

Debian/GNU Linux Mailing

Overview of the Mailing

Károly Erdei

December 9, 2009



Agenda

- 1 Mailing
- 2 Protocols
- 3 SPAM
- 4 Antispam
- 5 Thunderbird
- 6 Domain Name System
- 7 Links

Agenda

- 1 Mailing
- 2 Protocols
- 3 SPAM
- 4 Antispam
- 5 Thunderbird
- 6 Domain Name System
- 7 Links

Mailing

Sending e-mails across the Internet

Basics, Terminology

- Message transfer between special hosts (Mail gateways)
 - Mail gateway: dedicated computers to process and transfer e-mails
 - MTA - Mail Transfer Agent: sendmail, exim, postfix..
 - Protocol: SMTP - Simple Mail Transfer Protocol (RFC 821, 1982)
- Message retrieval by mail user agent (MUA)
 - MUAs: Thinderbird, xfmil, pine, etc.
 - POP3: Post Office Protocol, version 3
 - IMAP: Internet Message Access Protocol, version 4
- Representation of messages
 - RFC 822: Basic Message Format (7-bit text only)
 - MIME: Multipurpose Internet Mail Extension (1992)
 - S/MIME: Secure MIME; PGP/MIME: Pretty Good Privacy

Structure and meaning of the e-mail address

E-Mail address: name@domain

- **name:** real name, symbolic name, alias, mailbox name
 - example: john.shaw, secretary, research, johnny
 - mailbox: the place where the messages on the receiving mail gateway will be stored in formats **mbox** or **maildir**
 - mbox format: the messages will be stored in one file; new message will be appended; delimiter: empty line; begins with: ^ From
 - maildir: each message will be stored as a separate file in the directory
 - alias: an alternative name which translates to the name of the mailbox
- **domain:** DNS domain name (risc.jku.at, jku.at)
 - defines MX resource record which host deliver the messages to
 - there can be more mail exchangers (mail gateways) for the domain

```
;; QUESTION SECTION:
;risc.uni-linz.ac.at.          IN      MX
;; ANSWER SECTION:
risc.uni-linz.ac.at. 1363 IN  MX  20 bullfinch.risc.uni-linz.ac.at.
risc.uni-linz.ac.at. 1363 IN  MX  30 grauwal.risc.uni-linz.ac.at.
```

e-Mail Transfer Process

Message transfer process in overview

User sends a message

- to the local (e.g. RISC) mail gateway by the MUA (e.g. Thunderbird)
- Local mail gateway
 - first spools message locally in the spool area `/var/spool/mqueue`
 - after transfers message from the spool area to the recipients (remote) mail gateway

Local mail gateway receives a message for a user

- from the mail gateway of remote senders
- Received message is placed into the **mailbox** of the user on the local mail gateway

User downloads the message (e.g. by Firefox, POP) from

- the local mail gateway to laptop or PC's home directory

e-Mail Transfer Process - gateways

SMTP speaking processes on mail gateways transfer mails

Process for background transfer is client of remote mail server

- Uses DNS (Domain Name System) to determine name of mail exchanger for destination domain
 - DNS responses MX resource record for domain
- Uses DNS to map name of mail exchanger to IP address
- Creates TCP connection to server process on mail gateway
- Transfers copy of message to server, which stores copy in mailbox
- If transfer succeeds, sending process removes copy from mail queue
- If connection cannot be established, records time of transfer attempt in the mail queue entry for the message and terminates

Process for background transfer periodically sweeps spool area

- Spooled mail can be delivered as soon as mail exchanger is up again
- If spooled mail cannot be delivered after some extended time (default 5 days), process returns message to sender

Agenda

- 1 Mailing
- 2 Protocols
- 3 SPAM
- 4 Antispam
- 5 Thunderbird
- 6 Domain Name System
- 7 Links

Mailing, Internet Standards (STDs)

SMTP - Transfer Protocol

STD 10 / RFC 821: Simple Mail Transfer Protocol

- Specifies how messages are passed from one host to another
- Communication is based on readable ASCII text commands

```
R: 220 uhu.risc.uni-linz.ac.at ESMTP Sendmail 8.13.8
S: HELO sender hostname                      R: 250 OK
S: MAIL FROM: <e-mail address>              R: 250 OK
S: RCPT TO:  <e-mail address>                R: 250 OK
S: DATA
R: 354 Start mail input; end with <CRLF>.<CRLF>
S: <CRLF>.<CRLF>                             R: 250 OK
S: quit                                       R: 221 name closing
```

