ΕΝΟΤΗΤΑ ΙΙ

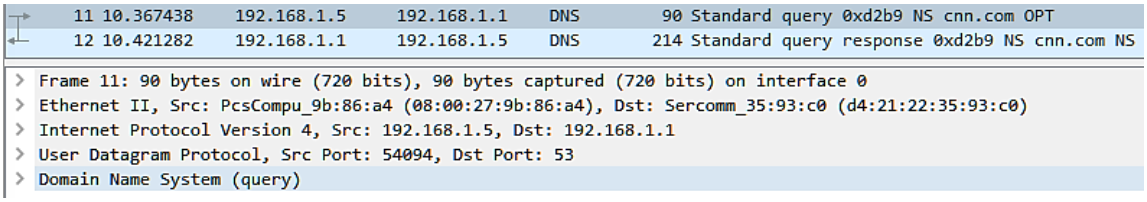
3. ΚΑΤΑΝΟΗΣΗ PROTOCOL DATA UNITS (PDUs) ΜΕΣΑ ΑΠΟ ΤΟ ΠΡΩΤΟΚΟΛΛΟ DNS

Παρακάτω θα αναλύσουμε ερωτήματα και αποκρίσεις του πρωτοκόλλου DNS το οποίο ανήκει στο 5ο επίπεδο εφαρμογής (application). Θα κατανοήσουμε πως τα **δεδομένα (data)** που αποτελούν το PDU στο L5, μεταφέρονται σε **τμήματα (segments)** στο L4 (μεταφοράς - transport), τα οποία εγκιβωτίζονται σε **πακέτα IPv4** (IPv4 packet encapsulation) στο L3 (δικτύου - network), τα οποία με την σειρά τους εγκιβωτίζονται μέσα σε **πλαίσια (frames)** που είναι το PDU στο L2 (ζεύξης – data link). Για την καλύτερη κατανόηση των PDUs θα σας βοηθήσει να έχετε διαθέσιμη μπροστά σας την εικόνα 1.11 από το κεφάλαιο 1, όπου υπάρχουν τα επίπεδα και τα αντίστοιχα PDU του TCP Protocol Stack.

3.1 Ανάλυση καταγεγραμμένης επικοινωνίας DNS

3.1.1 Εργασία με αποθηκευμένο αρχείο καταγραφής

Κατεβάστε το αρχείο **dns_capture.pcapng** από τον ιστότοπο του μαθήματος, ξεκινήστε το Wireshark και αντί για καταγραφή ανοίξτε το αρχείο που μόλις κατεβάσατε από το μενού File -> Open. Περιορίστε την εμφάνιση στις γραμμές που υπάρχει στην στήλη protocol το DNS, χρησιμοποιώντας το κατάλληλο φίλτρο. Για να μελετήσετε τις δυνατότητες των φίλτρων στο Wireshark μπορείτε να ξεκινήσετε από την σελίδα https://wiki.wireshark.org/DisplayFilters Εκεί υπάρχουν παραδείγματα, μέσα στα οποία υπάρχει και το DNS.



Εικόνα 3.1: Καταγεγραμμένο ζεύγος ερωτήματος και απόκρισης DNS

Στο πρώτο (επάνω) panel πρέπει να εμφανίζονται μόνο οι γραμμές που σας ενδιαφέρουν και μέσα σε αυτές επιλέξτε μια που το περιεχόμενο στην στήλη Info ξεκινάει από “Standard query…”. Κατόπιν εστιάστε στο δεύτερο (μεσαίο) panel του Wireshark. Στην δεύτερη γραμμή εμφανίζεται το πλαίσιο (frame) του πρωτοκόλλου 2ου επιπέδου (Data Link) στο οποίο ενθυλακώνεται ένα πακέτο (packet) του πρωτοκόλλου του 3ου επιπέδου (Network). Το δεύτερο εμφανίζεται στην αμέσως επόμενη γραμμή (τρίτη), και με την σειρά του ενθυλακώνει ένα τμήμα (segment) του πρωτοκόλλου του 4ου επιπέδου (Transport) το οποίο εμφανίζεται στην τέταρτη γραμμή. Στο segment ενθυλακώνεται ένα μήνυμα του πρωτοκόλλου του 5ου επιπέδου (Application), που στην περίπτωση μας είναι DNS και εμφανίζεται στην πέμπτη γραμμή.

