arnes

Mreža znanja 2016

24. november 2016, Ljubljana

Forenzika e-pošte:
Mi je res pisala Pika Nogavička?

Mark Martinec

Institut »Jožef Stefan«

Mark.Martinec@ijs.si

Verjeti ali ne ?

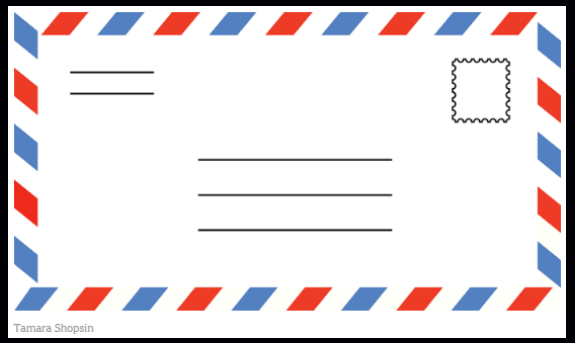
Nizozemska založba Elsevier bi rada vrnila uporabniku preveč plačano naročnino in ga prosi za številko bančnega računa ali kreditne kartice za nakazilo.

Verjeti ali ne ?

Nizozemska založba Elsevier bi rada vrnila uporabniku preveč plačano naročnino in ga prosi za številko bančnega računa ali kreditne kartice za nakazilo.

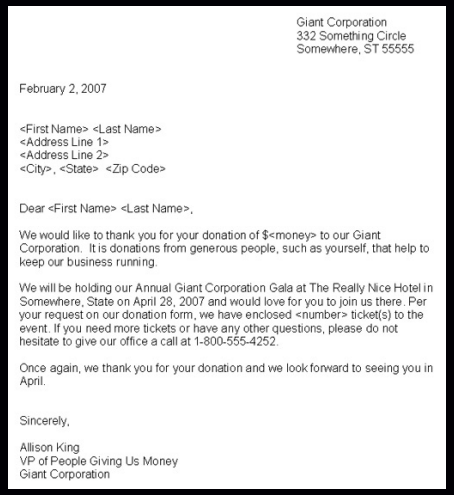
Vredno je poznati osnove delovanja e-pošte.

e-poštno sporočilo = ovojnica + vsebina



informacije potrebne za prenos in dostavo

RFC 5321 (SMTP)



Giant Corporation
332 Something Circle
Somewhere, ST 55555

February 2, 2007

<First Name> <Last Name>
<Address Line 1>
<Address Line 2>
<City>, <State> <Zip Code>

Dear <First Name> <Last Name>,

We would like to thank you for your donation of $<money> to our Giant Corporation. It is donations from generous people, such as yourself, that help to keep our business running.

We will be holding our Annual Giant Corporation Gala at The Really Nice Hotel in Somewhere, State on April 28, 2007 and would love for you to join us there. Per your request on our donation form, we have enclosed <number> ticket(s) to the event. If you need more tickets or have any other questions, please do not hesitate to give our office a call at 1-800-555-4252.

Once again, we thank you for your donation and we look forward to seeing you in April.

Sincerely,

Allison King
VP of People Giving Us Money
Giant Corporation

vsebina: glava + telo

RFC 5322

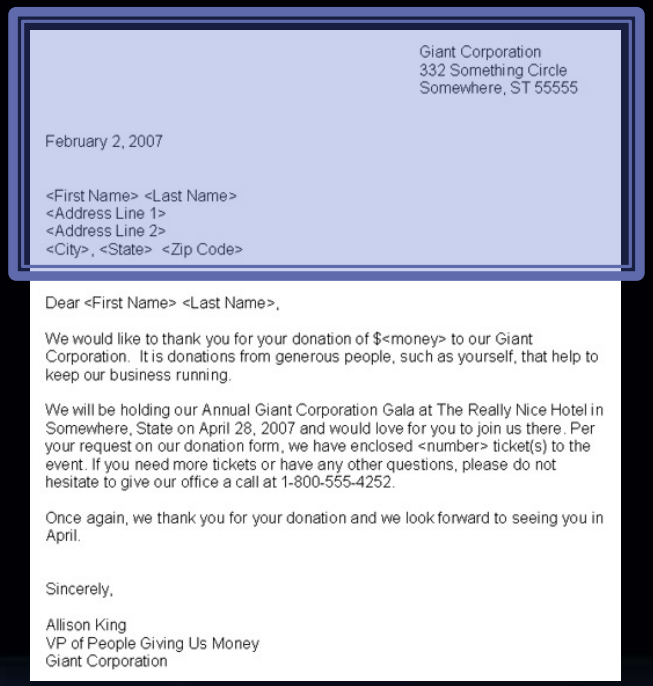
ovojnica – protokol SMTP – RFC 5321

MAIL FROM: <povratni-naslov @ domena>

RCPT TO: <prejemnik-1 @ domena>
RCPT TO: <prejemnik-2 @ domena>
RCPT TO: <prejemnik-3 @ domena>

terminologija: 5321.MailFrom (povratni naslov),
5321.RcptTo

vsebina = glava + telo



Giant Corporation
332 Something Circle
Somewhere, ST 55555

February 2, 2007

<First Name> <Last Name>
<Address Line 1>
<Address Line 2>
<City>, <State> <Zip Code>

