

Podpůrné nástroje CSIRTu

**Schedule-shift, Run-or-raise
Envelope, Convey**

Edvard Rejthar • edvard.rejthar@nic.cz • 14. 11. 2019



Spolufinancováno Evropskou unií
Nástroj pro propojení Evropy



cz.nic | SPRÁVCE
DOMÉNY CZ

Contents...

- Schedule-shift ...
- Run-or-raise ...
- Envelope ...
- Convey ...



Contents

- **Schedule-shift** <https://github.com/CZ-NIC/schedule-shift>
- Run-or-raise <https://extensions.gnome.org/extension/1336/run-or-raise/>
- Envelope `pip3 install envelope`
- Convey `pip3 install convey`



Schedule shift – overview



- Small team
- Several projects
- Notification
- Easy enough to be used
- SoGo backend



Schedule shift – frontend



Who's in the lead?

Edvard +11

Michal +10

Petr +9

Martin – suggested

csirtmaster

Save

Today

<

>

2019.11

Mon	Tue	Wed	Thu	Fri
28	29	30	31	1
Petr				
4	5	6	7	8
Petr				
11	12	13	14	15
Michal				
18	19	20	21	22
25	26	27	28	29
2	3	4	5	6

© NHN Entertainment Corp.



Schedule shift – frontend



Who's in the lead?

- ☐ Edvard +11
- ☐ Michal +10
- ☐ Petr +9
- ☒ Martin ← suggested

csirtmaster

Save Today < > 2019.11

Mon	Tue	Wed	Thu	Fri
28 Petr	29	30	31	1
4 Petr	5	6	7	8
11 Michal	12	13	14	15
18	19	20	21	22
25	26	27	28	29
2	3	4	5	6

© NHN Entertainment Corp.

Schedule shift – SoGo



Calendar interface showing a schedule for November 2019. The header includes navigation icons (calendar, left arrow, right arrow) and the text "Listopad 2019". The days of the week are listed above the columns: Pondělí, Úterý, Středa, Čtvrtek, Pátek. The dates are listed above the rows: 28, 29, 30, 31 Říjen, 1 Listopad, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15. The schedule is organized into three rows of shifts, each starting at 00:00.

Pondělí	Úterý	Středa	Čtvrtek	Pátek
28	29	30	31 Říjen	1 Listopad
00:00 csirtmaster Petr	csirtmaster Petr	csirtmaster Petr	csirtmaster Petr	csirtmaster Petr
4	5	6	7	8
00:00 csirtmaster Petr	csirtmaster Petr	csirtmaster Petr	csirtmaster Petr	csirtmaster Petr
11	12	13	14	15
00:00 csirtmaster Michal	csirtmaster Michal	csirtmaster Michal	csirtmaster Michal	csirtmaster Michal



Schedule shift – configuration

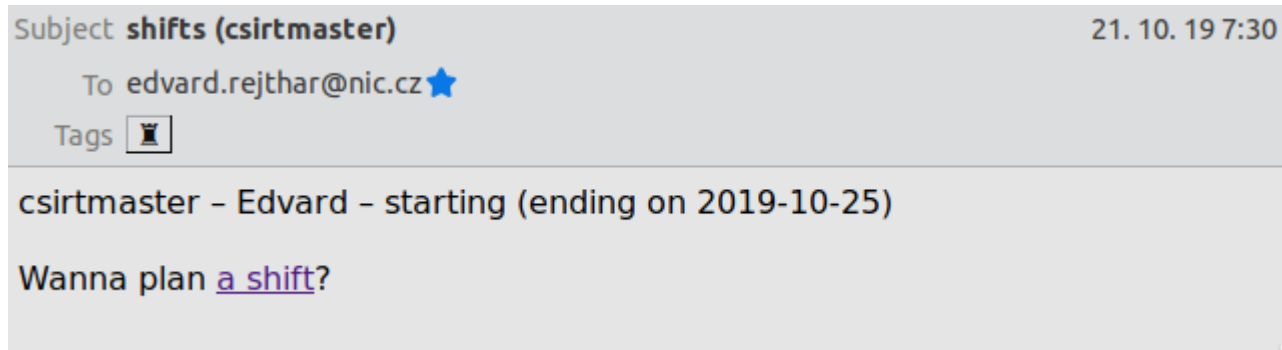


```
[team]
Edvard = edvard.rejthar@nic.cz
Michal = michal.prokop@nic.cz
Petr = petr.springer@nic.cz
Martin = martin.kunc@nic.cz

[projects]
csirtmaster = Edvard,Michal,Petr,Martin
```



Schedule shift – e-mail example



Schedule shift – notification



```
$/scheduler.py notify [project_name] [shift state] [whom to write] [fallback e-mail]  
$/scheduler.py notify all starting [all] [all]
```

- project name: all | custom name
- shift state: any | starting | proceeding | ending | none
 - any - (default) Any state, doesn't matter whether it's starting, ending or if nobody has it.
 - starting - When this is the first day of a new shift.
 - proceeding - When we are in the middle of a shift.
 - ending - When this is the last day of a shift.
 - none - Send the notification only when nobody's got the shift planned.
- whom to write: owner | all | custom e-mail
 - owner - (default) Send the notification to the shift owner only if set or to all members if nobody's got the shift.
- fallback e-mail: all | mute | custom e-mail



Contents...

- Schedule-shift ...
- Run-or-raise ...
- Envelope ...
- Convey ...



Contents

- Schedule-shift <https://github.com/CZ-NIC/schedule-shift>
- Run-or-raise <https://extensions.gnome.org/extension/1336/run-or-raise/>
- Envelope `pip3 install envelope`
- Convey `pip3 install convey`



Run-or-Raise – overview



- Launch or focus
- Custom shortcuts
- Alternatives: Xbindkeys, jumpapp, AutoHotkey
 - Gnome3 / Wayland



Run-or-Raise – syntax comparison



Xbindkeys + jumpapp

```
#1 Firefox launch
"jumpapp firefox"
  Mod2+Mod4 + plus
"jumpapp firefox"
  Mod2+Mod4 + KP_1

# ^1 Firebug
"jumpapp -t Firebug firefox"
  Control+Mod2+Mod4 + plus
"jumpapp -t "Developer Tools" firefox"
  Control+Mod2+Mod4 + KP_1
```

AutoHotkey

```
;Firefox launch
#Numpad1::ToggleWindow("Mozilla Firefox","Run","h:\QuickLaunch\firefox.lnk")
^#Numpad1::ToggleWindow("Firebug","Tip","Firebug nenalezen")
```

Run-or-Raise

```
# Firefox launch
<Super>1,firefox,,
<Super>KP_1,firefox,Firefox,
<Super><Ctrl>1,,,DevTools
<Super><Ctrl>KP_1,firefox,,Developer Tools
```



Run-or-Raise – syntax



shortcut,

[command],

[wm_class],

[title]



Run-or-Raise – syntax



shortcut, [command], [wm_class], [title]
<Super>h, notify-send Hello world



Run-or-Raise – syntax



shortcut,	[command],	[wm_class],	[title]
<Super>h,	notify-send Hello world		
<Super>f,	firefox,	Firefox,	
<Super>r,	gnome-terminal,	Gnome-terminal,	



Run-or-Raise – syntax



shortcut,	[command],	[wm_class],	[title]
<Super>h,	notify-send Hello world		
<Super>f,	firefox,	Firefox,	
<Super>r,	gnome-terminal,	Gnome-terminal,	
<Super>KP_3,	gtk-launch google-chrome.desktop,	/Google-chrome\$/,	
<Super><Shift>KP_3,	gtk-launch google-chrome-beta.desktop,	Google-chrome-beta,	



Run-or-Raise – syntax



shortcut,	[command],	[wm_class],	[title]
<Super>h,	notify-send Hello world		
<Super>f,	firefox,	Firefox,	
<Super>r,	gnome-terminal,	Gnome-terminal,	
<Super>KP_3,	gtk-launch google-chrome.desktop,	/Google-chrome\$/,	
<Super><Shift>KP_3,	gtk-launch google-chrome-beta.desktop,	Google-chrome-beta,	
<Super><Ctrl>4,	/opt/.../pycharm.sh,,		/(NetBeans IDE PyCharm)/
<Super><Ctrl>KP_4,	/opt/.../netbeans, ,		/(NetBeans IDE PyCharm)/



Run-or-Raise – syntax



shortcut,	[command],	[wm_class],	[title]
<Super>h,	notify-send Hello world		
<Super>f,	firefox,	Firefox,	
<Super>r,	gnome-terminal,	Gnome-terminal,	
<Super>KP_3,	gtk-launch google-chrome.desktop,	/Google-chrome\$/,	
<Super><Shift>KP_3,	gtk-launch google-chrome-beta.desktop,	Google-chrome-beta,	
<Super><Ctrl>4,	/opt/.../pycharm.sh,,	/(NetBeans IDE PyCharm)/	
<Super><Ctrl>KP_4,	/opt/.../netbeans, ,	/(NetBeans IDE PyCharm)/	
<Super>KP_1,	pidgin,	Pidgin,/^(?!Buddy List).)*\$/	



Run-or-Raise – syntax



shortcut,	[command],	[wm_class],	[title]
<Super>h,	notify-send Hello world		
<Super>f,	firefox,	Firefox,	
<Super>r,	gnome-terminal,	Gnome-terminal,	
<Super>KP_3,	gtk-launch google-chrome.desktop,	/Google-chrome\$/,	
<Super><Shift>KP_3,	gtk-launch google-chrome-beta.desktop,	Google-chrome-beta,	
<Super><Ctrl>4,	/opt/.../pycharm.sh,,	/(NetBeans IDE PyCharm)/	
<Super><Ctrl>KP_4,	/opt/.../netbeans, ,	/(NetBeans IDE PyCharm)/	
<Super>KP_1,	pidgin,	Pidgin,/^(?!Buddy List).)*\$/	
Pause,	bash -c "sleep 0.06 && xdotool click 1"		



Run-or-Raise – installation



<https://extensions.gnome.org/extension/1336/run-or-raise/>



Run or raise by [e2rd](#)



Launch or focus the window or
define custom shortcuts in a text file

Extension Homepage

<https://github.com/CZ-NIC/run-or-raise>

Download

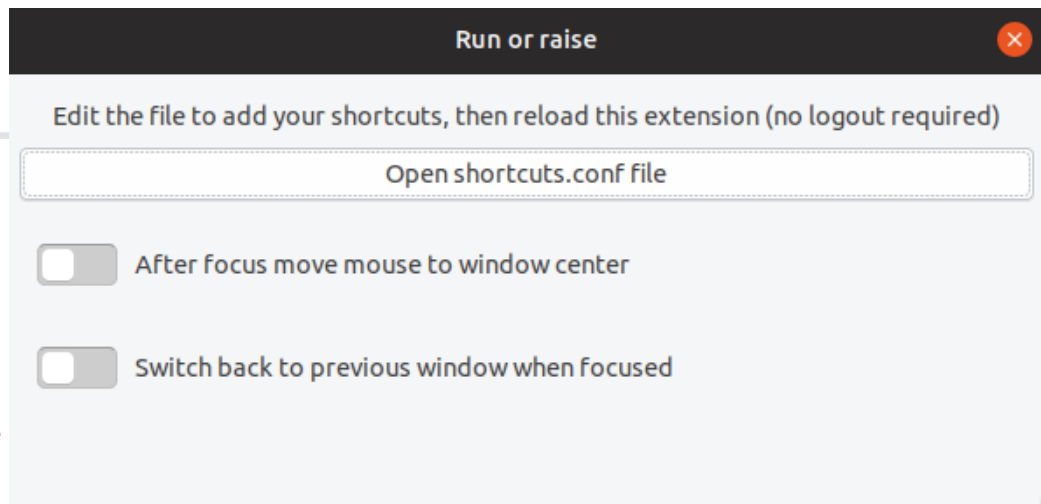
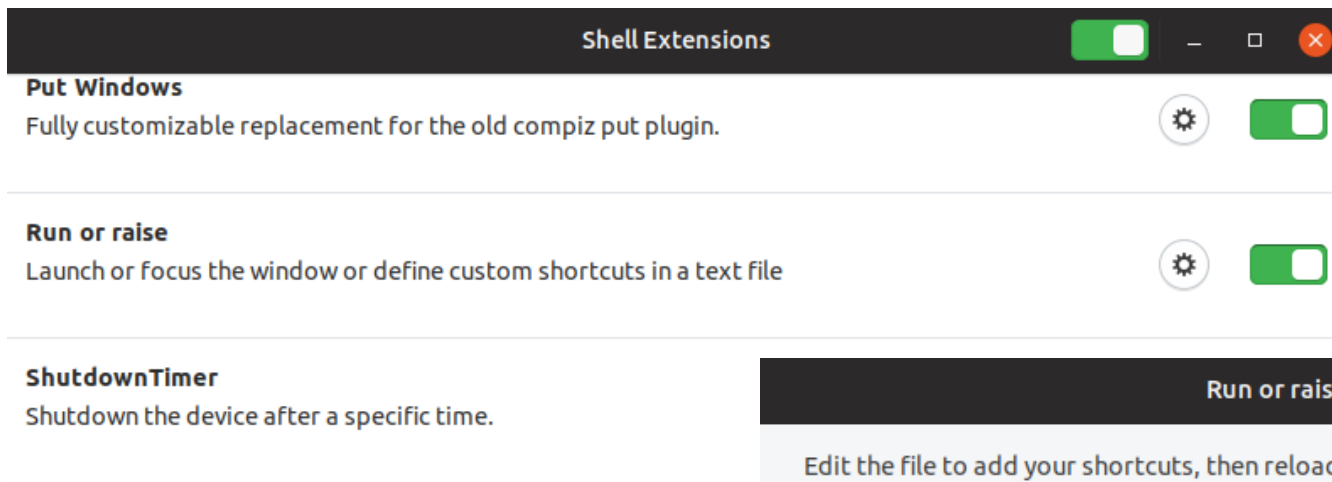
Shell version... ▼



