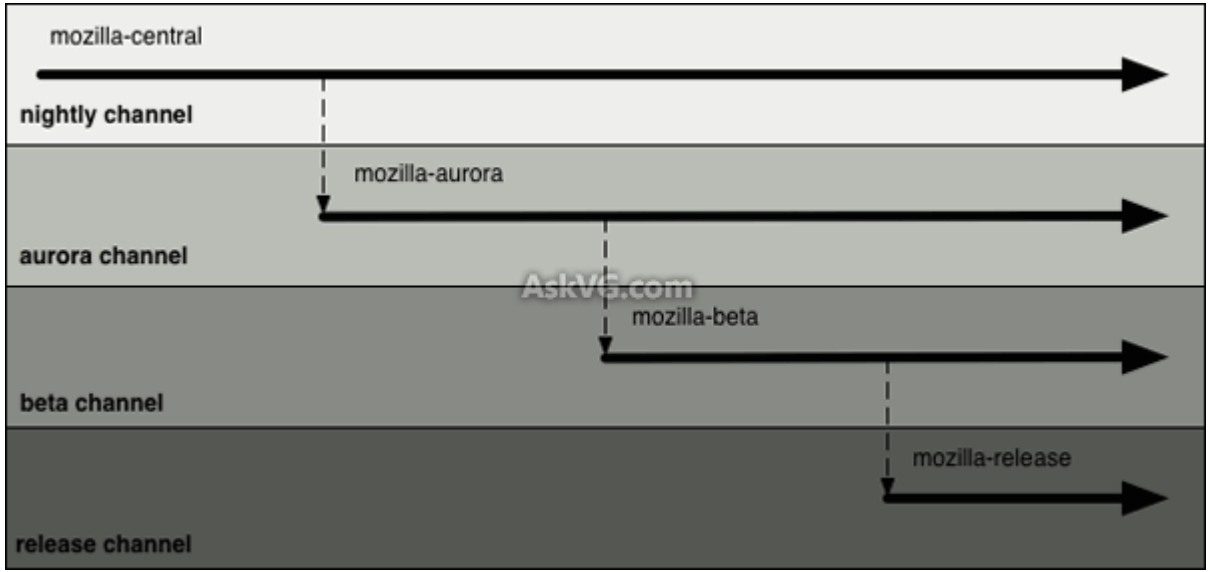
Firefox with TUF

Team Orange

Introduction

- Mozilla uses “four-channel system”



TUF Metadata Scheme

- Nightly and Aurora built daily
  - Delegated role ; automatic signing
  - Online key
- Beta and Stable built less often
  - Offline key ; Mozilla developer signs
  - No need for delegated rule
  - Use Target rule

TUF Metadata Scheme

- Current implementation supports v24=>v25
- Scheme will support
  - 26.0b4 => 26.0b6 (beta)
  - 27.0a1 => 27.0a2 (alpha,aurora)
  - 28.0a1 => 28.0a2 (pre-alpha,nightly)

Security Impact

- Indefinite Freeze Attack
  - TUF metadata would be version-aware
  - Firefox sends request for bad version => TUF disregards and gets correct version

Security Impact

- Endless Data Attack
  - If update.xml compromised, then Firefox update mechanism may be susceptible
  - Tuf maintains integrity of files => update.xml cannot be compromised

Security Impact

- Slow Retrieval Attack
  - Target files will be retrieved from TUF repo
  - Since TUF repo will be previously verified, attack is not possible