Dear <First Name> <Last Name>,

We would like to thank you for your donation of $<money> to our Giant Corporation. It is donations from generous people, such as yourself, that help to keep our business running.

We will be holding our Annual Giant Corporation Gala at The Really Nice Hotel in Somewhere, State on April 28, 2007 and would love for you to join us there. Per your request on our donation form, we have enclosed <number> ticket(s) to the event. If you need more tickets or have any other questions, please do not hesitate to give our office a call at 1-800-555-4252.

Once again, we thank you for your donation and we look forward to seeing you in April.

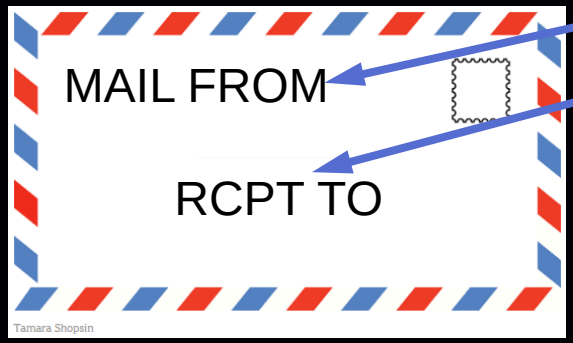
Sincerely,

Allison King
VP of People Giving Us Money
Giant Corporation

From:
To:
Date:
Subject:
Message-ID:
…

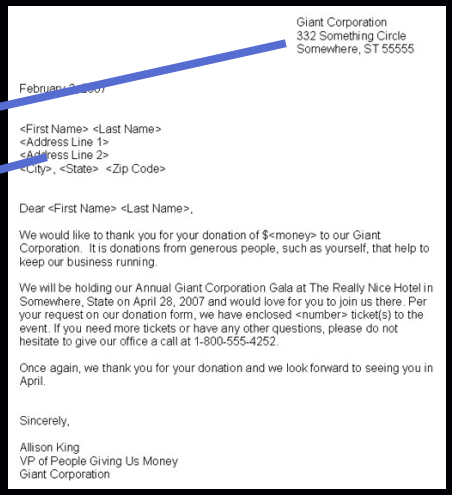
prazna vrstica
loči telo od glave
sporočila

MSA – mail submission agent (strežnik za prevzem pošte)



To:
Cc:
Bcc:

From:
Sender:
Reply-To:



Giant Corporation
332 Something Circle
Somewhere, ST 55555

February [illegible], 2007

<First Name> <Last Name>
<Address Line 1>
<Address Line 2>
<City>, <State> <Zip Code>

Dear <First Name> <Last Name>,

We would like to thank you for your donation of $<money> to our Giant Corporation. It is donations from generous people, such as yourself, that help to keep our business running.

We will be holding our Annual Giant Corporation Gala at The Really Nice Hotel in Somewhere, State on April 28, 2007 and would love for you to join us there. Per your request on our donation form, we have enclosed <number> ticket(s) to the event. If you need more tickets or have any other questions, please do not hesitate to give our office a call at 1-800-555-4252.

Once again, we thank you for your donation and we look forward to seeing you in April.

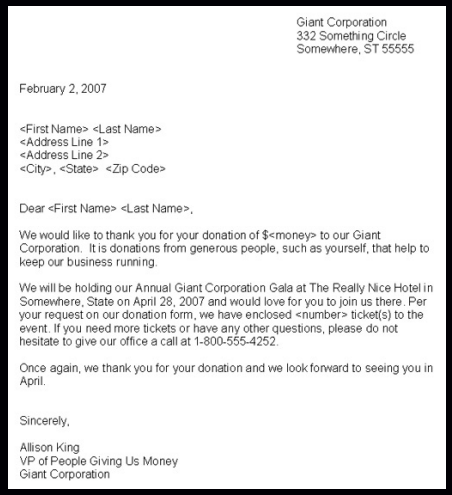
Sincerely,

Allison King
VP of People Giving Us Money
Giant Corporation

MSA lahko uporabi naslove iz glave
in jih uporabi za tvorjenje naslovov v ovojnici
(v protokolu SMTP)

MTA – mail transfer agent (strežnik za prenos pošte)

To:
Cc:
Bcc:



Giant Corporation
332 Something Circle
Somewhere, ST 55555

February 2, 2007

<First Name> <Last Name>
<Address Line 1>
<Address Line 2>
<City>, <State> <Zip Code>

Dear <First Name> <Last Name>,

We would like to thank you for your donation of $<money> to our Giant Corporation. It is donations from generous people, such as yourself, that help to keep our business running.