Άσκηση 3.1:

Εφαρμόστε φίλτρα πάνω στην αποθηκευμένη καταγραφή ώστε:

1. Να εμφανιστούν μόνο οι γραμμές στο πάνω πάνελ που αφορούν το πρωτόκολλο DNS
2. Το φίλτρο που εφαρμόσατε στο Wireshark με το περιεχόμενο ποιας στήλης ταιριάζει;
3. Να φιλτράρετε περαιτέρω τις γραμμές ώστε να εμφανίζονται αυτές που αφορούν το DNS αλλά έχουν διεύθυνση source 192.168.1.5

Άσκηση 3.2:

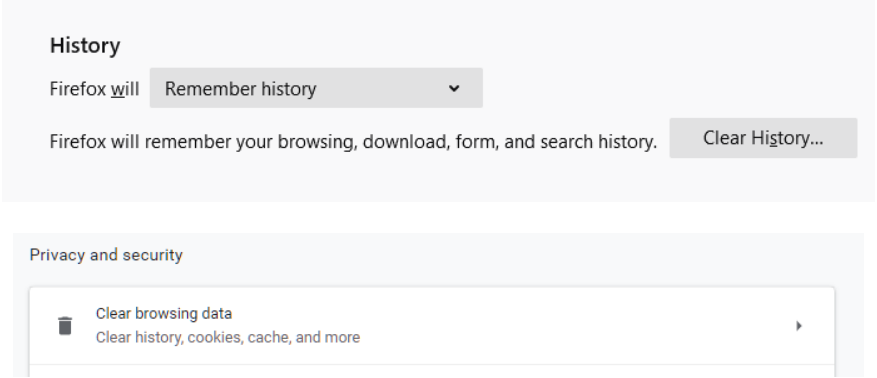
Εργαστείτε πάνω στην καταγραφή ώστε να είστε σε θέση να απαντήσετε τα παρακάτω ερωτήματα. Μπορείτε να αναπτύξετε την κάθε γραμμή στο δεύτερο (μεσαίο) panel και να δείτε δομημένη πληροφορία για ένα PDU που είναι γνωστό στο Wireshark.

1. Το μήνυμα που στέλνει ένας DNS client (πελάτης) σε έναν DNS server (εξυπηρετητή) ονομάζεται DNS query (ερώτημα) και στο Wireshark υπάρχει στο Info ως **"Standard query {ένας δεκαεξαδικός αριθμός} …".** Εμφανίστε και καταγράψτε τα πεδία του δεύτερου DNS query.
2. Στην συγκεκριμένη γραμμή καταγραφής και για κάθε επίπεδο του μοντέλου πρωτοκόλλων του TCP/IP, καταγράψτε τα πρωτόκολλα που πήραν μέρος στην επικοινωνία με τον DNS server.
3. Καταγράψτε την τοπική (local) και την απομακρυσμένη (remote) IP διεύθυνση της επικοινωνίας, σκεπτόμενοι ότι το query αποστέλλεται από τον υπολογιστή μας.
4. Καταγράψτε τα port προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν για το DNS query που εστάλη στον DNS server.
5. Με βάση τα δύο παραπάνω (3 και 4) σημειώστε το socket από το οποίο απέστειλε τα segments η τοπική διεργασία στον υπολογιστή μας και το socket που τα παρέλαβε η απομακρυσμένη διεργασία του DNS server.
6. Ποιο είναι το πρωτόκολλο με το οποίο μεταφέρονται τα δεδομένα του πρωτόκολλου επιπέδου εφαρμογής DNS; Δηλαδή ποιο είναι το πρωτόκολλο επιπέδου μεταφοράς;
7. Σε ποιο προκαθορισμένο αριθμό port αναμένει queries ένας DNS server;
8. Εντοπίστε το κείμενο της ερώτησης που γίνεται προς τον DNS server, μέσω του συγκεκριμένου query που αναλύουμε.
9. Το μήνυμα που επιστρέφει ένας DNS server σε έναν DNS client ονομάζεται DNS response (απόκριση) και στο Wireshark υπάρχει στο info ως **"Standard query response {ένας δεκαεξαδικός αριθμός} …"**. Εντοπίστε την γραμμή στο πρώτο πάνελ για το αντίστοιχο response στο request που έχουμε ήδη αναλύσει.
10. Καταγράψτε τα socket προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν για την μεταφορά της απόκρισης από τον DNS server προς τον DNS client.
11. Εμφανίστε και καταγράψτε τα πεδία του DNS response. Μέσα σε αυτά μπορείτε να βρείτε ποιοι είναι οι δηλωμένοι nameservers οι οποίοι περιέχουν τις εγγραφές για το domain που υπάρχει στο request;
12. Μπορείτε να βρείτε που βρίσκεται και ποια είναι η τιμή στο δεκαεξαδικό άθροισμα ελέγχου (checksum) για την ερώτηση και για την απάντηση;
13. Για ποιο λόγο χρειαζόμαστε ένα checksum; Η απάντηση συνδέεται με το πρωτόκολλο και το επίπεδο στο οποίο θα το βρείτε.