Run-or-Raise – options



```
$ sudo apt install gnome-shell-extension-prefs
```



Contents...

- Schedule-shift ...
- Run-or-raise ...
- Envelope ...
- Convey ...



Contents

- Schedule-shift <https://github.com/CZ-NIC/schedule-shift>
- Run-or-raise <https://extensions.gnome.org/extension/1336/run-or-raise/>
- Envelope `pip3 install envelope`
- Convey `pip3 install convey`



Envelope – overview



- email

```
email = EmailMessage()  
email["Subject"] = "Encrypted message" # real subject should be revealed when decrypted  
email.set_type("multipart/encrypted")  
email.set_param("protocol", "application/pgp-encrypted")  
email.set_payload(text)
```



Envelope – overview



- email
- smtplib

```
email = EmailMessage()
email["Subject"] = "Encrypted message" # real subject should be revealed when decrypted
email.set_type("multipart/encrypted")
email.set_param("protocol", "application/pgp-encrypted")
email.set_payload(text)

smtp = smtplib.SMTP(self.host, self.port)
if self.security == "starttls":
    smtp.starttls()
smtp.login(self.user, self.password)
```



Envelope – overview



- email
- smtplib
- python-gnupg

```
email = EmailMessage()
email["Subject"] = "Encrypted message" # real subject should be revealed when decrypted
email.set_type("multipart/encrypted")
email.set_param("protocol", "application/pgp-encrypted")
email.set_payload(text)
```

```
smtp = smtplib.SMTP(self.host, self.port)
if self.security == "starttls":
    smtp.starttls()
smtp.login(self.user, self.password)
```

```
gpg = gnupg.GPG(gnupghome=self._get_gnupg_home(), options=["--trust-model=always"])
gpg.sign(message,
          extra_args=["--textmode"],
          keyid=sign if sign and sign is not True else None,
          passphrase=self._passphrase if self._passphrase else None,
          detach=True if send is not None else None,
          )
```



Envelope – overview



- email

- smtplib

- python-gnupg

- smime

- magic

```
email = EmailMessage()
email["Subject"] = "Encrypted message" # real subject should be revealed when decrypted
email.set_type("multipart/encrypted")
email.set_param("protocol", "application/pgp-encrypted")
email.set_payload(text)
```

```
smtp = smtplib.SMTP(self.host, self.port)
if self.security == "starttls":
    smtp.starttls()
smtp.login(self.user, self.password)
```

```
gpg = gnupg.GPG(gnupghome=self._get_gnupg_home(), options=["--trust-model=always"])
gpg.sign(message,
          extra_args=["--textmode"],
          keyid=sign if sign and sign is not True else None,
          passphrase=self._passphrase if self._passphrase else None,
          detach=True if send is not None else None,
          )
```



Envelope – e-mail structure (RFC-3156)



MAIL
headers
subject
text



Envelope – e-mail structure (RFC-3156)



MAIL

headers

subject

text

Attachment

Attachment



Envelope – e-mail structure (RFC-3156)



SUBJECT
text/rfc822-headers
subject

MAIL
headers
subject
text
Attachment
Attachment



Envelope – e-mail structure (RFC-3156)



PROTECTED-HEADERS

SUBJECT

text/rfc822-headers
subject

MAIL

headers
subject
text

Attachment

Attachment



Envelope – e-mail structure (RFC-3156)



VERSION

PROTECTED-HEADERS

SUBJECT

text/rfc822-headers
subject

MAIL

headers
subject
text

Attachment

Attachment



Envelope – e-mail structure (RFC-3156)



application/octet-stream

VERSION

PROTECTED-HEADERS

SUBJECT

text/rfc822-headers

subject

MAIL

headers

subject

text

Attachment

Attachment



Envelope – e-mail structure (RFC-3156)



PGP-ENCRYPTED

application/octet-stream

VERSION

PROTECTED-HEADERS

SUBJECT

text/rfc822-headers
subject

MAIL

headers
subject
text

Attachment

Attachment



Envelope – interfaces



- One-liner
- Fluent
- CLI

```
envelope("my message")  
  .subject("hello world")  
  .to("example@example.com")  
  .attach(file_contents, filename="attached-file.txt")  
  .smtp("localhost", 587, "user", "pass", "starttls")  
  .signature()  
  .send()
```



Envelope – interfaces



FLUENT



```
import envelope
envelope().message("Hello world")
    .output("/tmp/output_file")
    .sender("me@example.com")
    .to("remote_person@example.com")
    .encrypt(key_path="/tmp/remote_key.asc")
```



Envelope – interfaces



FLUENT



```
import envelope
envelope().message("Hello world")
    .output("/tmp/output_file")
    .sender("me@example.com")
    .to("remote_person@example.com")
    .encrypt(key_path="/tmp/remote_key.asc")
```

```
import envelope
envelope(message="Hello world",
    output="/tmp/output_file",
    sender="me@example.com",
    to="remote_person@example.com",
    encrypt="/tmp/remote_key.asc")
```



ONE-LINER



Envelope – interfaces



FLUENT



```
import envelope
envelope().message("Hello world")
    .output("/tmp/output_file")
    .sender("me@example.com")
    .to("remote_person@example.com")
    .encrypt(key_path="/tmp/remote_key.asc")
```

```
envelope --message "Hello world"
    --output "/tmp/output_file"
    --sender "me@example.com"
    --to "remote_person@example.com"
    --encrypt-path "/tmp/remote_key.asc"
```



CLI



```
import envelope
envelope(message="Hello world",
    output="/tmp/output_file",
    sender="me@example.com",
    to="remote_person@example.com",
    encrypt="/tmp/remote_key.asc")
```

ONE-LINER



Envelope – related affairs



- SMTP
- GPG
- SPF, DKIM, DMARC

- check

```
$ envelope --smtp localhost 25 --sender me@example.com --check
SPF found on the domain example.com: v=spf1 -all
See: dig -t SPF example.com && dig -t TXT example.com
DKIM found: ['v=DKIM1; g=*; k=rsa; p=...']
Could not spot DMARC.
Trying to connect to the SMTP...
Check succeeded.
```



Envelope – test before send



```
$ envelope --to "user@example.org" --message "Hello world" --send 0
```

```
*****
```

Have not been sent from to user@example.org

Content-Type: text/html; charset="utf-8"

Content-Transfer-Encoding: 7bit

MIME-Version: 1.0

Subject:

From:

To: user@example.org

Date: Mon, 07 Oct 2019 16:13:37 +0200

Message-ID: <157045761791.29779.5279828659897745855@...>

Hello world



Contents...

- Schedule-shift ...
- Run-or-raise ...
- Envelope ...
- Convey ...



Contents

- Schedule-shift <https://github.com/CZ-NIC/schedule-shift>
- Run-or-raise <https://extensions.gnome.org/extension/1336/run-or-raise/>
- Envelope `pip3 install envelope`
- Convey `pip3 install convey`



Convey – source file juggling



edvard@edvard-jezevec: /home/edvard

```
edvard@edvard-jezevec:~$ cat IP_2 |
> while read line
> do
> COUNTRY=$(whois -h ripedb2.nic.cz -- $line | grep country | cut -d: -f2 | sed 's/^ *///;s/ *$//')
> pole=$(cat zdroj | grep "$line")
> #echo "$line" "$pole" >> $COUNTRY
> echo "$pole" >> $COUNTRY
> done
```

edvard@edvard-jezevec: /home/edvard

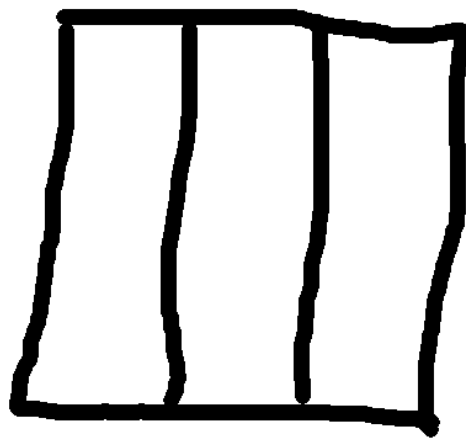
```
edvard@edvard-jezevec:~$ while read line; do
> p=$(ls | grep $line | cut -d@ -f2 | cut -d. -f-1)
> mv "$line" "$p"
>
> done < maily
```

edvard@edvard-jezevec: /home/edvard

```
edvard@edvard-jezevec:~$ sort contacts_1 >> contacts_2 &&
> while read kontakt_2 IP_adresa; do
> kontakt=$(echo $kontakt_2 | sed -e 's/,/, /g') #Aby bylo mozne poslat maily, musi byt me
zi nima carka a mezera
> echo IP:' ' "$IP_adresa\n"CONTACTS:' ' "$kontakt\n" >> contacts
> #echo IP:' ' "$pole\n"CONTACTS:' ' "$kontakt\n" >> contacts
> done < contacts_2 #Stejne maily jsou serazeny pod sebe
```



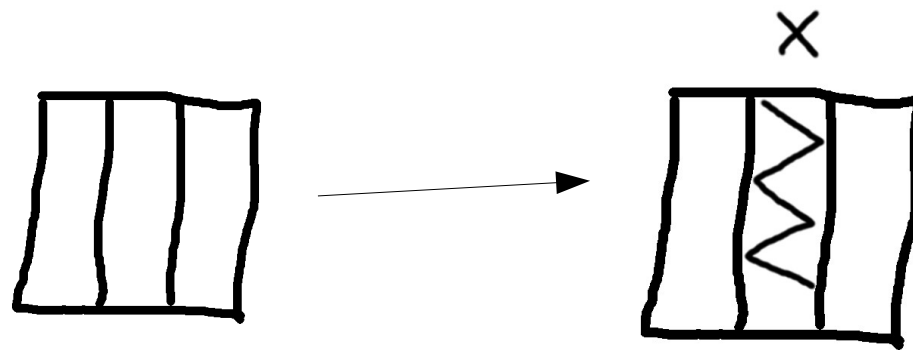
Column manipulation



Column manipulation



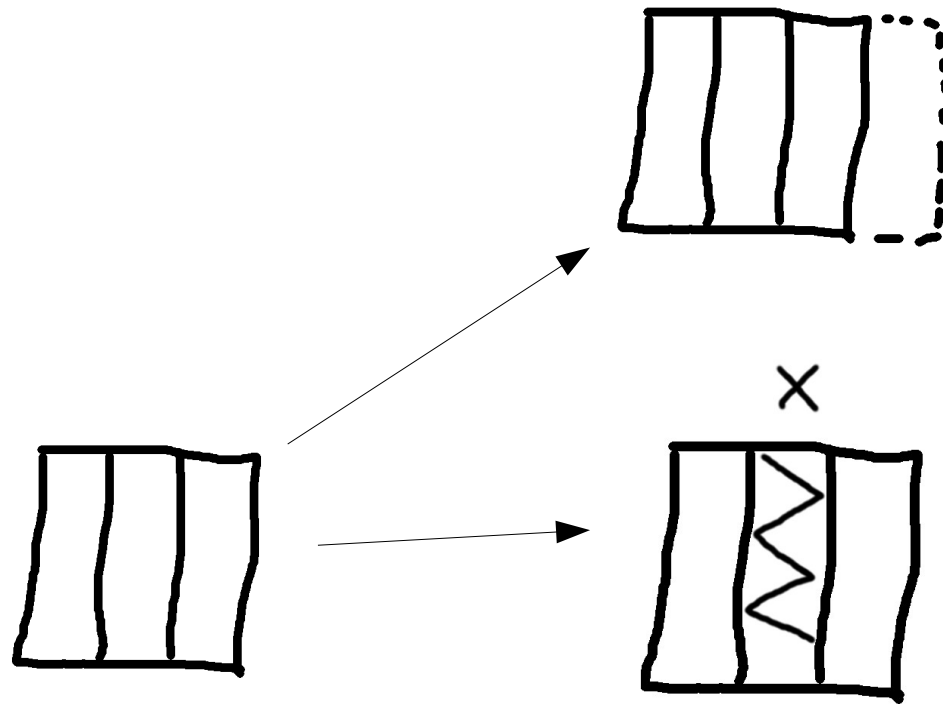
- Delete a column
- ...



