Προγραμματισμός και **Συστήματα στον Παγκόσμιο Ιστό**

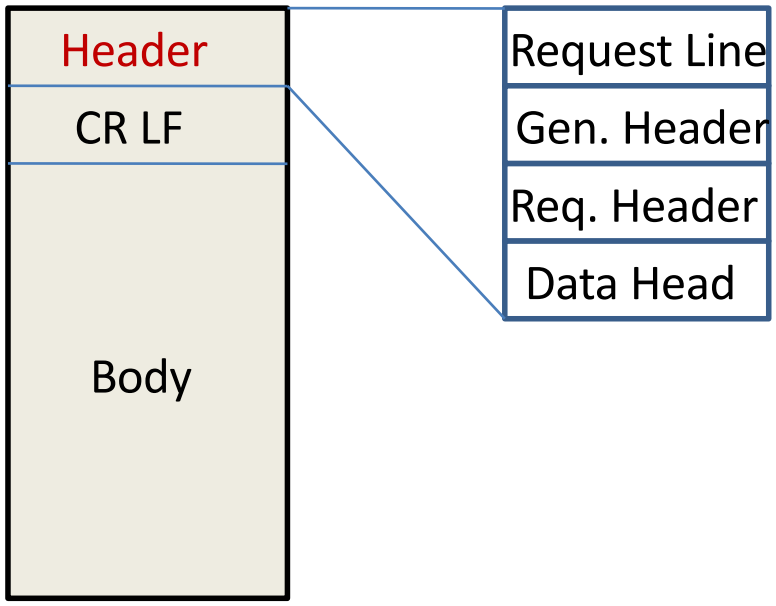
Κεφάλαιο 3:
HTTP Υποστήριξη για Κρυφές Μνήμες και Αντίγραφα

HTTP Γενικά

- Πρωτόκολλο **αίτησης-απάντησης** (request-reply).
- HTTP μήνυμα:
  - HTTP αίτηση ενός πελάτη
  - HTTP απάντηση ενός εξυπηρέτη
- HTTP κεφαλίδα / σώμα (header / body).

HTTP Γενικά

- **HTTP Request:** Header/body
  - Body = δεδομένα που ανεβαίνουν στον εξυπηρέτη
- Request line:
  - τί θα κάνει ο εξυπηρέτης
- General headers:
  - για αιτήσεις και απαντήσεις
  - Ζεύγη <κλειδολέξη, τιμή>



- Request headers:
  - χαρακτηριστικά πελάτη, username/passwd,
  - Ελέγχει caching ...

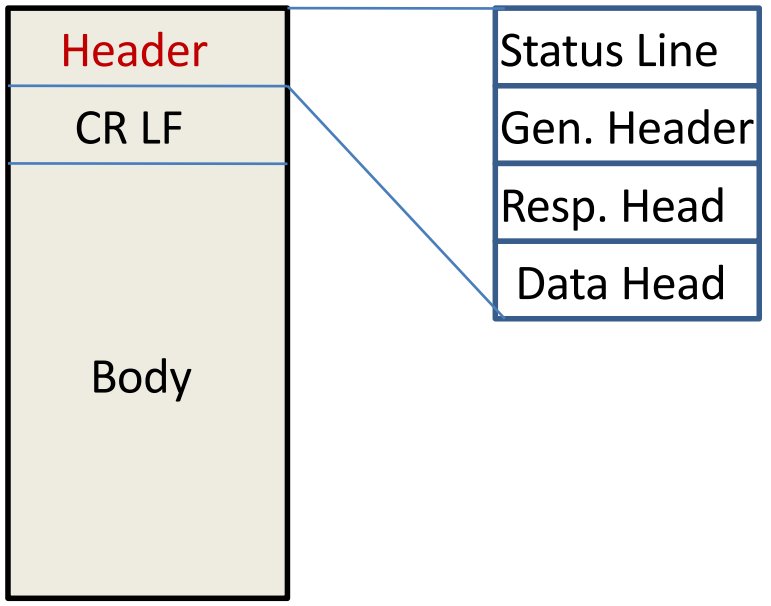
HTTP Γενικά

- Request line: ποιά μέθοδος του εξυπηρέτη καλείται, το μονοπάτι στο URL, και η έκδοση του HTTP.
  - "GET/index.html HTTP/1.1"
  - Προσέξτε το index.html είναι 'σχετικό' όνομα.
  - GET, HEAD, OPTIONS, POST, PUT, DELETE, TRACE
- Ασφαλείς: GET, HEAD, OPTIONS, TRACE
  - Αυτοδύναμες (idempotent)
- POST, PUT: για μεταφορά δεδομένων (φόρμες) και δημιουργία νέων αντικειμένων, αντίστοιχα.

  - http://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html

HTTP Γενικά

- **HTTP Response:**
- Status line: κωδικός
  - Επιτυχία,
  - σφάλμα πελάτη:
    - URL, passwd, μέθοδος, ...
  - σφάλμα εξυπηρέτη:
    - Μη διαθεσιμότητα, μέθοδος
  - αναπροώθηση αίτησης:
    - Για caching, server προβλήματα
  - “HTTP/1.1 200 OK”



- Body = δεδομένα που στέλνονται από τον εξυπηρέτη

https://www.lowendguide.com/3/webservers/http-status-codes-cheat-sheet/

GET www.ceid.upatras.gr

Request Headers view parsed

```
GET / HTTP/1.1
Host: www.ceid.upatras.gr
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: none
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en;q=0.9,en-US;q=0.8,el;q=0.7
Cookie: roundcube_134_sessid=tv1tsa4h862sfoh8urem194pg2; has_js=1; ceidwebmail_s
```

Response Headers view parsed

```
HTTP/1.1 200 OK
Date: Fri, 25 Oct 2019 10:02:21 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Powered-By: PHP/7.0.33
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: el
X-Frame-Options: SAMEORIGIN, SAMEORIGIN
Link: <https://www.ceid.upatras.gr/el/humans.txt>; type="text/plain"; rel="author",
d.upatras.gr/el>; rel="shortlink"
X-Generator: Drupal 7 (http://drupal.org)
Vary: Accept-Encoding
Content-Encoding: gzip
X-XSS-Protection: 1; mode=block
Content-Length: 16615
Keep-Alive: timeout=5, max=1000
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
```

Chrome developer tools

Get request

```
1  GET  HTTP/1.1
2  Host: www.ceid.upatras.gr
3  User-Agent: PostmanRuntime/7.18.0
4  Accept: */*
5  Cache-Control: no-cache
6  Postman-Token: b7d0dd28-a1d3-4c84-97d1-6f37ae5c1661,1f6f7998-7888-4861-8bd0
       -b87b08c95e65
7  Accept-Encoding: gzip, deflate
8  Referer: http://www.ceid.upatras.gr/
9  Connection: keep-alive
10 cache-control: no-cache
11
12
```

GET | www.ceid.upatras.gr

Params | Authorization | Headers (7)

Headers (0)

KEY	Value	Description
Key		

Temporary Headers (7)

KEY	VALUE
User-Agent	PostmanRuntime/7.18.0
Accept	*/*
Cache-Control	no-cache
Postman-Token	b7d0dd28-a1d3-4c84-97d1-6f37ae5c1661
Accept-Encoding	gzip, deflate
Referer	http://www.ceid.upatras.gr/
Connection	keep-alive

HTTP Υποστήριξη για Κρυφές Μνήμες και Αντίγραφα

- Αιτήσεις υπό συνθήκη – εξαρτώμενες αιτήσεις (**conditional requests**)
  - Έχουν συνθήκες στις κεφαλίδες μηνυμάτων
  - Εξυπηρέτης εκτελεί τέτοιες αιτήσεις μόνο εάν η συνθήκη ισχύει
  - Άλλως, απαντά με ένα κωδικό λάθους (304 not modified ή 412 precondition failed).
  - Πελάτες χρησιμοποιούν μετα-πληροφορία για να ορίσουν τις συνθήκες ...
  - Χρησιμοποιώντας συγκεκριμένες κεφαλίδες (conditional headers)

HTTP Υποστήριξη για Κρυφές Μνήμες

- Κεφαλίδες με συνθήκες:

Κλειδολέξη κεφαλίδας	Τιμή	Νόημα
If-modified-since	Last-modified-date	Εκτέλεσε αίτηση (GET) αν το ζητούμενο αντικείμενο έχει ενημερωθεί από τη Last-modified-date.
If-none-match	Etag	Εκτέλεσε αίτηση (GET) αν το Etag του ζητούμενου αντικειμένου είναι διαφορετικό.

- Το Etag (entity tag) είναι μοναδικό αναγνωριστικό (αποτύπωμα) του αντικειμένου – π.χ. Με τη χρήση της MD5 συνάρτησης κατακερματισμού.

HTTP Υποστήριξη για Κρυφές Μνήμες

- Και οι δυο κεφαλίδες χρησιμοποιούνται για να αποφευχθεί η μεταφορά του αντικειμένου από τον εξυπηρέτη στον πελάτη, στην περίπτωση που η έκδοση του αντικειμένου που έχει στην κρυφή του μνήμη ο πελάτης είναι η πλεόν ενήμερη.
  - Σε αυτήν την περίπτωση ο εξυπηρέτης απαντά με “304 not modified”
- Αντίθετα, αν τα περιεχόμενα της κρυφής μνήμης είναι «απηρχαιωμένα», τότε ο εξυπηρέτης στέλνει το αντικείμενο στον πελάτη.
- Η κεφαλίδα “If-none-match” είναι προτιμότερη, γιατί τα Last-modified-date έχουν ακρίβεια μόνο δευτερολέπτου.
  - Αν και το If-modified-since είναι πιο δημοφιλές επειδή υπήρχε στο 1ο HTTP πρωτόκολλο.
- IMS requests

HTTP Υποστήριξη για Αντίγραφα

- Εξαρτώμενες αιτήσεις χρησιμοποιούνται και για διαχείριση αντιγράφων
- Με αντίγραφα (είτε καθρέπτες, είτε ανάστροφοι αντιπρόσωποι) που χρησιμοποιούν το **HTTP.**
- Κατα τη χρήση POST, PUT, DELETE
  - Post: μερική ενημέρωση
  - Put: ολική ενημέρωση αντικειμένου
  - Συγκρουόμενες ενημερώσεις απο διαφορετικούς πελάτες σε διαφορετικά αντίγραφα
    - Δεν πρέπει να γίνουν δεκτές (→ χαμένες ενημερώσεις)
  - Διαγραφή σε έναν εξυπηρέτη δεν πρέπει να εκτελεστεί σε άλλον πιο ενημερωμένο εξυπηρέτη.
  - Απαιτείται εμπλοκή ανθρώπινου διαχειριστή...