3.1.2 Καταγραφή επικοινωνίας DNS που συμβαίνει στο παρασκήνιο και η κρυφή μνήμη (DNS).

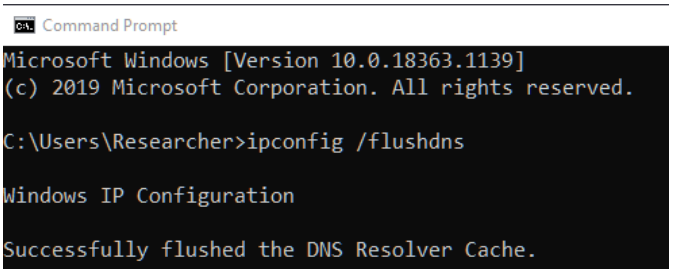
Μπορούμε να αναλύσουμε ερωτήματα DNS που λαμβάνουν χωρά στο παρασκήνιο από τις διαδικτυακές εφαρμογές που χρησιμοποιούμε. Παρακάτω θα δούμε το αρχικό στάδιο για το κατέβασμα μια ιστοσελίδας κατά το οποίο πρέπει να βρεθεί η διεύθυνση IPv4. Σε επόμενα βήματα σε συνδυασμό με την αντίστοιχη θύρα, το απομακρυσμένο socket χρησιμοποιείται για να μεταφέρει τα δεδομένα του επιπέδου παρουσίασης όπως HTML, CSS, εικόνες, κ.α. από τον εξυπηρετητή Web.

Κλείστε εντελώς όλα τα παράθυρα του browser που χρησιμοποιείτε. Κατόπιν εκκινήστε τον browser και ανοίξτε μια νέα καρτέλα ιδιωτικής περιήγησης (Firefox: Private Window, Chrome: Incognito Window). Αυτό γίνεται ώστε να μπορείτε να επαναλάβετε την διαδικασία, καθώς οι browsers θα επιστρέψουν μια σελίδα που έχετε επισκεφτεί από την τοπική κρυφή μνήμη (browser cache) που συντηρείται στον δίσκο σας. Εναλλακτικά αν δεν καταγράψετε δεδομένα, πρέπει να εκκαθαρίσετε την browser cache με τον αντίστοιχο χειρισμό.



Εικόνα 3.2: Εκκαθάριση ιστορικού από τις ρυθμίσεις Firefox (επάνω) και Chrome κάτω.

Εκτός αυτού τα λειτουργικά συστήματα έχουν και κρυφή μνήμη για αιτήματα και αποκρίσεις DNS, την DNS cache. Πρέπει να την καθαρίσετε για να εκτελεστεί ξανά το ίδιο ερώτημα DNS. Στα Windows εκτελούμε από την γραμμή εντολών `ipconfig /flushdns` και στο Linux την `sudo system-resolve –flush-caches` για εκκαθάριση και κατόπιν για επιβεβαίωση `sudo systemd-resolve –statistics`.



Εικόνα 3.3: Εκκαθάριση της dns cache σε Windows.