- other commands: VRFY Smith; EXTN secretary
- Mail server/clients understand extended version (ESMTP)
 - ESMTP is requested by client via EHLO instead of HELO
 - ENHANCEDSTATUSCODES, 8BITMIME, AUTH DIGEST-MD5
CRAM-MD5 PLAIN, STARTTLS

Mailing, Internet Standards (STDs)

Message Format for english text

STD 11 / RFC 822: Basic Message Format

- 7-bit ASCII format, primarily for english text
 - only plain text, binary must be converted
- Mail header and Mail body is separated by an empty line
 - Mail header begins with a **From** line in mbox format
- Mail header - User Fields - provided by MUA
 - From: To: Cc: Subject: Sender: Bcc:
 - Bcc: not visible in header
 - All of them can be set by most of the MUA: used by spammers, they fake the header lines
- Mail header - Automatic Fields - provided by MUA,MTA
 - Date: Message-Id: **Return-path:** **Received:**, X-fields
 - Received: can follow the mail gateways as e-mails pass them

MIME: Multipurpose Internet Mail Extension

How to send other contents as ASCII text

RFC 1341: Messages in other character sets and with binary contents

- Use RFC 822 basic message format
 - MIME messages can be transferred by normal (older) SMTP agents
 - Only mail reader/writer (MUA) must be MIME enabled
- Define additional header fields:
 - MIME-Version: , Content-Id:
 - Content-Transfer-Encoding: How content is encoded as ASCII
 - Content-Type: MIME-type of content
 - Content-Description: Human-readable description of content
- Content-Transfer-Encoding:
 - 7-bit, Quoted-Printable, Base64 (for binary data); 8-bit; Binary
- Content-Type: 7 MIME types with multiple subtypes
 - Text, Image, Audio, Video, Application, Message, Multipart,
- Content Subtypes: text/plain, text/richtext, message/rfc822
 - application/octet-stream, application/PostScript multipart/mixed, multipart/alternative

e-Mail Security

Use cryptographic methods !

Email is not a secure communication medium

- **Reliability:** messages may be lost
 - Only transfer from mail queue to next mail server is guaranteed
 - User may be asked to confirm receipt of a message
 - Header field `Disposition-Notification-To:` *address*
- **Privacy:** messages may be read by unauthorized persons
 - Messages are transferred in clear text
- **Authenticity:** message sender may be faked
 - It is easy to create messages with faked `From:` fields
- **Integrity:** message content may be changed
 - Intermediate transfer agent may modify message
- Integrity, Authenticity, Privacy achieved by cryptographic methods
 - Privacy: by Encryption
 - Integrity, Authenticity: by Digital signatures

Emails are as secure as postcards are without cryptographic methods

Agenda

- 1 Mailing
- 2 Protocols
- 3 SPAM
- 4 Antispam
- 5 Thunderbird
- 6 Domain Name System
- 7 Links

SPAM living with it

spam is dangerous

What is SPAM

- nearly identical messages sent to numerous recipients by e-mail
- any email message where the senders identity is forged
- common synonyms for spam
 - UBE: unsolicited bulk e-mail
 - UCE: unsolicited commercial e-mail

Problems with SPAM

- contains an attachment which is a **virus/trojan**
 - to became your Windows PC a **bot net** host
- **phishing**: spam ask users to enter personal information on fake Web sites using e-mail forged to look like it is from a bank or other organization such as PayPal
- **spoofing**: your e-mail address used as sender of spam
 - you get all bounced mails (500-5000 in short time)
- spam contains links to advertised/malicious web sites

SPAM living with it

How spammers work

- collecting e-mail addresses
 - from chatrooms, websites, newsgroups
 - infecting Windows PCs, where viruses collect address books
- sending spam mails
 - using open mail gateways (not anymore)
 - using **bot nets**, by infecting Windows PCs with viruses, Trojans
- dictionary attacks
 - spammer sends e-mail based on dictionary
 - 150.000 rejected by blacklists + 40.000 dictionary attack

Main problem to fight SPAM

- governments did not accept appropriate law against spammers, SPAM
- law only in some countries: in EU, Australia
- EU: SPAM for direct marketing are not allowed without the consent or in respect of the subscriber (receiver of spam)

SPAM living with it

Origin of spam, statistics

Origin of SPAM

- Origin of spam refers to the geographical location of the computer from which the spam is sent
- the spammer, the hijacked spam-sending computer, the spamvertised server, and the user target of the spam are all often located in different countries
- As much as 80% of spam received by Internet users in North America and Europe can be traced to fewer than 200 spammers

