Debian/GNU Linux Mailing

Overview of the Mailing

Károly Erdei

November 15, 2010

Agenda

1. Mailing
2. Protocols
3. SPAM
4. Antispam
5. Thunderbird
6. Links

Agenda

1. Mailing
2. Protocols
3. SPAM
4. Antispam
5. Thunderbird
6. 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, xfmail, 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: ˆ 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.
risc.uni-linz.ac.at.  1363  IN  MX  30 grauwal.risc.uni-linz.ac
```

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

Agenda

1 Mailing

2 Protocols

3 SPAM

4 Antispam

5 Thunderbird

6 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

```
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)
  - ESMPT is requested by client via `EHLO` instead of `HELO`
  - ENHANCEDSTATUSCODES, 8BITMIME, AUTH DIGEST-MD5 CRAM-MD5 PLAINE, 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 im 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 guarantueed
  - 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 achived by cryptographic methods
  - Privacy: by Encryption
  - Integrity, Authenticity: by Digital signatures

Emails are as secure as postcards are without cryptographic methods

POP - Post Office Protocol

POP - available and supported by ISP

- Many e-mail clients support POP and IMAP to retrieve messages
- supports simple download-and-delete requirements for access to remote mailboxes
- POP3s uses SSL by the port 995
- handles also MIME emails
- simple message identifying mechanism

IMAP - Internet Mail Access Protocol

IMAP - should be preferred against POP

- current version IMAP4
- client can stay connected
- users with many or large messages get faster response times
- Multiple clients simultaneously connected to the same mailbox
- Access to MIME message parts and partial fetch
- Message state information (are stored on the server)
- Multiple mailboxes on the server
- Server-side search (client to ask the server to search messages; no prior download)
- complex IMAP server implementation problem
- IMAPs uses SSL over the port 993

Agenda

1 Mailing

2 Protocols

3 SPAM

4 Antispam

5 Thunderbird

6 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

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 collects 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 again 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)

Living with SPAM

Statistics (checked Dec 2009 by Wikipedia)

Origin of spam (volume) in the fourth quarter of 2008

* The United States (19.8%, up from 18.9% in Q2)
* China (9.9%, up from 5.4%)
* Russia (6.4%, down from 8.3%)
* Brazil (6.3%, up from 4.5%)
* Turkey (4.4%, up from 8.2%)

When grouped by continents, spam comes mostly from:

* Asia (37.8%, down from 39.8%)
* North America (23.6%, up from 21.8%)
* Europe (23.4%, down from 23.9%)
* South America (12.9%, down from 13.2%)

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 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
- uses large set of rules to decide e-mail is spam or ham

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
- use sa-learn to tune the Bayesian algoritm

```
sa-learn --spam --mbox /path/to/spaminput
```

Agenda

1 Mailing

2 Protocols

3 SPAM

4 Antispam

5 Thunderbird

6 Links

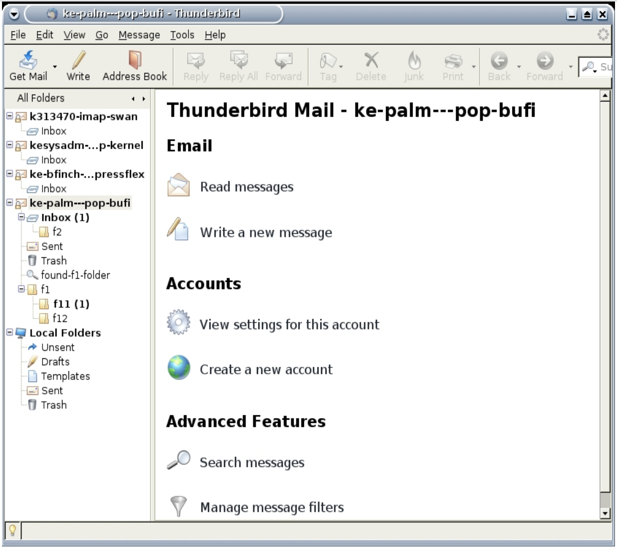
Mozilla Thunderbird

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
- Standars 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