HTTP Υποστήριξη για Αντίγραφα

- Κεφαλίδες με συνθήκες:

Κλειδολέξη κεφαλίδας	Τιμή	Νόημα
If-unmodified-since	date	Εκτέλεσε αίτηση (GET) αν το ζητούμενο αντικείμενο έχει τελευταία ενημέρωση ίση με το date.
If-match	Etag	Εκτέλεσε αίτηση (GET) αν το Etag του ζητούμενου αντικειμένου είναι το ίδιο με αυτό της αίτησης.

- Χρησιμοποιούνται για να εκτελεστούν οι ενημερώσεις ή να γίνουν διαγραφές με βάση τις συνθήκες.
- Άλλως, ο εξυπηρέτης δεν εκτελεί την αίτηση και επιστρέφει “412 precondition failed”.

HTTP Υποστήριξη για Κρυφές Μνήμες και Αντίγραφα: Ηλικία / εκπνοή

- Ηλικία (age) και εκπνοή (expiration) αντικειμένων
- Αντιπρόσωποι πρέπει να γνωρίζουν μέχρι πότε αντικείμενα στην κρυφή τους μνήμη είναι έγκυρα
- Λύση: Time-to-Live (TTL).
  - Αντικείμενα στην κρυφή μνήμη σχετίζονται με ένα TTL
  - Είναι έγκυρα μόνο για το χρόνο που ορίζεται στο TTL
  - Άλλως θεωρούνται άκυρα.
  - Μια αίτηση για ένα άκυρο αντικείμενο προκαλεί έλεγχο εγκυρότητας ενός αντικειμένου
  - → εξαρτώμενη αίτηση (GET) στον εξυπηρέτη
- Η ηλικία ορίζεται ως ο χρόνος που μεσολάβησε είτε από το χρόνο που ανακτήθηκε το αντικείμενο, είτε από τον τελευταίο επιτυχή έλεγχο εγκυρότητας.

HTTP Υποστήριξη για Κρυφές Μνήμες και Αντίγραφα: Ηλικία / εκπνοή

- Ένας **HTTP** εξυπηρέτης ορίζει TTL με τη χρήση “expires” και “max-age” κεφαλίδων.

Κλειδολέξη κεφαλίδας	Τιμή	Νόημα
expires	date	Ημερομηνία εγκυρότητας. Με την πάροδο, απαιτείται έλεγχος εγκυρότητας.
Max-age	Seconds	Μέγιστη ηλικία αντικειμένου πριν θεωρηθεί άκυρο. Με την πάροδο, απαιτείται έλεγχος εγκυρότητας.
Age	Seconds	Ηλικία αντικειμένου

HTTP Υποστήριξη για Κρυφές Μνήμες και Αντίγραφα: Ηλικία / εκπνοή

- Απόλυτο TTL: Αυτό που ορίζεται στο “expires”
- Σχετικό TTL: Αυτό που ορίζεται στο “max-age”
  - Δηλ. είναι έγκυρο για τόσο χρόνο μετά τον τελευταίο έλεγχο..
- Με σχετικά TTL ο αντιπρόσωπος πρέπει να μπορεί να προσδιορίζει την ηλικία αντικειμένων.
  - Δύσκολο όταν υπάρχει αλυσίδα αντιπροσώπων μεταξύ αυτού και του εξυπηρέτη-πηγής.
  - Ο αντιπρόσωπος που ανακτά το αντικέιμενο απευθείας από την πηγή, ενθυλακώνει μια age-κεφαλίδα στο αντικέιμενο και
  - Πριν το μεταφέρει σε άλλον αντιπρόσωπο, ενημερώνει την ηλικία με βάση την τιμή της age-κεφαλίδας και το πόσο έμεινε σε αυτόν.
  - Έτσι, ο κάθε αντιπρόσωπος σε μια αλυσίδα αντιπροσώπων μπορεί να προσδιορίσει την ηλικία αντικειμένων που προέρχονται από κρυφές μνήμες.
- Αλλά, πρέπει η πηγή να ορίσει TTL με κάθε αντικέιμενο – πράγμα που δεν ισχύει πάντα.

HTTP Υποστήριξη για Κρυφές Μνήμες και Αντίγραφα: Ανακατεύθυνση

- Ανακατεύθυνση (redirection) αιτήσεων από έναν εξυπηρέτη σε άλλον
  - Για λόγους αποτυχιών, απόδοσης, χρήσης ανιγράφων και κρυφών μνημών αντιπροσώπων
- Ένας εξυπηρέτης μπορεί
  - να ανακατευθύνει μια αίτηση σε άλλον εξυπηρέτη ή
  - Να ενημερώσει τον πελάτη για εναλλακτικούς εξυπηρέτες/αντιπρόσωπους
- HTTP εξυπηρέτες υλοποιούν τα παραπάνω μέσω απαντήσεων με ειδικούς κωδικούς ανακατεύθυνσης.

HTTP Υποστήριξη για Κρυφές Μνήμες και Αντίγραφα: Ανακατεύθυνση

Κωδικός Κατάστασης	Πληροφορίες ανακατεύθυνσης
300 multiple choices	Entity body – λίστα αυτών που μπορούν να δώσουν το αντικείμενο.
301 moved permanently	Location κεφαλίδα – νέα θέση (URL) αντικειμένου
302 found	Location κεφαλίδα
303 see other	Location κεφαλίδα – το αντικείμενο πρέπει να αναζητηθεί στο νέο URL που επιστρέφεται.
305 use proxy	Location κεφαλίδα – URL του αντιπροσώπου που έχει το αντικέιμενο.
307 temporary redirect	Location κεφαλίδα – προσωρινή νέα θέση (URL) αντικειμένου.

HTTP Υποστήριξη για Κρυφές Μνήμες και Αντίγραφα: αιτήσεις εύρους

- Συχνά, αντιπρόσωποι μπορεί να έχουν ένα υποσύνολο των επιμέρους αντικειμένων που συναπαρτίζουν ένα σύνθετο αντικείμενο
  - Πχ διακοπή κατα το κατέβασμα του αντικειμένου από την πηγή.
  - → απαιτείται μηχανισμός αίτησης μόνο του τμήματος ενός αντικειμένου που λείπει...
- Πελάτης ορίζει το εύρος των ψηφίων που λείπουν → αιτήσεις εύρους.
- Εξυπηρέτες εκτελούν την αίτηση κανονικά, αλλά επιστρέφουν μόνο τα συγκεκριμένα ψηφία.

HTTP Υποστήριξη για Κρυφές Μνήμες – Κεφαλίδες ελέγχου κρυφών μνημών

- Γενικές κεφαλίδες
- Επιτρέπουν τον έλεγχο μνημών από τον πελάτη-περιηγητή μέχρι την πηγή.
  - Και στην κρυφή μνήμη των browser
  - Και στην ΚΜ των αντιπροσώπων.
- Τα περιεχόμενα των κεφαλίδων είναι στην ουσία εντολές που δίνονται στους διαχειριστές κρυφών μνημών.
- Οι εντολές είναι αρκετά ευρείου περιεχομένου, ώστε να
  - παρέχονται εγγυήσεις σε πελάτες και εξυπηρέτες
    - σχετικά με τη φρεσκάδα
    - και την ποιότητα των αντικειμένων που ανακτώνται,
  - αλλά σεβόμενες πάντα
    - ευαίσθητα δεδομένα και
    - Πόρους του Διαδικτύου.

HTTP Υποστήριξη για Κρυφές Μνήμες – Κεφαλίδες ελέγχου κρυφών μνημών

ΚΕΦΑΛΙΔΕΣ ΣΕ HTTP ΑΙΤΗΣΕΙΣ

Κλειδολέξη εντολής	Τιμή	Εξήγηση
No-cache	None	Μη χρήση της ΚΜ για την ανάκτηση αντικειμένου.
No-store	None	Μη αποθήκευση στην ΚΜ η απάντηση στην αίτηση
Max-age	Seconds	Χρήση ΚΜ μόνο για νεώτερα αντικείμενα
Min-fresh	Seconds	Χρήση ΚΜ μόνο για αντικ. Που θα είναι έγκυρα για τόσα secs.
Max-stale	Seconds	Χρήση ΚΜ ακόμα και για άκυρα αντικ. Μ.εχρι τόσο χρόνο.
No-transform	None	Κανένας μετασχηματισμός (πχ αλλαγή διαστάσεων εικόνας).
Only-if-cached	None	Αν δεν υπάρχει το αντικ. Στην ΚΜ, μην προωθείς την αίτηση.