Άσκηση 3.3: Διαδικασία DNS resolution (αποσαφήνισης) κατά την λειτουργία του web browser: (1/2) - DNS Query

Ξεκινήστε μια νέα καταγραφή με το Wireshark. Γράψτε στη γραμμή URL **www.google.com** και αφού εμφανιστεί η σελίδα σταματήστε την καταγραφή του Wireshark. Εφαρμόστε το κατάλληλο φίλτρο για να βλέπετε μόνο τις γραμμές DNS. Αν δεν εμφανιστούν μετά την εφαρμογή του φίλτρου, είναι επειδή βρέθηκε σε κάποιες από τις cache. Αναλύστε την καταγραφή:

1. Καταγράψτε την IPv4 διεύθυνση και τη φυσική διεύθυνση (MAC address) του υπολογιστή σας από το πρώτο DNS query που υπάρχει.
2. Καταγράψτε την IPv4 διεύθυνση και την φυσική διεύθυνση (MAC address) του DNS server που διεκπεραίωσε το αίτημα σας.
3. Τρέξτε την εντολή `ipconfig /all` και βρείτε την διεύθυνση IP από το 2 μέσα στις ρυθμίσεις ενός από τα NIC του συστήματος σας. Παρατηρείτε την ίδια διεύθυνση και σε κάποιο άλλο πεδίο, ιδιαίτερα αν είναι εσωτερική διεύθυνση στο δίκτυο σας;
4. Αναπτύξτε την γραμμή που εμφανίζει το πρωτόκολλο του επιπέδου μεταφοράς (transport). Για χρήση με το DNS είναι πάντα το UDP. Έχει μικρή κεφαλίδα όπως φαίνεται στις εικόνες 3.4 και 3.5

```
0000  d4 21 22 35 93 c0 08 00  27 9b 86 a4 08 00 45 00
0010  00 52 65 2a 00 00 80 11  00 00 c0 a8 01 05 c0 a8
0020  01 01 d3 4d 00 35 00 3e  83 a6 b2 85 01 20 00 01
0030  00 00 00 00 00 01 09 6b  61 73 70 65 72 73 6b 79
0040  03 63 6f 6d 00 00 02 00  01 00 00 29 10 00 00 00
0050  00 00 00 0c 00 0a 00 08  82 b0 81 9c 84 75 5b bc
```

Εικόνα 3.4: Η κεφαλίδα του UDP σε raw δεκαεξαδική μορφή, υπερφωτίζεται στο τρίτο panel (κάτω) του Wireshark εφόσον κάνουμε κλικ στην αντίστοιχη γραμμή για το πρωτόκολλο μεταφοράς.

UDP Datagram Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Length		Header and Data Checksum	

Εικόνα 3.5: Η διαμόρφωση των 64 bits της κεφαλίδας UDP με τα πεδία από-ως bit, τα οποία εμφανίζει το Wireshark προς τον χρήστη σε δομημένη μορφή.

5. Συμπληρώστε τα παρακάτω πεδία που εμφανίζονται στο Wireshark, εντοπίζοντας τα παράλληλα και στα raw bytes του τρίτου panel:

Source IP Address		Source Port	
Destination IP Address		Destination Port	
Source MAC Address			
Destination MAC Address			
Frame Size:			

Άσκηση 3.4: Διαδικασία DNS resolution (αποσαφήνισης) κατά την λειτουργία του web browser: (2/2) DNS response.

Εντοπίστε το κατάλληλο DNS response για το query που έγινε κατά την εκτέλεση της προηγούμενης άσκησης 3.3 και αφορούσε το **www.google.com** . Παρατηρείστε ότι η απάντηση είναι πάντα μεγαλύτερη από το ερώτημα που θέσατε.

1. Ποιες είναι τώρα οι φυσικές διευθύνσεις του αποστολέα και του παραλήπτη;
2. Σε ποιες συσκευές αντιστοιχούν (αντιπαραβάλετε τις πληροφορίες σε σχέση με το DNS query).
3. Τι παρατηρείτε για τις διευθύνσεις IPv4 μεταξύ αποστολέα και παραλήπτη; Ισχύει το ίδιο και για τις ports που χρησιμοποιήθηκαν ;
4. Ποια είναι πιστεύετε η χρησιμότητα του UDP ως πρωτόκολλο μεταφοράς για το DNS σε σχέση με το TCP που ονομάζει τη σουίτα των πρωτοκόλλων του Internet; Αφού προσπαθήσετε να δώσετε την απάντηση, κοιτάξτε το υπόμνημα από την θεωρία στην παράγραφο 3.1.5.