Thunderbird Mail - ke-palm---pop-bufi

Email

Read messages

Write a new message

Accounts

View settings for this account

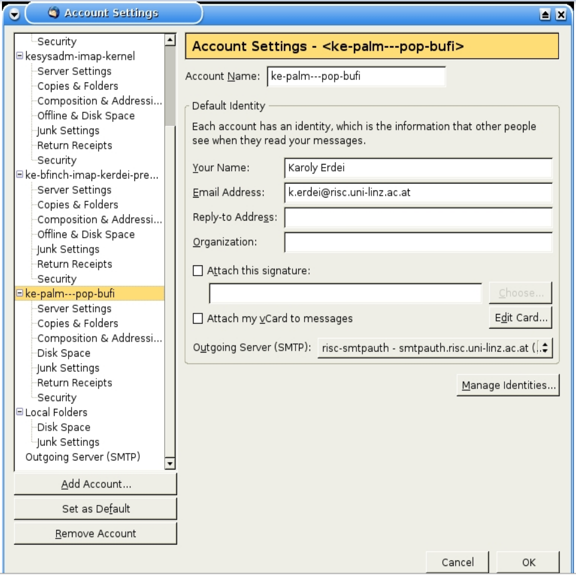
Create a new account

Advanced Features

Search messages

Manage message filters

Settings for an email account



Account Settings - <ke-palm---pop-bufi>

Account Name: ke-palm---pop-bufi

Default Identity

Each account has an identity, which is the information that other people see when they read your messages.

Your Name: Karoly Erdei

Email Address: k.erdei@risc.uni-linz.ac.at

Reply-to Address:

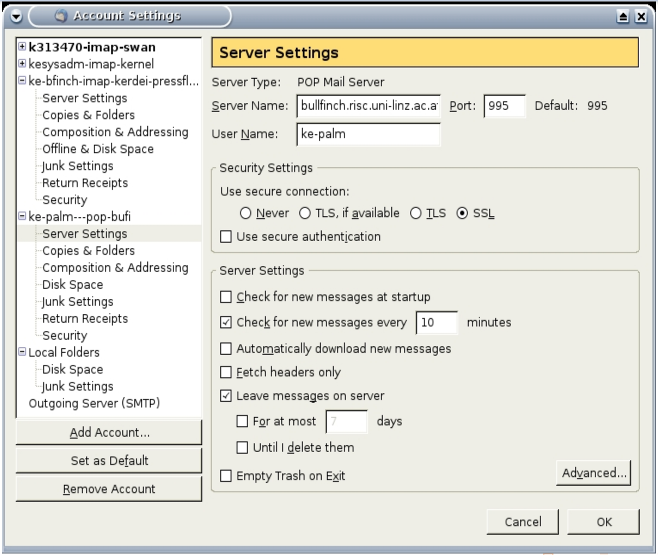
Organization:

☐ Attach this signature:

☐ Attach my vCard to messages

Outgoing Server (SMTP): risc-smtpauth - smtpauth.risc.uni-linz.ac.at (...

Setting the incoming mail server



Server Settings

Server Type: POP Mail Server

Server Name: bullfinch.risc.uni-linz.ac.a Port: 995 Default: 995

User Name: ke-palm

Security Settings

Use secure connection:

○ Never ○ TLS, if available ○ TLS ● SSL

□ Use secure authentication

Server Settings

□ Check for new messages at startup

☑ Check for new messages every 10 minutes

□ Automatically download new messages

□ Fetch headers only

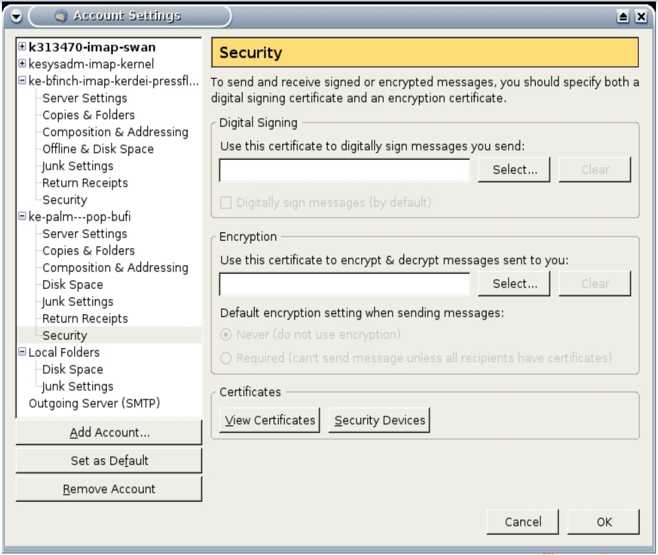
☑ Leave messages on server

□ For at most 7 days

□ Until I delete them

□ Empty Trash on Exit

Security setting: sign and encrypt an e-mail



Account Settings

- ⊞ **k313470-imap-swan**
- ⊞ kesysadm-imap-kernel
- ⊟ ke-bfinch-imap-kerdei-pressfl...
  - Server Settings
  - Copies & Folders
  - Composition & Addressing
  - Offline & Disk Space
  - Junk Settings
  - Return Receipts
  - Security
- ⊟ ke-palm---pop-bufi
  - Server Settings
  - Copies & Folders
  - Composition & Addressing
  - Disk Space
  - Junk Settings
  - Return Receipts
  - Security
- ⊟ Local Folders
  - Disk Space
  - Junk Settings
- Outgoing Server (SMTP)

Security

To send and receive signed or encrypted messages, you should specify both a digital signing certificate and an encryption certificate.

Digital Signing

Use this certificate to digitally sign messages you send:

☐ Digitally sign messages (by default)

Encryption

Use this certificate to encrypt & decrypt messages sent to you:

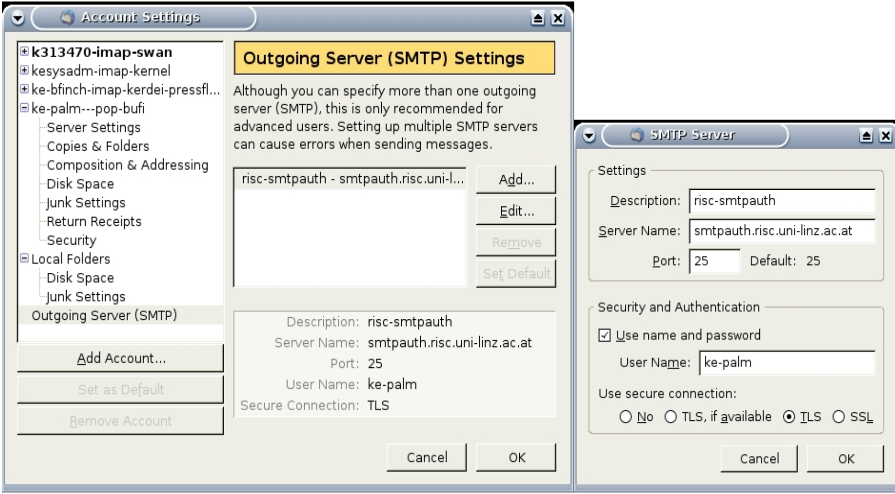
Default encryption setting when sending messages:

● Never (do not use encryption)

○ Required (can't send message unless all recipients have certificates)

Certificates

Setting the stmp out host



Outgoing Server (SMTP) Settings

Although you can specify more than one outgoing server (SMTP), this is only recommended for advanced users. Setting up multiple SMTP servers can cause errors when sending messages.

risc-smtpauth - smtpauth.risc.uni-l...