Κεφαλίδες ελέγχου κρυφών μνημών

ΚΕΦΑΛΙΔΕΣ ΣΕ HTTP ΑΠΑΝΤΗΣΕΙΣ

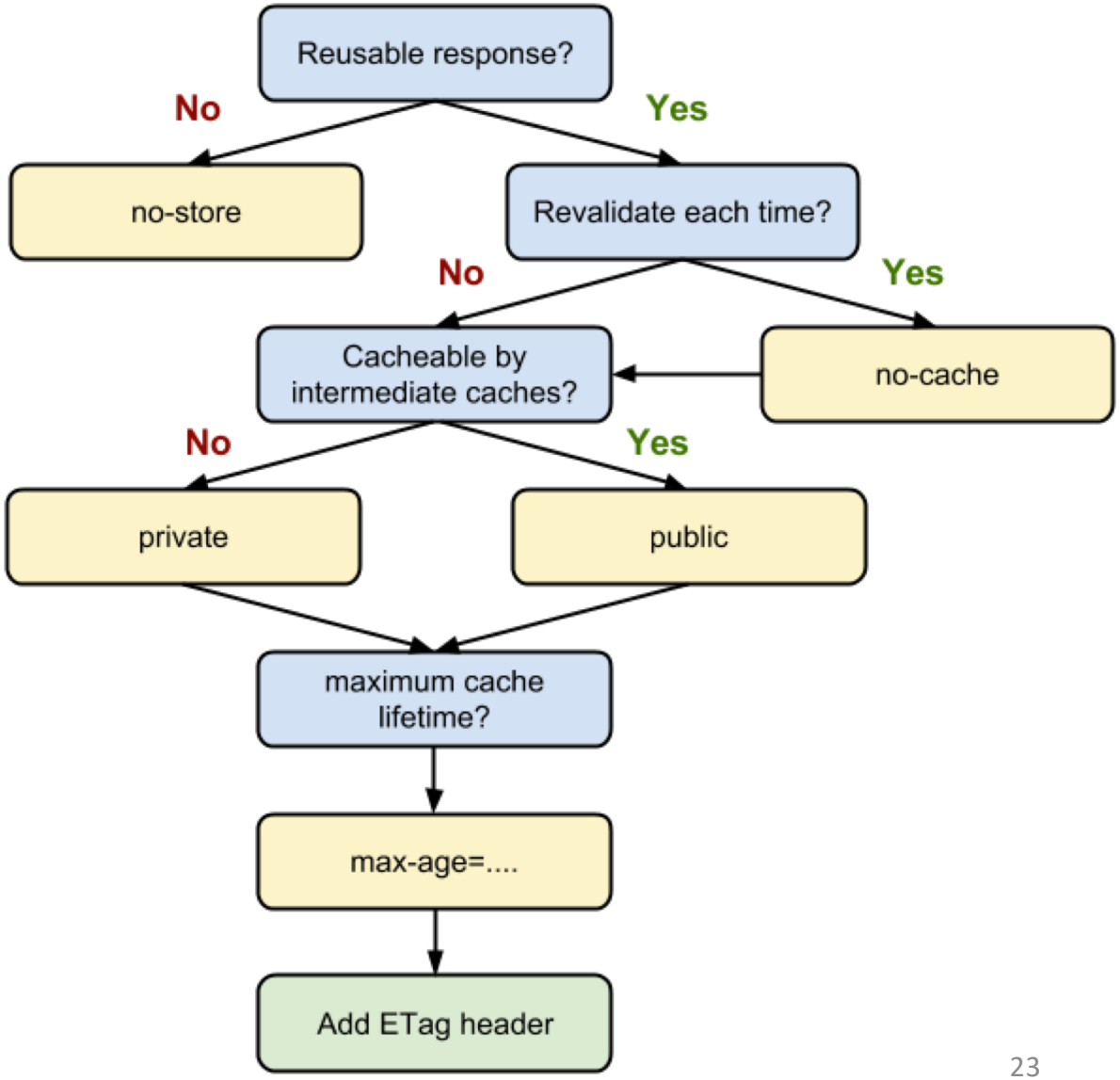
Κλειδολέξη εντολής	Τιμή	Εξήγηση
No-cache	None	Μη χρήση της ΚΜ για το αντικ.
No-store	None	Μη χρήση της ΚΜ για το αντικ. Ακόμα και για browsers.
Max-age / s-maxage	Seconds	Κάθε ΚΜ πρέπει να κάνει έλεγχο εγκυρότητας όταν η ηλικία του ανιτκ. φτάσει εκεί... / μόνο για proxies
private	none	Χρήση ΚΜ ΟΚ αλλά μόνο για τον τον ίδιο πελάτη.
public	none	Χρήση ΚΜ ΟΚ για όλους.
No-transform	None	Κανένας μετασχηματισμός (πχ αλλαγή διαστάσεων εικόνας).
Must-revalidate Proxy-revalidate	None None	Κάθε ΚΜ πρέπει να κάνει έλεγχο εγκυρότητας σε κάθε αίτηση → εξαρτώμενη GET. Μόνο για proxies.

HTTP Υποστήριξη για Κρυφές Μνήμες – Κεφαλίδες ελέγχου κρυφών μνημών

- Ο σχεδιαστής ιστότοπων (Web Designer) πρέπει να γνωρίζει τα παραπάνω
  - Δημόσιες/προσωπικές πληροφορίες (πχ δυναμικές σελίδες με ευαίσθητα δεδομένα → public/private)
  - Προσφορές σε νέους επισκέπτες → must revalidate.
  - Αν νέες προσφορές σε προιόντα αλλάζουν κάθε 2 ώρες → max-age.
- Παρομοίως και οι πελάτες: πχ
  - 3G/4G networks: →max-stale,
  - ADSL: → no-transform, max-age

Πρακτικές συμβουλές

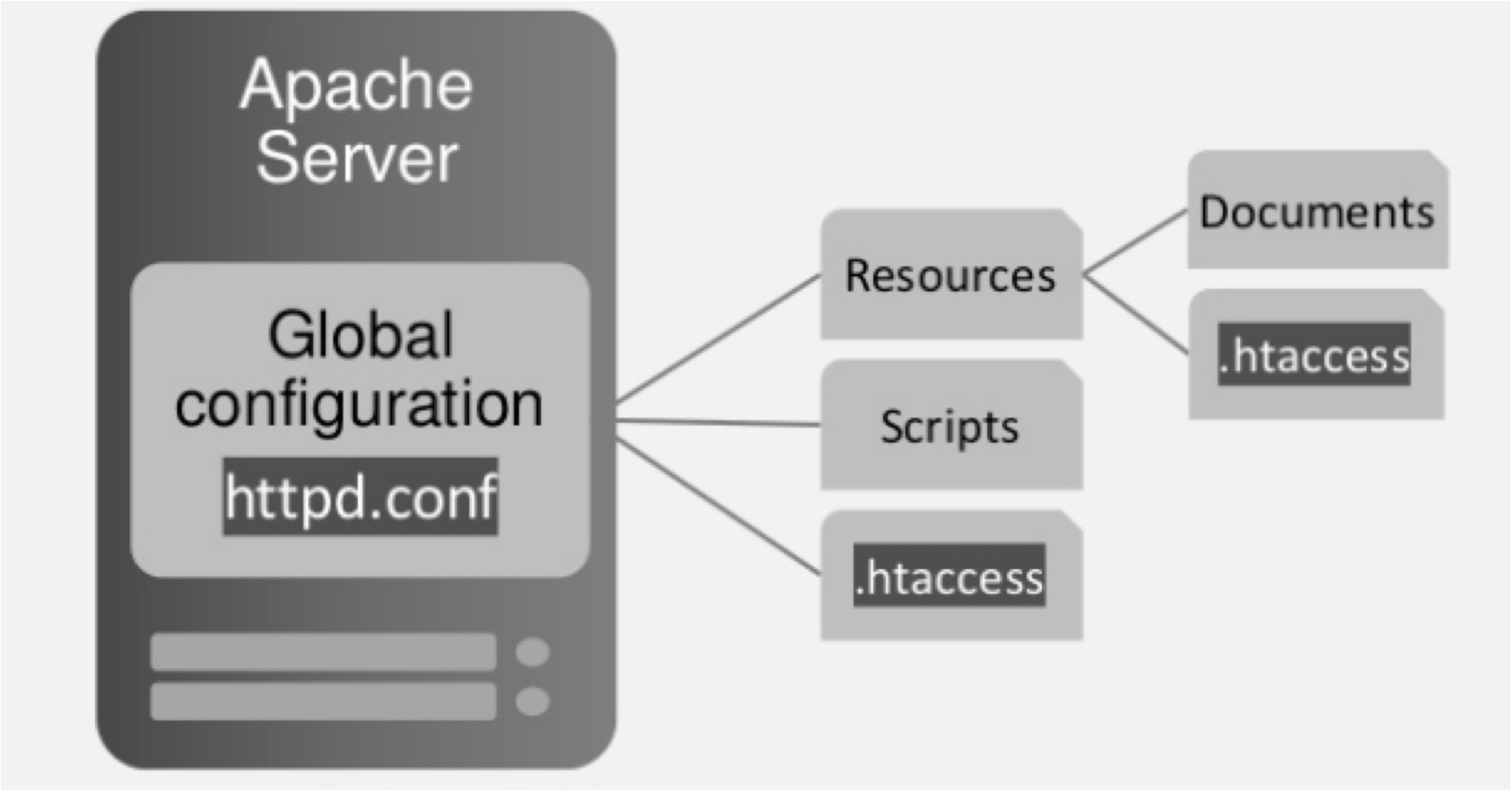
- Ιδανικά, ρυθμίζουμε τον εξυπηρέτη ώστε να χρησιμοποιείται όσο το δυνατόν περισσότερο η cache του πελάτη (ή ενδιαμέσων – proxies)
- Η διαδικασία απαιτεί χειροκίνητη επισκόπηση των πόρων που διατίθενται προς το κοινό (content audit)



Ρυθμίσεις εξυπηρέτη

- Ανά directory
  - Apache: .htaccess
  - Ειδικό αρχείο παραμετροποίησης πρόσβασης / μεταφοράς, που μπορεί να τοποθετηθεί σε κάθε (sub) directory
- Ανά ιστοσελίδα
  - PHP: συνάρτηση header
  - Ενσωμάτωση στον κώδικα που παράγει την ιστοσελίδα

.htaccess

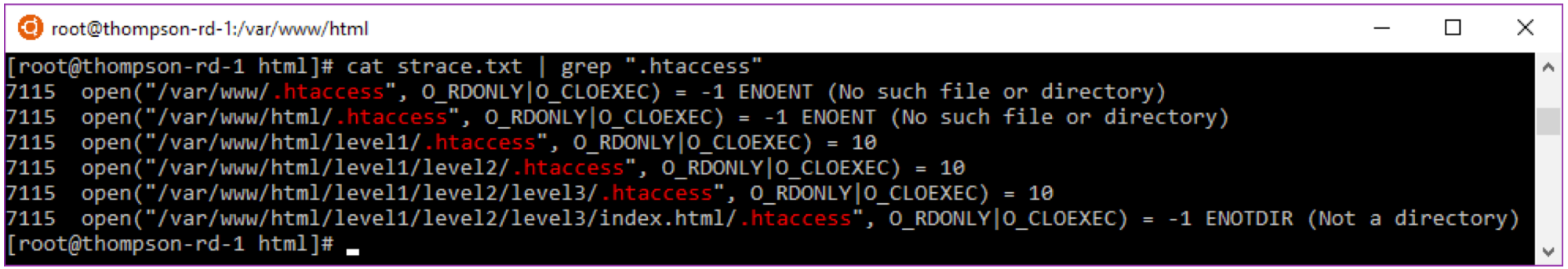

Apache
Server
Global
configuration
httpd.conf
Resources
Documents
.htaccess
Scripts
.htaccess

Ιεραρχική αποτίμηση

- Το .htaccess μπορεί να υπάρχει σε >1 τοποθεσίες στο file system

```
./.htaccess
./level1/.htaccess
./level1/level2/.htaccess
./level1/level2/level3/index.html
```

- Το parsing των κανόνων γίνεται ιεραρχικά και σειριακά
- Τοπικοί κανόνες «παρακάμπτουν» τους γενικότερους