Column manipulation



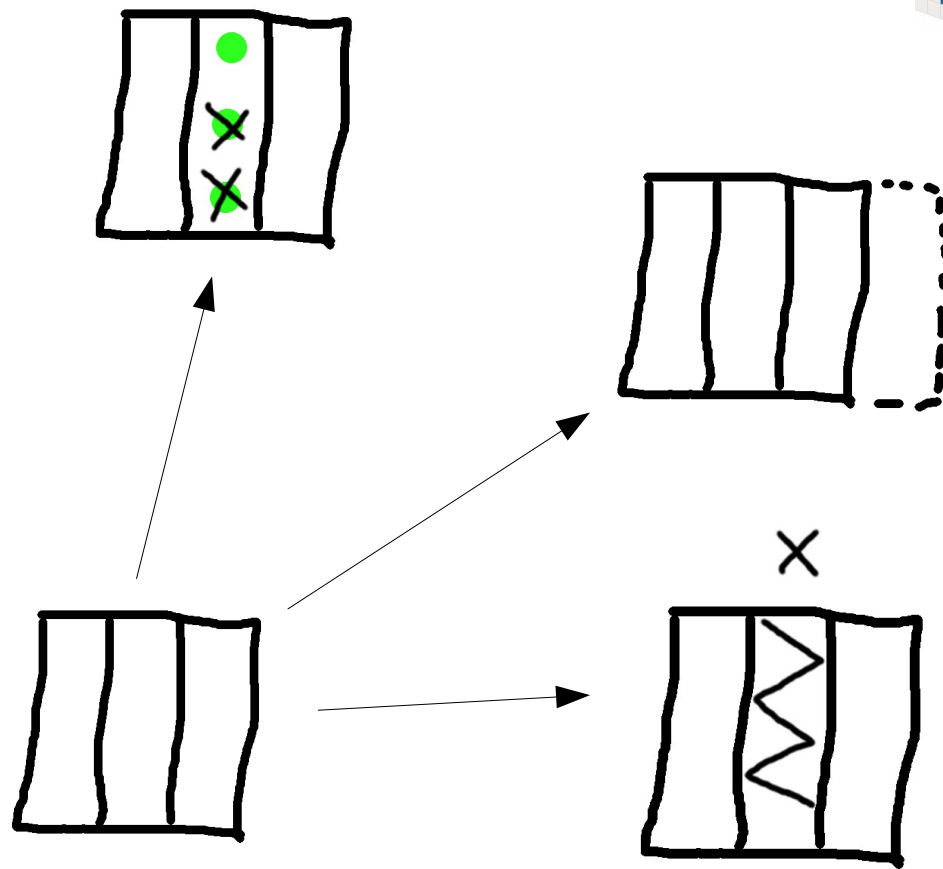
- Delete a column
- Compute new column
- ...



Column manipulation



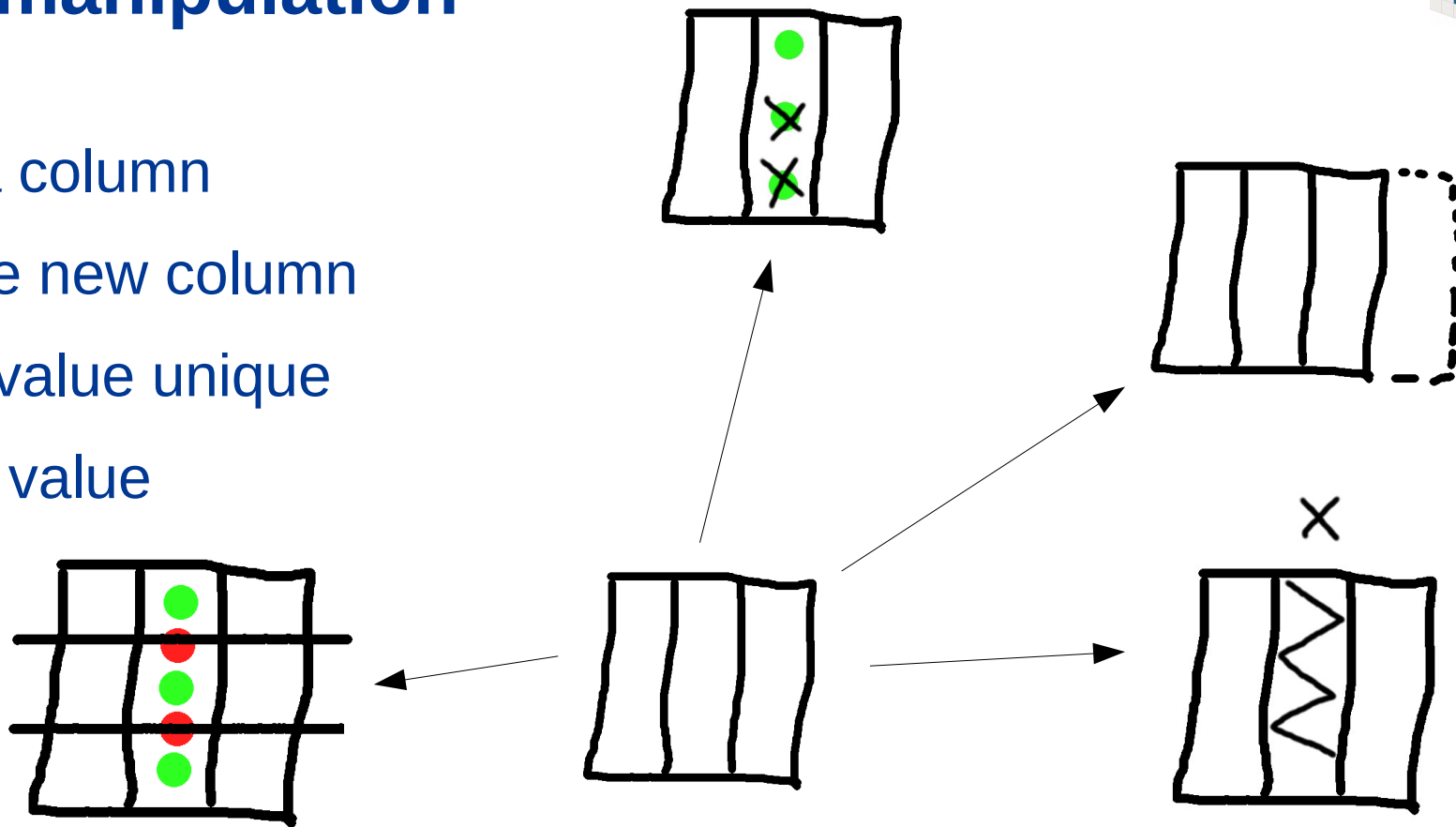
- Delete a column
- Compute new column
- Make a value unique
- ...



Column manipulation



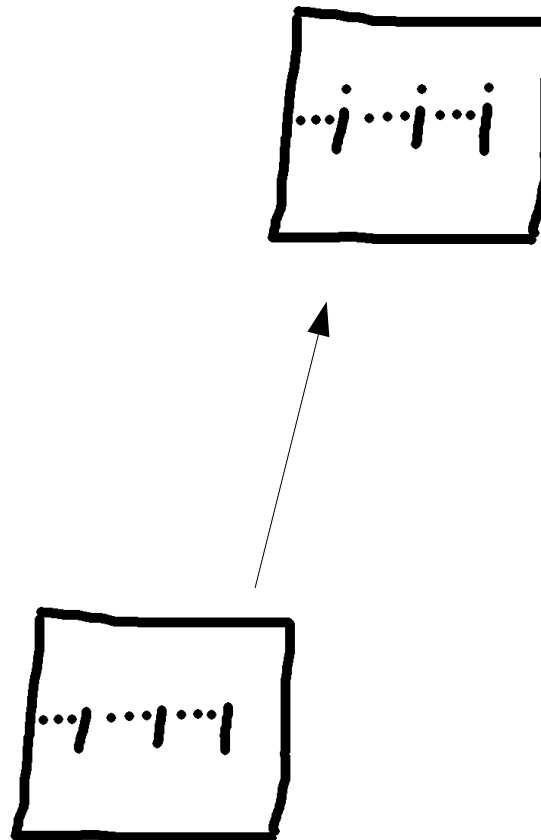
- Delete a column
- Compute new column
- Make a value unique
- Filter by value
- ...



Column manipulation



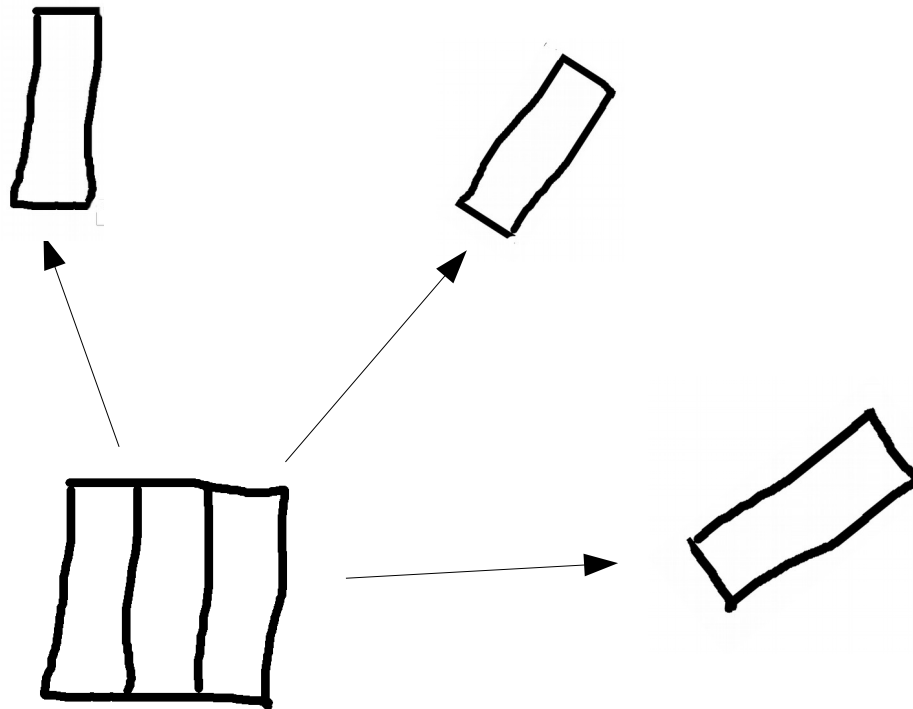
- Delete a column
- Compute new column
- Make a value unique
- Filter by value
- Change dialect
- ...



