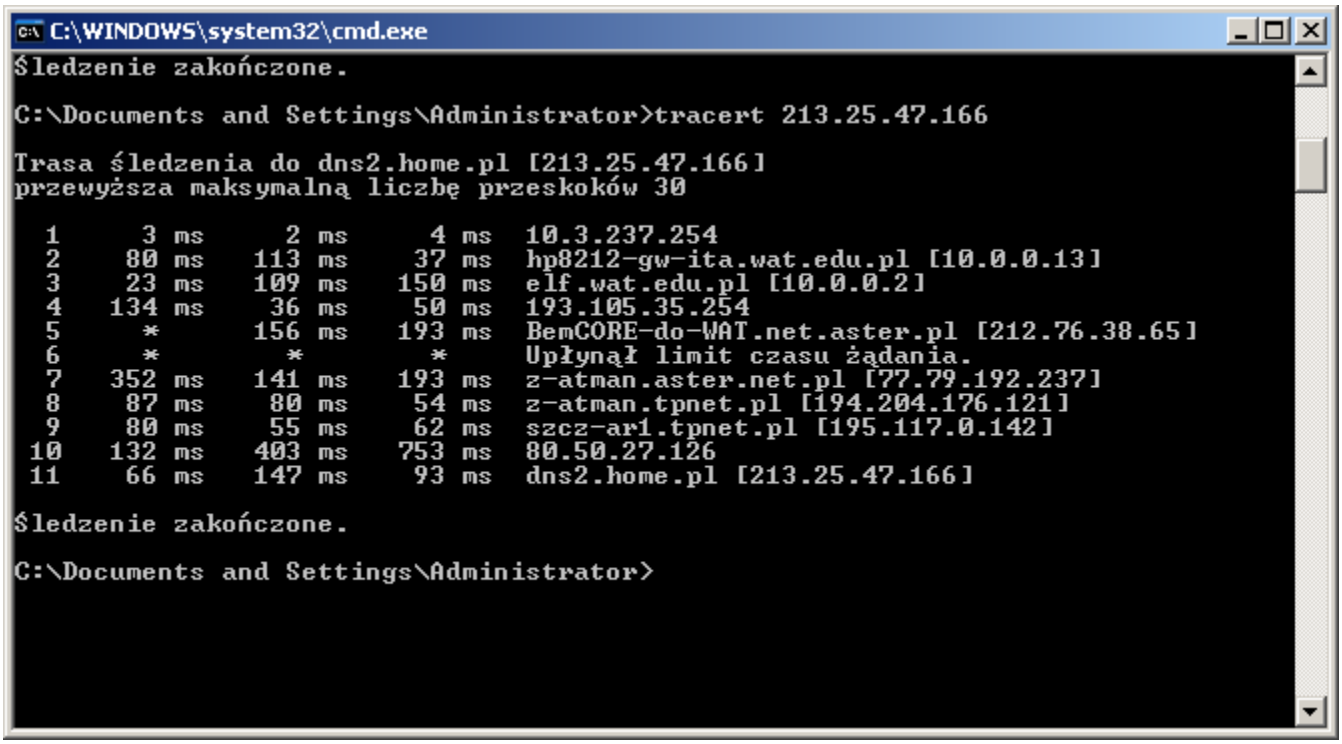
1. 62.129.252.30



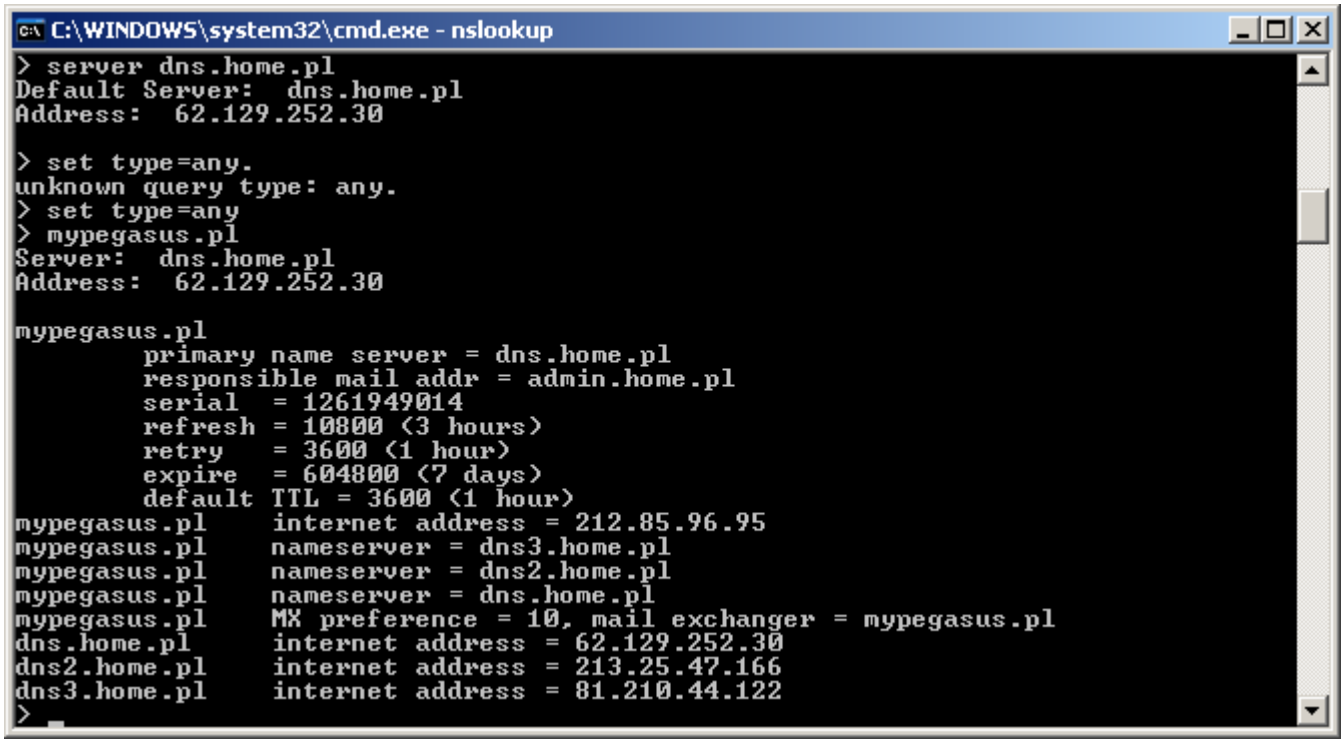
2. 81.210.44.122

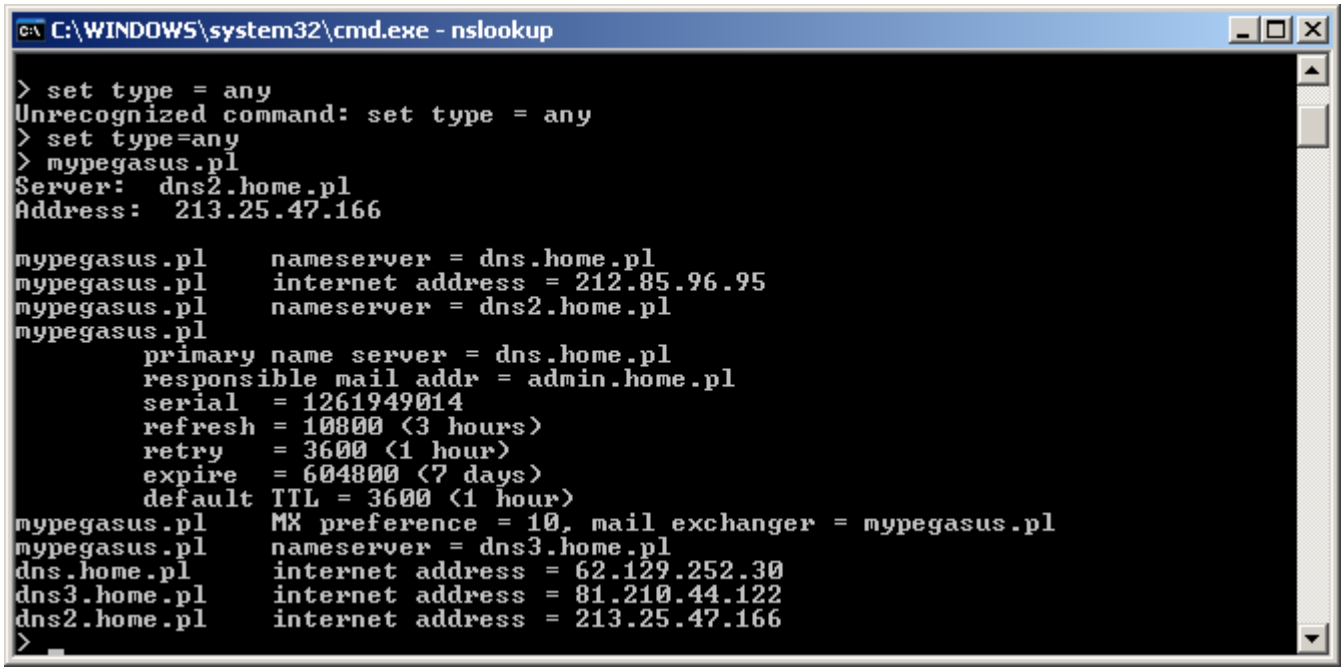


3. 213.25.47.166

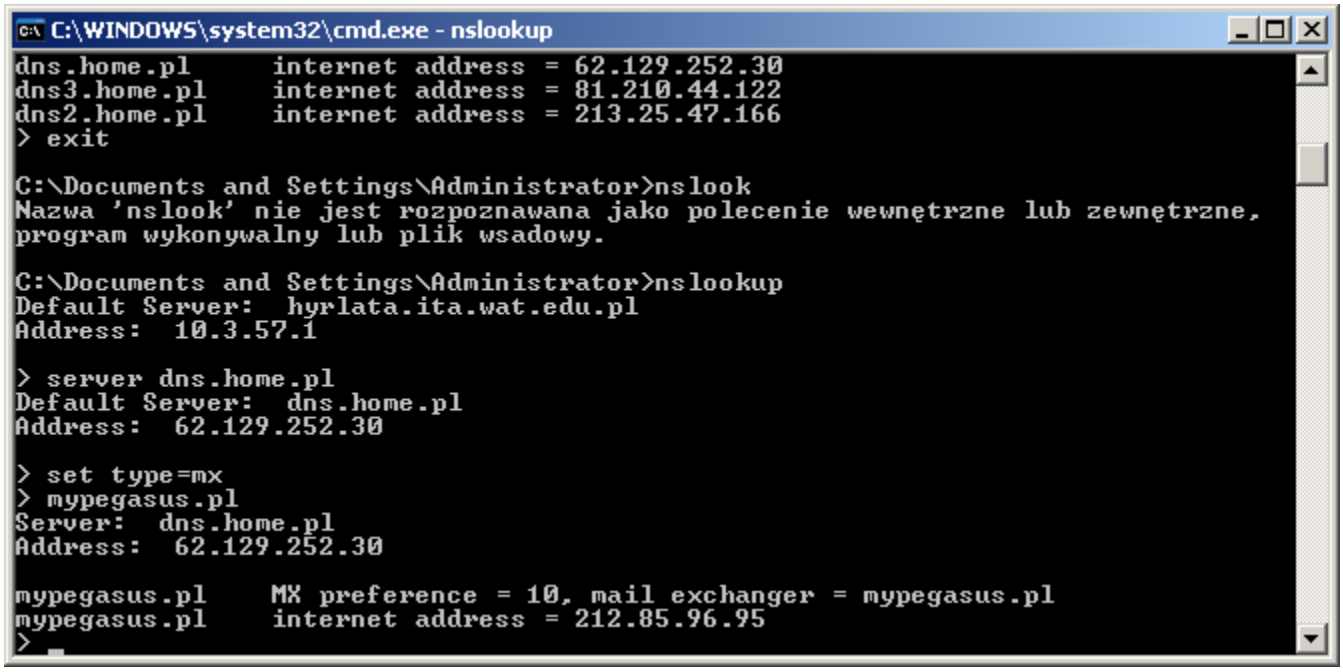


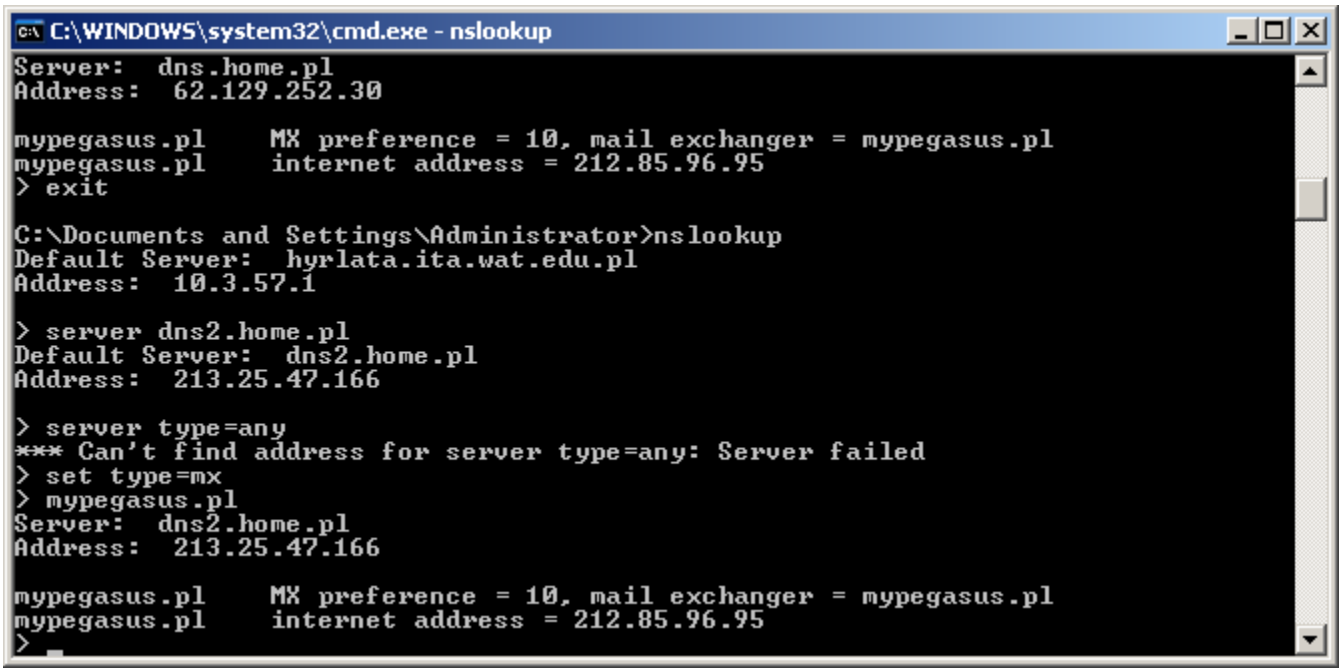
Rys. 5 (poniżej) Obrazy okien programu *nslookup* uzyskane w czasie realizacji próby uzyskania zawartości pliku strefowego z dwóch wybranych, autorytatywnych serwerów DNS badanej domeny





Rys. 6 (poniżej) Obrazy okien programu *nslookup* uzyskane w czasie realizacji próby uzyskania zawartości rekordów MX, CNAME, TXT z dwóch wybranych, autorytatywnych serwerów DNS badanej domeny





Rys. 7 (poniżej) Obrazy okien przeglądarki WWW uzyskane w czasie realizacji próby uzyskania zawartości rekordów MX, CNAME, TXT z dwóch wybranych autorytatywnych serwerów DNS badanej domeny

Wkleić obrazy okien

WŁASNE SPOSTRZEŻENIA I WNIOSKI:

Nie udało mi zrealizować wszystkich podpunktów wymaganych. Podpunkty, które wykonałem pokazują jak wiele informacji o stronach, administratorach jest jawnie dostępnych pobierając je całkowicie anonimowo.