Statistics

- total volume of spam April 2008: over 100 billion emails/day
- 90% of incoming email traffic is spam in NA,EU, Australasia
- 96.5% of e-mail received by businesses was spam by June 2008

Living with SPAM

Statistics (checked Dec 2009 by Wikipedia)

Origin of spam in the third quarter of 2008

- * The United States (18.9%, up from 14.9% in Q2)
- * Russia (8.3%, up from 7.5%)
- * Turkey (8.2%, up from 6.8%)
- * China (5.4%, down from 5.6%)
- * Brazil (4.5%, unchanged)

When grouped by continents, spam comes mostly from:

- * Asia (39.8%, up from 35.4%)
- * Europe (23.9%, down from 29.5%)
- * North America (21.8%, up from 18.2%)
- * South America (13.2%, down from 14.8%)

Number of IP addresses used for spamming

- * top three as the United States, China, and Russia
- * followed by Japan, Canada, and South Korea

Agenda

- 1 Mailing
- 2 Protocols
- 3 SPAM
- 4 Antispam
- 5 Thunderbird
- 6 Domain Name System
- 7 Links

Antispam techniques I

What the end user can and should do

Give your e-mail address only to trusted persons/sites

- never put your e-mail address in text form to a web site
- post to lists as anonym, use faked, invalid email address and name
- avoid responding to spam
 - dont use links: remove me from the list (you'll confirm your e-mail address)
 - be carefull with your **vacation** message: you can send a reply to a spammer
- don't use contact forms on web sites: (problems with server side scripting)
- don't register anywhere with real e-mail address (I hope, amazon.de is ok, but other sites ?)
- use temporary e-mail addresses (if possible)
 - the e-mail address (alias) expires after a given time

Do **NOT** read and send HTML emails

Antispam techniques II

Be careful using and configuring your mail program

- don't use html in e-mail programs (MUA) !
 - set the outgoing mail format to **PLAIN TEXT**
 - for an e-mail message it is not necessary to use html
 - you can use any type of attachment (to send .doc, .jpg, etc. files)
- RISKS by reading HTML formatted e-mails
 - mail client starts a browser or the function of browser is integrated
 - html browser interpret the contents automatically (check settings)
 - they start scripts, download, show images, without asking you
 - html spam can contain **scripst**, which allow spammer to spy your computer (address, etc) **spyware** will may be installed
 - html spam can contain web **bugs**, which allow spammer to get further information from you, save viruses, Trojans, you became a **bot net** host, etc.
- mail clients which don't display html, attachments, images have fewer risk !

Antispam techniques

Using SpamAssassin (SA)

SA - email spam filtering based on content-matching rules

- uses a variety of spam-detection techniques
 - DNS-based and checksum-based spam detection
 - Bayesian filtering, blacklists and online databases
- can be integrated with the mail server
 - to automatically filter all mail for a site
- awarded: Linux New Media Award 2006
 - Best Linux-based Anti-spam Solution

Operation

- uses large set of rules to decide e-mail is spam or ham
 - rule (called test in SA) bases mostly on regular expression to decide spam contents
- each test has a score value to assign to e-mail, if matches
 - positive value indicates spam, negative ham
- all test combine the results in a global score

SpamAssassin

The RISC setup, how to use it

How to tune the default configuration

- all e-mails at RISC will be checked by SA
- you can use **procmail** to sort your e-mails in folders
 - to learn: `man procmail`; `man .procmailrc`;
 - RISC User Guides: How to configure SpamAssassin for your needs
- configuration file: **`.spamassassin/user_prefs`**
- you can change, tune the values for different variables:
 - change the value for **`required_hits`** **3.0**
 - change the score value for the different checks by setting it to zero
- configure your white list or blacklist
 - `whitelist_from @jku.at`
 - this will let through all e-mails with `@jku.at`, faked addresses, too !
 - `blacklist_from @hknetmail.com`
- use **sa-learn** to tune the Bayesian algorithm
`sa-learn --spam --mbox /path/to/spaminput`

Agenda

- 1 Mailing
- 2 Protocols
- 3 SPAM
- 4 Antispam
- 5 Thunderbird
- 6 Domain Name System
- 7 Links