Column manipulation

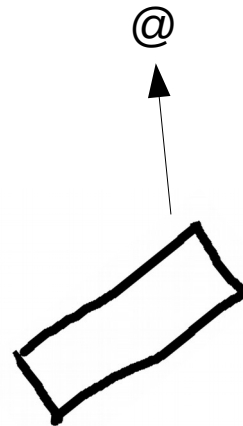
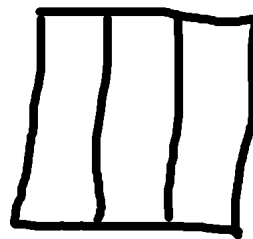
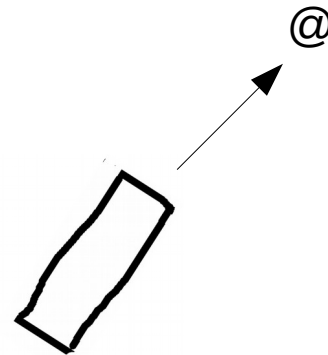
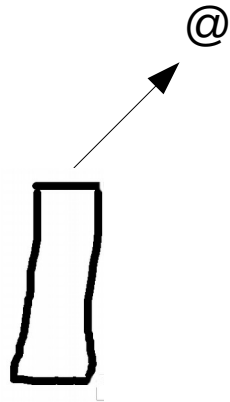


- Delete a column
- Compute new column
- Make a value unique
- Filter by value
- Change dialect
- Split to smaller files
- ...



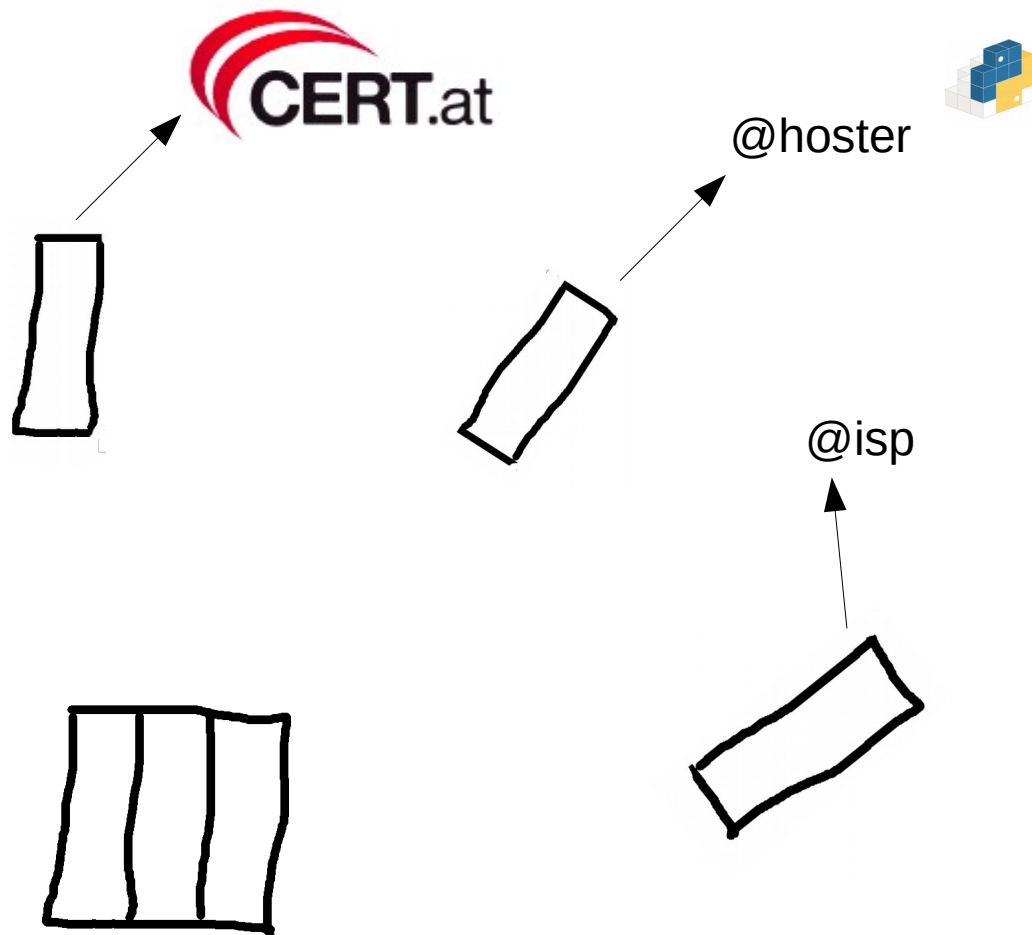
Column manipulation

- Delete a column
- Compute new column
- Make a value unique
- Filter by value
- Change dialect
- Split to smaller files
- ... and send them

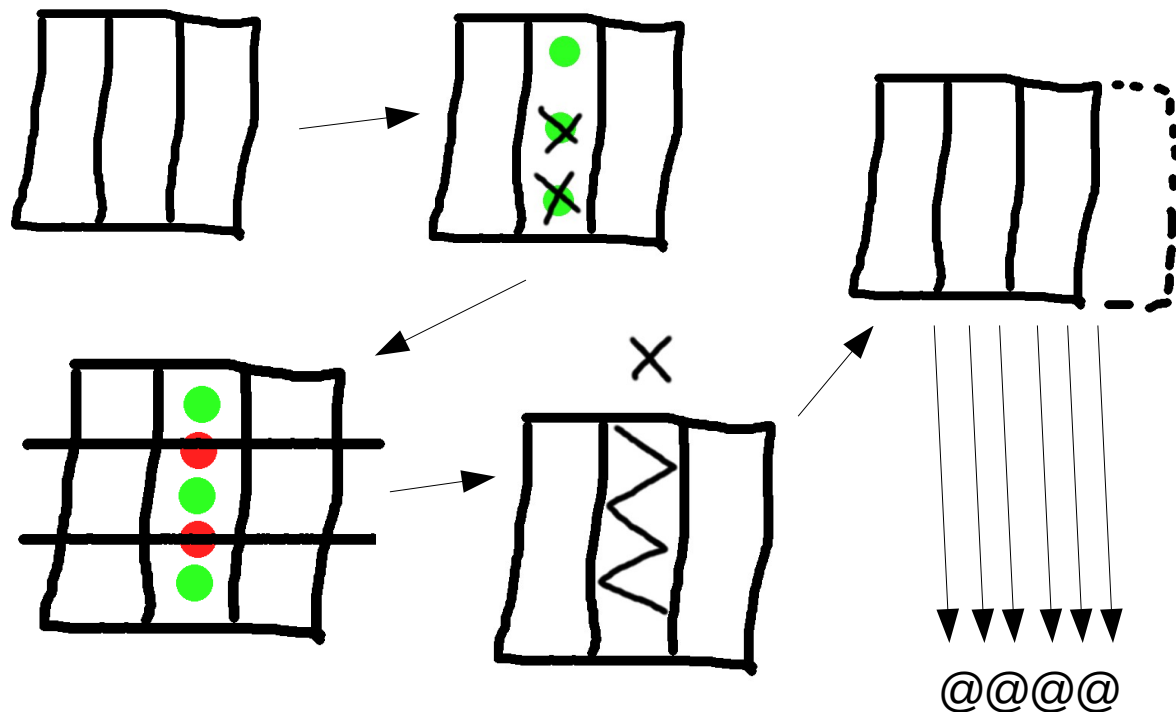


Column manipulation

- Delete a column
- Compute new column
- Make a value unique
- Filter by value
- Change dialect
- Split to smaller files
- ... and send them wherever



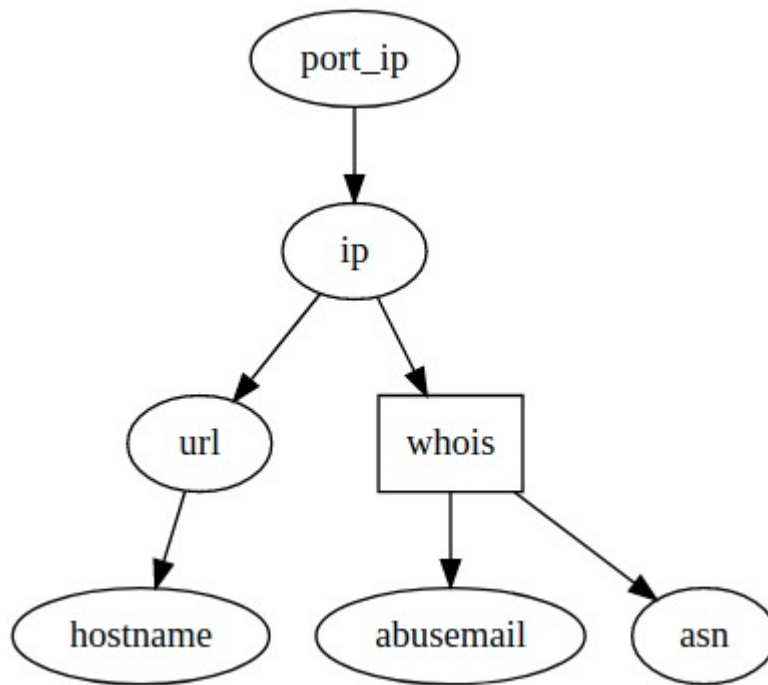
Column manipulation



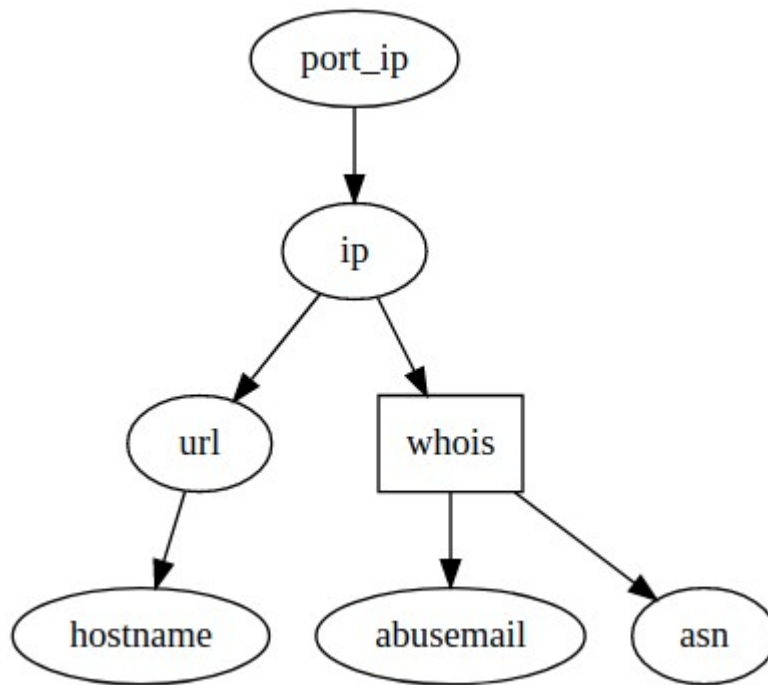
- or everything together
- virtual columns
- multi-descriptor performance