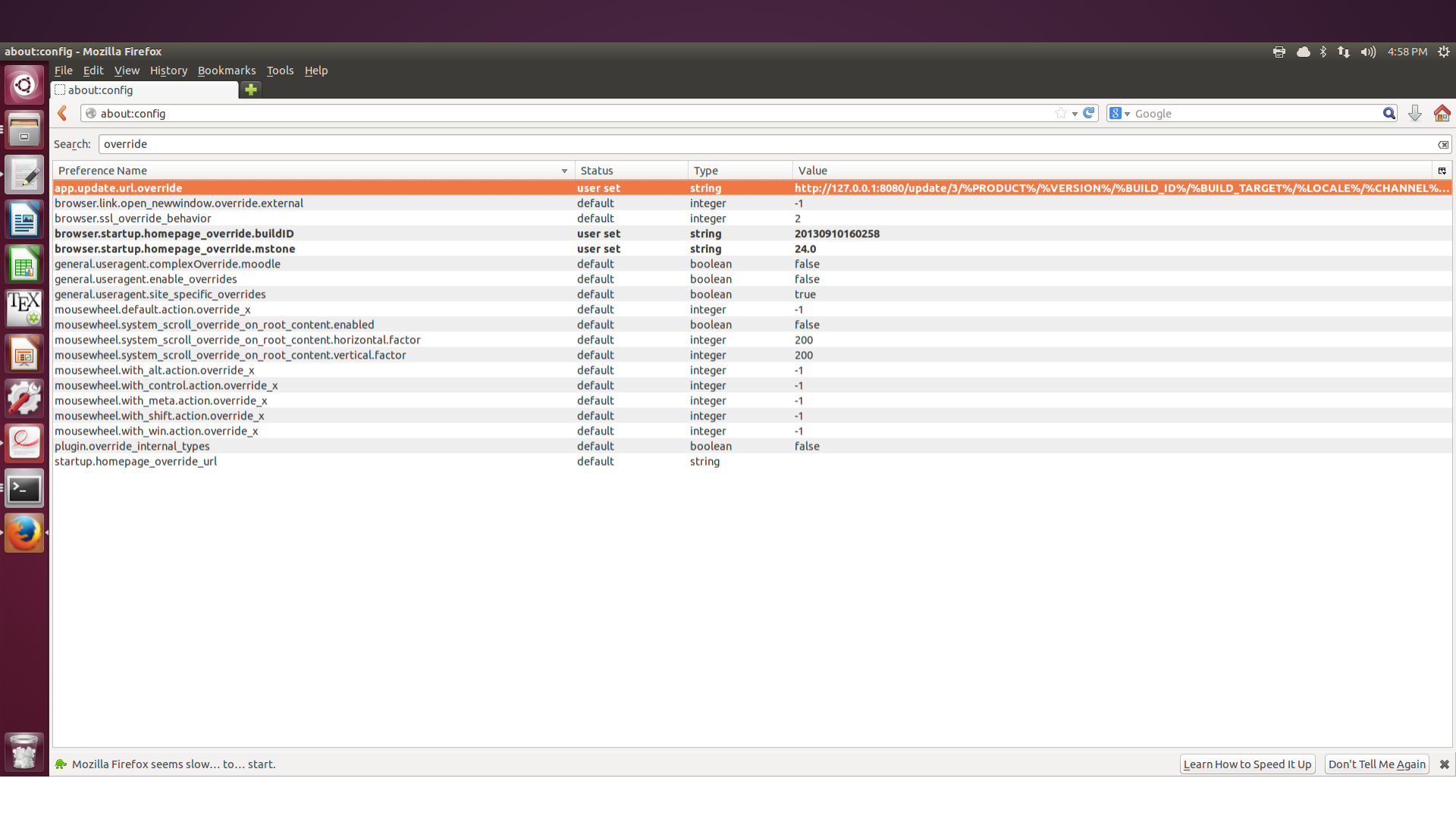
Usability Impact

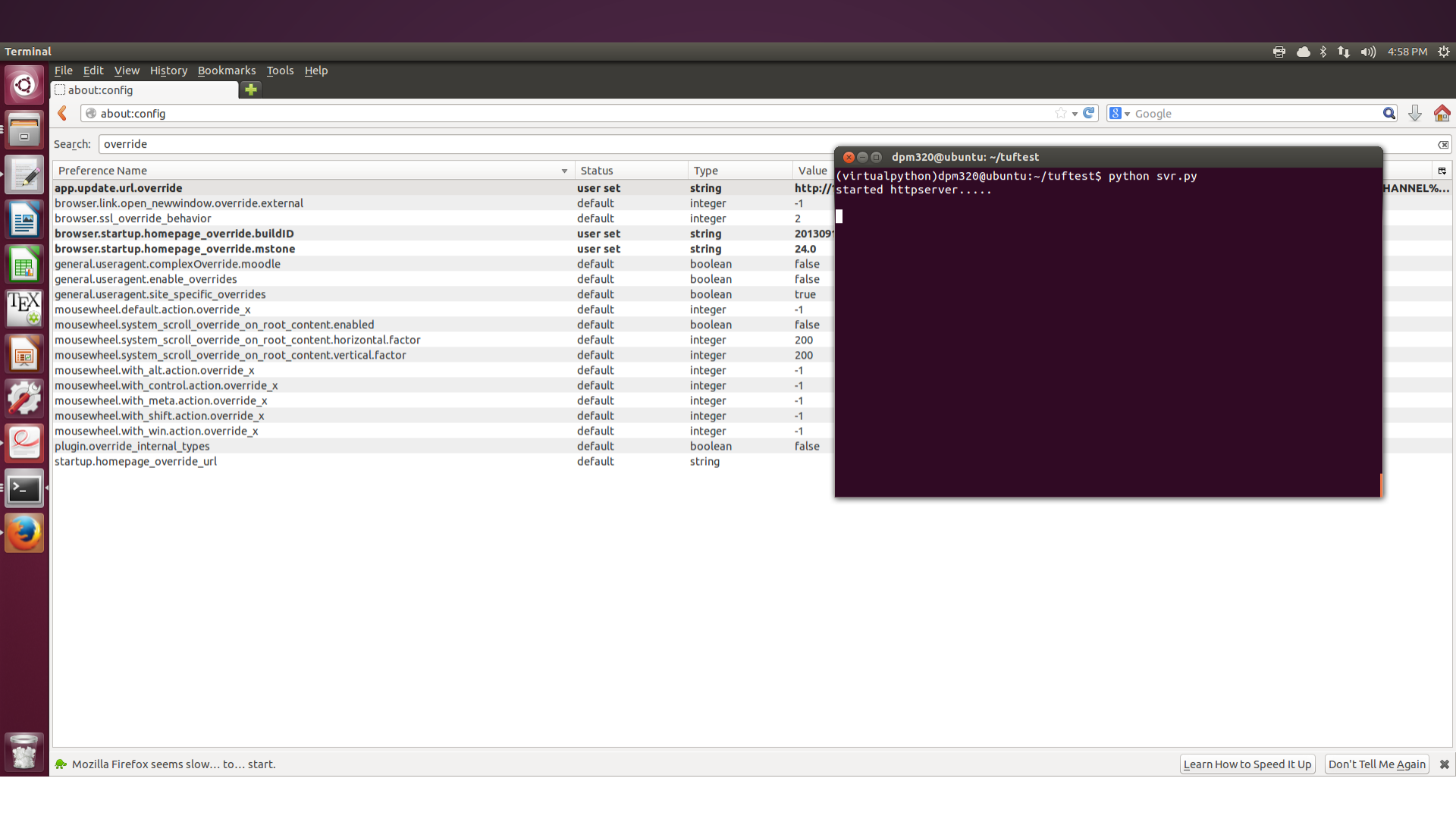
- Aurora/Nightly builds signed automatically
  - No impact
- Beta/Stable builds signed by developer
  - Impact of additional step