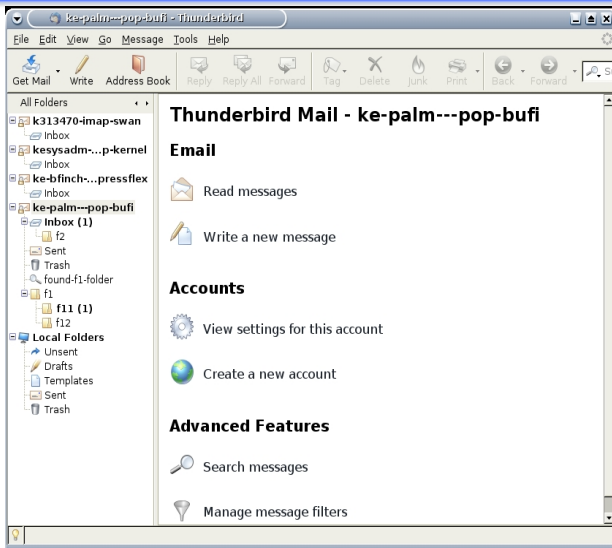
Mozilla Thunderbird

current version 2.0.0.23

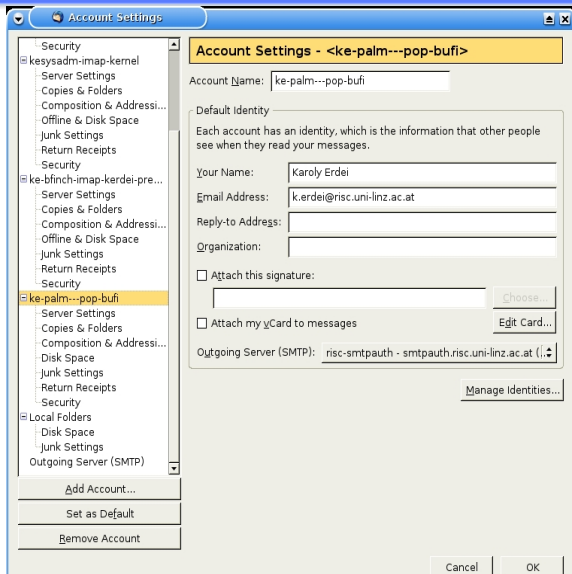
Thunderbird is the best free MUA

- free, open source, cross-platform e-mail and news client
- supports multiple e-mail, newsgroup and RSS accounts
 - supports multiple identities within accounts
- Spam mail filtering
 - own Bayesian spam filter
 - whitelist, based on the included address book
 - understands the classifications of SpamAssassin
- Standards supported natively
 - POP and IMAP with SSL/TLS,
 - S/MIME secure email (digital signing and message encryption using certificates)
 - PGP signing, encryption, and decryption by the **Enigmail** extension
- Security protection includes
 - disabling loading of remote images within messages
 - disabling JavaScript
- Additional features are available via extensions