Convey – computing fields



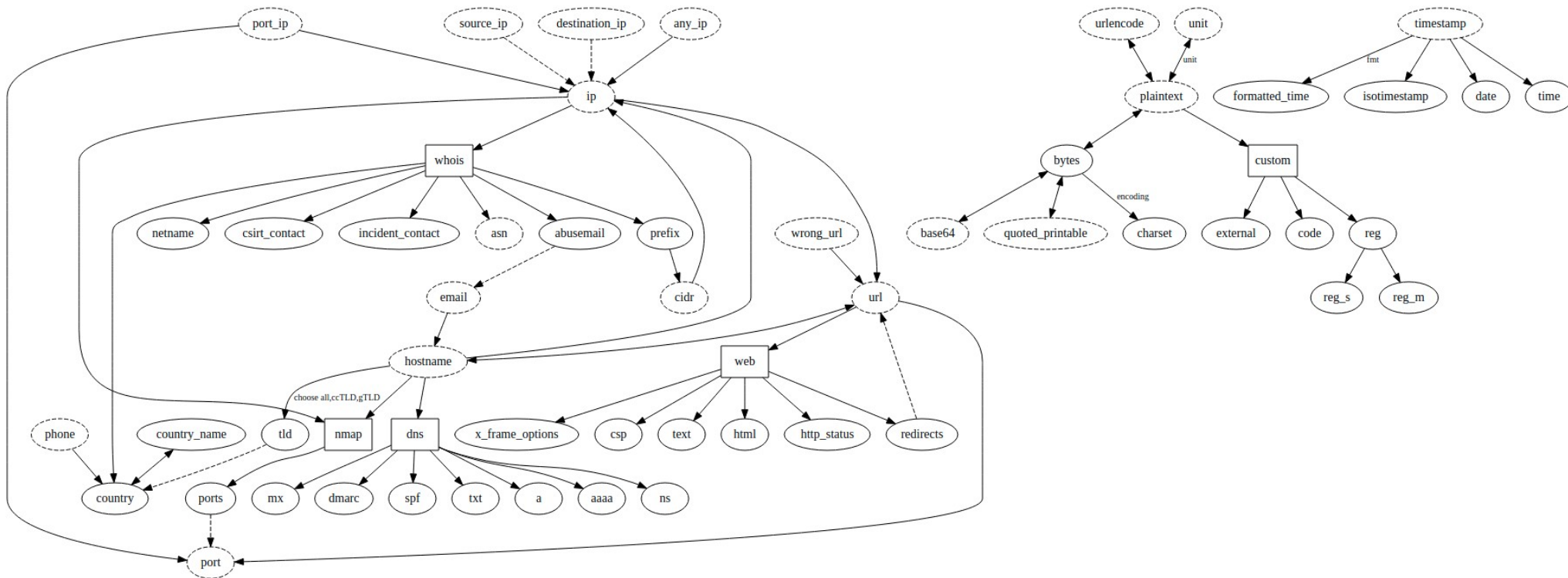
Convey – computing fields



```
$ convey --show-uml
```



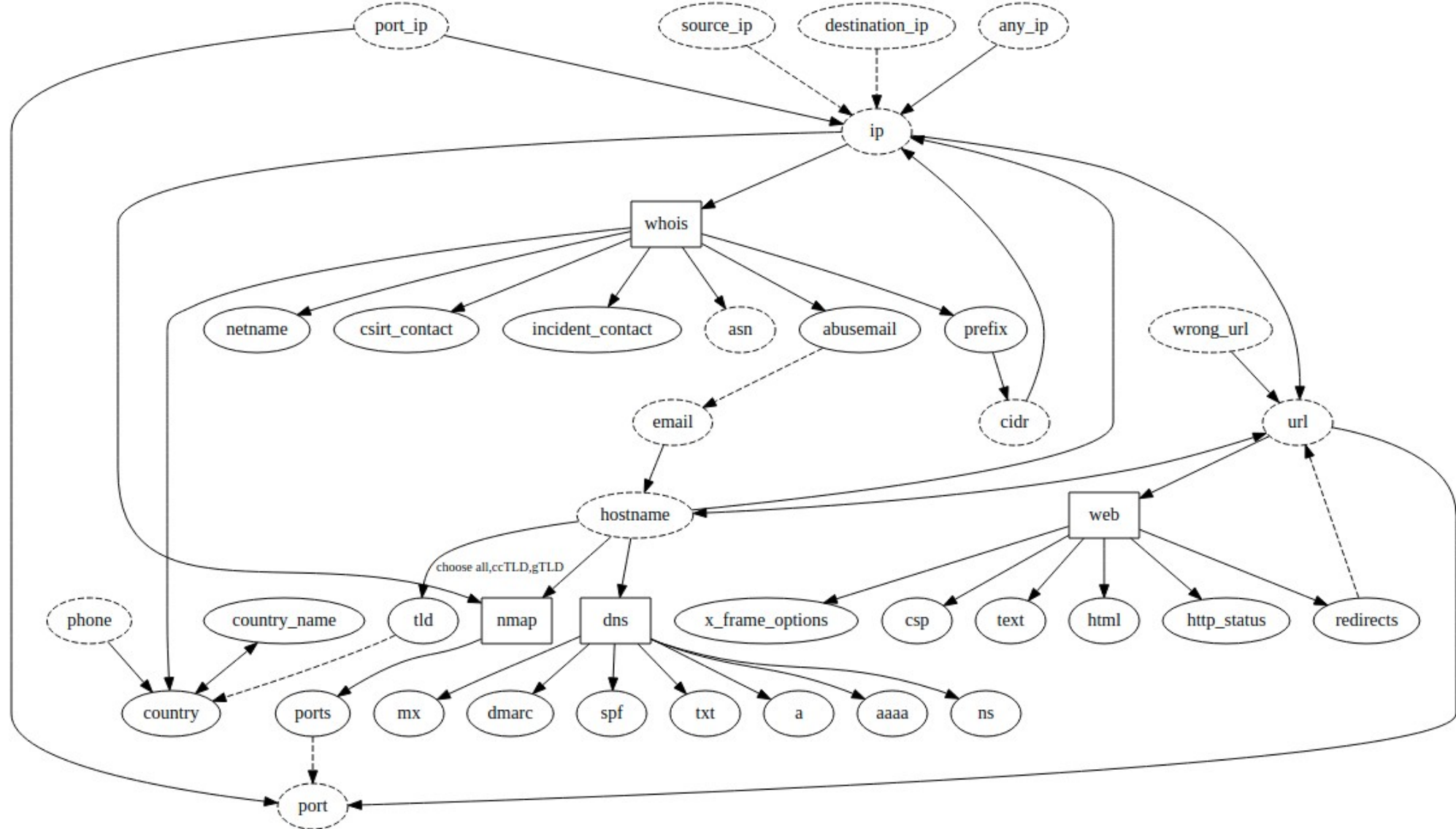
Convey – computing fields



Convey field types (dashed nodes = identifiable automatically, dashed edges = field identity)

\$ convey --show-uml





Convey field types (dashed nodes = identifiable automatically, dashed edges = field identity)

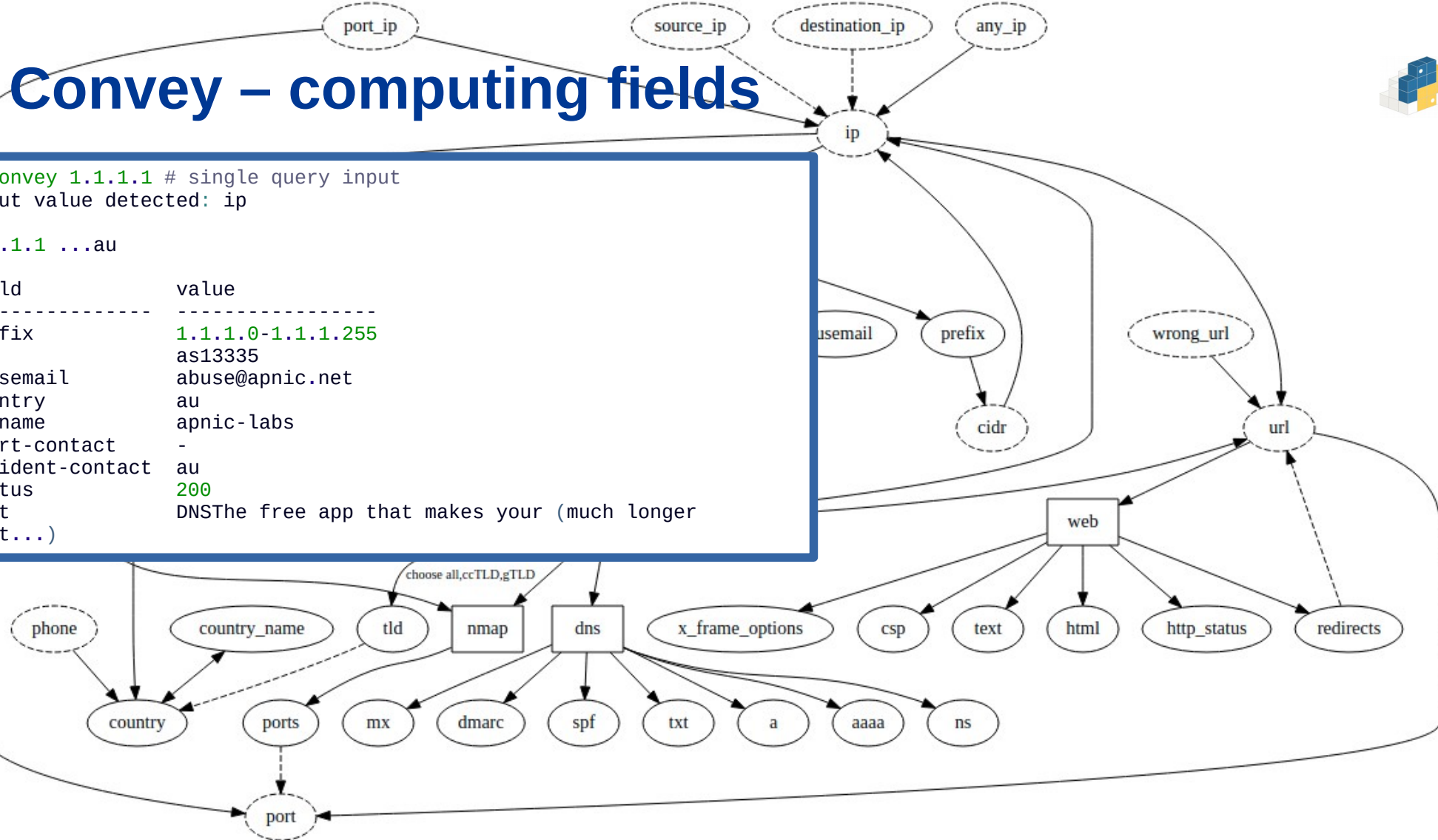
Convey – computing fields



```
$ convey 1.1.1.1 # single query input
Input value detected: ip
```

```
1.1.1.1 ...au
```

field	value
prefix	1.1.1.0-1.1.1.255
asn	as13335
abusemail	abuse@apnic.net
country	au
netname	apnic-labs
csirt-contact	-
incident-contact	au
status	200
text	DNSThe free app that makes your (much longer
text...)	



Convey field types (dashed nodes = identifiable automatically, dashed edges = field identity)

Convey – computing fields



```
$ convey 1.1.1.1 # single query input
Input value detected: ip
```

```
1.1.1.1 ...au
```

field	value
prefix	1.1.1.0-1.1.1.255
asn	as13335
abusemail	abuse@apnic.net
country	au
netname	apnic-labs
csirt-contact	-
incident-contact	au
status	200
text	DNSThe free app that makes you
text...	

```
$ curl http://localhost:26683/?q=example.com
```

```
{'ip': '93.184.216.34',
'prefix': '93.184.216.0-93.184.216.255',
'asn': '',
'abusemail': 'abuse@verizondigitalmedia.com',
'country': 'unknown',
'netname': 'edgecast-netblk-03',
'csirt-contact': '-',
'incident-contact': 'unknown',
'status': 200,
'text': 'DNSThe free app that makes your (much longer text...)'
}
```

Convey field types (dashed nodes = identifiable automatically, dashed edges = field identity)

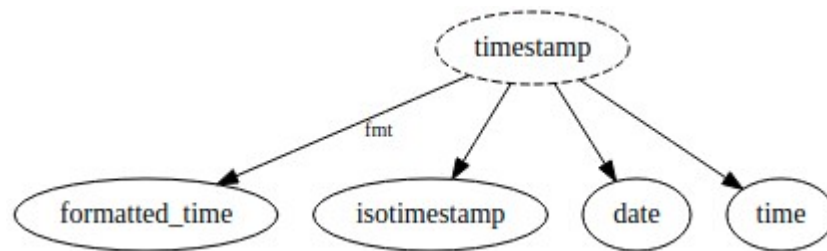
Convey – computing time fields



```
$ convey "today is March 13th 2016 3 hours PM"
```

Input value detected: timestamp

field	value
date	2016-03-13
isotimestamp	2016-03-13T15:00:00
time	15:00:00



Convey – computing time fields



```
$ convey "today is March 13th 2016 3 hours PM"
```

