

Εργαστήριο Wireshark: DNS



Έκδοση:2.0

© 2007 J.F. Kurose, K.W. Ross

Μετάφραση - Απόδοση: Σ. Τσακιρίδου

*Computer Networking: A Top-Down
Approach Featuring the Internet*

Όπως περιγράφεται στην Ενότητα 2.5 του βιβλίου, το Domain Name System (DNS) μεταφράζει ονόματα τερματικών συστημάτων (hostnames) σε διευθύνσεις IP, παίζοντας έτσι ένα σημαντικό ρόλο στην υποδομή του Διαδικτύου. Στο εργαστήριο αυτό θα εξετάσουμε την πλευρά του πελάτη (client) στο DNS. Υπενθυμίζεται ότι ο ρόλος του client στο DNS είναι σχετικά απλός: ο client στέλνει ένα *ερώτημα* (*query*) στον τοπικό DNS server από τον οποίο λαμβάνει μία *απόκριση* (*response*). Όπως φαίνεται στα Σχήματα 2.16 και 2.18 του βιβλίου, πολλά από τα μηνύματα που ανταλλάσσονται καθώς οι ιεραρχημένοι DNS servers επικοινωνούν μεταξύ τους είτε αναδρομικά (recursively) είτε επαναληπτικά (iteratively) για να απαντήσουν στο ερώτημα DNS του client δεν γίνονται αντιληπτά από τον DNS client. Από τη σκοπιά του DNS client το πρωτόκολλο είναι πολύ απλό: διατυπώνεται ένα ερώτημα στον τοπικό DNS server από τον οποίο λαμβάνεται μία απόκριση.

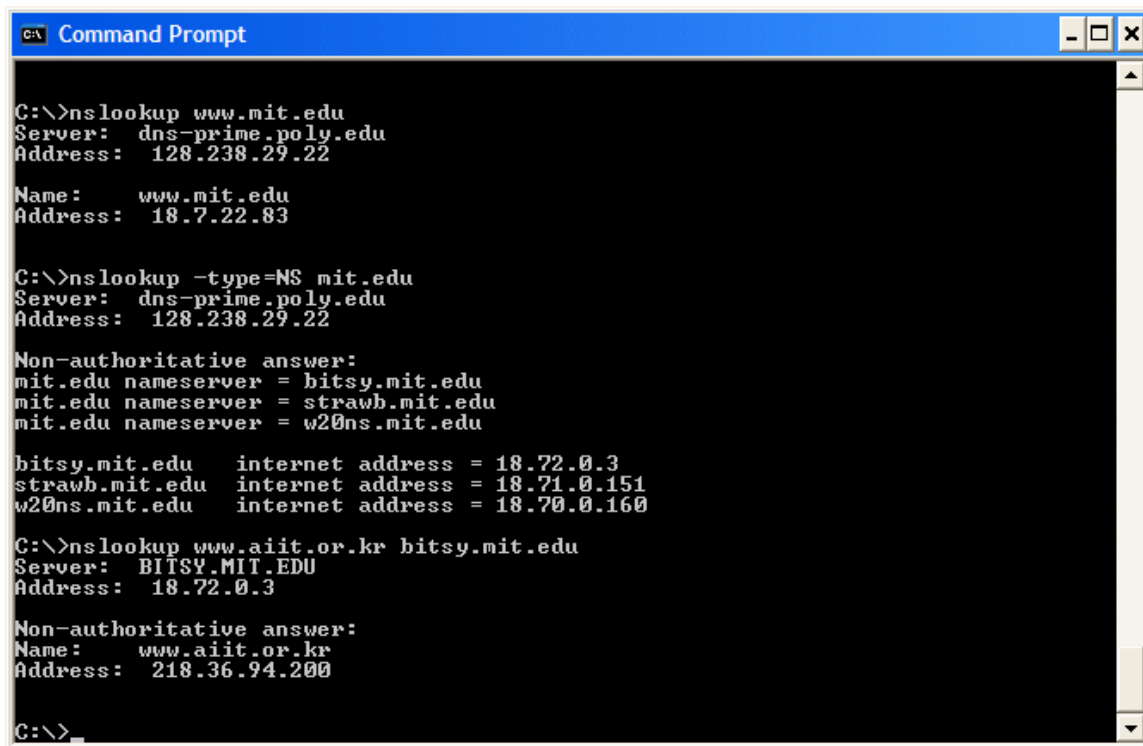
Πριν ξεκινήσετε αυτό το εργαστήριο, καλό θα ήταν να κάνετε μία ανασκόπηση του DNS στην Ενότητα 2.5 του βιβλίου σας και πιο συγκεκριμένα, της ύλης που αφορά τους **τοπικούς (local) DNS servers**, το **DNS caching**, τα **μηνύματα** και **εγγραφές (records) DNS**, καθώς και το πεδίο **TYPE** της εγγραφής DNS.