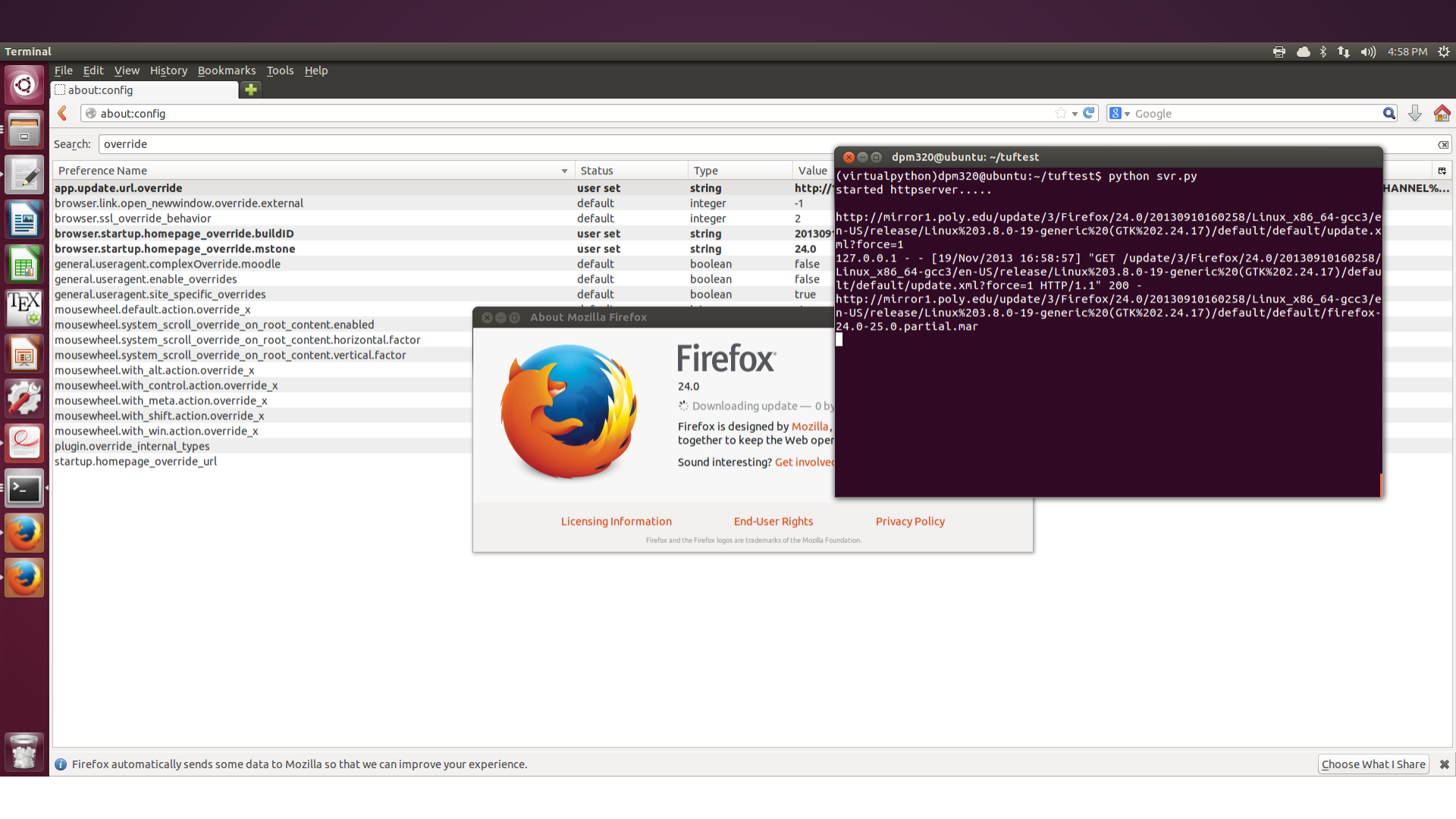
Efficiency Impact

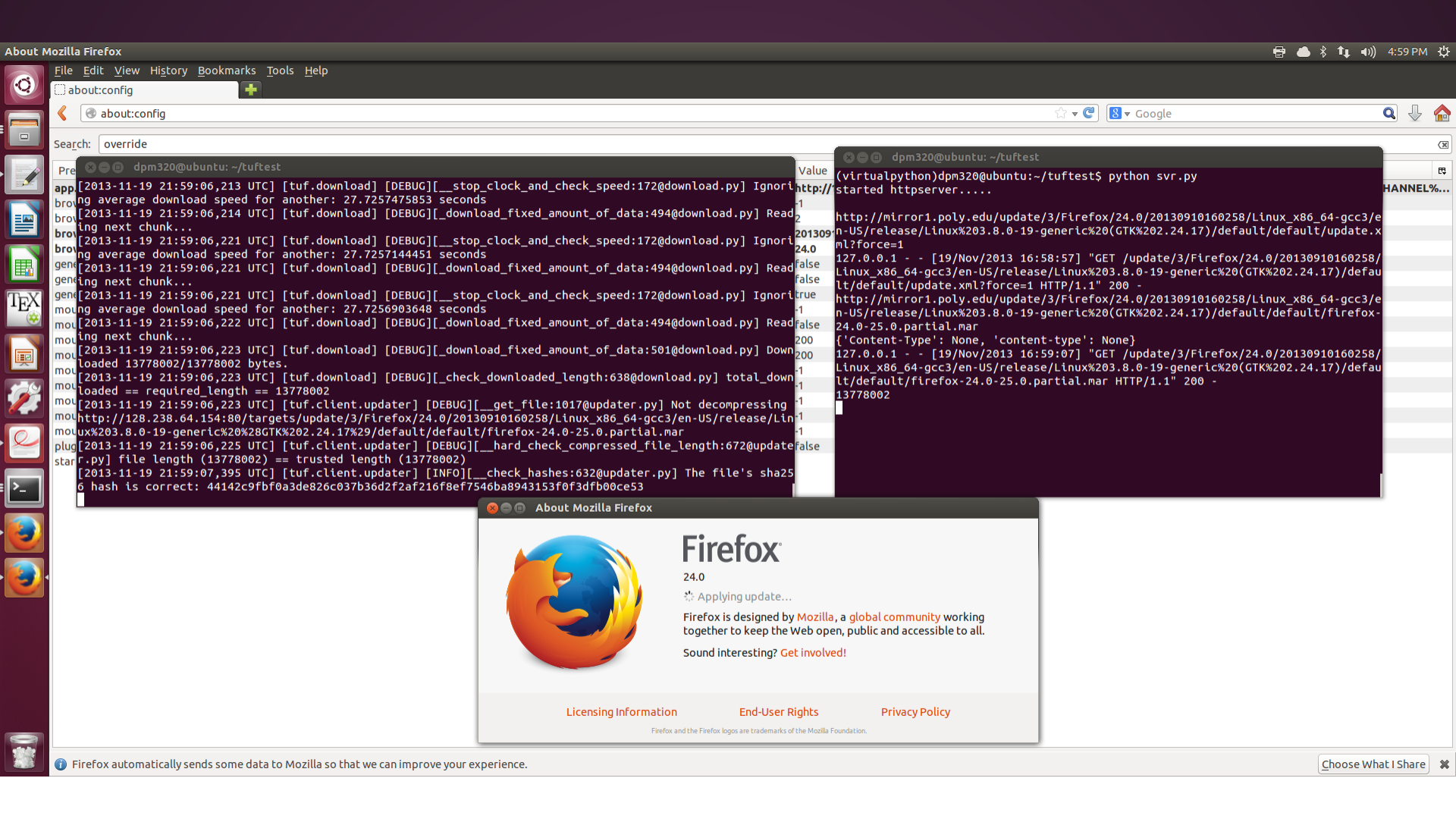
- Could possibly improve on speed
  - Put TUF mirror on fast network