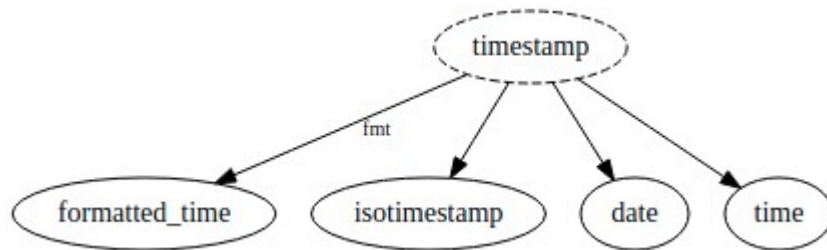
Input value detected: timestamp

field	value
date	2016-03-13
isotimestamp	2016-03-13T15:00:00
time	15:00:00

```
$ convey "today is March 13th 2016 3 hours PM" --field time
```

Input value detected: timestamp

field	value
time	15:00:00



Convey – computing time fields



```
$ convey "today is March 13th 2016 3 hours PM"
```

Input value detected: timestamp

field	value
date	2016-03-13
isotimestamp	2016-03-13T15:00:00
time	15:00:00

```
$ convey "today is March 13th 2016 3 hours PM" --field time
```

Input value detected: timestamp

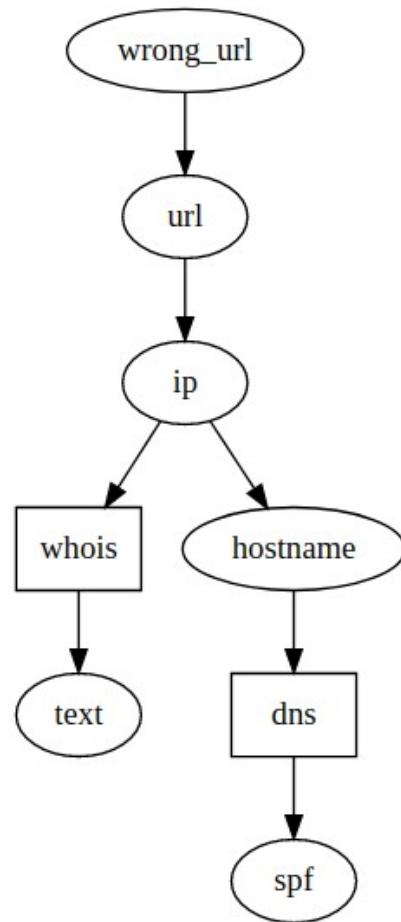
field	value
time	15:00:00

```
$ convey hxxp://example[.]com --field text --field spf
```

Input value detected: wrong_url

Scrapping http://example.com...

field	value
text	Example Domain This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission. More information...
spf	v=spf1 -all



Convey – computing fields

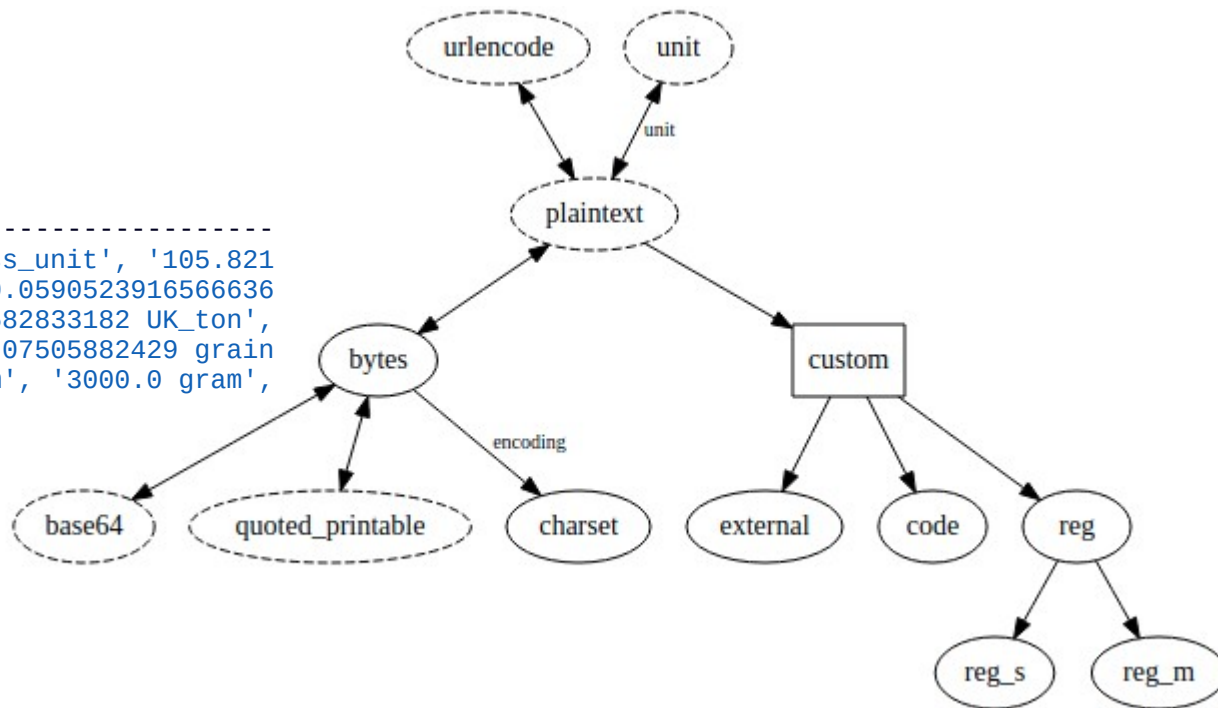


```
$ convey "3 kg"
```

Input value detected: unit

field	value
-------	-------

plaintext	['1.806642538265029e+27 atomic_mass_unit', '105.821 othecary_ounce', '0.0703602964419822 bag', '0.0590523916566636 867865546327 US_hundredweight', '0.002952619582833182 UK_ton', n', '1929.0447941176785 pennyweight', '46297.07505882429 grain ton_mass', '771.6179176470714 apothecary_dram', '3000.0 gram',
-----------	---



Convey – computing fields



```
$ convey "3 kg"
```

Input value detected: unit

field	value
-------	-------

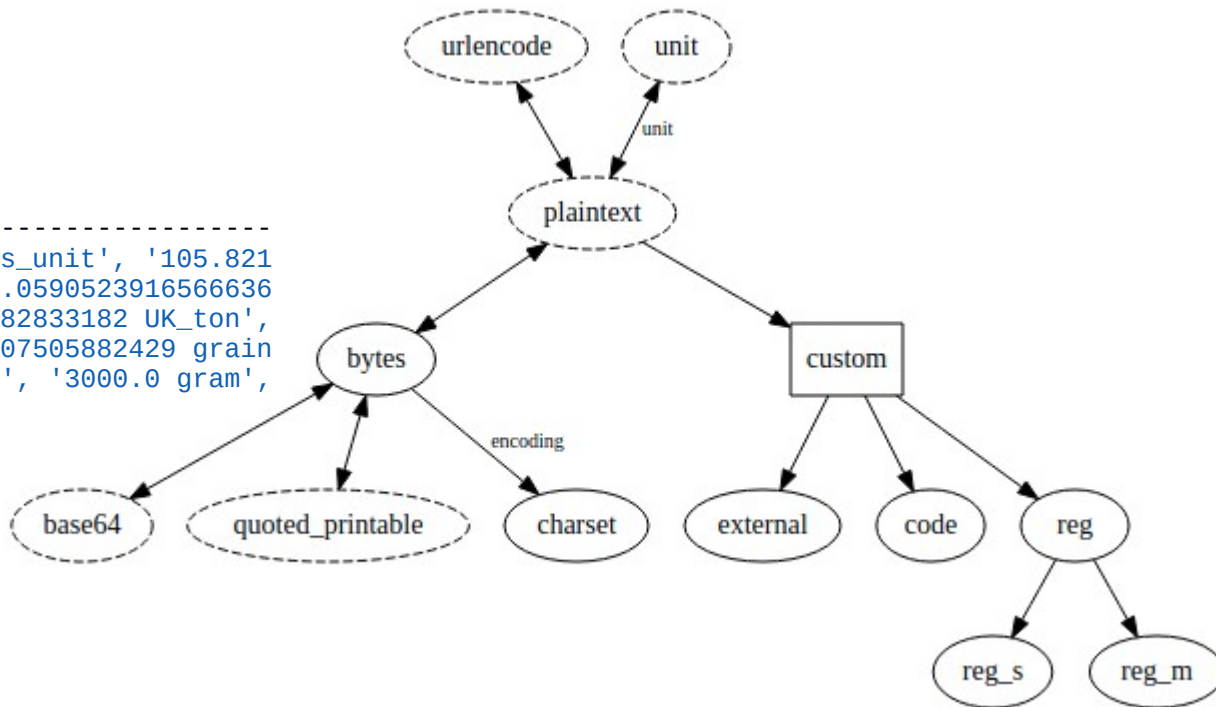
plaintext	['1.806642538265029e+27 atomic_mass_unit', '105.821 othecary_ounce', '0.0703602964419822 bag', '0.0590523916566636 867865546327 US_hundredweight', '0.002952619582833182 UK_ton', 'n', '1929.0447941176785 pennyweight', '46297.07505882429 grain ton_mass', '771.6179176470714 apothecary_dram', '3000.0 gram',
-----------	--

```
$ convey "3 kg" --field unit[g]
```

Input value detected: unit

field	value
-------	-------

unit	3000.0 gram
------	-------------



Convey – computing fields



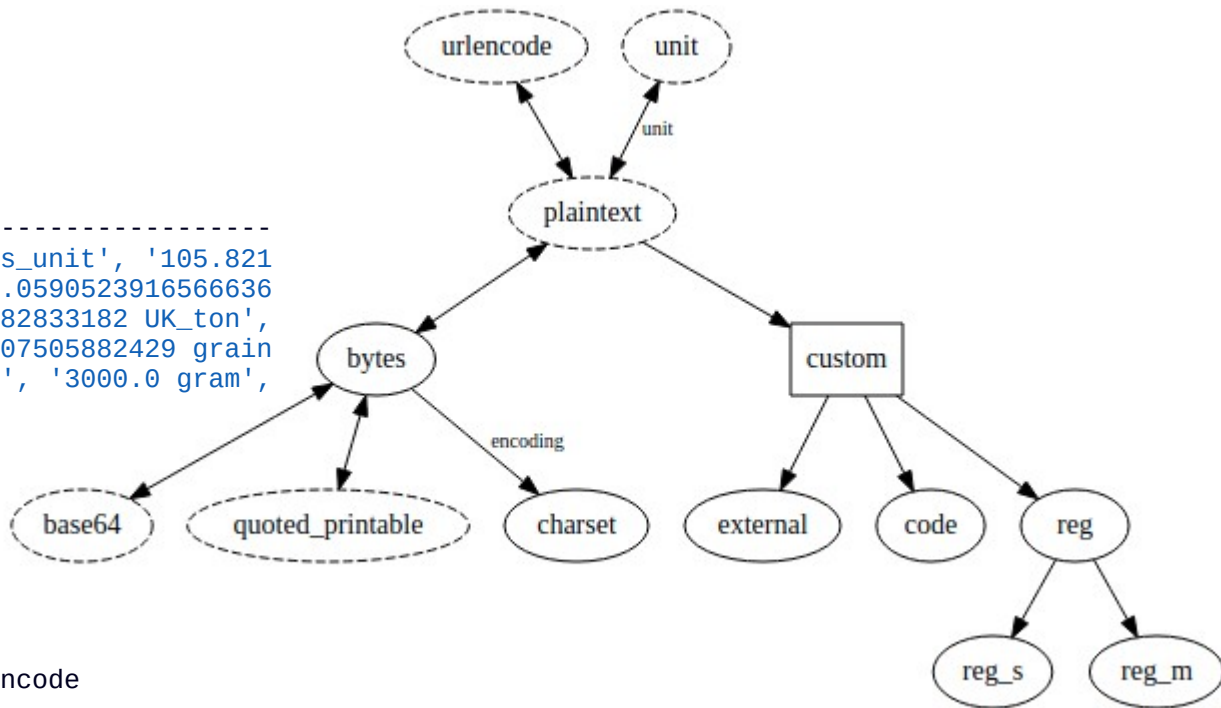
```
$ convey "3 kg"
Input value detected: unit
```

field	value
plaintext	['1.806642538265029e+27 atomic_mass_unit', '105.821 othecary_ounce', '0.0703602964419822 bag', '0.0590523916566636 867865546327 US_hundredweight', '0.002952619582833182 UK_ton', 'n', '1929.0447941176785 pennyweight', '46297.07505882429 grain ton_mass', '771.6179176470714 apothecary_dram', '3000.0 gram',

```
$ convey "3 kg" --field unit[g]
Input value detected: unit
```

field	value
unit	3000.0 gram

```
$ convey "my long and cool text" --field urlencode
Input value seems to be plaintext.
field      value
-----
urlencode  my%20long%20and%20cool%20text
```