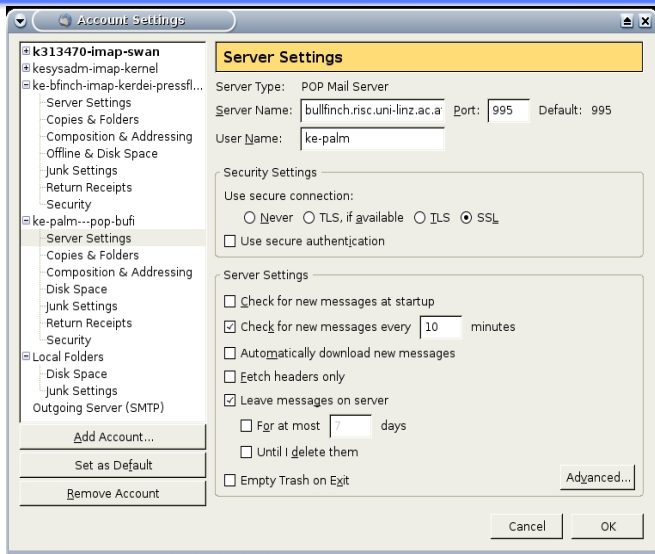
Main Window of Thunderbird



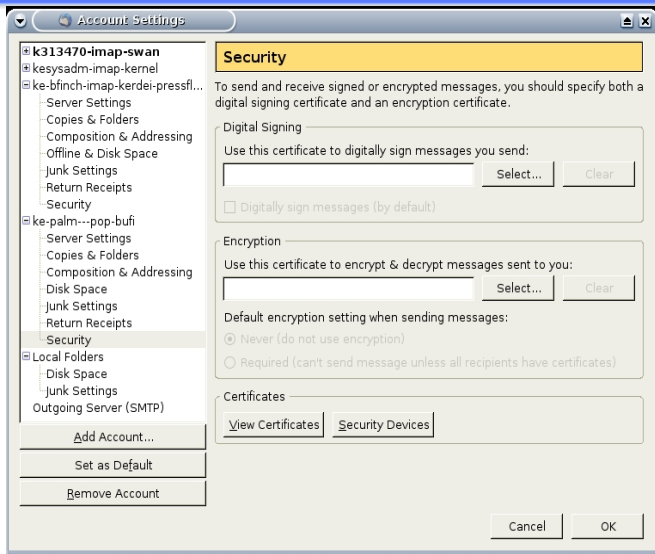
Settings for an email account



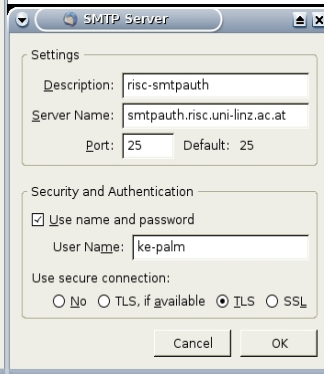
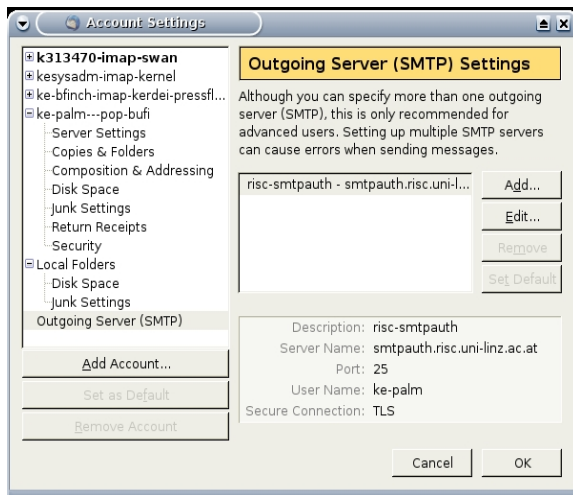
Setting the incoming mail server