1. nslookup

Στο εργαστήριο αυτό θα χρησιμοποιήσετε εκτενώς το εργαλείο *nslookup* το οποίο είναι σήμερα διαθέσιμο στα περισσότερα συστήματα Linux/Unix και Microsoft. Για να τρέξετε το *nslookup* σε περιβάλλον Linux/Unix, πληκτρολογείτε την εντολή *nslookup* στη γραμμή εντολών. Για να το τρέξετε σε περιβάλλον Windows, ανοίγετε το παράθυρο Command Prompt και τρέχετε το *nslookup* στη γραμμή εντολών.

Στην απλούστερη λειτουργία του το *nslookup* επιτρέπει στο τερματικό σύστημα στο οποίο τρέχει να στείλει ένα ερώτημα DNS για μία εγγραφή DNS σε οποιοδήποτε καθορισμένο DNS server. Ο DNS server στον οποίο στέλνεται το ερώτημα μπορεί να είναι ένας root DNS server, ένας top-level-domain DNS server, ένας authoritative DNS server ή ένας ενδιάμεσος DNS server (συμβουλευθείτε το βιβλίο σχετικά με τον ορισμό αυτών των όρων). Για την επίτευξη αυτού του έργου, το *nslookup*

στέλνει ένα ερώτημα DNS στον καθορισμένο DNS server, λαμβάνει μία απόκριση DNS από τον ίδιο DNS server και απεικονίζει το αποτέλεσμα.



```
C:\>nslookup www.mit.edu
Server: dns-prime.poly.edu
Address: 128.238.29.22

Name: www.mit.edu
Address: 18.7.22.83

C:\>nslookup -type=NS mit.edu
Server: dns-prime.poly.edu
Address: 128.238.29.22

Non-authoritative answer:
mit.edu nameserver = bitsy.mit.edu
mit.edu nameserver = straub.mit.edu
mit.edu nameserver = w20ns.mit.edu

bitsy.mit.edu internet address = 18.72.0.3
straub.mit.edu internet address = 18.71.0.151
w20ns.mit.edu internet address = 18.70.0.160

C:\>nslookup www.aiit.or.kr bitsy.mit.edu
Server: BITSY.MIT.EDU
Address: 18.72.0.3

Non-authoritative answer:
Name: www.aiit.or.kr
Address: 218.36.94.200

C:\>
```

Το παραπάνω screenshot δείχνει τα αποτελέσματα τριών ανεξάρτητων εντολών *nslookup* όπως απεικονίζονται στο παράθυρο Command Prompt των Windows. Στο παράδειγμα αυτό ο client βρίσκεται στην πανεπιστημιούπολη του Polytechnic University των ΗΠΑ και ο τοπικός του DNS server έχει το όνομα dns-prime.poly.edu. Εάν δεν έχει καθορισθεί ο DNS server, το *nslookup* στέλνει το ερώτημα στον προεπιλεγμένο DNS server που στην προκειμένη περίπτωση είναι ο dns-prime.poly.edu. Θεωρείστε την πρώτη εντολή:

`nslookup www.mit.edu`

Με την παραπάνω εντολή ο DNS client ζητά να του αποσταλεί η διεύθυνση IP του host www.mit.edu. Όπως φαίνεται στο screenshot, η απόκριση στην εντολή αυτή περιλαμβάνει δύο κομμάτια πληροφορίας: (1) το όνομα και τη διεύθυνση IP του DNS server που παρέχει την απάντηση, και (2) την ίδια την απάντηση που αποτελείται από το όνομα και τη διεύθυνση IP του www.mit.edu. Αν και η απόκριση προήλθε από τον τοπικό DNS server του Polytechnic University, είναι αρκετά πιθανό ο τοπικός αυτός DNS server να έχει επικοινωνήσει με τρόπο επαναληπτικό με αρκετούς άλλους DNS προκειμένου να λάβει την απάντηση, όπως περιγράφεται στην Ενότητα 2.5 του βιβλίου.