We will be holding our Annual Giant Corporation Gala at The Really Nice Hotel in Somewhere, State on April 28, 2007 and would love for you to join us there. Per your request on our donation form, we have enclosed <number> ticket(s) to the event. If you need more tickets or have any other questions, please do not hesitate to give our office a call at 1-800-555-4252.

Once again, we thank you for your donation and we look forward to seeing you in April.

Sincerely,

Allison King
VP of People Giving Us Money
Giant Corporation

From:
Sender:
Reply-To:

- naslovi v ovojnici so neodvisni od naslovov v glavi sporočila
- naslovi v glavi ne vplivajo na prenos in dostavo

MTA – mail transfer agent (strežnik za prenos pošte)

Received: from … IP-addr
by … for <prejemnik>;
datum-ura-cona

MDA – mail delivery agent (strežnik za dostavo pošte)

Return-Path:
<povratni naslov>

Received: from … IP-addr
by … for <prejemnik>;
datum-ura-cona

Zakaj sem dobil to sporočilo, čeprav nisem na spisku prejemnikov To ali Cc ?

- naslovi v ovojnici so neodvisni
  od naslovov v glavi sporočila

- naslovi v glavi ne vplivajo na prenos in dostavo

Zakaj sem dobil to sporočilo, čeprav nisem na spisku prejemnikov To ali Cc ?

- Bcc (blind carbon copy)

- preusmeritev na poštnem strežniku
  (npr. dekliški priimek → novi priimek,
  stara zaposlitev → nova zaposlitev)

- poštni seznam
  (To: SINOG <nog@sinog.si>)

- masovna sporočila (avtomatska, marketing)
- nezaželena pošta (spam / virus / prevara)

vsebina sporočila (RFC 5322)

- je zaporedje znakov (US-ASCII, pogojno UTF-8) razdeljeno na vrstice (CR LF)

- glava sporočila (header section)
- ena prazna vrstica (samo CR LF)
- vse ostalo je telo sporočila (telo ni obvezno)

glava (header section)

- sestavljajo polja glave (header field)
- polje glave = ime polja : telo polja
  (header field = field name : field body)

```
From: "Janez K. Novak" <jnovak@postar.example>
To: Marija Medved <marija@example.net>
Subject: Pozdrav
  z morja
Date: Tue, 16 Aug 2016 14:33:30 +0200 (CEST)
Message-ID: <1234@local.postar.example>

Lep pozdrav, Janez
```

obvezna polja glave

- From … en ali (redko) več avtorjev sporočila
- Date … datum in ura nastanka sporočila (MUA)

sta edini dve obvezni polji !

'skoraj' obvezno polje:

- Message-ID … enolična identifikacija sporočila

nanj se sklicujejo: In-Reply-To, References, dnevnik strežnika

neobvezna (a običajna) polja

- Sender … pošiljatelj (če je različen od avtorja)
- Reply-To … naslov za odgovore
- To … seznam prejemnikov
- Cc … seznam dodatnih prejemnikov
- Bcc … skriti seznam dodatnih prejemnikov
- Subject … naslov sporočila