.htaccess

Apache httpd

```
<IfModule mod_gzip.c>
mod_gzip_on Yes
mod_gzip_dechunk Yes
mod_gzip_item_include file .(html?|txt|css|js|php|pl)$
mod_gzip_item_include handler ^cgi-script$
mod_gzip_item_include mime ^text/.*
mod_gzip_item_include mime ^application/x-javascript.*
mod_gzip_item_exclude mime ^image/.*
mod_gzip_item_exclude rspheader ^Content-Encoding:.*gzip.*
</IfModule>

##Tweaks##
Header set X-Frame-Options SAMEORIGIN

## EXPIRES CACHING ##
<IfModule mod_expires.c>
ExpiresActive On
ExpiresByType image/jpg "access 1 year"
ExpiresByType image/jpeg "access 1 year"
ExpiresByType image/gif "access 1 year"
ExpiresByType image/png "access 1 year"
ExpiresByType text/css "access 1 month"
ExpiresByType text/html "access 1 month"
ExpiresByType application/pdf "access 1 month"
ExpiresByType text/x-javascript "access 1 month"
ExpiresByType application/x-shockwave-flash "access 1 month"
ExpiresByType image/x-icon "access 1 year"
ExpiresDefault "access 1 month"
</IfModule>
## EXPIRES CACHING ##

<IfModule mod_headers.c>
    Header set Connection keep-alive
    <filesmatch "\.(ico|flv|gif|swf|eot|woff|otf|ttf|svg)$">
        Header set Cache-Control "max-age=2592000, public"
    </filesmatch>
    <filesmatch "\.(jpg|jpeg|png)$">
        Header set Cache-Control "max-age=1209600, public"
    </filesmatch>
    # css and js should use private for proxy caching
    # https://developers.google.com/speed/docs/best-practices/caching#LeverageProxyCaching
    <filesmatch "\.(css)$">
        Header set Cache-Control "max-age=31536000, private"
    </filesmatch>
    <filesmatch "\.(js)$">
        Header set Cache-Control "max-age=1209600, private"
    </filesmatch>
    <filesMatch "\.(x?html?|php)$">
        Header set Cache-Control "max-age=600, private, must-revalidate"
      </filesMatch>
</IfModule>
```

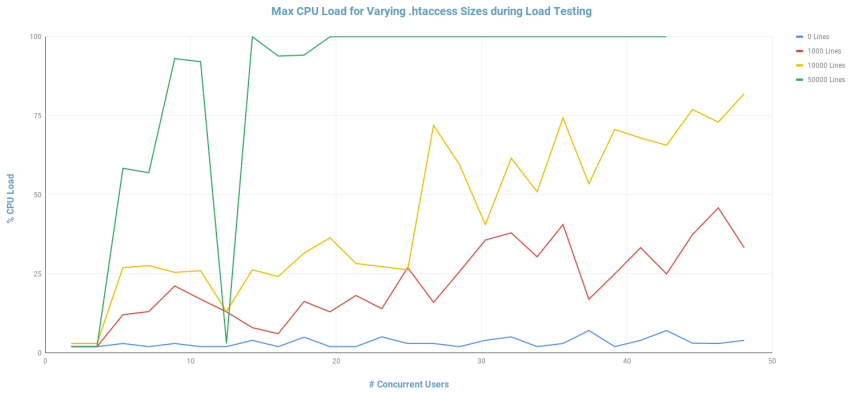
Όλα τα .jpg λήγουν 1 έτος μετά την πρόσβαση

Εύρεση αρχείων με regex

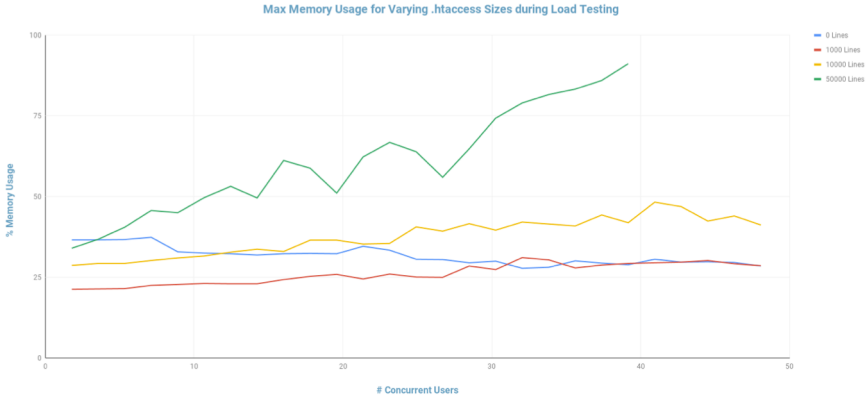
Αντικατάσταση υπάρχοντων headers με αυτόν

Επίπτωση στην απόδοση

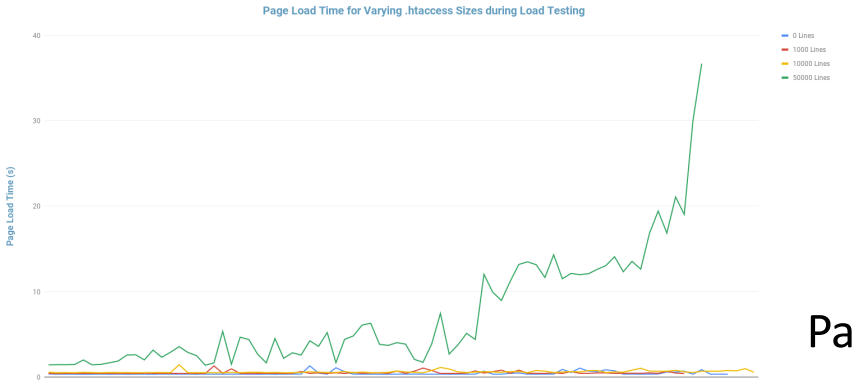
- Περισσότεροι κανόνες = μεγαλύτερη καθυστέρηση



CPU load



Memory load



Page load time

Συμβουλές

- Προσθέτουμε εντολές στο httpd.conf
- Χρήση patterns όπου είναι δυνατό (regex)
- Αν δεν είναι δυνατή η μετονομασία αρχείων ώστε να βολεύεται η κάλυψη μέσω regex, χρήση 301 (redirect) μέσω κώδικα
- Caching των 301 όπου είναι δυνατό

https://strategiq.co/does-the-number-of-htaccess-rules-impact-performance-and-scalability/

Php – header()

```php
<?php
  //set headers to NOT cache a page
  header("Cache-Control: no-cache, must-revalidate"); //HTTP 1.1
  header("Pragma: no-cache"); //HTTP 1.0
  header("Expires: Sat, 26 Jul 1997 05:00:00 GMT"); // Date in the past

  //or, if you DO want a file to cache, use:
  header("Cache-Control: max-age=2592000"); //30days (60sec * 60min * 24hours * 30days)

?>
```

Trick!

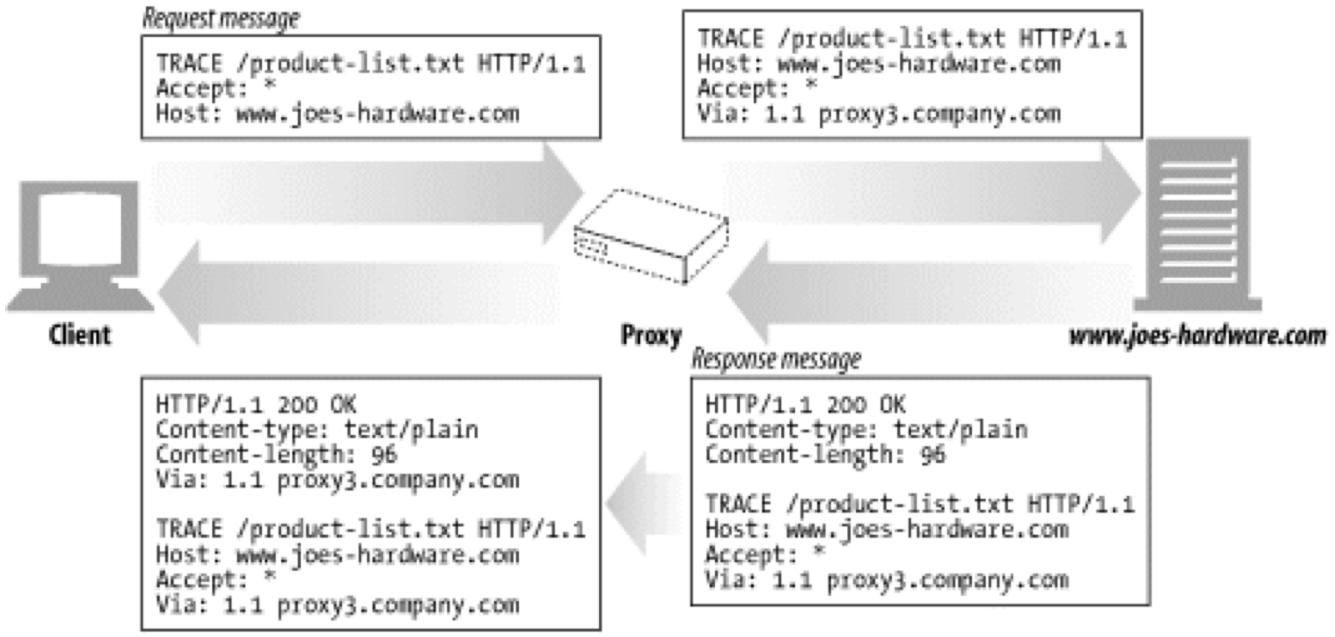
```html
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Beinn Bike</title>
    <link href="https://fonts.googleapis.com/css?family=Antic" rel="stylesheet">
    <link rel="stylesheet" type="text/css" href="main2.css<?php echo "?".time(); ?>">
    <link rel="stylesheet" type="text/css" href="defaultosm.css<?php echo "?".time(); ?>">
```

HTTP Υποστήριξη για Κρυφές Μνήμες – Αλυσίδες Αντιπροσώπων

- TRACE: επιστρέφει το request πίσω στον πελάτη
- Χρήσιμο για πελάτες να ξέρουν αν και ποιοι αντιπρόσωποι παρεμβάλλονται – πχ για να χρησιμοποιήσουν “no-cache”/ revalidate…
- HTTP υποστηρίζει αυτό μέσω κεφαλίδων «via headers» και της μεθόδου TRACE.
- Κεφαλίδες via χρησιμοποιούνται από κάθε ενδιάμεσο αντιπρόσωπο όπου προσθέτει το όνομά του και την έκδοση του πρωτοκόλλου που χρησιμοποιεί.
- Οι αιτήσεις TRACE συνήθως δεν είναι cacheable → φτάνουν στην πηγή.
- Η πηγή βλέπει στις κεφαλίδες via όλους τους ενδιάμεσους αντιπροσώπους και τους επιστρέφει στην απάντηση που στέλνει στην αίτηση TRACE του πελάτη.

TRACE

- curl -I -X TRACE <some host>



Examining the entity, the client can see that its request was upgraded to protocol Version 1.1. Along with the upgrade came a few additional request headers.