Θεωρείστε τώρα τη δεύτερη εντολή:

`nslookup -type=NS mit.edu`

Στο παράδειγμα αυτό παρέχουμε την προαιρετική επιλογή “-type=NS” και το domain name “mit.edu”. Αυτό έχει ως αποτέλεσμα το *nslookup* να στείλει ένα ερώτημα για μία εγγραφή τύπου NS στον προεπιλεγμένο τοπικό DNS server. Με το ερώτημα αυτό το ο DNS client ζητά να του αποσταλούν τα ονόματα των authoritative DNS servers για το domain name “mit.edu”. (Όταν δεν χρησιμοποιείται η επιλογή -type, το *nslookup* χρησιμοποιεί εκ προεπιλογής type = A.) Στην απάντηση, η οποία απεικονίζεται στο παραπάνω screenshot, υποδεικνύεται ο DNS server που την παρείχε (δηλαδή ο προεπιλεγμένος τοπικός DNS server) καθώς και τα ονόματα τριών nameservers στο MIT. Καθένας από τους τρεις αυτούς servers είναι ένας authoritative DNS server για τους hosts της πανεπιστημιούπολης του MIT. Το *nslookup* υποδεικνύει επίσης ότι η απάντηση είναι “non-authoritative”, δηλαδή ότι προήρθε από την cache κάποιου server και όχι από έναν authoritative DNS server του MIT. Τέλος, η απάντηση περιλαμβάνει επίσης τις διευθύνσεις IP των authoritative DNS servers στο MIT. (Αν και το ερώτημα τύπου NS που έστειλε το *nslookup* δεν ζητούσε με τρόπο ρητό τις διευθύνσεις IP, ο τοπικός DNS server παρείχε “δωρεάν” αυτή την πληροφορία την οποία απεικόνισε το *nslookup*.)

Θεωρείστε, τέλος, την τρίτη εντολή:

```
nslookup www.aiit.or.kr bitsy.mit.edu
```

Στο παράδειγμα αυτό υποδεικνύουμε ότι θέλουμε το ερώτημα να σταλεί στον DNS server bitsy.mit.edu αντί του τοπικού DNS server (dns-prime.poly.edu). Έτσι η ανταλλαγή ερωτήματος και απόκρισης γίνεται απευθείας μεταξύ του host που στέλνει το ερώτημα και του server bitsy.mit.edu. Ο DNS server bitsy.mit.edu παρέχει τη διεύθυνση IP του host www.aiit.or.kr, ενός web server στο Advanced Institute of Information Technology της Κορέας.

Μετά από τα παραπάνω ενδεικτικά παραδείγματα ακολουθεί η γενική σύνταξη των εντολών *nslookup* που έχει ως εξής:

```
nslookup -option1 -option2 host-to-find dns-server
```

Το *nslookup* μπορεί να εκτελεσθεί χωρίς καμία, με μία, δύο ή περισσότερες προαιρετικές επιλογές. Όπως φαίνεται από τα παραπάνω παραδείγματα, το όνομα του DNS server είναι επίσης προαιρετικό: εάν δεν το παρέχουμε, το ερώτημα στέλνεται στον προεπιλεγμένο τοπικό DNS server.