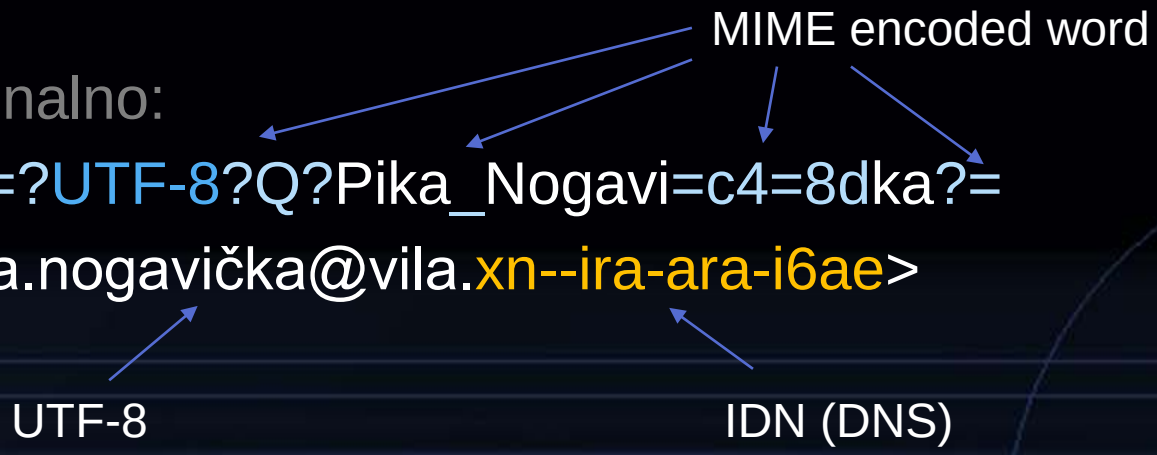
kodiranje besedila in domene v glavi sporočila

EAI – internationalized e-mail (RFC 6530 – RFC 6533).
UTF-8 v 5321.MailFrom, 5321.RcptTo, *in* v poljih glave:

From: "Pika Nogavička"
<pika.nogavička@vila.Čira-čara>

tradicionalno:

From: =?UTF-8?Q?Pika_Nogavi=c4=8dka?=
<pika.nogavička@vila.xn--ira-ara-i6ae>



IDNA: Internationalizing Domain Name in Applications
ACE: ASCII-compatible encoding

Shannon.00@xn--80afflzul.su … A-label (xn-- punicode)
Shannon.00@интегра.su … U-label (UTF-8)

Gill.85083@xn--foroporlaniez-skb.org.ar
Gill.85083@foroporlaniñez.org.ar

Mel670@xn--rhne-gra.no
Mel670@røhne.no

Baird.42126@xn--rindlw-0xa.se
Baird.42126@rindlöw.se

IDN zgornje-nivojske domene: ccTLD, TLD

.рф	.xn--p1ai	(Rusija)
.укр	.xn--j1amh	(Ukrajina)
.бг	.xn--90ae	(Bolgarija)
.срб	.xn--90a3ac	(Srbija)
.ελ	.xn--qxam	(el, Grčija)
.台灣	.xn--kpry57d	(Tajvan .tw)
.москва	.xn--80adxhks	(Moskva)

…

Avtentikacija – polja v glavi

- Authentication-Results (rezultat preverjanja SPF, DKIM)

- DKIM-Signature
- DomainKey-Signature (historical)

- RFC 4954: SMTP Service Extension for Authentication (AUTH)

Avtentikacija

- SPF (Sender Policy Framework) primerja pošiljateljev naslov IP in domeno v povratnem naslovu (Return-Path)

  http://www.kitterman.com/spf/validate.html
  http://mxtoolbox.com/spf.aspx

Elsevier primerek iz uvoda?

Avtentikacija

- DKIM (DomainKeys Identified Mail) s kriptografskim podpisom overja vsebino sporočila (glavo in telo) glede na domeno naslova avtorja (From)

Avtentikacija – DKIM, RFC 6376

Authentication-Results: dorothy.ijs.si (amavisd-new);
    dkim=pass (2048-bit key) header.d=gmail.com

Authentication-Results: spamd4-us-west.apache.org;
    dkim=pass (2048-bit key) header.d=gmail.com

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
   d=gmail.com; s=20120113;
   h= mime-version : from : date : message-id : subject : to : cc;
   bh=LIrvkwZ1i/9R48ZYk2Rl9DYHdw2Z8W6u7hso2mZG7vo=;
   b=P0jSraMNb6apM9q21eIm77p3C4UNoWBzF998sYtJs4TMV8ptrA4tojcqhpaLY5o7qH
    /SDKukpdYUXsLMRRAli4hl6vh/t6+e2bB2mHeEzYdcTENdDTvlR6PJ1LvImkip3XsOM0
    RcOMYLHCR/U0faUzjPEAWwk7IeM/v9cfay/syRY9QyFdVpe/uwVGy+6xrkueJxsBI4p/
    FsAKbmgj/YJ5wc6uvclGYn67lab0o/VDm6mJ/Vy/EqgcxcFj/nZph58b8aSsTpW/4dAG
    GFMyQy/DbeXhLTkg5ullr7D0s93ffmJEW+sFrslY2eh/JGAl8Rj0X+N+zr+Y852PBl33
    rLyQ==

$ dig 20120113._domainkey.gmail.com -t TXT +short
"k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAO…X5jYchHjPY/wIDAQAB"

polja za sledenje poti – trace header fields
(RFC 5321)