Ασφάλεια στο διαδίκτυο

- Το HTTP δεν είναι ασφαλές πρωτόκολλο
  - Απλή και stateless εφαρμογή client/server που τρέχει πάνω από το TCP/IP
- Χρειάζονται πρόσφατα μέτρα ασφάλειας
  - Θα εξετάσουμε το SSL (Secure Socket Layer) και το TLS (Transport Layer Security)
  - HTTPS
    - Ασφαλές πρωτόκολλο HTTP
- Υπάρχει υποστήριξη για SSL για πολλές εφαρμογές του TCP/IP
  - POP3, SMTP, FTP, News, ...

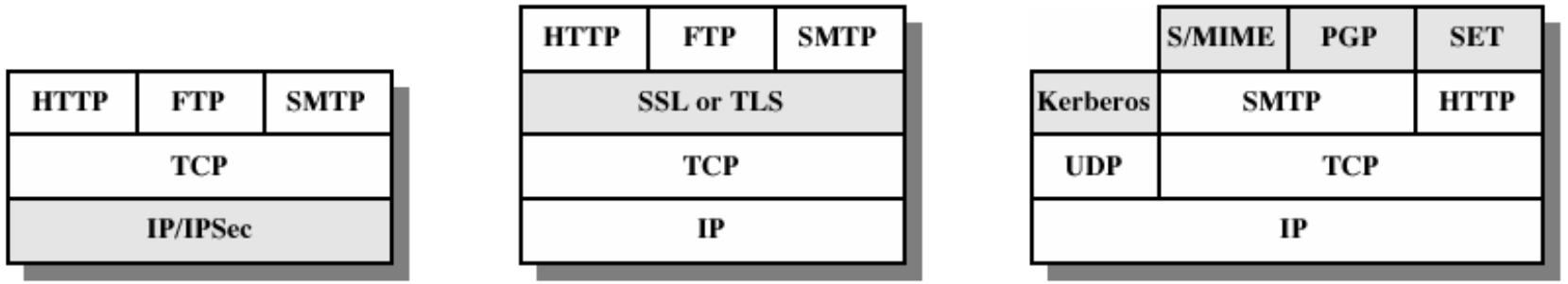
Ασφάλεια στο διαδίκτυο

- Απειλές και αντίμετρα
  - Ακεραιότητα - Integrity
    - Τροποποίηση δεδομένων, εισαγωγή
  - Εμπιστευτικότητα – Confidentiality
    - Κρυφάκουσμα στο δίκτυο
    - Κλοπή από τον εξυπηρέτη
  - Ταυτοποίηση - Authentication
    - Προσποίηση ταυτότητας, παραχάραξη δεδομένων
  - Denial of service, hacked web servers

Πεδίο εφαρμογής του SSL / TLS

Που παρέχεται η ασφάλεια;

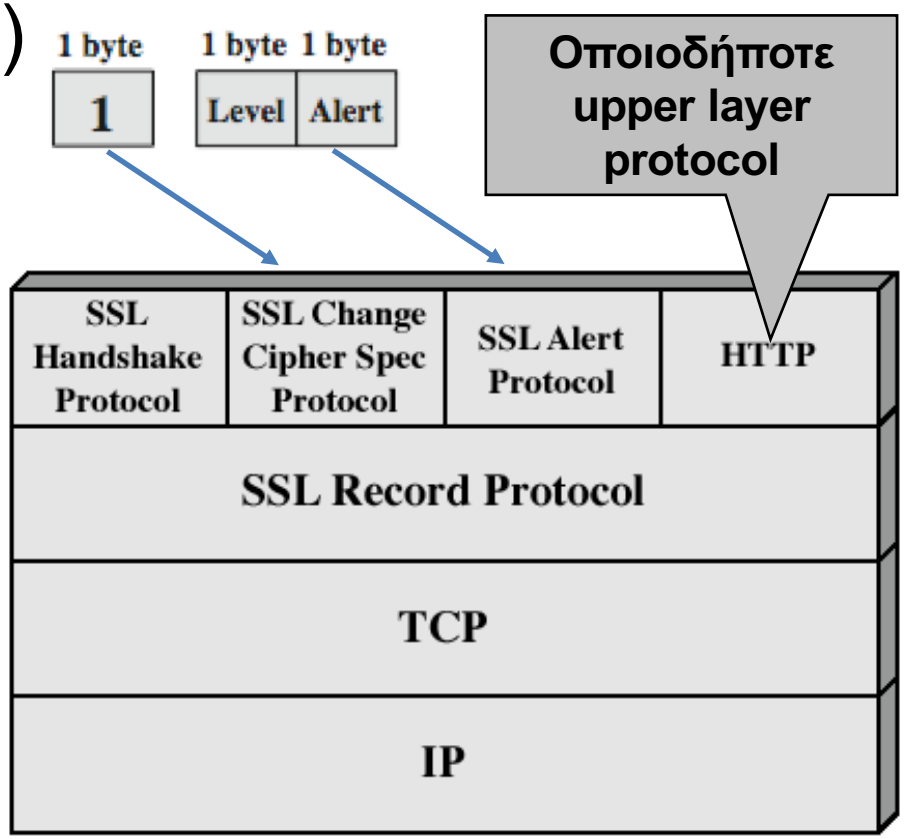
- Μεγάλη συζήτηση χωρίς σαφές συμπέρασμα!



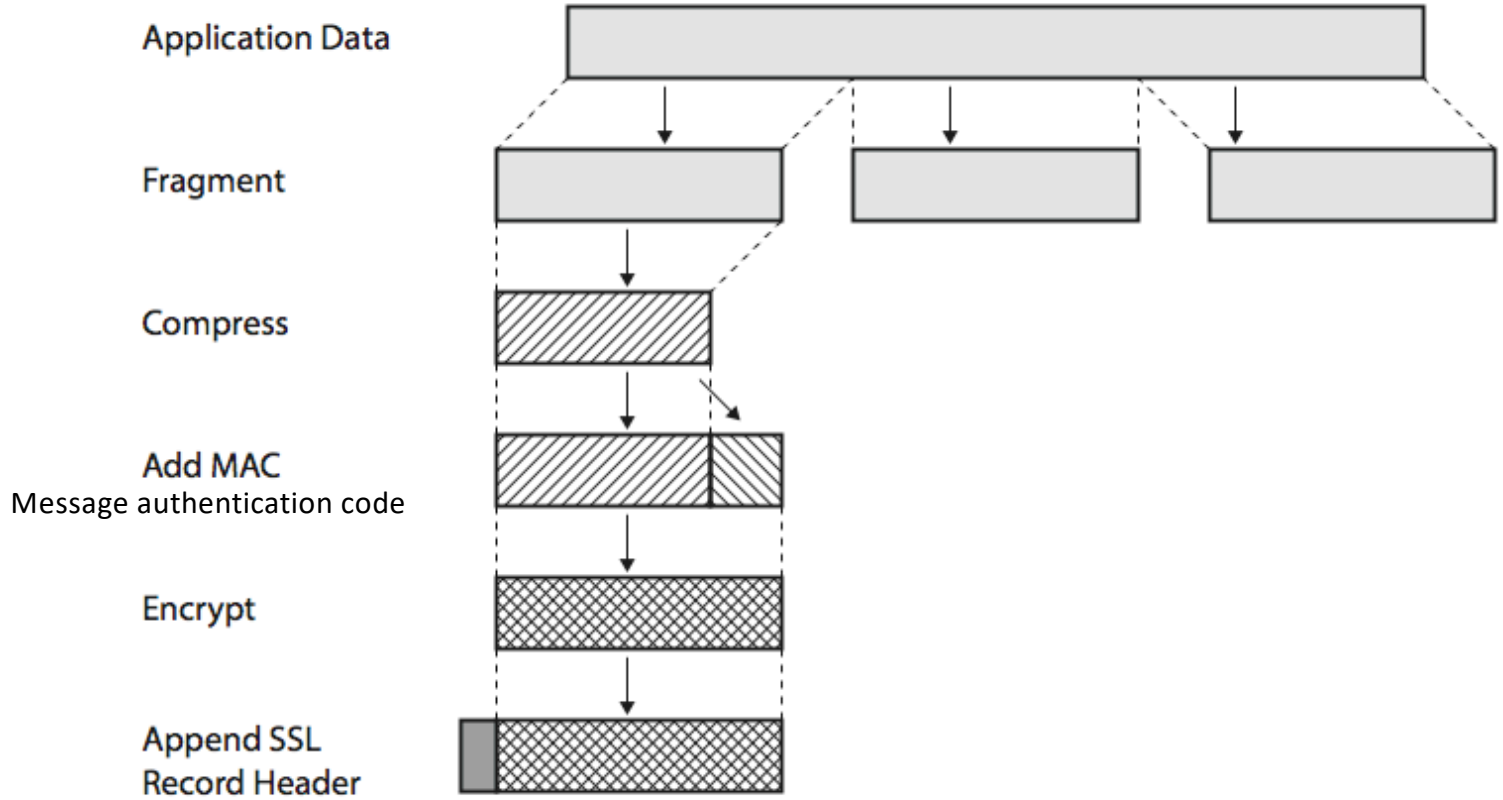
Η σημερινή διάλεξη

SSL Protocol Stack

- Χρησιμοποιεί το TCP (αξιόπιστη μεταφορά δεδομένων end to end)
  - Προστίθενται χαρακτηριστικά ασφάλειας
    - Αξιόπιστη και ασφαλής μεταφορά δεδομένων
  - Το SSL δεν είναι μεμονωμένο πρωτόκολλο
    - Δύο επίπεδα πρωτοκόλλων