Description: risc-smtpauth
Server Name: smtpauth.risc.uni-linz.ac.at
Port: 25
User Name: ke-palm
Secure Connection: TLS

Settings

Description: risc-smtpauth
Server Name: smtpauth.risc.uni-linz.ac.at
Port: 25 Default: 25

Security and Authentication

☑ Use name and password

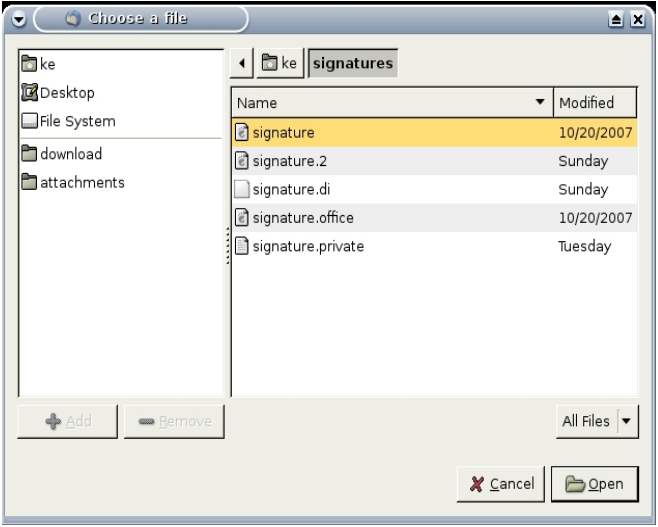
User Name: ke-palm

Use secure connection:

○ No ○ TLS, if available ● TLS ○ SSL

Using more signatures

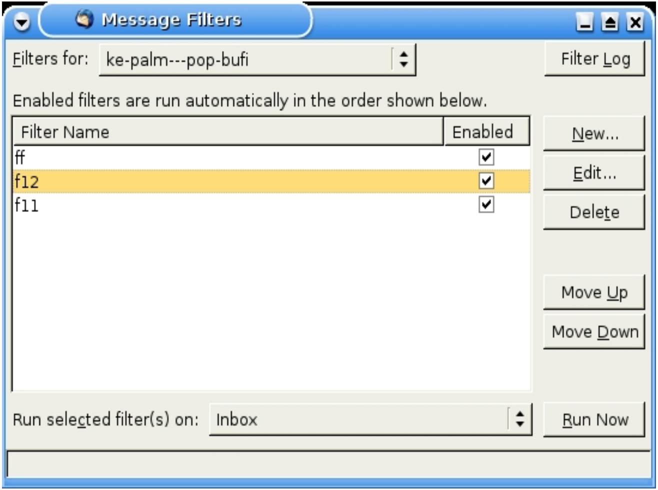
Account properties



Name	Modified
signature	10/20/2007
signature.2	Sunday
signature.di	Sunday
signature.office	10/20/2007
signature.private	Tuesday

Using message filters

Tools/Message Filters



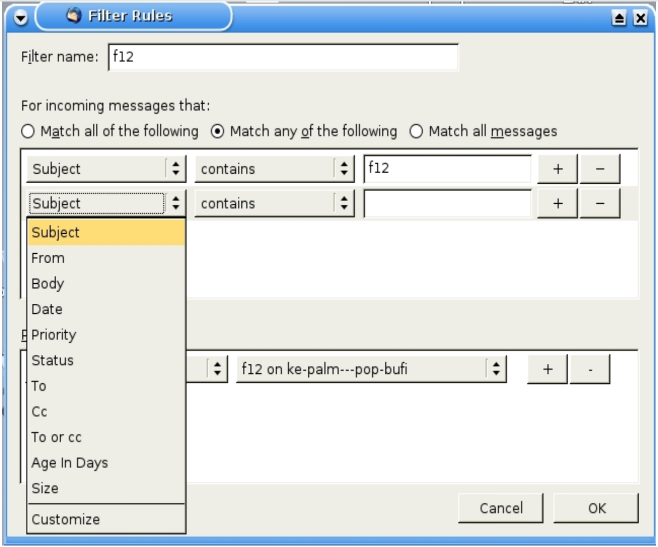
Filters for: ke-palm---pop-bufi

Enabled filters are run automatically in the order shown below.