- Return-Path … povratni naslov 5321.MailFrom
- Received … naslov IP (from, by), protokol, prejemnik 5321.RcptTo, čas prevzema s časovno cono

sled poti (trace) – primer

```
Return-Path: <povratni.naslov@domena>

Received:
  from mildred.ijs.si (mailbox.ijs.si [IPv6:2001:1470:ff80::143:1])
  by mail.ijs.si (Postfix)
  with ESMTP
  id 3sDBbt35PRz1R1
  for <prejemnik@example.net>;
  Tue, 16 Aug 2016 14:33:30 +0200 (CEST)

Received: from mx1.freebsd.org
     (mx1.freebsd.org [IPv6:2001:1900:2254:206a::19:1])
  (using TLSv1.2 with cipher AECDH-AES256-SHA (256/256 bits))
  (No client certificate requested)
  by mx2.freebsd.org (Postfix) with ESMTPS id 6D1AD68986;
  Mon,  3 Oct 2016 06:21:54 +0000 (UTC)
  (envelope-from owner-freebsd-perl@freebsd.org)
```

RFC 5321 – sekcija 4.4

- poštni strežnik NE SME spremeniti ali zbrisati polja Received, ki je bilo predhodno dodano v glavo sporočila
- SMTP strežniki MORAJO dodati polje Received na vrh glave sporočila
- in NE SMEJO spremeniti vrstnega reda obstoječih vrstic glave ali vstaviti Received polje na kakšno drugo mesto

pošljimo sporočilo: (izzivamo z UTF-8)

SMTP ovojnica:

EHLO Villa-Villekulla.gmail.com
MAIL FROM:<Pippi.Langstrump@gmail.com>
RCPT TO:<Mark.Martinec@ijs.si>

sporočilo (SMTPUTF8, podpora ni razširjena, gmail jo podpira):

Subject: Pozdravček
To: Tomaž, Anica
From: Pika Nogavička <pika@vila.Čira-čara>
Message-ID: <123@vila.Čira-čara>
Date: Mon, 3 Oct 2016 16:55:28 +0200
Received: from mail-it0-f50.google.com
      (mail-it0-f50.google.com [209.85.214.50])
   by mail.ijs.si (Postfix) with ESMTP id 64BC45FB0F
   for <Annika.Settergren@ijs.si>; Mon, 3 Oct 2016 14:55:25 +0000 (UTC)

Hoj, Tomaž in Anica!

pošljimo sporočilo: (klasično kodirano)

SMTP ovojnica:

EHLO Villa-Villekulla.gmail.com
MAIL FROM:<Pippi.Langstrump@gmail.com>
RCPT TO:<Mark.Martinec@ijs.si>

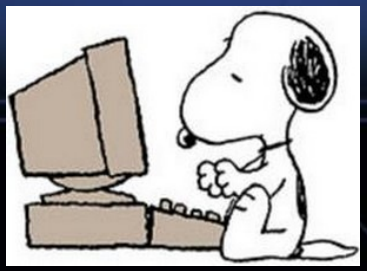
sporočilo:

```
Subject: =?UTF-8?Q?Pozdrav=c4=8dek?=
To: =?UTF-8?Q?Toma=c5=be?= <Tomaz>, Anica
From: =?UTF-8?Q?Pika_Nogavi=c4=8dka?= <pika@vila.xn--ira-ara-i6ae>
Message-ID: <123@vila.xn--ira-ara-i6ae>
Date: Mon, 3 Oct 2016 16:55:28 +0200
Received: from mail-it0-f50.google.com
      (mail-it0-f50.google.com [209.85.214.50])
   by mail.ijs.si (Postfix) with ESMTP id 64BC45FB0F
   for <Annika.Settergren@ijs.si>; Mon, 3 Oct 2016 14:55:25 +0000 (UTC)

Hoj, Tomaž in Anica!
```

```
$ telnet mail.ijs.si 25
220 mail.ijs.si ESMTP Postfix
EHLO Villa-Villekulla.gmail.com
250-mail.ijs.si
250-PIPELINING
250-ENHANCEDSTATUSCODES
250-DSN
MAIL FROM:<Pippi.Langstrump@gmail.com>
250 2.1.0 Ok
RCPT TO:<Mark.Martinec@ijs.si>
250 2.1.5 Ok
RCPT TO:<Tommy.Settergren@ijs.si>
550 5.1.1 <Tommy.Settergren@ijs.si>: Recipient address rejected: User unknown in virtual alias table
RCPT TO:<Annika.Settergren@ijs.si>
550 5.1.1 <Annika.Settergren@ijs.si>: Recipient address rejected: User unknown in virtual alias table
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Pozdravček
To: Tomaž, Anica
From: Pika Nogavička <pika@vila.Čira-čara>
Message-ID: <123@vila.Čira-čara>
Date: Mon, 3 Oct 2016 16:55:28 +0200
Received: from mail-it0-f50.google.com
      (mail-it0-f50.google.com [209.85.214.50])
   by mail.ijs.si (Postfix) with ESMTP id 64BC45FB0F
   for <Annika.Settergren@ijs.si>; Mon, 3 Oct 2016 14:55:25 +0000 (UTC)

Hoj, Tomaž in Anica!
.
250 2.0.0 from MTA(smtp:[::1]:10011): 250 2.0.0 Ok: queued as 3snn2132MLzWv
QUIT
221 2.0.0 Bye
```