SSL

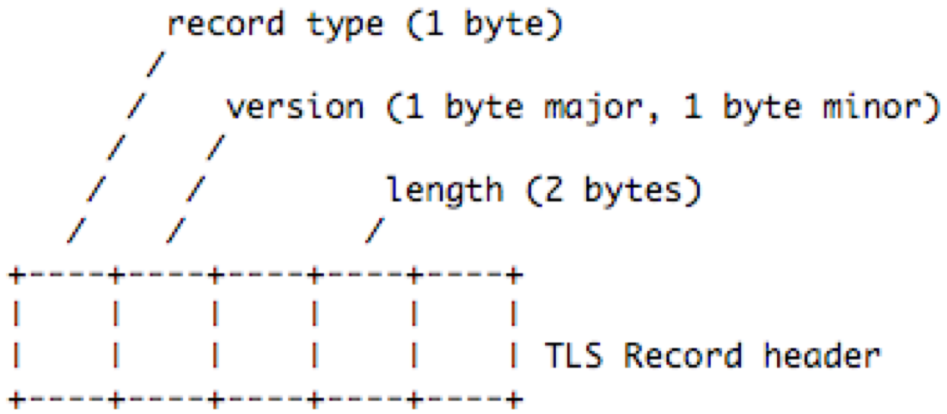


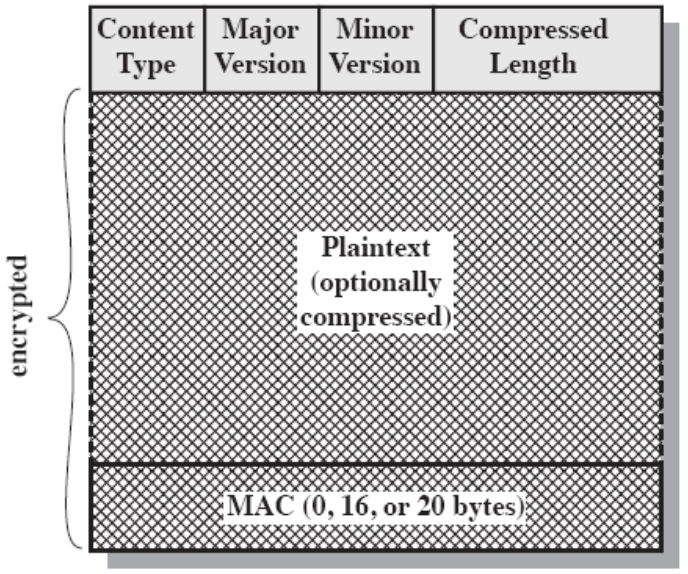
Πεδία κεφαλίδας

- Τύπος περιεχόμενου (higher layer protocol)
  - change_cipher_spec, alert, handshake, application data
- έκδοση
- Μήκος κατόπιν συμπίεσης (ή μήκος plaintext αν δεν χρησιμοποιείται) του fragment

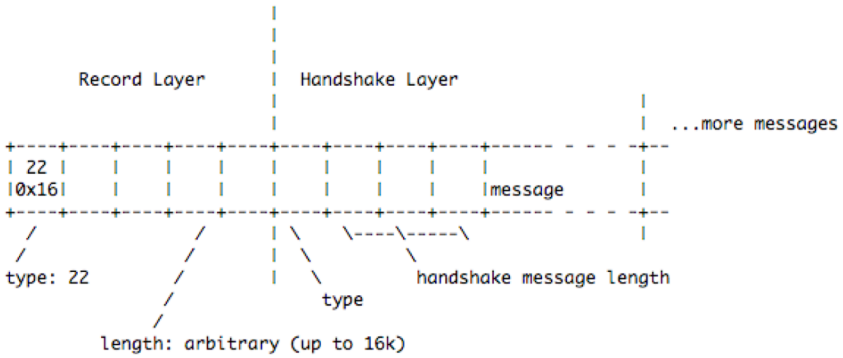
SSL record protocol

- Byte 0: TLS record type
- Bytes 1-2: TLS version
- Bytes 3-4: Μήκος δεδομένων (πλην κεφαλίδας), μέγιστο 16384 (16k)

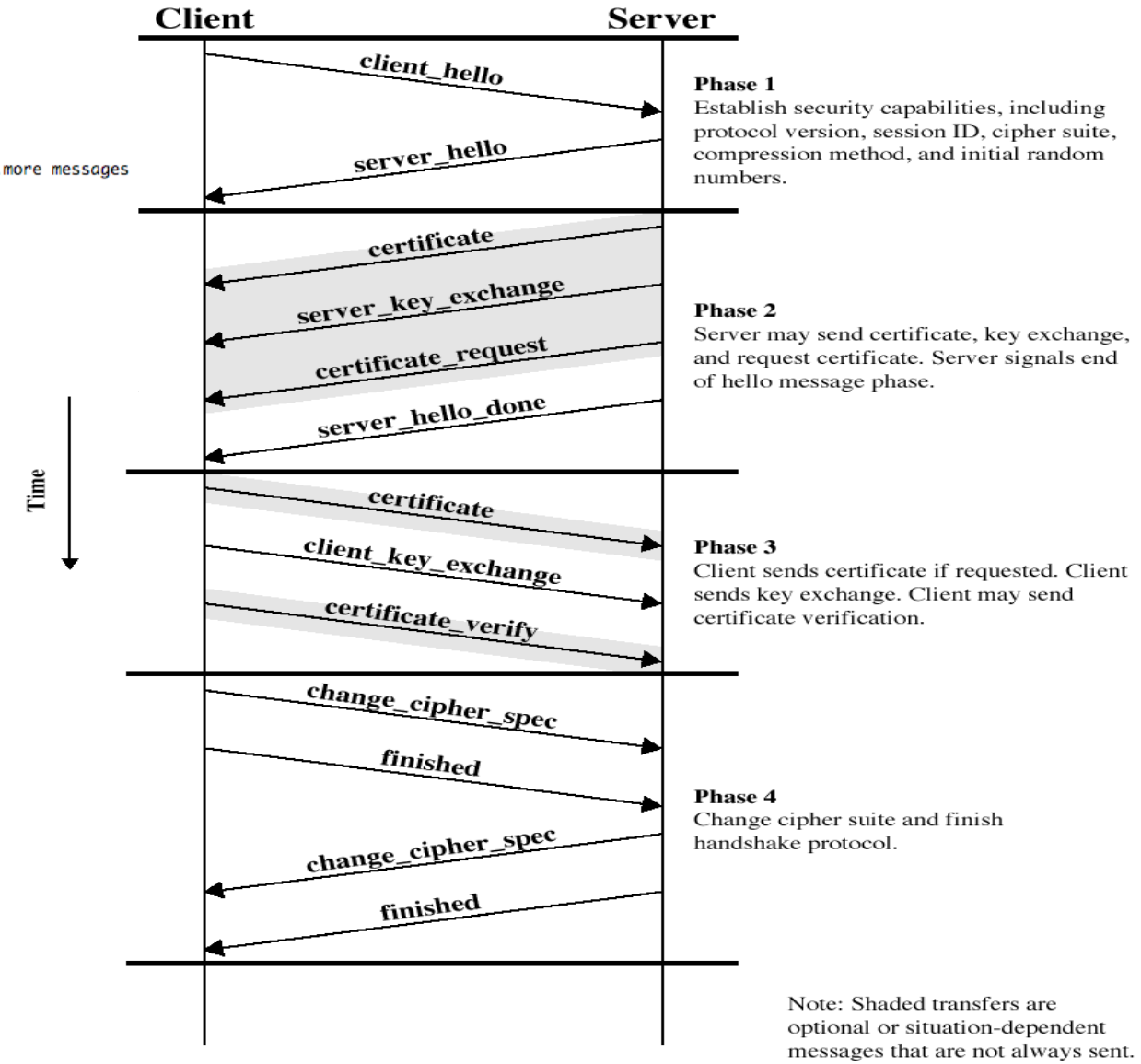




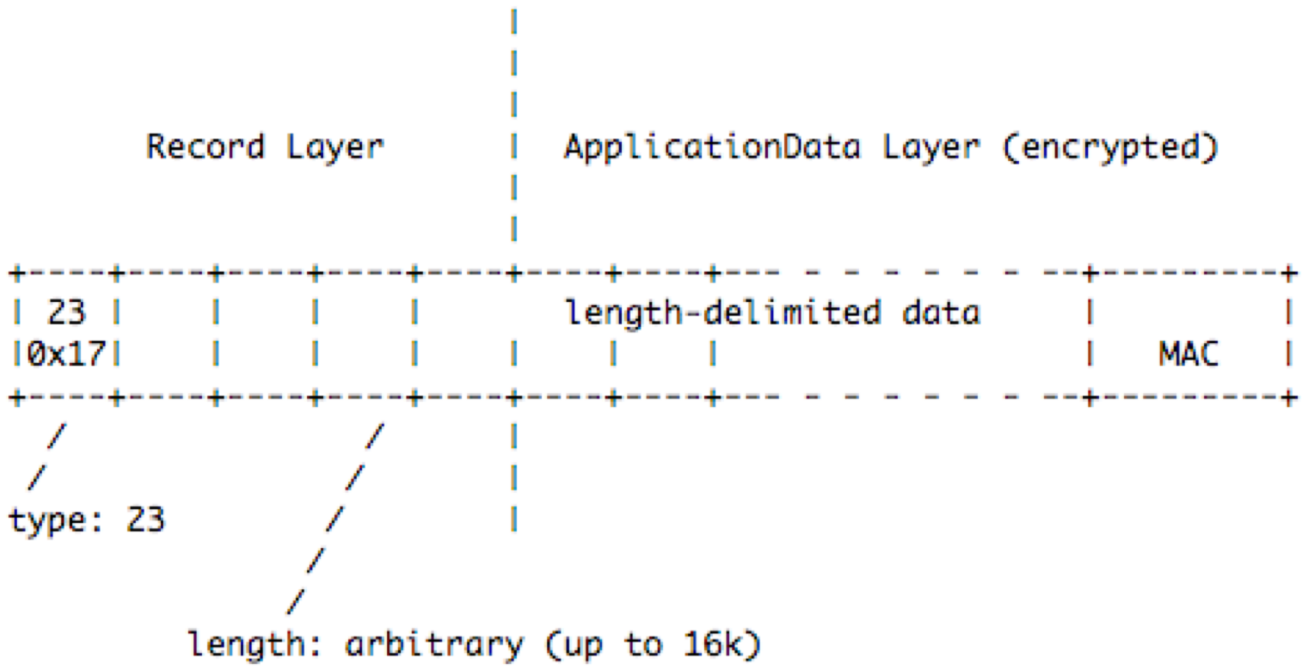
Handshake Protocol



Handshake Type Values	dec	hex
HELLO_REQUEST	0	0x00
CLIENT_HELLO	1	0x01
SERVER_HELLO	2	0x02
CERTIFICATE	11	0x0b
SERVER_KEY_EXCHANGE	12	0x0c
CERTIFICATE_REQUEST	13	0x0d
SERVER_DONE	14	0x0e
CERTIFICATE_VERIFY	15	0x0f
CLIENT_KEY_EXCHANGE	16	0x10
FINISHED	20	0x14



Application data protocol



HTTPS

- HTTPS (HTTP over SSL/TLS)
  - Συνδυασμός HTTP & SSL/TLS για τη διασφάλιση επικοινωνίας μεταξύ browser & web server
    - documented στο RFC2818
    - Καμμία διαφορά στη χρήση SSL ή TLS; Και τα δύο αναφέρονται σαν HTTPS
- Χρήση `https://` URL αντί για `http://`
  - Θύρα 443 αντί για 80
- κρυπτογραφεί
  - URL (όχι το domain name, αλλά το path & το searchpart)
  - περιεχόμενα κειμένου, δεδομένα φορμών, cookies, HTTP headers