Filter Name	Enabled
ff	☑
f12	☑
f11	☑

Run selected filter(s) on: Inbox

Using message filters - Which field to filter



Filter name: f12

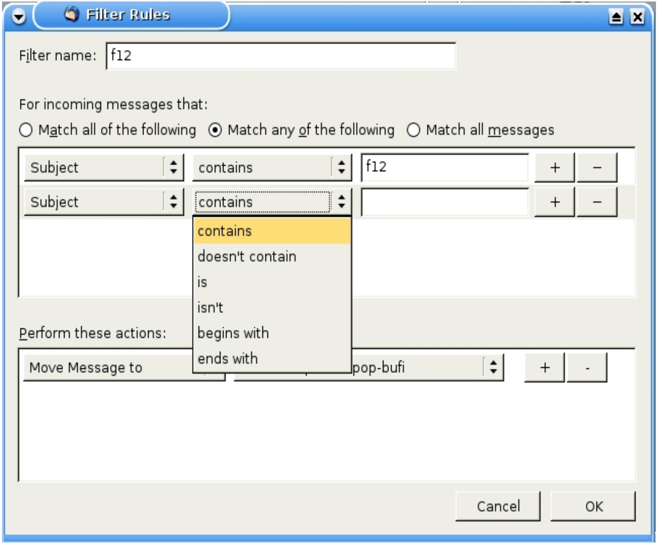
For incoming messages that:

○ Match all of the following ● Match any of the following ○ Match all messages

Subject contains f12

Subject contains

Using message filters - Set relation



Filter name: f12

For incoming messages that:

○ Match all of the following ● Match any of the following ○ Match all messages

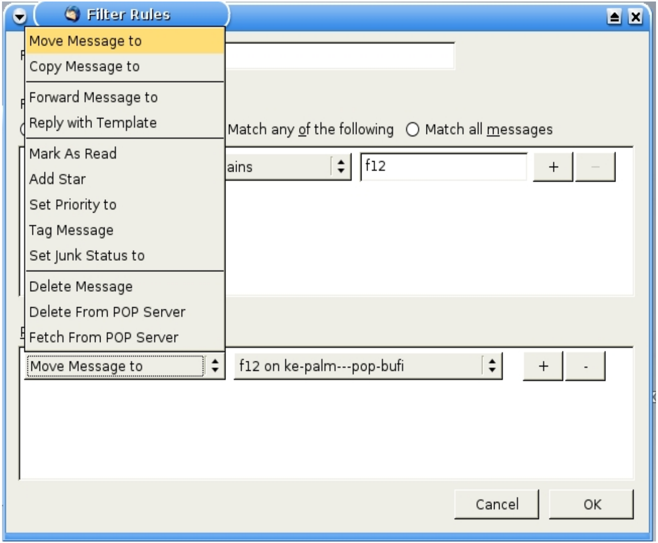
Subject contains f12

Subject contains

Perform these actions:

Move Message to pop-bufi

Using message filters - Set action

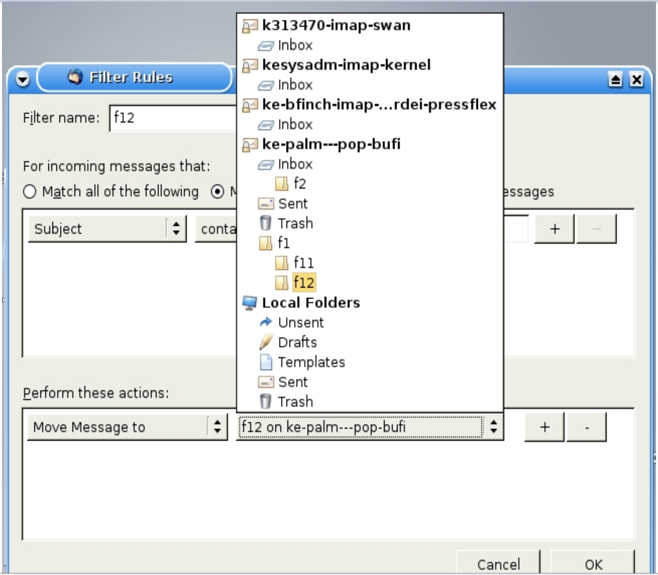


Match any of the following ○ Match all messages

ains f12

Move Message to f12 on ke-palm---pop-bufi

Using message filters - Set destination



Filter Rules

Filter name: f12

For incoming messages that:

○ Match all of the following ● M

Subject | conta

Perform these actions:

Move Message to | f12 on ke-palm---pop-bufi

Using Folders and Virtual Folders

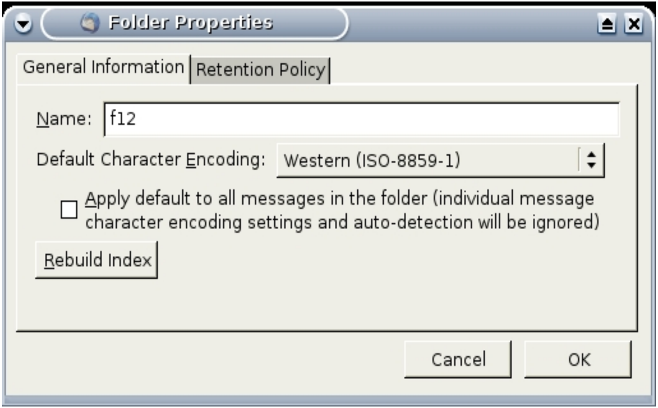
Using Folders

- 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 criteaaria
  - folder: CBWE; subfolders: questionaire, 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



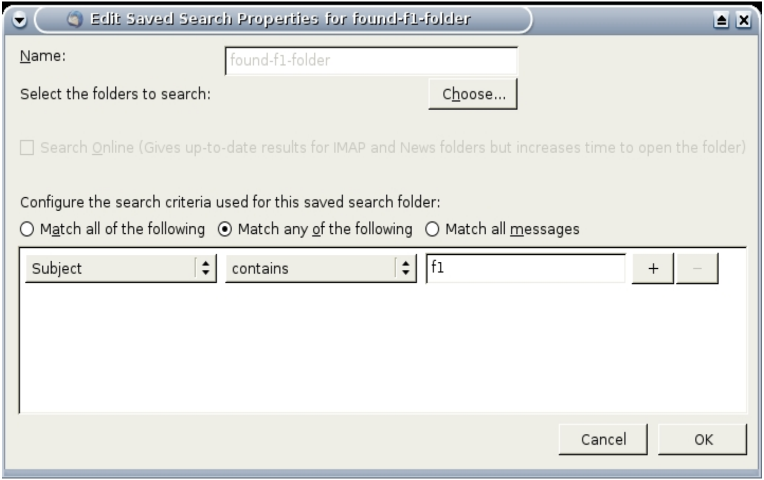
Folder Properties

Name: f12

Default Character Encoding: Western (ISO-8859-1)

□ Apply default to all messages in the folder (individual message character encoding settings and auto-detection will be ignored)

Virtual folder properties



Edit Saved Search Properties for found-f1-folder

Name: found-f1-folder

Select the folders to search:

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

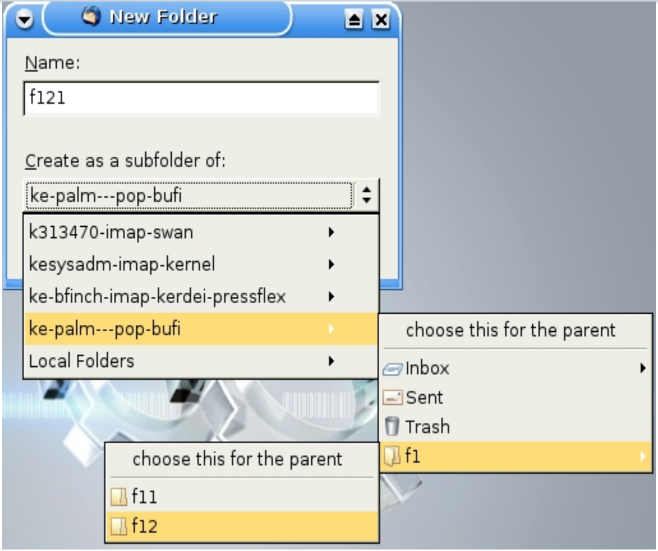
Configure the search criteria used for this saved search folder:

○ Match all of the following ● Match any of the following ○ Match all messages

Subject contains f1

Creating new folder

For accounts and folders as subfolder



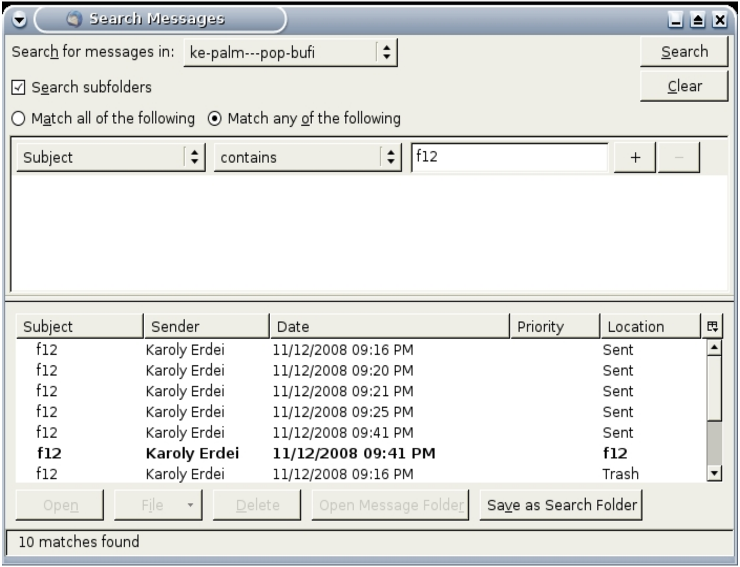
New Folder

Name: f121

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

Searching in folders

Preparing creation of Virtual Folder



Search for messages in: ke-palm---pop-bufi

☑ Search subfolders

○ Match all of the following ● Match any of the following

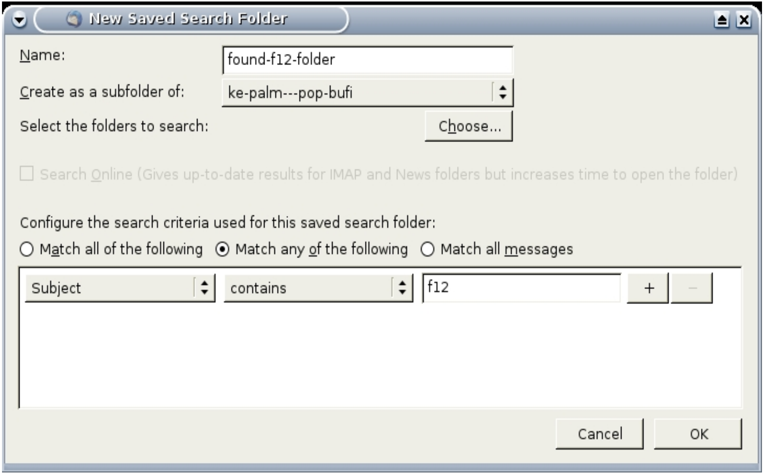
Subject contains f12

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



New Saved Search Folder

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

Agenda

1 Mailing

2 Protocols

3 SPAM

4 Antispam

5 Thunderbird

6 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 !