3.1.3 Χρήσιμες τεχνικές για την αποδοτικότερη χρήση του Wireshark

Capture Filter

Για να περιορίσουμε την καταγραφή μας μπορούμε να εφαρμόσουμε ένα φίλτρο καταγραφής (Capture Filter) είτε κατά την εκκίνηση του Wireshark είτε αφού έχει γίνει μια καταγραφή και πριν πατήσουμε το πλήκτρο ώστε να ξεκινήσει η επόμενη.

Εικόνα 3.6: Πεδίο Capture Filter κατά την εκκίνηση του Wireshark

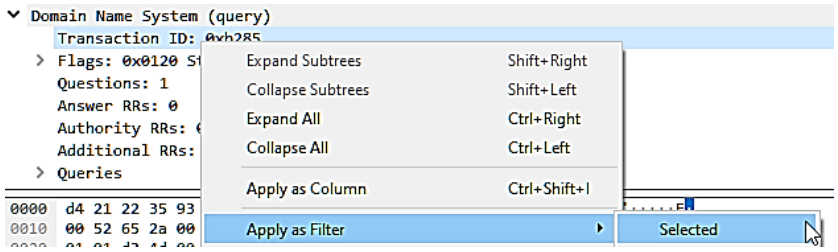
Στην δεύτερη περίπτωση επιλέγουμε το μενού Capture -> Options ώστε να εμφανιστεί το παράθυρο “Wireshark – Capture Interfaces” και γράφουμε στο πεδίο Capture filter for selected intefaces : **port 53.** Με την συγκεκριμένη επιλογή θα καταγράψει μόνο μεταφορά από την port του DNS. Ανάλογα θα μπορούσαμε να κάνουμε για οποιοδήποτε άλλο πρωτόκολλο χρησιμοποιώντας την port στην οποία λειτουργεί, από την λίστα γνωστών ports[1].

Εικόνα 3.7: Πεδίο Capture Filter από το παράθυρο Wireshark – Capture Interfaces

[1] https://www.wikiwand.com/en/List_of_TCP_and_UDP_port_numbers

Apply as Filter

Για να βρούμε το response από τον DNS server πηγαίνουμε στο μεσαίο panel αφού έχουμε επιλέξει request και επεκτείνουμε τις πληροφορίες τους επιπέδου εφαρμογής. Βρίσκουμε το πεδίο **Transaction ID** και ενώ το έχουμε επιλεγμένο κάνουμε δεξί κλικ στο ποντίκι ώστε να εμφανιστεί το context menu και από τις επιλογές διαλέγουμε **Apply as Filter** και μετά **Selected.** Αυτός ο χειρισμός μπορεί να γίνει πάνω σε οποιοδήποτε πεδίο πληροφορίας για οποιοδήποτε πρωτόκολλο αναγνωρίζει το Wireshark.



Εικόνα 3.8: Το context menu που εμφανίζεται στα πεδία πληροφοριών πρωτοκόλλου και η εφαρμογή φίλτρου από πληροφορία που εμφανίζει το Wireshark.

Μπορούμε τώρα να απομονώσουμε τις αποκρίσεις επιλέγοντας από μια απόκριση το **Flags** και κατόπιν **Apply as Filter** -> **Selected**

Apply as Column

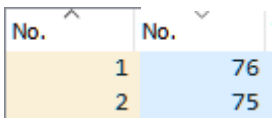
Για να καταγράψουμε τους χρόνους απόκρισης στα ερωτήματα DNS μπορούμε να επιλέξουμε μια απόκριση και να βρούμε το χρόνο στο πεδίο [Response In: {χρόνος}]. Από το context menu των πεδίων πληροφορίας μπορούμε να επιλέξουμε **Apply as Column** και έτσι να δούμε το χρόνο απόκρισης σε όλες τις απαντήσεις των queries σε μια νέα στήλη στο πρώτο panel. Αφαιρώντας τα φίλτρα οι στήλες παραμένουν και έτσι μπορούμε να δούμε όλους τους χρόνους απόκρισης στα DNS queries.