Convey – usecase



```
$ convey my-file.csv --field abusemail
```



Convey

```
$ convey my-file.csv
```

```
--field abusemail
```

```
Source file: /tmp/ram/test/my-file.csv, delimiter: ',', quoting: '"', header: not used
Identified columns: 109.107.199.245 (ip), 1995-07-27T22:20:21-05:00 (timestamp)
Computed columns: abusemail (from 109.107.199.245)
Log lines: 2271
Whois servers asked: whois.ripe.net (7×); 7 prefixes discovered
```

Sample:

```
109.107.199.245,25,1995-07-27T22:20:21-05:00,16019,CZ
109.107.200.106,443,1995-07-09T01:12:26-05:00,16019,CZ
109.107.200.149,25,1995-07-28T02:27:21-05:00,16019,CZ
109.107.200.242,25,1995-07-28T11:58:09-05:00,16019,CZ
```

Preview:

109.107.199.245 (ip)	25	1995-07-27T22:20:21-05:00 (timestamp)	16019	CZ	abusemail from: 109.107.199.245
109.107.199.245	25	1995-07-27T22:20:...	16019	CZ	abuse@vodafone.cz
109.107.200.106	443	1995-07-09T01:12:...	16019	CZ	abuse@vodafone.cz
109.107.200.149	25	1995-07-28T02:27:...	16019	CZ	abuse@vodafone.cz
109.107.200.242	25	1995-07-28T11:58:...	16019	CZ	abuse@vodafone.cz
109.107.201.10	110	1995-07-26T15:00:...	16019	CZ	abuse@vodafone.cz
109.107.201.10	25	1995-07-28T11:27:...	16019	CZ	abuse@vodafone.cz
109.107.201.10	995	1995-07-16T10:36:...	16019	CZ	abuse@vodafone.cz
109.107.201.162	25	1995-07-27T14:16:...	16019	CZ	abuse@vodafone.cz
109.107.201.18	443	1995-07-09T13:12:...	16019	CZ	abuse@vodafone.cz

Main menu - how the file should be processed?

- 1) Pick or delete columns
- 2) Add a column
- 3) Unique filter
- 4) Value filter
- 5) Split by a column
- 6) Change CSV dialect
- p) process ←←←←←
- ~) send (split first)
- ~) show all details (process first)
- r) Refresh...
- c) Config...
- x) exit
- ?



Convey

\$ convey my-file.csv

--field abusemail

```
Source file: /tmp/ram/test/my-file.csv, delimiter: ',', quoting: '"', header: not used
Identified columns: 109.107.199.245 (ip), 1995-07-27T22:20:21-05:00 (timestamp)
Computed columns: abusemail (from 109.107.199.245)
Log lines processed: 329/2271, 15 %, 0:00:02, 180 lines / s, 1 file descriptors open
Whois servers asked: whois.ripe.net (34x); 34 prefixes discovered

Sample:
109.107.199.245,25,1995-07-27T22:20:21-05:00,16019,CZ
109.107.200.106,443,1995-07-09T01:12:26-05:00,16019,CZ
109.107.200.149,25,1995-07-28T02:27:21-05:00,16019,CZ
109.107.200.242,25,1995-07-28T11:58:09-05:00,16019,CZ

Preview:
109.107.199.245      25  1995-07-27T22:20:21-05:00      16019  CZ  abusemail from:
      (ip)              (timestamp)
-----
109.107.199.245      25  1995-07-27T22:20:...      16019  CZ  abuse@vodafone.cz
109.107.200.106      443  1995-07-09T01:12:...      16019  CZ  abuse@vodafone.cz
109.107.200.149      25  1995-07-28T02:27:...      16019  CZ  abuse@vodafone.cz
109.107.200.242      25  1995-07-28T11:58:...      16019  CZ  abuse@vodafone.cz
109.107.201.10       110  1995-07-26T15:00:...      16019  CZ  abuse@vodafone.cz
109.107.201.10       25  1995-07-28T11:27:...      16019  CZ  abuse@vodafone.cz
109.107.201.10       995  1995-07-16T10:36:...      16019  CZ  abuse@vodafone.cz
109.107.201.162      25  1995-07-27T14:16:...      16019  CZ  abuse@vodafone.cz
109.107.201.18       443  1995-07-09T13:12:...      16019  CZ  abuse@vodafone.cz
Whois 109.123.222.102... abuse@casablanca.cz
Whois 109.123.222.130... abuse@casablanca.cz
Whois 109.123.222.18... abuse@casablanca.cz
Whois 109.123.222.201... abuse@casablanca.cz
Whois 109.123.222.34... abuse@casablanca.cz
Whois 109.123.222.4... abuse@casablanca.cz
Whois 109.123.222.9... abuse@casablanca.cz
Whois 109.123.223.155... abuse@casablanca.cz
Whois 109.164.0.132... abuse@sitkom.cz
Whois 109.164.116.3... info@novamorava.net
Whois 109.164.118.110... ^FKeyboard interrupting on line number: 437
Keyboard interrupt caught. Options: continue (default, do the line again), [s]kip the line,
[d]ebug, [e]nd processing earlier, [q]uit:
```



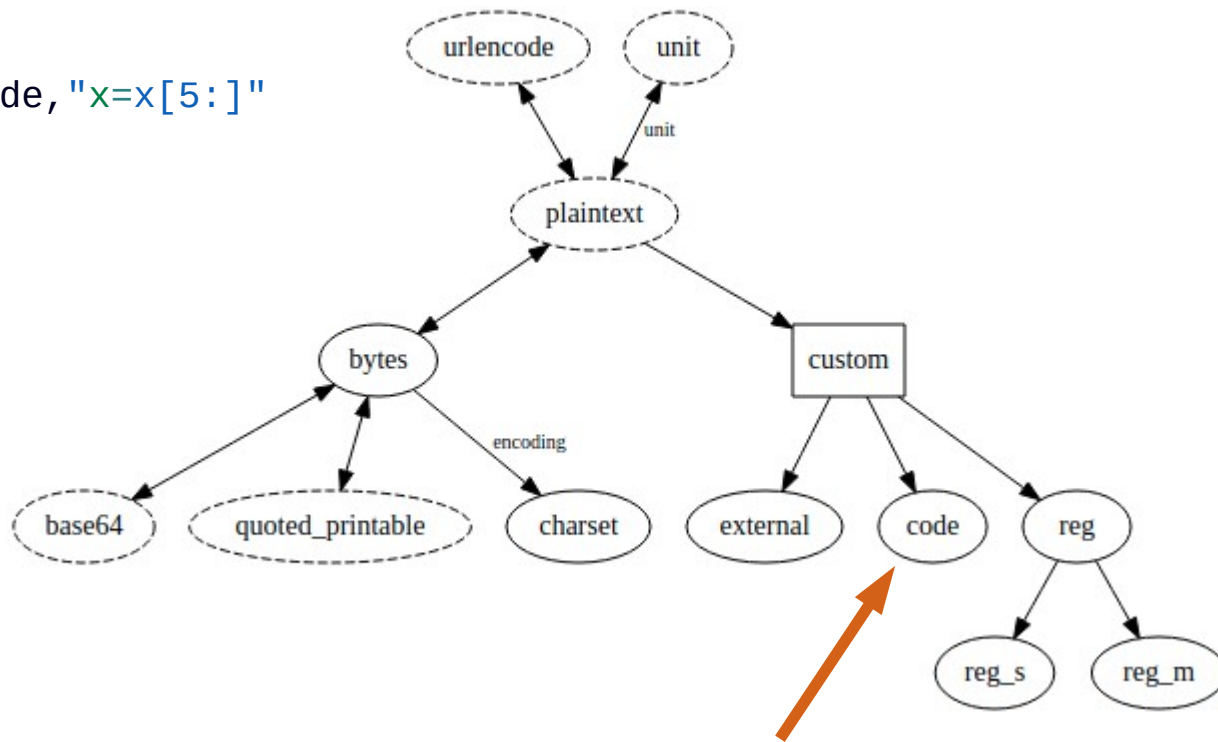
Convey – custom fields



```
$ convey email@example.com -f code, "x=x[5:]"
```