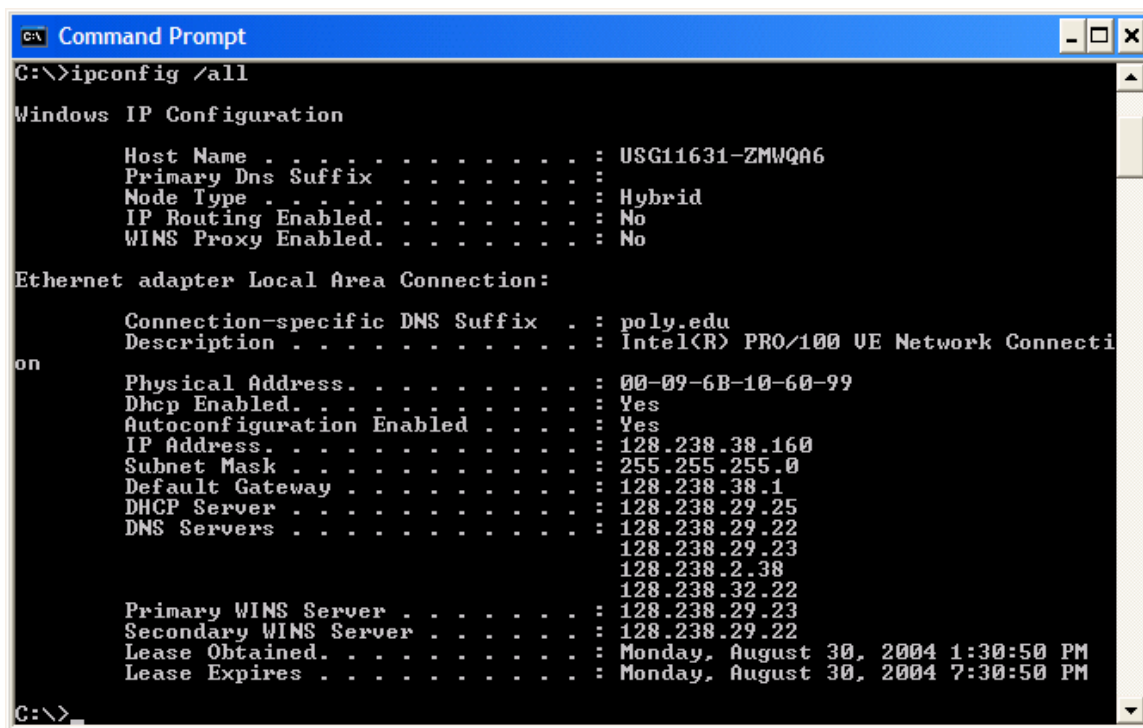
Μετά από αυτή την ανασκόπηση του *nslookup*, πειραματισθείτε οι ίδιοι εκτελώντας τα ακόλουθα:

1. Τρέξτε το *nslookup* ώστε να αποκτήσετε τη διεύθυνση IP ενός Web server που βρίσκεται στην Ασία.
2. Τρέξτε το *nslookup* ώστε να προσδιορίσετε τους authoritative DNS servers για κάποιο πανεπιστήμιο των ΗΠΑ.
3. Τρέξτε το *nslookup* ώστε ένας από τους DNS servers της απάντησης στην ερώτηση 2 να ερωτηθεί σχετικά με τους mail servers του Yahoo!mail.

2. ipconfig

Το *ipconfig* (στα Windows) και το *ifconfig* (στα Linux/Unix) είναι από τα πιο χρήσιμα εργαλεία στο τερματικό σας σύστημα. Θα περιγράψουμε μόνο το *ipconfig*, αν και το *ifconfig* σε Linux/Unix είναι παρόμοιο. Το *ipconfig* μπορεί να χρησιμοποιηθεί για να δείξει πληροφορία σχετική με το TCP/IP που τρέχει στο τερματικό σας σύστημα, π.χ., διεύθυνση IP τερματικού συστήματος, διεύθυνση IP DNS server, είδος adapter κ.α. Μπορείτε να δείτε όλη αυτή την πληροφορία εισάγοντας την εντολή `ipconfig /all`

στο παράθυρο Command Prompt όπως φαίνεται στο ακόλουθο screenshot.



```
C:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : USG11631-ZMWQA6
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : poly.edu
    Description . . . . . : Intel(R) PRO/100 VE Network Connecti
on
    Physical Address. . . . . : 00-09-6B-10-60-99
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 128.238.38.160
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 128.238.38.1
    DHCP Server . . . . . : 128.238.29.25
    DNS Servers . . . . . : 128.238.29.22
                           128.238.29.23
                           128.238.2.38
                           128.238.32.22
    Primary WINS Server . . . . . : 128.238.29.23
    Secondary WINS Server . . . . . : 128.238.29.22
    Lease Obtained. . . . . : Monday, August 30, 2004 1:30:50 PM
    Lease Expires . . . . . : Monday, August 30, 2004 7:30:50 PM

C:\>
```

Το *ipconfig* είναι επίσης πολύ χρήσιμο για πληροφορίες DNS που είναι αποθηκευμένες στο τερματικό σας σύστημα. Στην Ενότητα 2.5 μάθαμε ότι ένας host μπορεί να αποθηκεύσει εγγραφές DNS που έχουν αποκτηθεί πρόσφατα. Για να δείτε αυτές τις εγγραφές που είναι αποθηκευμένες στην προσωρινή μνήμη (cache), εισάγετε την ακόλουθη εντολή στο παράθυρο Command Prompt:

```
ipconfig /displaydns
```

Σε κάθε καταχώρηση φαίνεται ο εναπομένον χρόνος ζωής (Time to Live - TTL) σε δευτερόλεπτα. Για να αδειάσετε την cache, εισάγετε

```
ipconfig /flushdns
```

στο Command Prompt. Με την εντολή αυτή διαγράφονται όλες οι καταχωρήσεις της DNS cache και ξαναφορτώνονται οι καταχωρήσεις από το αρχείο hosts του τερματικού συστήματος.