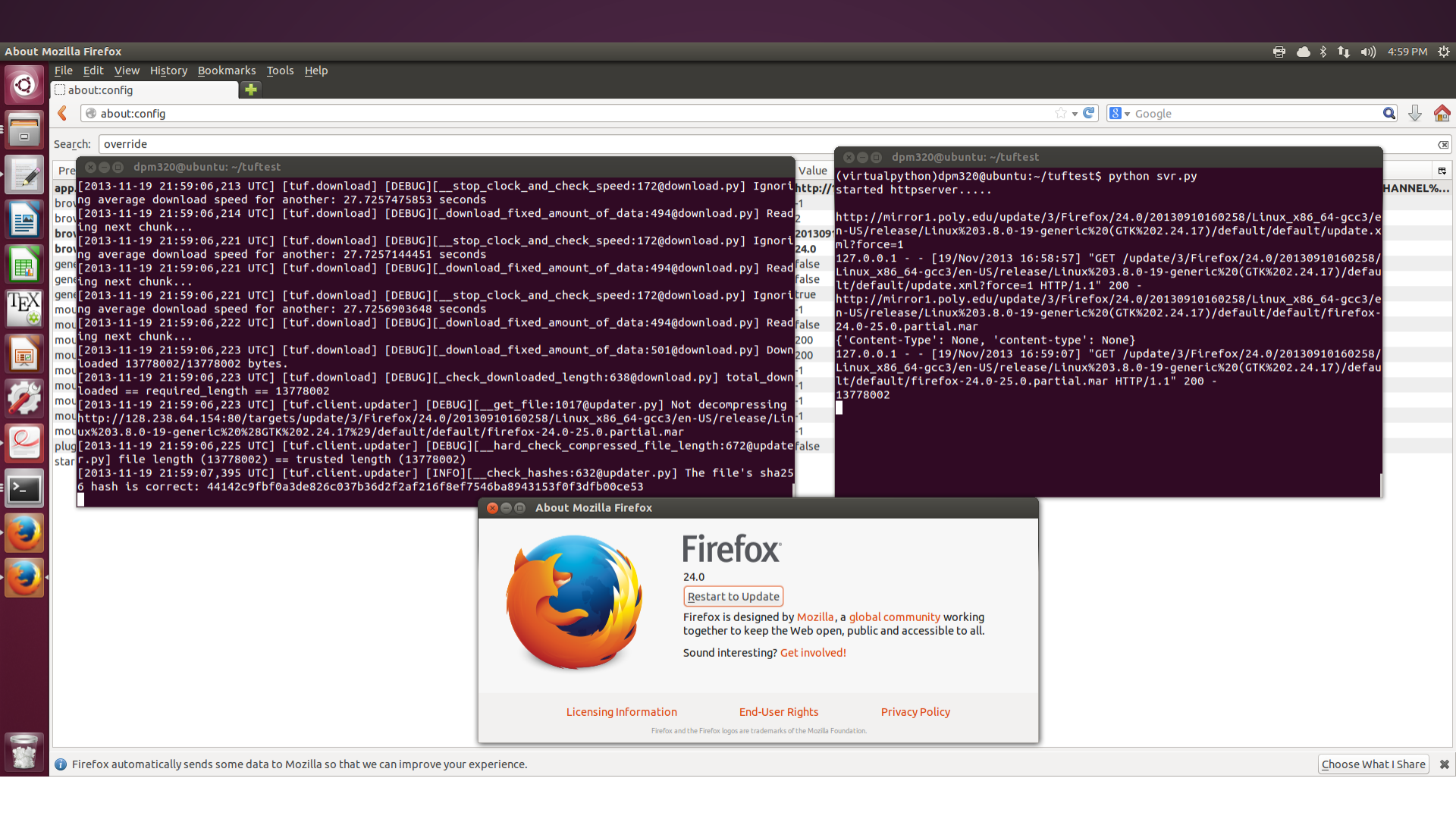
Demo


about:config - Mozilla Firefox
4:58 PM
File Edit View History Bookmarks Tools Help
about:config
about:config
Google
Search: override
Preference Name
Status
Type
Value
app.update.url.override
user set
string
http://127.0.0.1:8080/update/3/%PRODUCT%/%VERSION%/%BUILD_ID%/%BUILD_TARGET%/%LOCALE%/%CHANNEL%...
browser.link.open_newwindow.override.external
default
integer
-1
browser.ssl_override_behavior
default
integer
2
browser.startup.homepage_override.buildID
user set
string
20130910160258
browser.startup.homepage_override.mstone
user set
string
24.0
general.useragent.complexOverride.moodle
default
boolean
false
general.useragent.enable_overrides
default
boolean
false
general.useragent.site_specific_overrides
default
boolean
true
mousewheel.default.action.override_x
default
integer
-1
mousewheel.system_scroll_override_on_root_content.enabled
default
boolean
false
mousewheel.system_scroll_override_on_root_content.horizontal.factor
default
integer
200
mousewheel.system_scroll_override_on_root_content.vertical.factor
default
integer
200
mousewheel.with_alt.action.override_x
default
integer
-1
mousewheel.with_control.action.override_x
default
integer
-1
mousewheel.with_meta.action.override_x
default
integer
-1
mousewheel.with_shift.action.override_x
default
integer
-1
mousewheel.with_win.action.override_x
default
integer
-1
plugin.override_internal_types
default
boolean
false
startup.homepage_override_url
default
string
Mozilla Firefox seems slow... to... start.
Learn How to Speed It Up
Don't Tell Me Again


Terminal
4:58 PM
File Edit View History Bookmarks Tools Help
about:config
about:config
Google
Search: override
Preference Name
Status
Type
Value
app.update.url.override user set string http://
HANNEL%...
browser.link.open_newwindow.override.external default integer -1
browser.ssl_override_behavior default integer 2
browser.startup.homepage_override.buildID user set string 201309
browser.startup.homepage_override.mstone user set string 24.0
general.useragent.complexOverride.moodle default boolean false
general.useragent.enable_overrides default boolean false
general.useragent.site_specific_overrides default boolean true
mousewheel.default.action.override_x default integer -1
mousewheel.system_scroll_override_on_root_content.enabled default boolean false
mousewheel.system_scroll_override_on_root_content.horizontal.factor default integer 200
mousewheel.system_scroll_override_on_root_content.vertical.factor default integer 200
mousewheel.with_alt.action.override_x default integer -1
mousewheel.with_control.action.override_x default integer -1
