2. kolokvij RK 3.6.2010 Sežana

1) Na strežniku je spletna stran, ki vsebuje spodnjo kodo:

```
<html>
<head>
  <link rel="stylesheet" type="text/css" href="lrk.css" />
  <title>Področja našega dela in raziskovanja</title>
</head>
<body>
  <img border="0" src="images/omara.jpg" width="306" height="321">
  <ul>
    <li><a href="index2.html">Komunikacije</a></li>
    <li><a href="http://marvin.fri.uni-lj.si/izo.html">Izobraževanje</a></li>
  </ul>
</html>
```

   a) Koliko zahtev HTTP mora poslati naš spletni brskalnik, da nam prikaže zgornjo spletno stran?
   b) Kaj pomeni vrstica Keep-alive, če se pojavi v glavi (header) zahteve HTTP? Ali uporaba te vrstice kaj spremeni število zahtev, ki jih mora naš brskalnik poslati?
   c) Kaj pomeni, če nam strežnik odgovori s HTTP odgovorom z oznako 404 (Not found)? Gre za napako odjemalca ali napako na strežniku?

2) S programom Wireshark smo zajeli paket, katerega del prikazuje spodnja slika:

```
⊟ Domain Name System (response)
    [Request In: 82]
    [Time: 0.006503000 seconds]
    Transaction ID: 0x0004
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 3
    Additional RRs: 2
  ⊟ Queries
    ⊟ fri.uni-lj.si: type MX, class IN
        Name: fri.uni-lj.si
        Type: MX (Mail exchange)
        Class: IN (0x0001)
  ⊟ Answers
    ⊟ fri.uni-lj.si: type MX, class IN, preference 10, mx ns.fri.uni-lj.si
        Name: fri.uni-lj.si
        Type: MX (Mail exchange)
        Class: IN (0x0001)
        Time to live: 1 minute
        Data length: 7
        Preference: 10
        Mail exchange: ns.fri.uni-lj.si
  ⊟ Authoritative nameservers
    ⊞ fri.uni-lj.si: type NS, class IN, ns metulj.uni-lj.si
    ⊞ fri.uni-lj.si: type NS, class IN, ns ns.fri.uni-lj.si
    ⊞ fri.uni-lj.si: type NS, class IN, ns ns.uni-lj.si
  ⊟ Additional records
    ⊞ ns.uni-lj.si: type A, class IN, addr 193.2.64.45
    ⊞ metulj.uni-lj.si: type A, class IN, addr 193.2.64.46
```

   a) Del katerega protokola so odgovori takšnega tipa?
   b) Po katerem tipu zapisa smo poizvedovali?
   c) Kakšen je strežnikov odgovor na našo poizvedbo? Napišite samo ime računalnika in domeno.
   d) Kaj vsebuje del odgovora Additional information? Zakaj je pomemben?

3) S programom Wireshark smo zajeli spodnjo sejo:

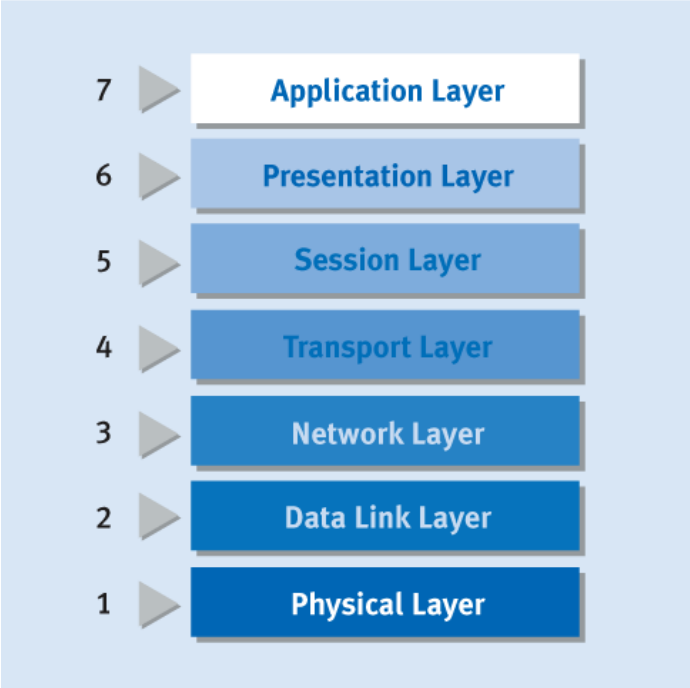
```
+OK POP3 server ready <1896.697170952@rk.local>
USER rdeca
+OK
PASS kapica
+OK rdeca's maildrop has 2 messages (320 octets)
STAT
+OK 2 320
LIST
+OK 2 messages (320 octets)
1 120
2 200
.
RETR 1
```