3. Παρακολούθηση του DNS με το Wireshark

Μετά την εξοικείωση με το *nslookup* και το *ipconfig*, θα χρησιμοποιήσουμε το Wireshark για να συλλάβουμε τα πακέτα DNS που δημιουργούνται κατά τη συνηθισμένη δραστηριότητα πλοήγησης του Παγκόσμιου Ιστού.

- Χρησιμοποιήστε το *ipconfig* για να αδειάσετε την DNS cache του host σας.
- Ανοίξτε το web browser σας και αδειάστε την cache του. (Στην περίπτωση του Internet Explorer, πηγαίνετε στο μενού Tools και επιλέγετε Internet Options, στη συνέχεια επιλέγετε Delete Files στην καρτέλα General.)
- Ανοίξτε το Wireshark και εισάγετε “ip.addr == διεύθυνση_IP_host” στο φίλτρο. Χρησιμοποιήστε το *ipconfig* για να βρείτε τη διεύθυνση IP του host σας (διεύθυνση_IP_host). Το φίλτρο αυτό απομακρύνει όλα τα πακέτα που δεν προέρχονται από ούτε προορίζονται για τον host σας.
- Ξεκινήστε τη σύλληψη πακέτων από το Wireshark.
- Με τη βοήθεια του browser, επισκεφθείτε την ιστοσελίδα: <http://www.ietf.org>
- Σταματήστε τη σύλληψη πακέτων.

Εάν δεν είστε σε θέση να τρέξετε το Wireshark σε μία ζωντανή σύνδεση δικτύου, μπορείτε να φορτώσετε ένα trace πακέτων το οποίο δημιουργήθηκε ακολουθώντας τα παραπάνω βήματα¹.

Απαντήστε στις ακόλουθες ερωτήσεις:

4. Εντοπίστε τα μηνύματα ερωτημάτων (query) και αποκρίσεων (response) του DNS. Ποιο πρωτόκολλο μεταφοράς χρησιμοποιείται για τη μεταφορά τους, UDP ή TCP;
5. Ποια η θύρα προορισμού (destination port) του μηνύματος ερωτήματος; Ποια η θύρα πηγής (source port) του μηνύματος απόκρισης;
6. Σε ποια διεύθυνση IP στάλθηκε το μήνυμα ερωτήματος; Χρησιμοποιήστε το *ipconfig* για να προσδιορίσετε τη διεύθυνση IP του τοπικού σας DNS server. Τι σχέση έχουν μεταξύ τους οι δύο διευθύνσεις IP;
7. Εξετάστε το μήνυμα ερωτήματος. Ποιο το “είδος” (“Type”) του ερωτήματος; Περιέχονται “απαντήσεις” (“answers”) στο μήνυμα ερωτήματος;
8. Εξετάστε το μήνυμα απόκρισης. Πόσες “απαντήσεις” περιέχονται στο μήνυμα αυτό; Τι περιέχει καθεμία από τις απαντήσεις αυτές;
9. Θεωρείστε το επακόλουθο πακέτο SYN (SYN packet ή SYN segment) που στέλνει το TCP που τρέχει στον host σας. Η διεύθυνση προορισμού αυτού του πακέτου αντιστοιχεί σε καμία από τις διευθύνσεις IP που παρέχονται στο μήνυμα απόκρισης του DNS;