mousewheel.with_meta.action.override_x default integer -1
mousewheel.with_shift.action.override_x default integer -1
mousewheel.with_win.action.override_x default integer -1
plugin.override_internal_types default boolean false
startup.homepage_override_url default string
dpm320@ubuntu: ~/tuftest
(virtualpython)dpm320@ubuntu:~/tuftest$ python svr.py
started httpserver.....
Mozilla Firefox seems slow... to... start.
Learn How to Speed It Up
Don't Tell Me Again


Terminal
4:58 PM
File Edit View History Bookmarks Tools Help
about:config
about:config
Google
Search: override
Preference Name
Status
Type
Value
app.update.url.override
user set
string
http://
HANNEL%...
browser.link.open_newwindow.override.external
default
integer
-1
browser.ssl_override_behavior
default
integer
2
browser.startup.homepage_override.buildID
user set
string
201309
browser.startup.homepage_override.mstone
user set
string
24.0
general.useragent.complexOverride.moodle
default
boolean
false
general.useragent.enable_overrides
default
boolean
false
general.useragent.site_specific_overrides
default
boolean
true
mousewheel.default.action.override_x
mousewheel.system_scroll_override_on_root_content.enabled
mousewheel.system_scroll_override_on_root_content.horizontal.factor
mousewheel.system_scroll_override_on_root_content.vertical.factor
mousewheel.with_alt.action.override_x
mousewheel.with_control.action.override_x
mousewheel.with_meta.action.override_x
mousewheel.with_shift.action.override_x
mousewheel.with_win.action.override_x
plugin.override_internal_types
startup.homepage_override_url
About Mozilla Firefox
Firefox
24.0
Downloading update — 0 by
Firefox is designed by Mozilla,
together to keep the Web oper
Sound interesting? Get involve
Licensing Information
End-User Rights
Privacy Policy
Firefox and the Firefox logos are trademarks of the Mozilla Foundation.
dpm320@ubuntu: ~/tuftest
(virtualpython)dpm320@ubuntu:~/tuftest$ python svr.py
started httpserver.....
http://mirror1.poly.edu/update/3/Firefox/24.0/20130910160258/Linux_x86_64-gcc3/en-US/release/Linux%203.8.0-19-generic%20(GTK%202.24.17)/default/default/update.xml?force=1
127.0.0.1 - - [19/Nov/2013 16:58:57] "GET /update/3/Firefox/24.0/20130910160258/Linux_x86_64-gcc3/en-US/release/Linux%203.8.0-19-generic%20(GTK%202.24.17)/default/default/update.xml?force=1 HTTP/1.1" 200 -
http://mirror1.poly.edu/update/3/Firefox/24.0/20130910160258/Linux_x86_64-gcc3/en-US/release/Linux%203.8.0-19-generic%20(GTK%202.24.17)/default/default/firefox-24.0-25.0.partial.mar
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share