dnevnik poštnega strežnika (MTA)

Oct 3 18:04:39 dorothy postfix/smtpd[13932]: connect from upc.si.94.140.99.99.dc.cable.static.telemach.net[94.140.99.99]
Oct 3 18:05:13 dorothy postfix-10011/smtpd[10922]: 3snn2132MLzWv: client=upc.si.94.140.99.99.dc.cable.static.telemach.net[94.140.99.99]
Oct 3 18:05:13 dorothy postfix/cleanup[17913]: 3snn2132MLzWv: message-id=<123@vila.Čira-čara>
Oct 3 18:05:13 dorothy postfix/qmgr[41712]: 3snn2132MLzWv: from=<Pippi.Langstrump@gmail.com>, size=1739, nrcpt=1 (queue active)
Oct 3 18:05:13 dorothy postfix/smtp[17691]: 3snn2132MLzWv: to=<mark@mailbox.ijs.si>, orig_to=<Mark.Martinec@ijs.si>, relay=mailbox.ijs.si[2001:1470:ff80::143:1]:125, delay=0.02, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as 3snn2138rrz154)
Oct 3 18:05:13 dorothy postfix/qmgr[41712]: 3snn2132MLzWv: removed
Oct 3 18:05:13 dorothy postfix/smtpd[13932]: proxy-accept: END-OF-MESSAGE: 250 2.0.0 from MTA(smtp:[::1]:10011): 250 2.0.0 Ok: queued as 3snn2132MLzWv; from=<Pippi.Langstrump@gmail.com> to=<Mark.Martinec@ijs.si> proto=ESMTP helo=<Villa-Villekulla.gmail.com>
Oct 3 18:05:16 dorothy postfix/smtpd[13932]: disconnect from upc.si.94.140.99.99.dc.cable.static.telemach.net[94.140.99.99] ehlo=1 mail=1 rcpt=1/3

```
Return-Path: <Pippi.Langstrump@gmail.com>
Received: from mildred.ijs.si ([unix socket])
   by mailbox.ijs.si with LMTPA;
   Mon, 03 Oct 2016 18:05:13 +0200
Received: from mail.ijs.si (mail.ijs.si [IPv6:2001:1470:ff80::25])
   (using TLSv1.2 with cipher AECDH-AES256-SHA (256/256 bits))
   (No client certificate requested)
   by mildred.ijs.si (Postfix) with ESMTPS id 3snn2138rrz154
   for <mark@mailbox.ijs.si>; Mon,  3 Oct 2016 18:05:13 +0200 (CEST)
Received: from amavis-proxy-mx.ijs.si (localhost [IPv6:::1])
   (using TLSv1.2 with cipher ECDHE-RSA-AES128-GCM-SHA256 (128/128 bits))
   (No client certificate requested)
   by mail.ijs.si (Postfix) with ESMTPS id 3snn2132MLzWv
   for <Mark.Martinec@ijs.si>; Mon,  3 Oct 2016 18:05:13 +0200 (CEST)
X-Virus-Scanned: amavisd-new at ijs.si
X-Spam-Status: No, score=4.547 ...
X-Spam-ASN: AS12644 94.140.64.0/19
Received: from mail.ijs.si ([IPv6:::1])
   by amavis-proxy-mx.ijs.si (mail.ijs.si [IPv6:::1]) (amavisd-new, port 10010)
   with ESMTP id GxNLo8pRkdy4 for <Mark.Martinec@ijs.si>;
   Mon,  3 Oct 2016 18:05:10 +0200 (CEST)
Received: from Villa-Villekulla.gmail.com