Security setting: sign and encrypt an e-mail

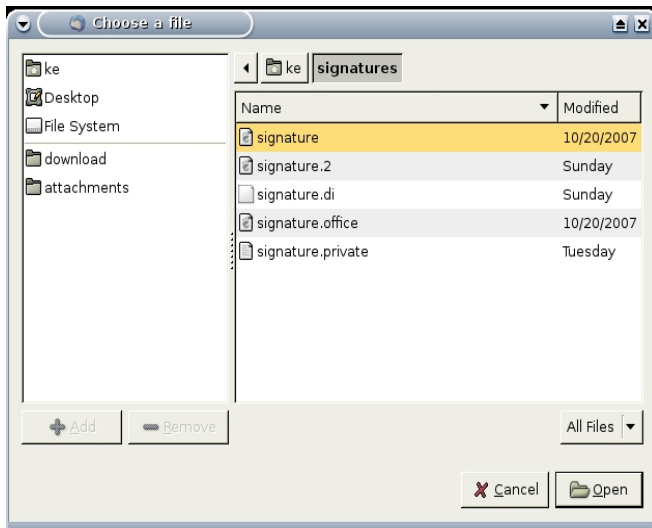


Setting the smtp out host



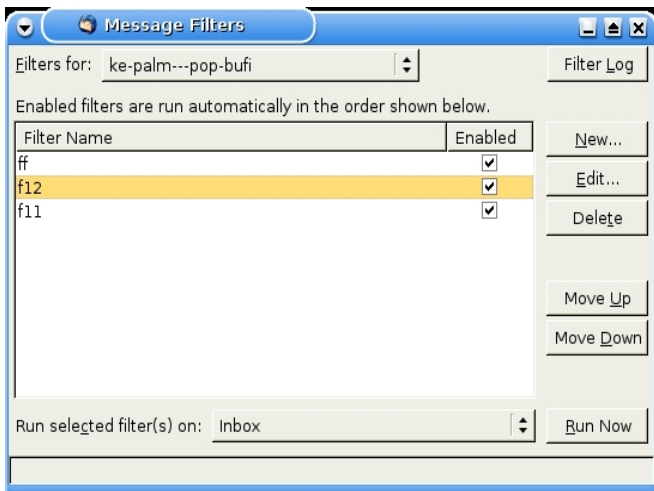
Using more signatures

Account properties

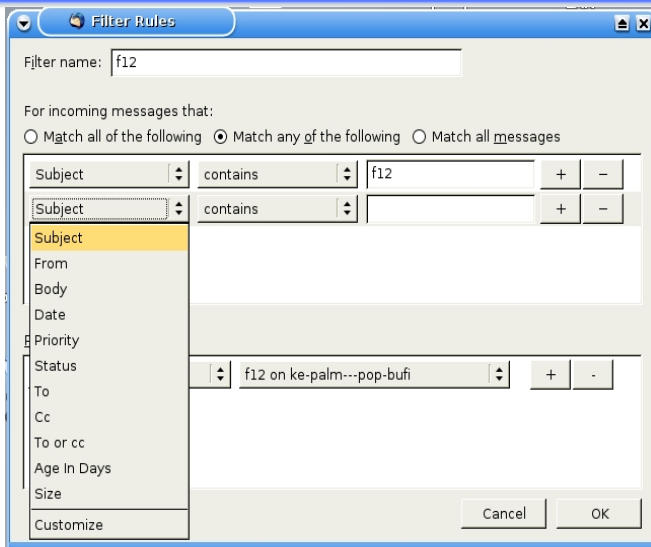


Using message filters

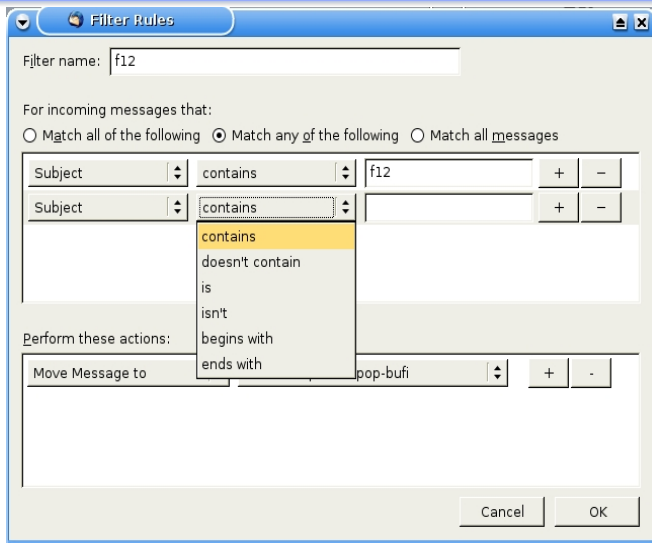
Tools/Message Filters



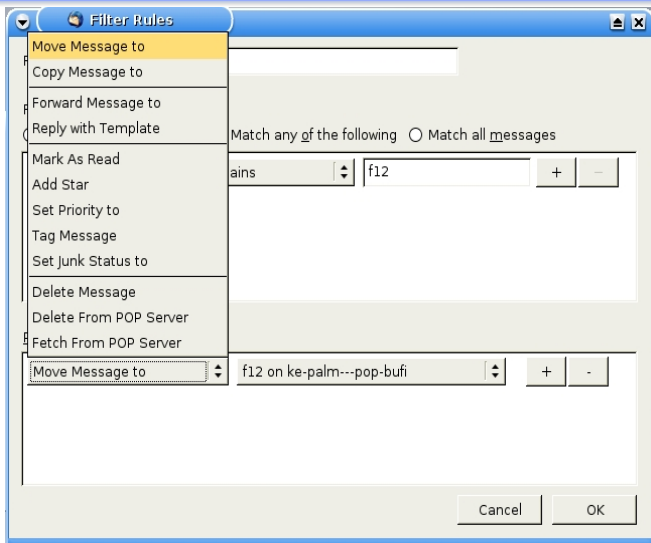
Using message filters - Which field to filter