About Mozilla Firefox
4:59 PM
File Edit View History Bookmarks Tools Help
about:config
about:config
Google
Search: override
dpm320@ubuntu: ~/tuftest
[2013-11-19 21:59:06,213 UTC] [tuf.download] [DEBUG][__stop_clock_and_check_speed:172@download.py] Ignoring average download speed for another: 27.7257475853 seconds
[2013-11-19 21:59:06,214 UTC] [tuf.download] [DEBUG][_download_fixed_amount_of_data:494@download.py] Reading next chunk...
[2013-11-19 21:59:06,221 UTC] [tuf.download] [DEBUG][__stop_clock_and_check_speed:172@download.py] Ignoring average download speed for another: 27.7257144451 seconds
[2013-11-19 21:59:06,221 UTC] [tuf.download] [DEBUG][_download_fixed_amount_of_data:494@download.py] Reading next chunk...
[2013-11-19 21:59:06,221 UTC] [tuf.download] [DEBUG][__stop_clock_and_check_speed:172@download.py] Ignoring average download speed for another: 27.7256903648 seconds
[2013-11-19 21:59:06,222 UTC] [tuf.download] [DEBUG][_download_fixed_amount_of_data:494@download.py] Reading next chunk...
[2013-11-19 21:59:06,223 UTC] [tuf.download] [DEBUG][_download_fixed_amount_of_data:501@download.py] Downloaded 13778002/13778002 bytes.
[2013-11-19 21:59:06,223 UTC] [tuf.download] [DEBUG][_check_downloaded_length:638@download.py] total_downloaded == required_length == 13778002
[2013-11-19 21:59:06,223 UTC] [tuf.client.updater] [DEBUG][__get_file:1017@updater.py] Not decompressing http://128.238.64.154:80/targets/update/3/Firefox/24.0/20130910160258/Linux_x86_64-gcc3/en-US/release/Linux%203.8.0-19-generic%20%28GTK%202.24.17%29/default/default/firefox-24.0-25.0.partial.mar
[2013-11-19 21:59:06,225 UTC] [tuf.client.updater] [DEBUG][__hard_check_compressed_file_length:672@updater.py] file length (13778002) == trusted length (13778002)
[2013-11-19 21:59:07,395 UTC] [tuf.client.updater] [INFO][__check_hashes:632@updater.py] The file's sha256 hash is correct: 44142c9fbf0a3de826c037b36d2f2af216f8ef7546ba8943153f0f3dfb00ce53
dpm320@ubuntu: ~/tuftest
(virtualpython)dpm320@ubuntu:~/tuftest$ python svr.py
started httpserver.....
http://mirror1.poly.edu/update/3/Firefox/24.0/20130910160258/Linux_x86_64-gcc3/en-US/release/Linux%203.8.0-19-generic%20(GTK%202.24.17)/default/default/update.xml?force=1
127.0.0.1 - - [19/Nov/2013 16:58:57] "GET /update/3/Firefox/24.0/20130910160258/Linux_x86_64-gcc3/en-US/release/Linux%203.8.0-19-generic%20(GTK%202.24.17)/default/default/update.xml?force=1 HTTP/1.1" 200 -
http://mirror1.poly.edu/update/3/Firefox/24.0/20130910160258/Linux_x86_64-gcc3/en-US/release/Linux%203.8.0-19-generic%20(GTK%202.24.17)/default/default/firefox-24.0-25.0.partial.mar
{'Content-Type': None, 'content-type': None}
127.0.0.1 - - [19/Nov/2013 16:59:07] "GET /update/3/Firefox/24.0/20130910160258/Linux_x86_64-gcc3/en-US/release/Linux%203.8.0-19-generic%20(GTK%202.24.17)/default/default/firefox-24.0-25.0.partial.mar HTTP/1.1" 200 -
13778002
About Mozilla Firefox
Firefox
24.0
Applying update…
Firefox is designed by Mozilla, a global community working together to keep the Web open, public and accessible to all.
Sound interesting? Get involved!
Licensing Information
End-User Rights
Privacy Policy
Firefox and the Firefox logos are trademarks of the Mozilla Foundation.
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share