   (upc.si.94.140.99.99.dc.cable.static.telemach.net [94.140.99.99])
   by mail.ijs.si (Postfix) with ESMTP
   for <Mark.Martinec@ijs.si>; Mon,  3 Oct 2016 18:04:50 +0200 (CEST)
```

```
Subject: Pozdravček
To: Tomaž@mailbox.ijs.si, Anica@mailbox.ijs.si
From: Pika Nogavička <pika@vila.Čira-čara>
Message-ID: <123@vila.Čira-čara>
Date: Mon, 3 Oct 2016 16:55:28 +0200
Received: from mail-it0-f50.google.com
      (mail-it0-f50.google.com [209.85.214.50])
   by mail.ijs.si (Postfix) with ESMTP id 64BC45FB0F
   for <Annika.Settergren@ijs.si>; Mon, 3 Oct 2016 14:55:25 +0000 (UTC)

Hoj, Tomaž in Anica!
```

```
Return-Path: <Pippi.Langstrump@gmail.com>
Received: from mildred.ijs.si ([unix socket])
   by mailbox.ijs.si with LMTPA;
   Mon, 03 Oct 2016 18:05:13 +0200
Received: from mail.ijs.si (mail.ijs.si [IPv6:2001:1470:ff80::25])
   (using TLSv1.2 with cipher AECDH-AES256-SHA (256/256 bits))
   (No client certificate requested)
   by mildred.ijs.si (Postfix) with ESMTPS id 3snn2138rrz154
   for <mark@mailbox.ijs.si>; Mon,  3 Oct 2016 18:05:13 +0200 (CEST)
Received: from amavis-proxy-mx.ijs.si (localhost [IPv6:::1])
   (using TLSv1.2 with cipher ECDHE-RSA-AES128-GCM-SHA256 (128/128 bits))
   (No client certificate requested)
   by mail.ijs.si (Postfix) with ESMTPS id 3snn2132MLzWv
   for <Mark.Martinec@ijs.si>; Mon,  3 Oct 2016 18:05:13 +0200 (CEST)
X-Virus-Scanned: amavisd-new at ijs.si
X-Spam-Status: No, score=4.547 ...
X-Spam-ASN: AS12644 94.140.64.0/19
Received: from mail.ijs.si ([IPv6:::1])
   by amavis-proxy-mx.ijs.si (mail.ijs.si [IPv6:::1]) (amavisd-new, port 10010)
   with ESMTP id GxNLo8pRkdy4 for <Mark.Martinec@ijs.si>;
   Mon,  3 Oct 2016 18:05:10 +0200 (CEST)
Received: from Villa-Villekulla.gmail.com
   (upc.si.94.140.99.99.dc.cable.static.telemach.net [94.140.99.99])
   by mail.ijs.si (Postfix) with ESMTP
   for <Mark.Martinec@ijs.si>; Mon,  3 Oct 2016 18:04:50 +0200 (CEST)
```

```
Subject: Pozdravček
To: Tomaž@mailbox.ijs.si, Anica@mailbox.ijs.si
From: Pika Nogavička <pika@vila.Čira-čara>
Message-ID: <123@vila.Čira-čara>
Date: Mon, 3 Oct 2016 16:55:28 +0200
Received: from mail-it0-f50.google.com
      (mail-it0-f50.google.com [209.85.214.50])
   by mail.ijs.si (Postfix) with ESMTP id 64BC45FB0F
   for <Annika.Settergren@ijs.si>; Mon, 3 Oct 2016 14:55:25 +0000 (UTC)

Hoj, Tomaž in Anica!
```