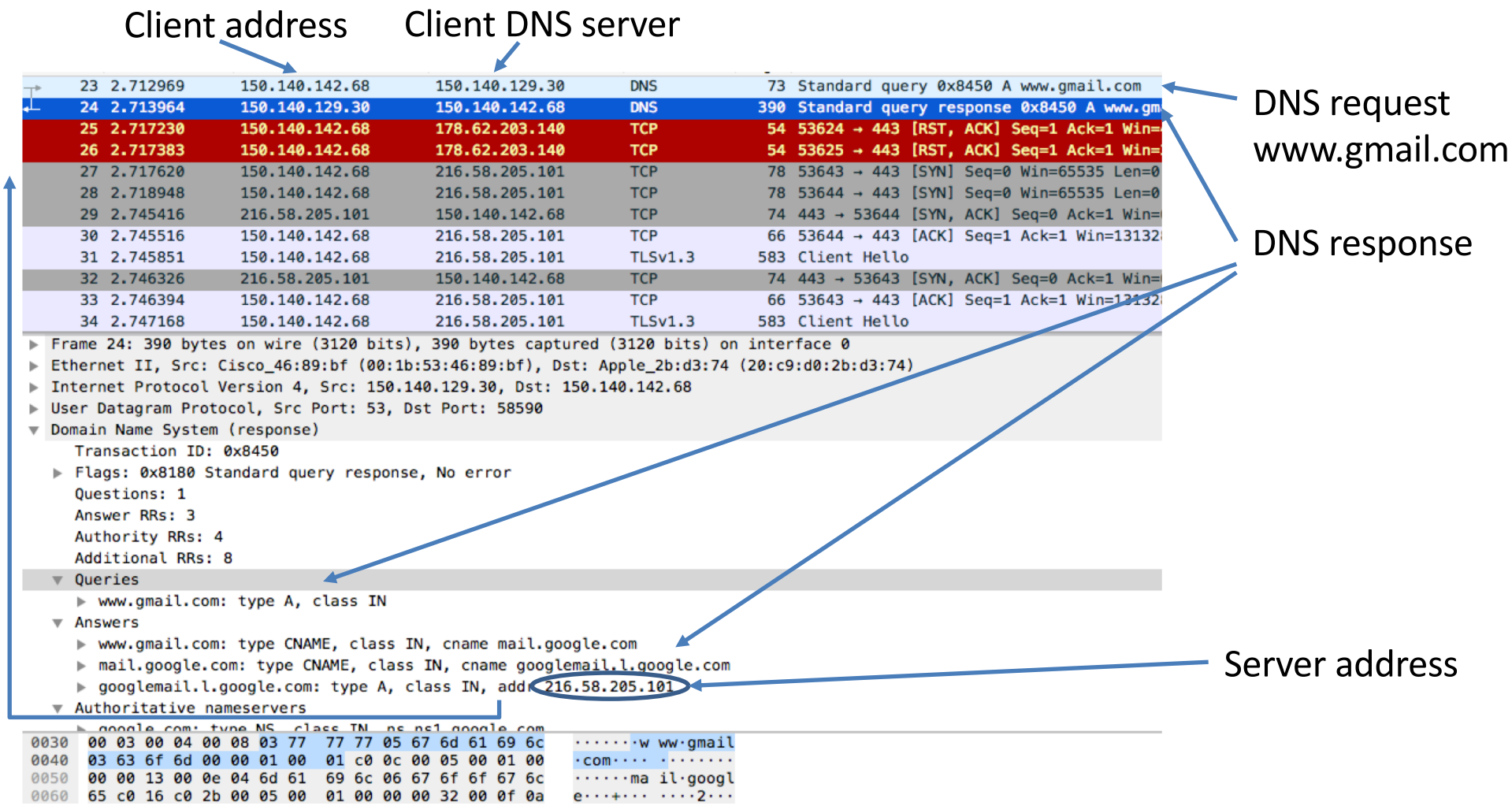
Αρχή HTTPS Connection

- Αρχικά, SSL/TLS handshake
  - HTTP client (browser) είναι ο SSL/TLS client
- Μετά το handshake αποστέλλονται HTTP request(s)
  - Όλα τα HTTP data καλό είναι να στέλνονται μέσα από το SSL/TLS record protocol

Κλείσιμο HTTPS Connection

- Κλείσιμο σύνδεσης
  - Έχουμε “Connection: close” στα HTTP headers
    - Κανονικά κλείνει μια απλή TCP σύνδεση
    - Αλλά έχουμε SSL/TLS πρωτόκολλα μεταξύ του HTTP και του TCP
    - Συνεπώς, το SSL/TLS πρέπει να ελέγχει ο κλείσιμο στο TCP level
  - Στο επίπεδο SSL/TLS ανταλλάσσονται close_notify alerts
  - Τότε μπορεί να κλείσει και η TCP σύνδεση

Παράδειγμα (wireshark)