2. nalo
aa)DNS protok
lb)MX ozirom a MaileXchan **g**
?c)ns.fri.uni-lj.
id)Vsebuje IP naslov(e) strežnika za pošto. Brez tega dela odgovora se ne bi mogli povezati a ns.fri.uni-lj.si, saj nam je DNS strežnik odgovoril z imenom namesto z IPjem strežnik

3. nalo
aa)PO
3b)Uporablja se za elektronsko pošto. POP3 strežnik shranjuje naše prihodna sporočila dokle r jih uporabnik ne prebere(prenese na lokalni računalnik). Strežnika posluša na vratih 11
.c)Podatki potujejo od uporabnika do strežnika kot golo besedilo, vključno z geslo
.d)Z enkripcijo promet

5. nalo
aa)T
Pb)T
Pc)T
Pd)U
Pe)U
Pf)T
Pg)T

7. nalo



Predstavitvena plast zagotavlja različne načine kodiranja in sisteme pretvorb za aplikacijsko plast. Pretvarja podatke, poslane po omrežju, iz ene v drugo obliko, določa sintakso, transformacijo in formiranje podatkov. Naloge predstavitvene plasti pri modelu TCP/IP sodijo v aplikacjisko plast.

8. naloga
a)MIME ali Multipurpose Internet Mail Extensions se uporablja pri e-pošti, kot razširitev, ki omogoča večpredstavna sporočila in dodatne znake, kot so č,š,ž in podobni.
b)Uporablja se na aplikacijski plasti
c)Quoted-printable, Base 64, Binary.
d)
e)

9. naloga

Zloraba piškotkov:

Cookie hijacking – "ugrabitev" piškotkov

Če je še kdo na istem omrežju kot jaz in strežnik in ima dovoljeno branje iz omrežja, lahko ukrade piškotke. Zaradi tega, ker piškotki vsebujejo osebne podatke (uporabniška imena, gesla, ipd.), njihova vsebina ne sme biti dostopna do ostalih računalnikov.

Cookie poisoning – "zastrupljanje" piškotkov

Medtem, ko naj bi se piškotki samo hranili na računalniku in pošiljali strežniku nazaj nespremenjeni, lahko napadalec spremeni njihove vrednosti preden jih naprej posreduje strežniku. Na primer: piškotek vsebuje ceno nekega plačila, ki ga mora uporabnik plačati. Če spremenimo to vrednost, lahko plačamo manj ali več.

10.naloga

INTEGRITETA SPOROČILA

- Ali je bilo sporočilo med prenosom spremenjeno?
- Uporabimo digitalni izvleček, ga podpišemo in pošljemo skupaj s sporočilom
- Zgoščevalne funkcije
    -
    - Prstni odtis (hash) sporočila m: f = h(m)
    - m poljubno dolgo sporočilo; f je kratek, omejene dolžine
    - kolizija: različna sporočila imajo enak prstni odtis
    - pri vseh možnih vhodih je frekvenca (hash) rezultatov enaka
    - mala sprememba vhoda povzroči veliko spremembo podpisa
    - težko najti drugačno vhodno vrednost za isti podpis
    - bitne operacije brez ključa
    - MD5 (osnova za sha1, uporaba v bazah za shranjevanje gesel)
    - SHA-1 (najpomembnejši 160 bitov)
    - SHA 256 – 256 bitov