Input value detected: email

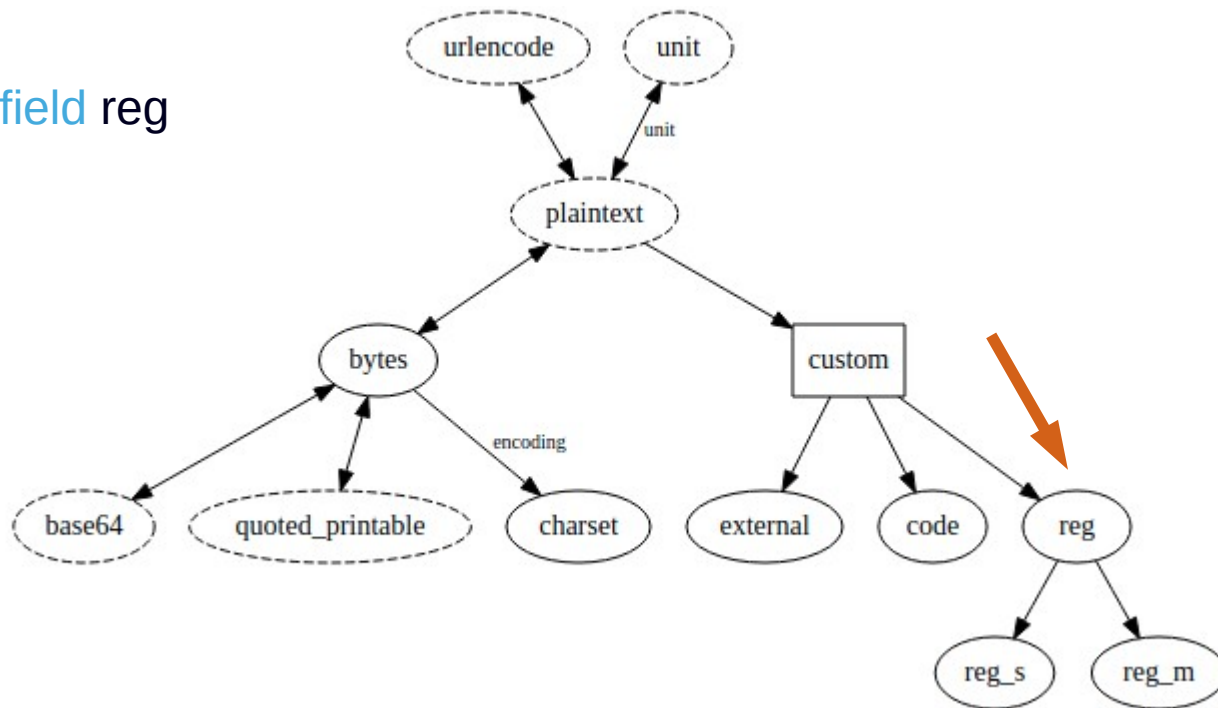
field	value
code	@example.com



Convey – custom fields



\$ convey email@example.com --field reg



Convey – custom fields



\$ convey email@example.com --field reg

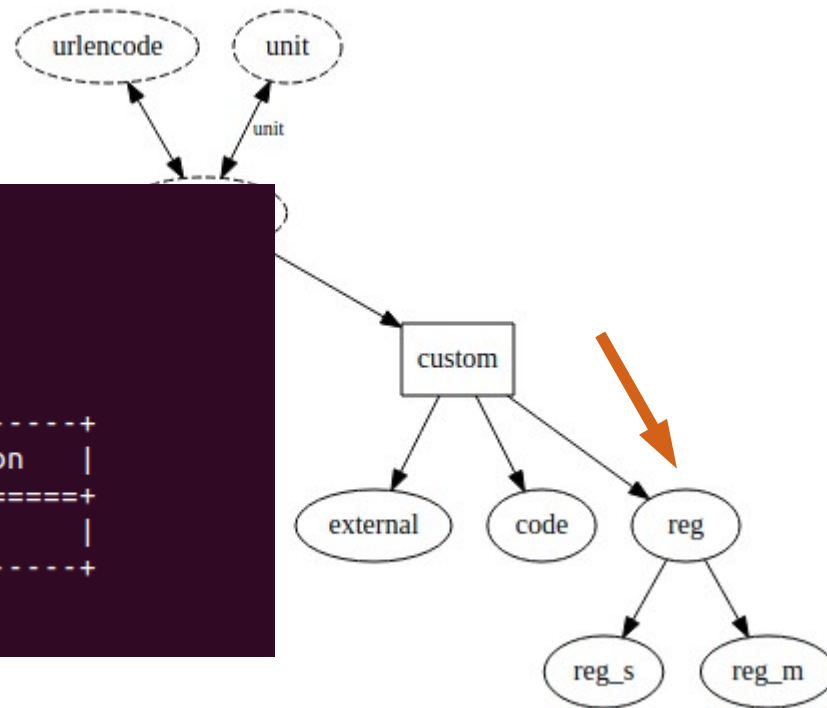
Input value detected: email

Regular match: █

Preview

original	group {0}	match	substitution
email@example.com			

. - any char, \w - word, \d - digit, () - matching group



Convey – custom fields



\$ convey email@example.com --field reg

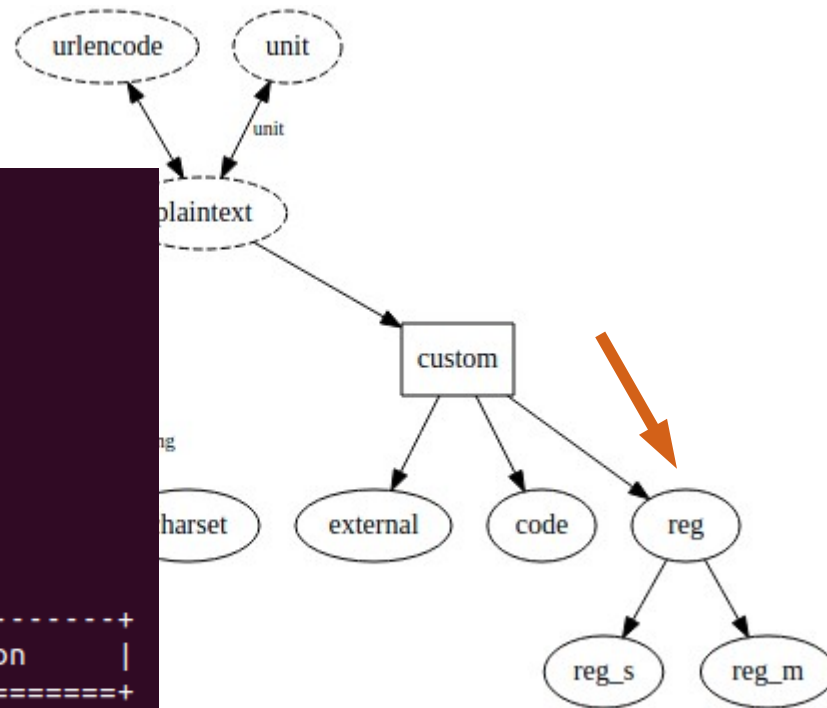
Input value detected: email

Regular match: @

Preview

original	group {0}	match	substitution
email@example.com	@	@	emailexample.com

. - any char, \w - word, \d - digit, () - matching group



Convey – custom fields



\$ convey email@example.com --field reg

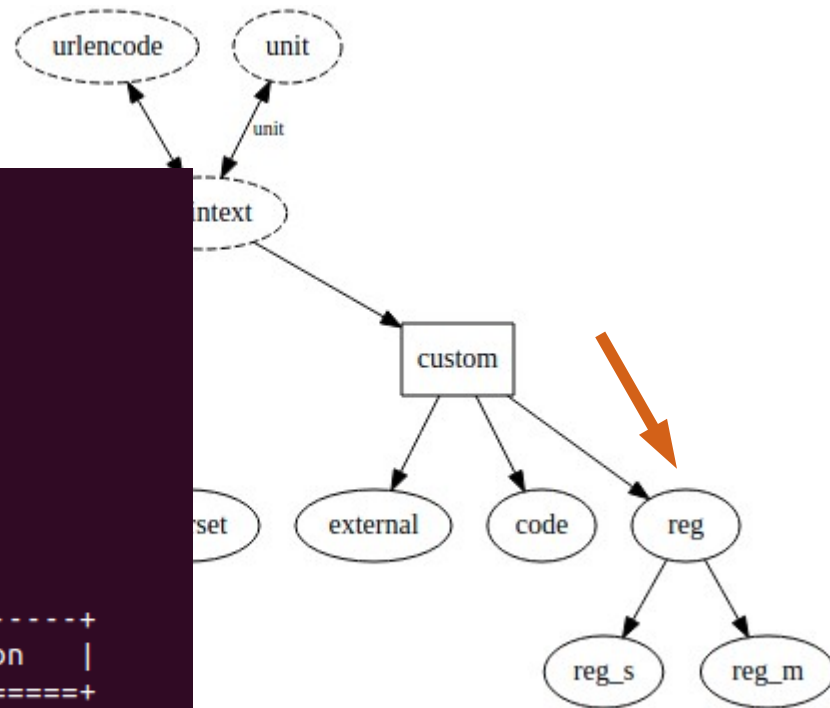
Input value detected: email

Regular match: @[a-z]{3}

Preview

original	group {0}	match	substitution
email@example.com	@exa	@exa	emailmple.com

. - any char, \w - word, \d - digit, () - matching group



Convey – custom fields



\$ convey email@example.com --field reg

Input value detected: email

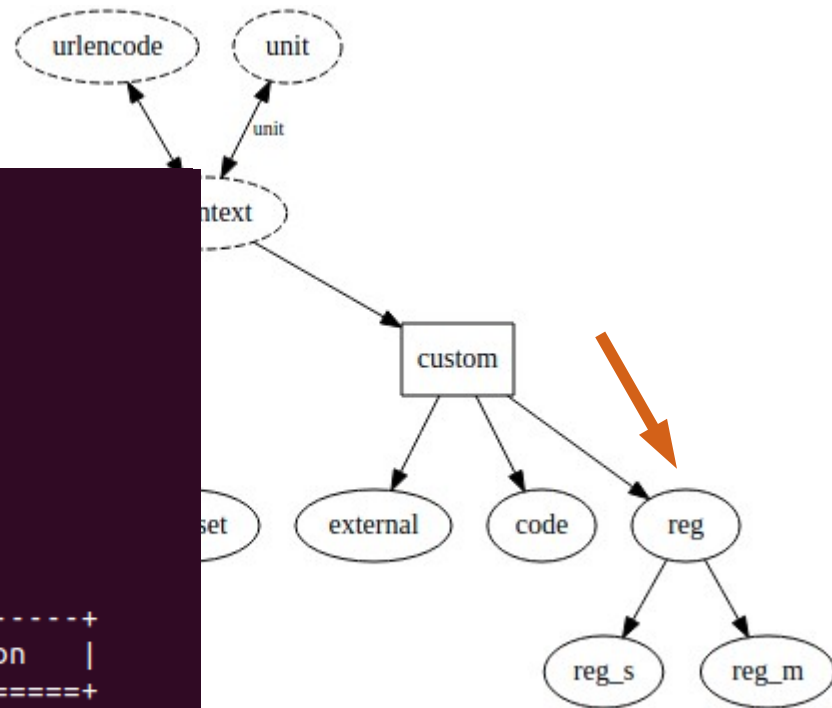
Regular match: @[a-z]{3}

Regular replace:

Preview

original	group {0}	match	substitution
email@example.com	@exa	@exa	emailmple.com

Access matched parts with {0}, ex: string {1} string.



Convey – custom fields



\$ convey email@example.com --field reg

```
Input value detected: email
```

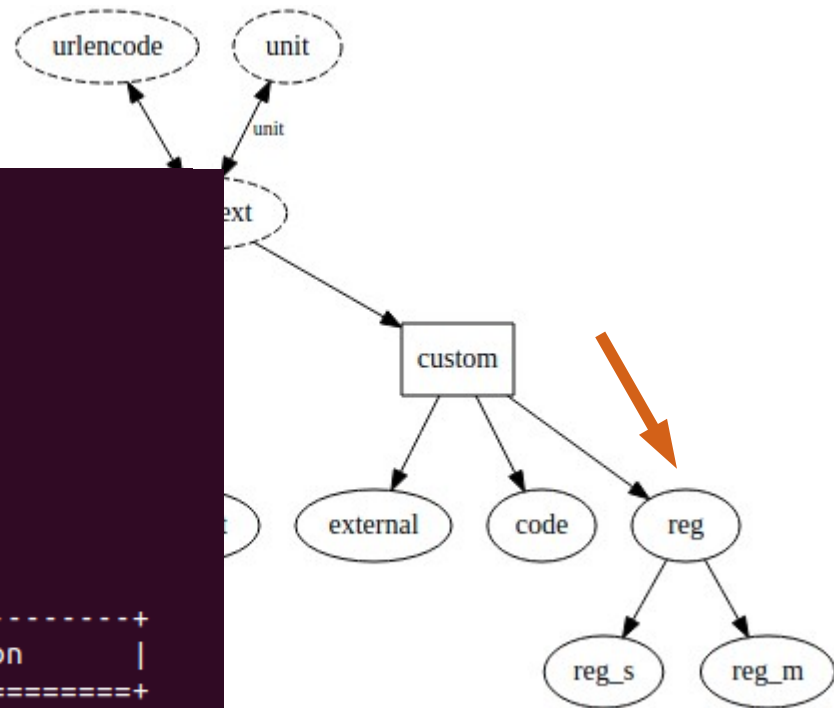
```
Regular match: @[a-z]{3}
```

```
Regular replace: @foo
```

```
Preview
```

original	group {0}	match	substitution
email@example.com	@exa	@foo	email@foomple.com

```
Access matched parts with {0}, ex: string {1} string.
```



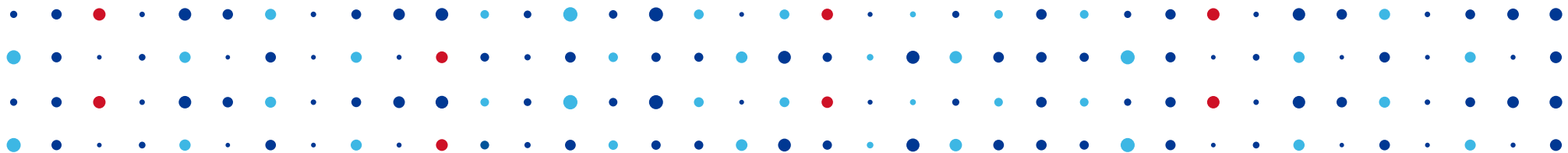
GAME

OVER

Contents

- Schedule-shift <https://github.com/CZ-NIC/schedule-shift>
- Run-or-raise <https://extensions.gnome.org/extension/1336/run-or-raise/>
- Envelope `pip3 install envelope`
- Convey `pip3 install convey`





`https://github.com/CZ-NIC/schedule-shift`

Thanks

`https://extensions.gnome.org/extension/1336/run-or-raise/`

`pip3 install envelope`

`pip3 install convey`

Edvard Rejthar • edvard.rejthar@nic.cz



Spolufinancováno Evropskou unií
Nástroj pro propojení Evropy



cz.nic | SPRÁVCE
DOMÉNY CZ