Edit Column

Μπορούμε επίσης να αλλάξουμε την εμφάνιση και τα περιεχόμενα μιας στήλης, π.χ. της Time σε ότι επιθυμούμε. Αφού τοποθετήσουμε τον δείκτη πάνω στην κεφαλίδα της στήλης και κάνουμε δεξί κλικ με το ποντίκι εμφανίζεται ένα context menu για τις στήλες όπου υπάρχει η επιλογή **Edit Column**. Εκεί στο πεδίο Title μπορείτε να δώσετε τον επιθυμητό τίτλο.

Sort Column

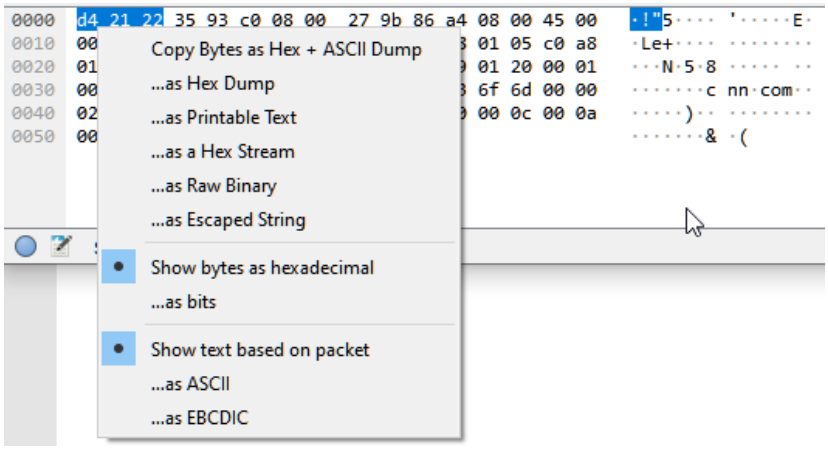
Με αριστερό κλικ πάνω στην κεφαλίδα της στήλης ταξινομείται είτε σε φθίνουσα ή αύξουσα σειρά η οποία γίνεται αντιληπτή από ένα βέλος που δείχνει προς την μικρότερη τιμή



Εικόνα 3.9: Αύξουσα και φθίνουσα ταξινόμηση στην στήλη με τον αύξων αριθμό του καταγεγραμμένου frame.

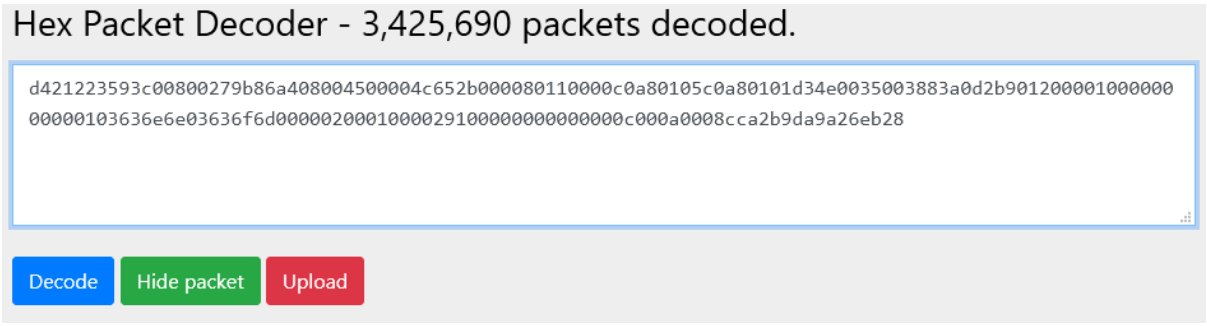
3.1.4 Ανάλυση ενός πλαισίου (frame).

Η κάθε γραμμή στο Wireshark αντιστοιχεί σε ένα πλαίσιο (frame) που διακινήθηκε από και προς το επιλεγμένο NIC στο οποίο έτρεξε η καταγραφή. Μπορούμε να αντιγράψουμε τα bytes ή octets του σε δεκαεξαδική μορφή τοποθετώντας τον δείκτη του ποντικιού πάνω στην δεκαεξαδική εμφάνιση τους στο τρίτο (κάτω) panel, δεξί κλικ για το context menu, επιλογή (**Copy) … as Hex Stream**.