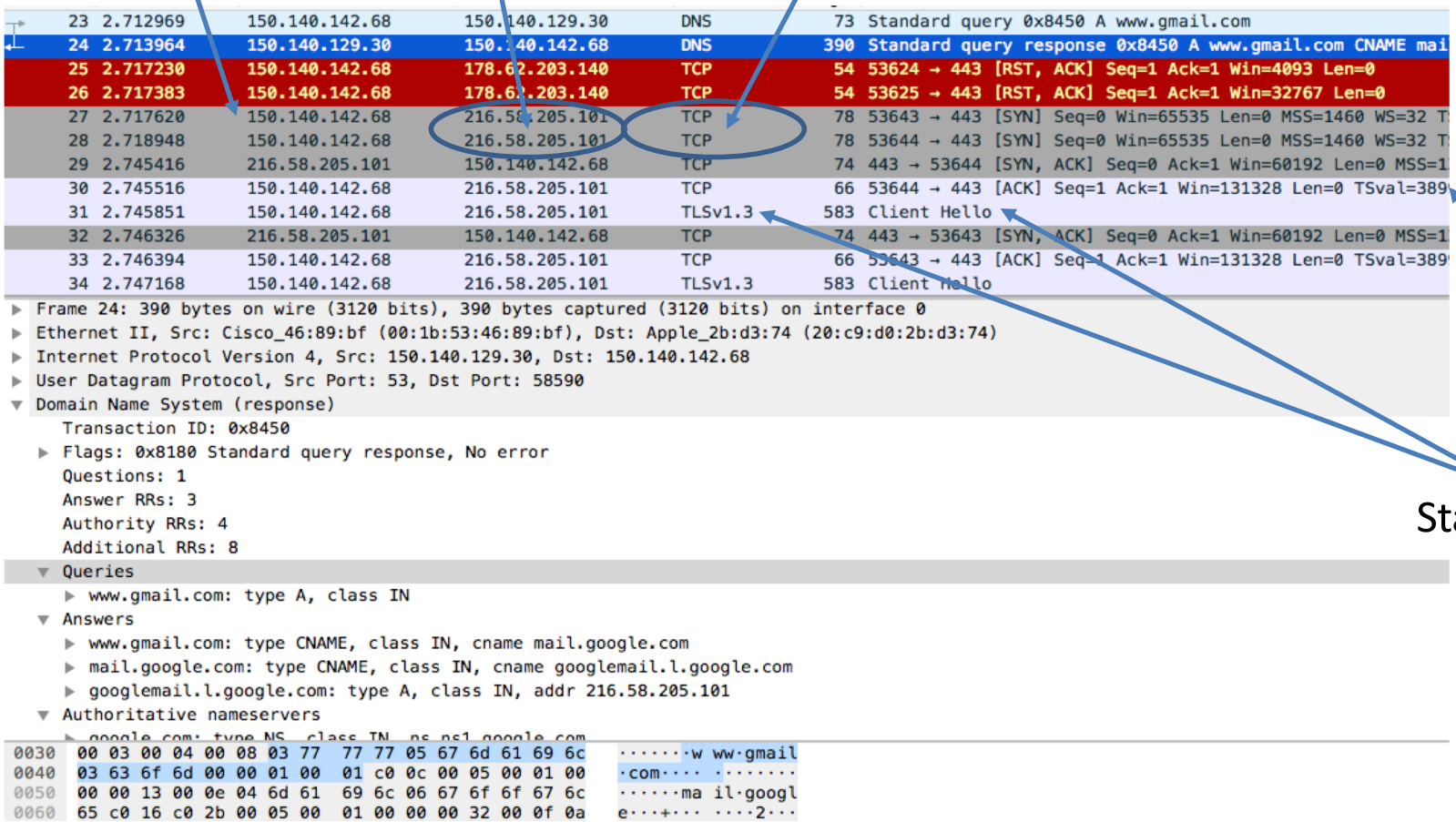


https://www.wireshark.org/

Client address

Server address

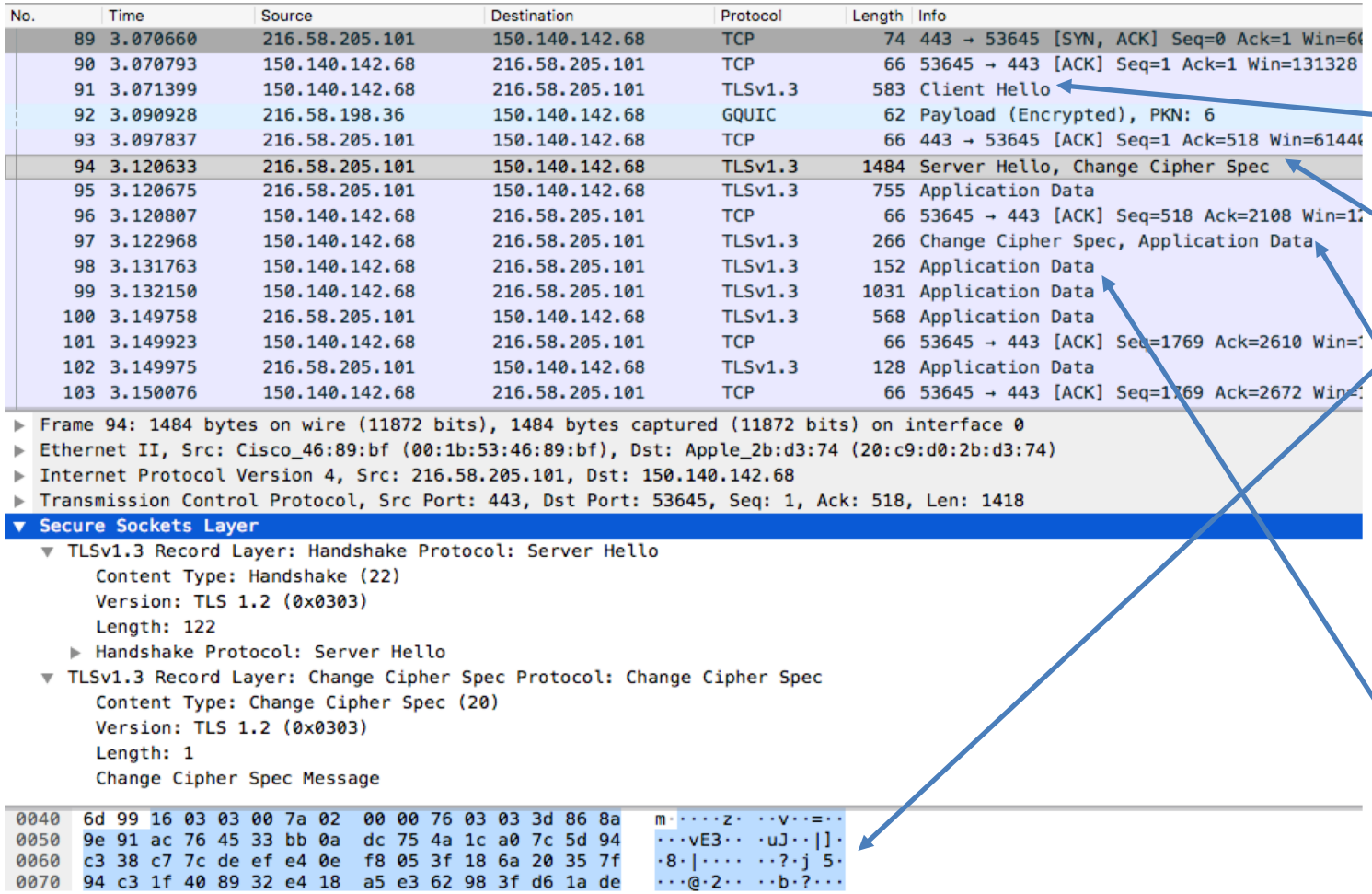
Άνοιγμα 2 παράλληλων συνδέσεων TCP



TCP establish connection

TCP port fwd -> 443 (secure https)

Start TLS connection



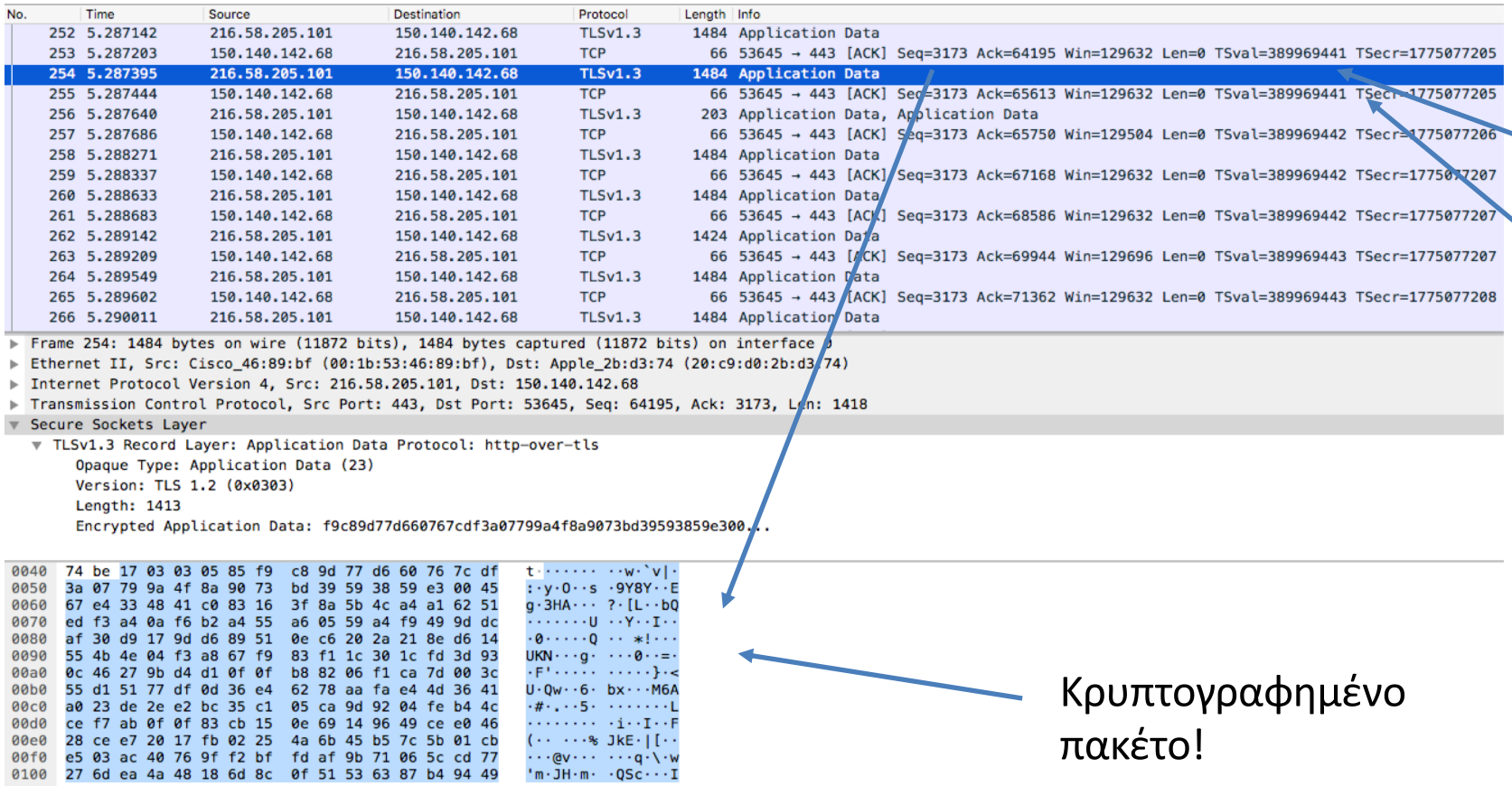
Κρυπτογραφημένο!

Client hello

Server hello & change cipher spec

Client change cipher spec OK

Ανταλλαγή δεδομένων (πιθανότατα keys, certificates?)


No. Time Source Destination Protocol Length Info
252 5.287142 216.58.205.101 150.140.142.68 TLSv1.3 1484 Application Data
253 5.287203 150.140.142.68 216.58.205.101 TCP 66 53645 → 443 [ACK] Seq=3173 Ack=64195 Win=129632 Len=0 TSval=389969441 TSecr=1775077205
254 5.287395 216.58.205.101 150.140.142.68 TLSv1.3 1484 Application Data
255 5.287444 150.140.142.68 216.58.205.101 TCP 66 53645 → 443 [ACK] Seq=3173 Ack=65613 Win=129632 Len=0 TSval=389969441 TSecr=1775077205
256 5.287640 216.58.205.101 150.140.142.68 TLSv1.3 203 Application Data, Application Data
257 5.287686 150.140.142.68 216.58.205.101 TCP 66 53645 → 443 [ACK] Seq=3173 Ack=65750 Win=129504 Len=0 TSval=389969442 TSecr=1775077206
258 5.288271 216.58.205.101 150.140.142.68 TLSv1.3 1484 Application Data
259 5.288337 150.140.142.68 216.58.205.101 TCP 66 53645 → 443 [ACK] Seq=3173 Ack=67168 Win=129632 Len=0 TSval=389969442 TSecr=1775077207
260 5.288633 216.58.205.101 150.140.142.68 TLSv1.3 1484 Application Data
261 5.288683 150.140.142.68 216.58.205.101 TCP 66 53645 → 443 [ACK] Seq=3173 Ack=68586 Win=129632 Len=0 TSval=389969442 TSecr=1775077207
262 5.289142 216.58.205.101 150.140.142.68 TLSv1.3 1424 Application Data
263 5.289209 150.140.142.68 216.58.205.101 TCP 66 53645 → 443 [ACK] Seq=3173 Ack=69944 Win=129696 Len=0 TSval=389969443 TSecr=1775077207
264 5.289549 216.58.205.101 150.140.142.68 TLSv1.3 1484 Application Data
265 5.289602 150.140.142.68 216.58.205.101 TCP 66 53645 → 443 [ACK] Seq=3173 Ack=71362 Win=129632 Len=0 TSval=389969443 TSecr=1775077208
266 5.290011 216.58.205.101 150.140.142.68 TLSv1.3 1484 Application Data
Frame 254: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits) on interface 0
Ethernet II, Src: Cisco_46:89:bf (00:1b:53:46:89:bf), Dst: Apple_2b:d3:74 (20:c9:d0:2b:d3:74)
Internet Protocol Version 4, Src: 216.58.205.101, Dst: 150.140.142.68
Transmission Control Protocol, Src Port: 443, Dst Port: 53645, Seq: 64195, Ack: 3173, Len: 1418
Secure Sockets Layer
TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
Opaque Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 1413
Encrypted Application Data: f9c89d77d660767cdf3a07799a4f8a9073bd39593859e300...
0040 74 be 17 03 03 05 85 f9 c8 9d 77 d6 60 76 7c df
0050 3a 07 79 9a 4f 8a 90 73 bd 39 59 38 59 e3 00 45
0060 67 e4 33 48 41 c0 83 16 3f 8a 5b 4c a4 a1 62 51
0070 ed f3 a4 0a f6 b2 a4 55 a6 05 59 a4 f9 49 9d dc
0080 af 30 d9 17 9d d6 89 51 0e c6 20 2a 21 8e d6 14
0090 55 4b 4e 04 f3 a8 67 f9 83 f1 1c 30 1c fd 3d 93
00a0 0c 46 27 9b d4 d1 0f 0f b8 82 06 f1 ca 7d 00 3c
00b0 55 d1 51 77 df 0d 36 e4 62 78 aa fa e4 4d 36 41
00c0 a0 23 de 2e e2 bc 35 c1 05 ca 9d 92 04 fe b4 4c
00d0 ce f7 ab 0f 0f 83 cb 15 0e 69 14 96 49 ce e0 46
00e0 28 ce e7 20 17 fb 02 25 4a 6b 45 b5 7c 5b 01 cb
00f0 e5 03 ac 40 76 9f f2 bf fd af 9b 71 06 5c cd 77
0100 27 6d ea 4a 48 18 6d 8c 0f 51 53 63 87 b4 94 49
Εισερχόμενα δεδομένα
Επιβεβαίωση παραλαβής πακέτου (TCP)
Κρυπτογραφημένο πακέτο!