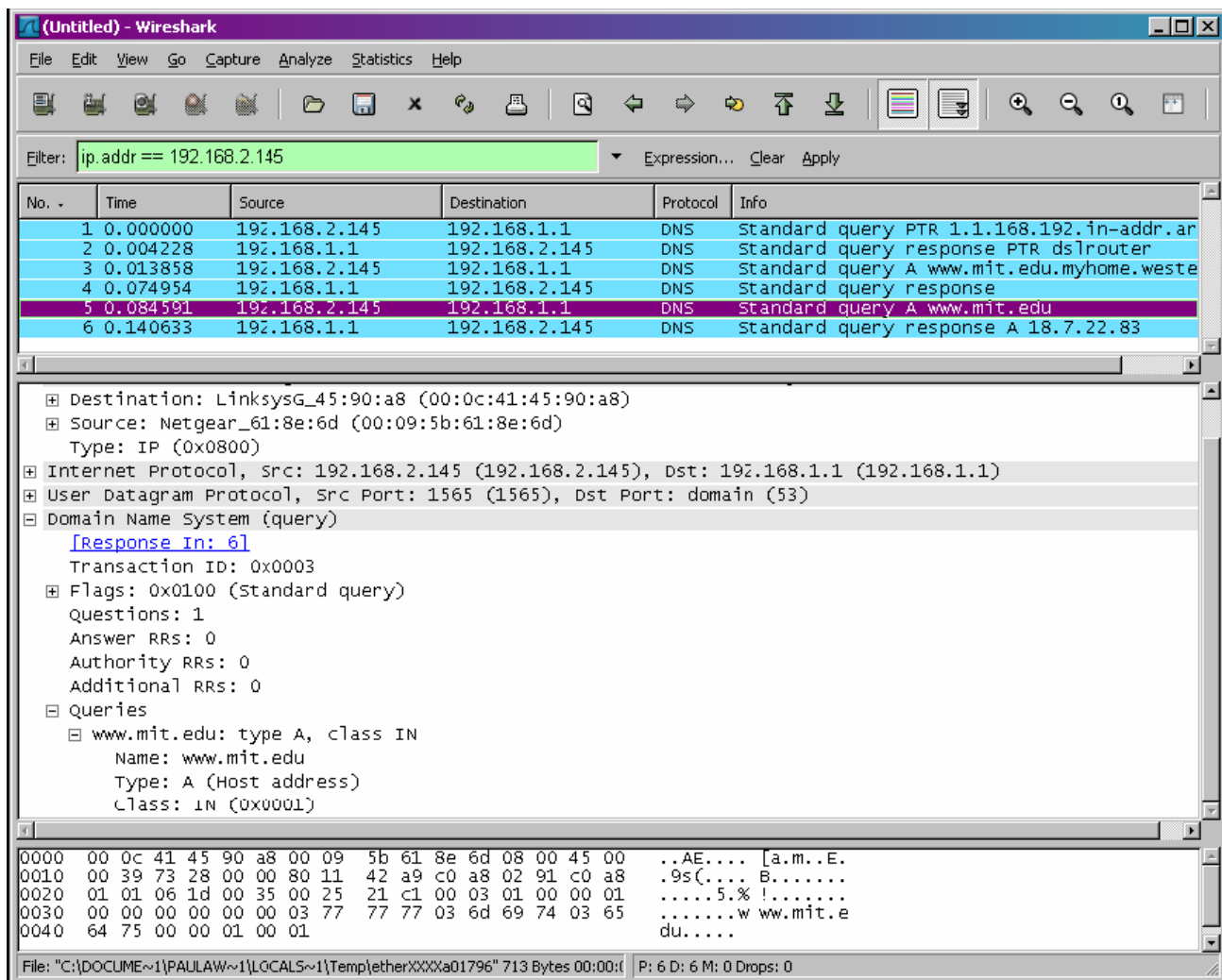
¹ Φορτώστε το αρχείο zip <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> και εξάγετε το αρχείο dns-ethereal-trace-1. Τα traces που περιέχονται σε αυτό το αρχείο zip συλλέχθηκαν από το Wireshark ενώ εκτελούνταν τα βήματα που περιγράφονται στο εργαστήριο Wireshark για το DNS στον υπολογιστή του συγγραφέα. Αφού λάβετε το trace, μπορείτε να το φορτώσετε στο Wireshark και να το δείτε στο παράθυρο χρησιμοποιώντας το μενού *File*, επιλέγοντας *Open* και στη συνέχεια επιλέγοντας το αρχείο dns-ethereal-trace-1 του trace.

10. Η ιστοσελίδα <http://www.ietf.org> περιέχει εικόνες. Χρειάζεται ο host σας να στείλει νέα ερωτήματα DNS πριν από την ανάκτηση κάθε εικόνας;

Ας ασχοληθούμε τώρα με το *nslookup*².

- Ξεκινήστε τη σύλληψη πακέτων.
- Τρέξτε το *nslookup* για το όνομα host *www.mit.edu*.
- Σταματήστε τη σύλληψη πακέτων.