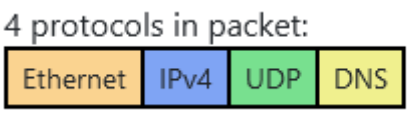
Εικόνα 3.10: Εξαγωγή καταγεγραμμένων bytes από το Wireshark.

Κατόπιν μπορούμε να επικολλήσουμε την δεκαεξαδική μορφή σε οποιοδήποτε επεξεργαστή κειμένου ώστε να την αποθηκεύσουμε σε αρχείο. Θα χρησιμοποιήσουμε το online εργαλείο ανάλυσης πλαισίου Hex Packet Decoder https://hpd.gasmi.net/ στο οποίο μπορούμε να επικολλήσουμε απευθείας ένα οποιοδήποτε string που περιέχει hex bytes.



Εικόνα 3.11: Επικόλληση δεκαεξαδικής ροής στο εργαλείο ανάλυσης πακέτων HPD v3.1

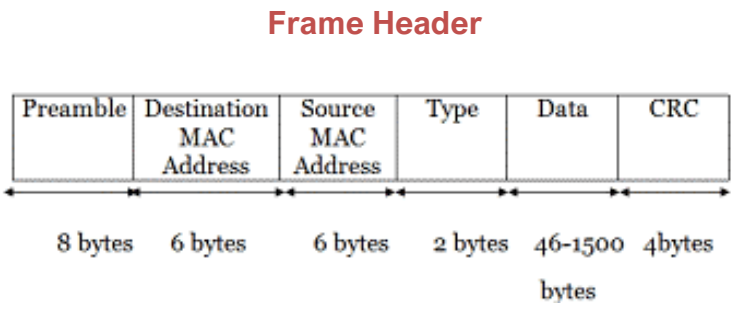
Εφόσον το string αντιστοιχεί σε ένα έγκυρο πακέτο θα εμφανίσει τον εγκιβωτισμό των PDUs στα διαφορετικά επίπεδα, χρωματίζοντας τα bytes που προστίθενται από αυτά ξεκινώντας από τα δεδομένα του επιπέδου παρουσίασης (L5) προς το επίπεδο ζεύξης (L2). Θα εμφανιστεί ένα υπόμνημα όπως το παρακάτω.



Εικόνα 1.12: Χρωματισμός που επιδεικνύει τον εγκιβωτισμό των PDUs στο Εφαρμογής (κίτρινο), Μεταφοράς (πράσινο), Δικτύου (μπλε) και Ζεύξης (πορτοκαλί).

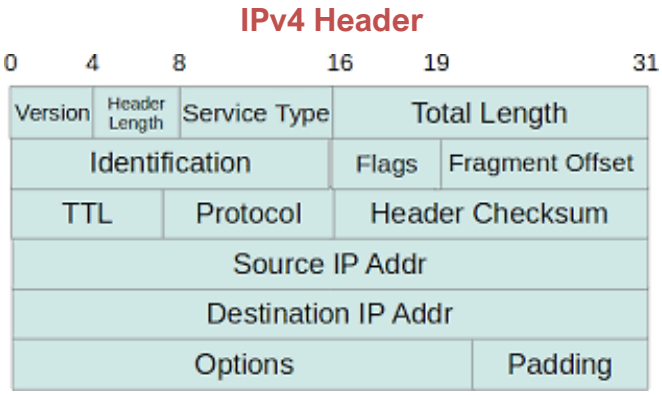
Άσκηση 3.5: Κατατόπιση στα πεδία των κεφαλίδων που υπάρχουν σε PDUs

Κατεβάστε το αρχείο **frame_example.pdf** από τον ιστότοπο του μαθήματος αντιγράψτε τα bytes στο online εργαλείο HPD. Προσπαθήστε να βρείτε την θέση των πεδίων αντίστοιχα με τις περιγραφές των κεφαλίδων των PDUs που υπάρχουν στις εικόνες 3.13, 3.14, 3.15 και 3.5 (για UDP). Κινήστε το ποντίκι πάνω στα bytes. Ποιες πληροφορίες μπορείτε να πάρετε από αυτό το εργαλείο;