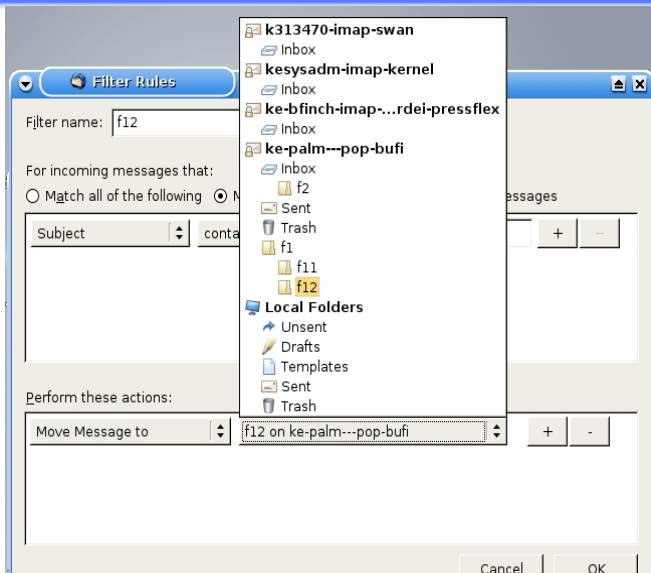
Using message filters - Set relation



Using message filters - Set action



Using message filters - Set destination



Using Folders and Virtual Folders

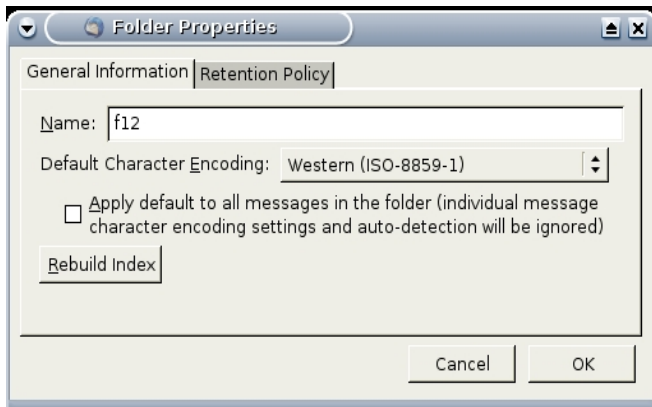
Using Folders

- Thunderbird uses **mbox** format to save the e-mails
- folder consist any number subfolders but only one mbox folder
- folders have tree structure
- you can create folders on static critearia
 - folder: CBWE; subfolders: questionnaire, lecturer, etc.

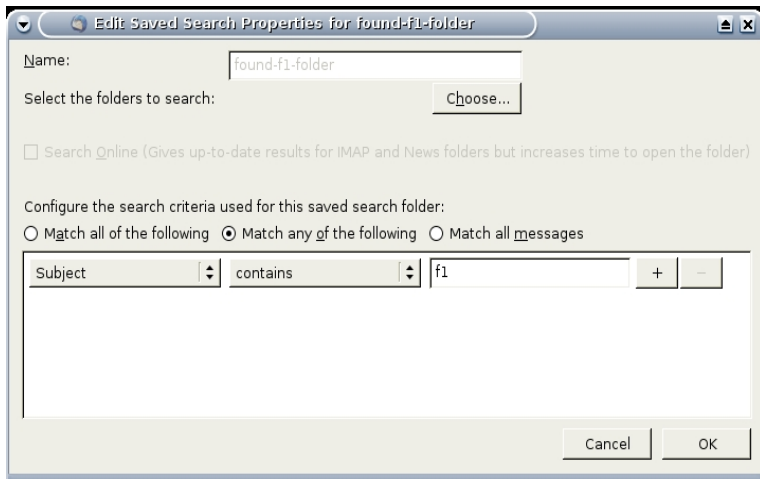
Using Virtual Folders (VF)

- creating virtual folders:
 - specify a set of search criteria on messages, accounts
 - save the search as a **virtual folder**
- you work with the virtual folders as a conventional folder
- you can dinamically rerun the search each time
- you can always modify the search criteria
- VF is not a real folder, no messages are moved into it

Folder properties

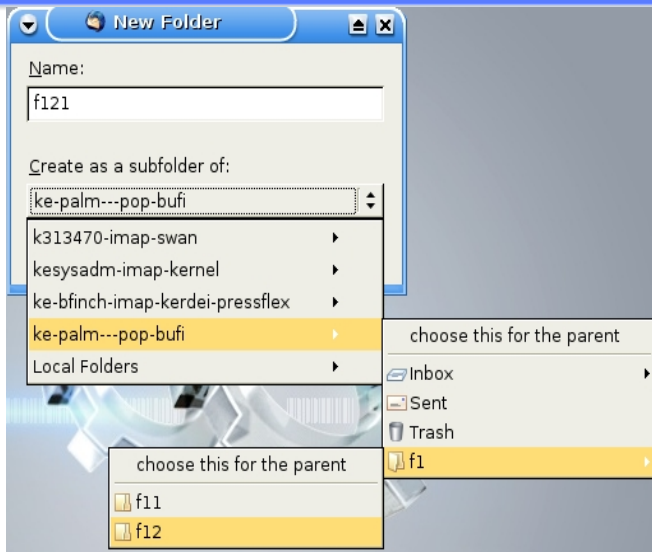


Virtual folder properties



Creating new folder

For accounts and folders as subfolder



Searching in folders

Preparing creation of Virtual Folder

Search Messages

Search for messages in:

☒ Search subfolders

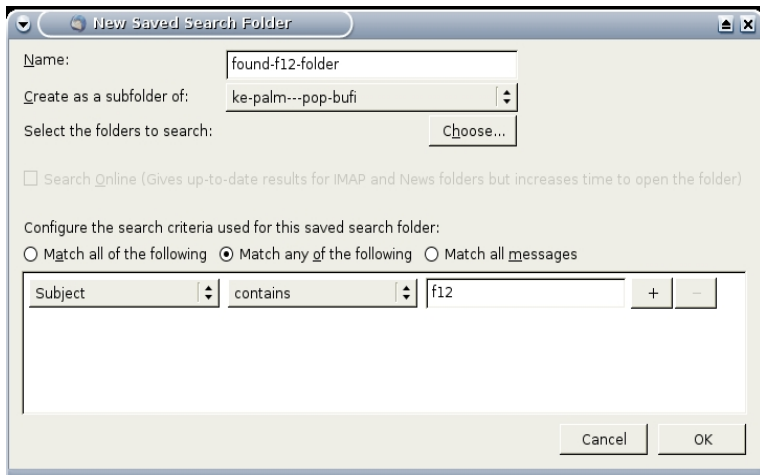
☐ Match all of the following ☒ Match any of the following

Subject	Sender	Date	Priority	Location	
f12	Karoly Erdei	11/12/2008 09:16 PM		Sent	
f12	Karoly Erdei	11/12/2008 09:20 PM		Sent	
f12	Karoly Erdei	11/12/2008 09:21 PM		Sent	
f12	Karoly Erdei	11/12/2008 09:25 PM		Sent	
f12	Karoly Erdei	11/12/2008 09:41 PM		Sent	
f12	Karoly Erdei	11/12/2008 09:41 PM		f12	
f12	Karoly Erdei	11/12/2008 09:16 PM		Trash	

10 matches found

New saved search folder

Create new Virtual Folder



The screenshot shows the 'New Saved Search Folder' dialog box. The title bar reads 'New Saved Search Folder'. Inside the dialog, the 'Name:' field contains 'found-f12-folder'. The 'Create as a subfolder of:' dropdown menu is set to 'ke-palm---pop-bufi'. Below this, the 'Select the folders to search:' label is followed by a 'Choose...' button. A checkbox for 'Search Online' is present, with a note in parentheses: '(Gives up-to-date results for IMAP and News folders but increases time to open the folder)'. Under the heading 'Configure the search criteria used for this saved search folder:', there are three radio buttons: 'Match all of the following' (unselected), 'Match any of the following' (selected), and 'Match all messages' (unselected). Below the radio buttons is a search criteria table with two columns: a dropdown menu for the field name and a text input for the search term. The first row shows 'Subject' in the dropdown, 'contains' in the operator dropdown, and 'f12' in the text input. To the right of the text input are '+' and '-' buttons. At the bottom right of the dialog are 'Cancel' and 'OK' buttons.

Name: found-f12-folder

Create as a subfolder of: ke-palm---pop-bufi

Select the folders to search: Choose...

☐ Search Online (Gives up-to-date results for IMAP and News folders but increases time to open the folder)

Configure the search criteria used for this saved search folder:

☐ Match all of the following ☒ Match any of the following ☐ Match all messages

Subject	contains	f12	+	-
---------	----------	-----	---	---

Cancel OK

Agenda

- 1 Mailing
- 2 Protocols
- 3 SPAM
- 4 Antispam
- 5 Thunderbird
- 6 Domain Name System
- 7 Links

Domain Names System

DNS - Domain Names

- This section has been removed from the course material 2009
- If you are interested in DNS please
 - search in Google for material
 - check the short overview in the CBWE 2008 material (Mailing)

Agenda

- 1 Mailing
- 2 Protocols
- 3 SPAM
- 4 Antispam
- 5 Thunderbird
- 6 Domain Name System
- 7 Links**

User Guides at RISC for Mailing

The RISC setup

Configuration Mailing

- <https://www.risc.uni-linz.ac.at/internals/userinformation/completeguide/userguides/mailing/client-ssl/client-ssl.html>
- <https://www.risc.uni-linz.ac.at/internals/userinformation/completeguide/userguides/mailing/smtp-relay/smtp-relay.html>

Procmail

- <https://www.risc.uni-linz.ac.at/internals/userinformation/completeguide/userguides/mailing/procmail.html>

Spamassassin

- <https://www.risc.uni-linz.ac.at/internals/userinformation/completeguide/userguides/mailing/spamassassin/spamassassin.html>

End of Mailing

Thanks for your attantion !