About Mozilla Firefox
4:59 PM
File Edit View History Bookmarks Tools Help
about:config
about:config
Google
Search: override
dpm320@ubuntu: ~/tuftest
[2013-11-19 21:59:06,213 UTC] [tuf.download] [DEBUG][__stop_clock_and_check_speed:172@download.py] Ignoring average download speed for another: 27.7257475853 seconds
[2013-11-19 21:59:06,214 UTC] [tuf.download] [DEBUG][_download_fixed_amount_of_data:494@download.py] Reading next chunk...
[2013-11-19 21:59:06,221 UTC] [tuf.download] [DEBUG][__stop_clock_and_check_speed:172@download.py] Ignoring average download speed for another: 27.7257144451 seconds
[2013-11-19 21:59:06,221 UTC] [tuf.download] [DEBUG][_download_fixed_amount_of_data:494@download.py] Reading next chunk...
[2013-11-19 21:59:06,221 UTC] [tuf.download] [DEBUG][__stop_clock_and_check_speed:172@download.py] Ignoring average download speed for another: 27.7256903648 seconds
[2013-11-19 21:59:06,222 UTC] [tuf.download] [DEBUG][_download_fixed_amount_of_data:494@download.py] Reading next chunk...
[2013-11-19 21:59:06,223 UTC] [tuf.download] [DEBUG][_download_fixed_amount_of_data:501@download.py] Downloaded 13778002/13778002 bytes.
[2013-11-19 21:59:06,223 UTC] [tuf.download] [DEBUG][_check_downloaded_length:638@download.py] total_downloaded == required_length == 13778002
[2013-11-19 21:59:06,223 UTC] [tuf.client.updater] [DEBUG][__get_file:1017@updater.py] Not decompressing http://128.238.64.154:80/targets/update/3/Firefox/24.0/20130910160258/Linux_x86_64-gcc3/en-US/release/Linux%203.8.0-19-generic%20%28GTK%202.24.17%29/default/default/firefox-24.0-25.0.partial.mar
[2013-11-19 21:59:06,225 UTC] [tuf.client.updater] [DEBUG][__hard_check_compressed_file_length:672@updater.py] file length (13778002) == trusted length (13778002)
[2013-11-19 21:59:07,395 UTC] [tuf.client.updater] [INFO][__check_hashes:632@updater.py] The file's sha256 hash is correct: 44142c9fbf0a3de826c037b36d2f2af216f8ef7546ba8943153f0f3dfb00ce53
dpm320@ubuntu: ~/tuftest
(virtualpython)dpm320@ubuntu:~/tuftest$ python svr.py
started httpserver.....
http://mirror1.poly.edu/update/3/Firefox/24.0/20130910160258/Linux_x86_64-gcc3/en-US/release/Linux%203.8.0-19-generic%20(GTK%202.24.17)/default/default/update.xml?force=1
127.0.0.1 - - [19/Nov/2013 16:58:57] "GET /update/3/Firefox/24.0/20130910160258/Linux_x86_64-gcc3/en-US/release/Linux%203.8.0-19-generic%20(GTK%202.24.17)/default/default/update.xml?force=1 HTTP/1.1" 200 -
http://mirror1.poly.edu/update/3/Firefox/24.0/20130910160258/Linux_x86_64-gcc3/en-US/release/Linux%203.8.0-19-generic%20(GTK%202.24.17)/default/default/firefox-24.0-25.0.partial.mar
{'Content-Type': None, 'content-type': None}
127.0.0.1 - - [19/Nov/2013 16:59:07] "GET /update/3/Firefox/24.0/20130910160258/Linux_x86_64-gcc3/en-US/release/Linux%203.8.0-19-generic%20(GTK%202.24.17)/default/default/firefox-24.0-25.0.partial.mar HTTP/1.1" 200 -
13778002
About Mozilla Firefox
Firefox
24.0
Restart to Update
Firefox is designed by Mozilla, a global community working together to keep the Web open, public and accessible to all.
Sound interesting? Get involved!
Licensing Information
End-User Rights
Privacy Policy
Firefox and the Firefox logos are trademarks of the Mozilla Foundation.
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share


About Mozilla Firefox
Firefox
25.0
Firefox is up to date
Firefox is designed by Mozilla, a global community working together to keep the Web open, public and accessible to all.
Sound interesting? Get involved!
Licensing Information
End-User Rights
Privacy Policy
Firefox and the Firefox logos are trademarks of the Mozilla Foundation.