Η ακολουθία των πακέτων (trace) που απεικονίζεται στο Wireshark θα πρέπει να μοιάζει με αυτήν που φαίνεται στο παρακάτω screenshot.



Όπως φαίνεται, το *nslookup* έστειλε στην πραγματικότητα τρία ερωτήματα DNS και έλαβε, αντίστοιχα, τρεις αποκρίσεις. Για να απαντήσετε στις παρακάτω ερωτήσεις αγνοήστε τα δύο πρώτα ζεύγη ερωτημάτων/αποκρίσεων καθώς αφορούν το *nslookup* και κατά κανόνα δεν δημιουργούνται

² Εάν δεν είστε σε θέση να τρέξετε το Wireshark, μπορείτε να χρησιμοποιήσετε το trace πακέτων *dns-ethereal-trace-2*

από συνήθεις Διαδικτυακές εφαρμογές. Επικεντρωθείτε, λοιπόν, στο τελευταίο ερώτημα και την τελευταία απόκριση DNS.

11. Ποια η θύρα προορισμού (destination port) του μηνύματος ερωτήματος; Ποια η θύρα πηγής (source port) του μηνύματος απόκρισης;
12. Σε ποια διεύθυνση IP στάλθηκε το μήνυμα ερωτήματος; Πρόκειται για τη διεύθυνση IP του τοπικού σας DNS server;
13. Εξετάστε το μήνυμα ερωτήματος. Ποιο το “είδος” (“Type”) του ερωτήματος; Περιέχονται “απαντήσεις” (“answers”) στο μήνυμα ερωτήματος;
14. Εξετάστε το μήνυμα απόκρισης. Πόσες “απαντήσεις” περιέχονται στο μήνυμα αυτό; Τι περιέχει καθεμία από τις απαντήσεις αυτές;
15. Παρέχετε ένα screenshot.

Επαναλάβετε το προηγούμενο πείραμα για την εντολή:

```
nslookup -type=NS mit.edu
```

Απαντήστε στις παρακάτω ερωτήσεις³:

16. Σε ποια διεύθυνση IP στάλθηκε το μήνυμα ερωτήματος; Πρόκειται για τη διεύθυνση IP του τοπικού σας DNS server;
17. Εξετάστε το μήνυμα ερωτήματος. Ποιο το “είδος” (“Type”) του ερωτήματος; Περιέχονται “απαντήσεις” (“answers”) στο μήνυμα ερωτήματος;
18. Εξετάστε το μήνυμα απόκρισης. Ποια ονόματα nameservers του MIT παρέχονται στο μήνυμα απόκρισης; Στο μήνυμα απόκρισης παρέχονται και οι διευθύνσεις IP των nameservers του MIT;
19. Παρέχετε ένα screenshot.

Επαναλάβετε το προηγούμενο πείραμα για την εντολή:

```
nslookup www.aiit.or.kr διεύθυνση_ip _του_bitsy.mit.edu
```

Απαντήστε στις ακόλουθες ερωτήσεις⁴:

20. Σε ποια διεύθυνση IP στάλθηκε το μήνυμα ερωτήματος; Πρόκειται για τη διεύθυνση IP του τοπικού σας DNS server; Εάν όχι, σε τι αντιστοιχεί η συγκεκριμένη διεύθυνση IP;
21. Εξετάστε το μήνυμα ερωτήματος. Ποιο το “είδος” (“Type”) του ερωτήματος; Περιέχονται “απαντήσεις” (“answers”) στο μήνυμα ερωτήματος;
22. Εξετάστε το μήνυμα απόκρισης. Πόσες “απαντήσεις” περιέχονται στο μήνυμα αυτό; Τι περιέχει καθεμία από τις απαντήσεις αυτές;
23. Παρέχετε ένα screenshot.
24. Εάν εκτελέσετε την εντολή `nslookup www.aiit.or.kr` αφού αδειάσετε την DNS cache, θα περάσετε από τους ίδιους nameservers για να λάβετε την απάντηση;

³ Εάν δεν είστε σε θέση να τρέξετε το Wireshark, μπορείτε να χρησιμοποιήσετε το trace πακέτων dns-ethereal-trace-3

⁴ Εάν δεν είστε σε θέση να τρέξετε το Wireshark, μπορείτε να χρησιμοποιήσετε το trace πακέτων dns-ethereal-trace-4