ključna informacija

MAIL FROM

Return-Path: <Pippi.Langstrump@gmail.com>

HELO / EHLO

Received:
from Villa-Villekulla.gmail.com
(upc.si.94.140.99.99.dc.cable.static.telemach.net
[94.140.99.99])

TCP info (naslov IP, DNS)

by mail.ijs.si (Postfix) with ESMTP

RCPT TO

for <Mark.Martinec@ijs.si>;
Mon, 3 Oct 2016 18:04:50 +0200 (CEST)

Avtomatična analiza glave e-sporočila?

http://whatismyipaddress.com/trace-email

trdi:

The source host name is "mail-it0-f50.google.com" and the source IP address is 209.85.214.50.
Geo-Location Information: Country United States

???

Avtomatična analiza glave e-sporočila?

http://whatismyipaddress.com/trace-email

trdi:

The source host name is "mail-it0-f50.google.com"
and the source IP address is 209.85.214.50.
Geo-Location Information: Country United States

!!! FAIL !!!

Ne ve, kje je meja med domačim (zaupanja vrednim) in tujim poštnim strežnikom.

Kako pridobiti kopijo *celotne neokrnjene* glave

Ne koristi skoraj ničemur:

Subject: RE: Domainverkauf bulkmail.at
Date: Tue, 04 Oct 2016 11:25:30 -0500
From: Walter Knappe <walterknappe24@gmail.com>
To: xxx@example.com

ali še slabše:

RE: Domainverkauf bulkmail.at
Pošiljatelj Walter Knappe le display name, manjka naslov
Prejemnik Me
Datum 2016-10-04 18:25 časovna cona pošiljatelja in sekunde?

Manjka vsaj: Message-ID, Received, Return-Path
Prav pride še: Authentication-Results, DKIM-Signature, …

Kako pridobiti kopijo *celotne neokrnjene* glave

- View → Message → Long headers
- View → Message source
- Options → Internet Headers
- Properties → Details
- Show Original
- View Source
- View Full Headers
- More → Show source / Download
- "hamburger menu" → View → Message source (Control-U)
- forward as attachment

Outlook Express:

1. desni klik na vrhu izbranega sporočila
2. "Properties"
3. "Details" tab
4. Izberi & Kopiraj celotno besedilo v škatli

Pridobili smo podatke: naslovi IP, DNS domene

Zanesljiv podatek:

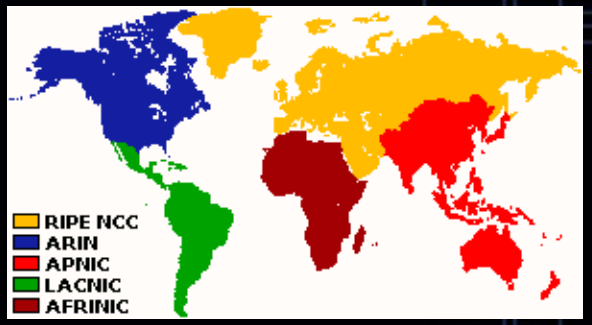
- naslov IP strežnika, ki je dostavil sporočilo v našo administrativno domeno

Zanesljivost ostalih podatkov (npr. From) je odvisna od kredibilnosti strežnikov na poti, prisotnosti veljavnega DKIM podpisa in/ali SPF

Čigav je naslov IP ?

Regional Internet registry (RIR) je organizacija, ki upravlja dodelitev in registracijo naslovov IP in AS številk v regiji sveta.

- RIPE NCC – Réseaux IP Européens Network Coordination Centre
  Evropa, Rusija, srednji vzhod, centralna Azija
- ARIN – American Registry for Internet Numbers
  ZDA, Kanada, deli Karibov, Antarktika
- APNIC – Asia-Pacific Network Information Centre
  Azija, Avstralija, Nova Zelandija in sosednje države
- LACNIC – Latin America and Caribbean Network Information Centre
  Latinska Amerika in deli Karibov
- AFRINIC – African Network Information Center
  Afrika



WHOIS in druga orodja za lociranje IP naslova

- whois klient (Unix/Linux, Sysinternals Windows, Bash on Ubuntu on Windows 10)
- dig, drill, host, nslookup
  (DNS poizvedba: naslov IP → domena)
- traceroute
- http://whatismyipaddress.com/ip-lookup

Geolokacija naslova IP

- država
- regija / zvezna država ZDA
- mesto (najboljši približek)
- zemljepisna širina in dolžina (približek)

  → http://maps.google.com/

Natančnost?

- država 99%
- regija ZDA (40 km polmer) 80%

Kaj pa domene? REGISTER

- neodvisno od naslovov IP, povezava je le DNS
- REGISTER domenskih imen je podatkovna baza imen in pripadajočih podatkov o registrantih. Večina registrov je za vrhnji nivo DNS domen in za drugi nivo.
- IANA (Internet Assigned Numbers Authority) upravlja vrh DNS drevesa in korenske DNS strežnike (in par posebnih DNS con, npr in-addr.arpa, ip6.arpa)
- IANA delegira vse ostale domene drugim registrom, ccTLD delegira nacionalnim registrom
- register.si je del Akademske in raziskovalne mreže Slovenije ARNES in upravlja .si domeno od leta 1992

WHOIS za domene

- whois klient (Unix/Linux, Sysinternals Windows, Bash on Ubuntu on Windows 10)

- http://whois.domaintools.com/
- https://www.whois.net/
- https://www.register.si/
- …

Domain privacy – zasebnost podatkov o domeni

Prijava zlorab

- https://support.google.com/mail/contact/abuse
- …
- abuse@domena, postmaster@domena

- Tržni inšpektorat Republike Slovenije
- SI-CERT: www.cert.si, cert@cert.si
- https://www.varninainternetu.si/

- veliko sreče ☺ …