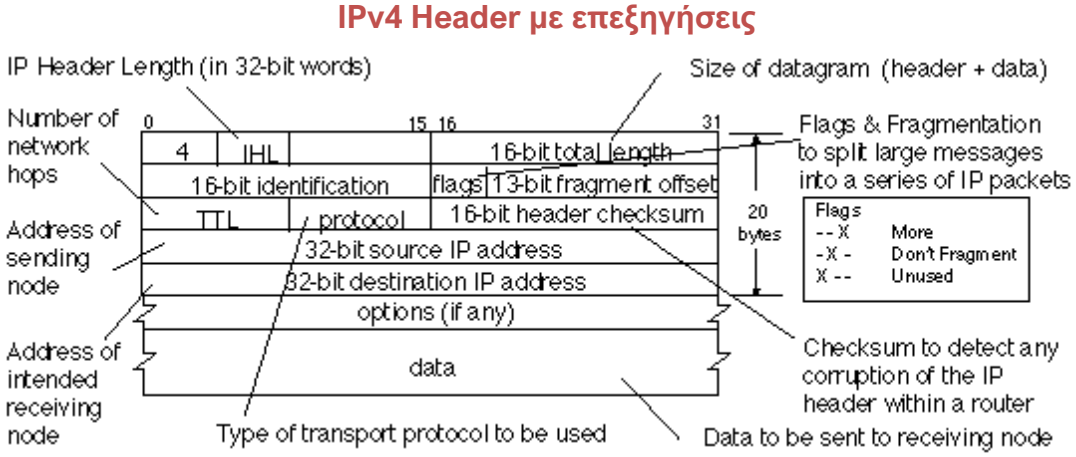


Εικόνα 3.13: Bytes σε κάθε πεδίο για πλαίσιο Ethernet.

Σημειώνεται ότι στα δεδομένα που διέρχονται από ένα NIC και καταγράφονται με χρήση λογισμικού δεν υπάρχει το Preamble και το CRC.



Εικόνα 3.14: Bytes σε κάθε πεδίο για πακέτο IPv4, με κάθε γραμμή να αντιστοιχεί σε 32 bytes.



Εικόνα 3.15: Bytes σε κάθε πεδίο για πακέτο IPv4, με επεξηγήσεις.

1. Ποιο είναι το μέγεθος των δεδομένων του επιπέδου εφαρμογής; Από ποιο πεδίο μπορούμε να το βρούμε. Υπάρχει η δυνατότητα να συνδυάσουμε και άλλο πεδίο και να βρούμε την ίδια απάντηση;
2. Θυμηθείτε τις ρυθμίσεις δικτύου στο CPT που είδατε στο κεφάλαιο 2: Μπορούμε από τις πληροφορίες που διαβάζουμε να κρίνουμε ότι είμαστε στο ίδιο υποδίκτυο; Τι χρειαζόμαστε για να είμαστε σίγουροι;
3. Γνωρίζοντας την διεύθυνση IPv4 του αποστολέα και του παραλήπτη, μπορούμε να έχουμε την πληροφορία του default gateway από την πλευρά του αποστολέα ή του παραλήπτη συνδυάζοντας πληροφορίες από το πλαίσιο που εξετάζουμε;

3.1.5 Υπόμνημα: Πρωτόκολλο UDP

Το UDP ως πρωτόκολλο μεταφοράς παρέχει γρήγορη εγκαθίδρυση της συνόδου (session) μεταφοράς, γρήγορη απόκριση, ελάχιστη επιβάρυνση σε πλήθος bytes, δεν χρειάζεται επαναπροσπάθειες (επειδή θεωρούμε αισιόδοξα ότι θα μεταφερθεί χωρίς προβλήματα), δεν υπάρχει επανασυναρμολόγηση (επειδή δεν γίνεται κατακερματισμός) και δεν απαιτεί παραλαβή μιας επιβεβαίωσης λήψης (acknowledgement).

4. ΚΑΤΑΝΟΗΣΗ ΤΗΣ ΜΕΤΑΦΟΡΑΣ ΜΕ TCP ΜΕΣΑ ΑΠΟ ΤΟ ΠΡΩΤΟΚΟΛΛΟ HTTP.