

Miscellaneous Linux Tricks

Paul Elliott
pelliott@io.com

<http://www.FreeBlackPatchPanel.com/pme/linux/MiscLinux.pdf>

Miscellaneous Linux Tricks



- Gnome Partition Editor (gparted) CD for partitions
- Mount lost partitions
- Linux boot floppy (with filesystem)
- Linux boot CD
- fetchmail with openssl

Gparted: Gnome Partition Editor

The screenshot shows the GParted application window with the following components:

- Toolbar:** New, Delete, Resize/Move, Copy, Paste, Undo, Apply.
- Device Selection:** /dev/sda (17.09 GB)
- Visual Representation:** A horizontal bar representing the disk layout. A yellow bar represents the /dev/sda3 partition (15.99 GB). A white bar represents unused space.
- Legend:** ext2 (blue square), linux-swap (red square), used (yellow square), unused (white square).
- Table:**

Partition	Filesystem	Size	Used	Unused	Flags
/dev/sda1	ext2	101.95 MB	13.34 MB	88.61 MB	boot
/dev/sda2	linux-swap	1019.76 MB	---	---	
/dev/sda3	ext2	15.99 GB	13.19 GB	2.81 GB	

0 operations pending

Gparted: Table of functionality

Are you sure you need to pay money for Partition Magic?

	Detect	Read	Create	Grow	Shrink	Move	Copy	Check	Required software
ext2	✓	✓	✓	✓	✓	✗	✓ [1]	✓	e2fsprogs
ext3	✓	✓	✓	✓	✓	✗	✓ [1]	✓	e2fsprogs
fat16	✓	✓	✓	✓ [4]	✓ [4]	✓ [4]	✓ [1]	✓	dosfstools
fat32	✓	✓	✓	✓ [4]	✓ [4]	✓ [4]	✓ [1]	✓	dosfstools
hfs	✓	✓	✓	✗	✓ [4]	✗	✓ [1]	✗	hfsutils
hfs+	✓	✓	✗	✗	✓ [4]	✗	✓ [1]	✗	
jfs	✓	✓	✓	✓ [2]	✗	✗	✓ [1]	✓	jfsutils
linux-swap	✓	✗	✓	✓	✓	✓	✓ [1]	✗	mkswap (part of util-linux)
ntfs	✓	✓	✓	✓	✓	✗	✓	✓	ntfsprogs
reiserfs	✓	✓	✓	✓	✓	✗	✓ [1]	✓	reiserfsprogs
reiser4	✓	✓	✓	✗	✗	✗	✓ [1]	✓	reiser4progs
ufs	✓	✗	✗	✗	✗	✗	✗	✗	
xfs	✓	✓	✓	✓ [2]	✗ [3]	✗	✓	✓	xfsprogs

[1] The actual copy is performed by 'dd'.

[2] You need kernel support for this filesystem if you want to grow it (module needs to be loaded).

[3] Although it's not possible to shrink an xfs filesystem directly, you can shrink it using GParted's copy functionality.

[4] Native available through libparted.

Use the gparted LiveCD

gparted comes with Ubuntu LiveCD and perhaps others.

The Gparted LiveCD does not lock any existing partitions.

Find at: <http://gparted.sourceforge.net/livecd.php>
download the iso and burn with K3B!
Boot the CD to use gparted!

Hey, save your partition setup!

Save your partition table:

```
sfdisk -d /dev/hda > hda.pt
```

To restore:

```
sfdisk /dev/hda < hda.pt
```

Save your MBR!

Save you MBR (Master boot record)

```
dd if=/dev/hda of=hda.mbr bs=512 count=1
```

to restore:

```
dd if=hda.mbr of=/dev/hda
```

back these files up in case of disk crash.

To restore the primary partition table without overwriting the MBR type:

```
dd if=hda.mbr of=/dev/hda bs=1 count=64 \  
skip=446 seek=446
```

Mount lost partitions!



- Suppose your partition table is wiped out.
- But the partitions themselves are intact!
- And you know where the partitions are!
- Then you can recover!

fdisk -l -u /dev/sdb

- Disk /dev/sdb: 73.4 GB, 73407865856 bytes
- 255 heads, 63 sectors/track, 8924 cylinders, total 143374738 sectors
- Units = sectors of 1 * 512 = 512 bytes

•

•	Device	Boot	Start	End	Blocks	Id	System
•	/dev/sdb1		59504760	143364059	41929650	83	Linux
•	/dev/sdb2		53207280	59504759	3148740	83	Linux
•	/dev/sdb3		63	16064	8001	83	Linux
•	/dev/sdb4		16065	53207279	26595607+	83	Linux

•

- $16065 * 512 = 8225280$ so offset of /dev/sdb4 is 8225280 bytes.

Suppose our partition table is wiped out!

- Of course, getting the offset by doing `fdisk -l` would be impossible, that uses the partition table.
- mounting the partition directly, would also be impossible for the same reason.
- suppose we had the offset by other means such as:
 - scanning for first block of partition. (`gpart`)
 - we wrote it down before hand.

gpart - guess PC-type hard disk partitions



- gpart is a program that scans a hard disk looking for blocks that look like the start of a partition! It prints the offset (in 1K blocks) out. Does not use the partition table (by default).
- Read the gpart manual page!

http://www.stud.uni-hannover.de/user/76201/gpart/

Location Edit View Go Bookmarks Tools Settings Window Help

Location: <http://www.stud.uni-hannover.de/user/76201/gpart/>

gpart - Google Search gpart - Guess PC-type hard ...

gpart

Download First Aid Man-Page Links German Changes Author

gpart - Guess PC-type hard disk partitions

Gpart is a tool which tries to guess the primary partition table of a PC-type hard disk in case the primary partition table in sector 0 is damaged, incorrect or deleted. The guessed table can be written to a file or device. Supported (guessable) filesystem or partition types:

- DOS/Windows FAT (FAT 12/16/32)
- Linux ext2
- Linux swap partitions versions 0 and 1 (Linux >= v2.2.X)
- OS/2 HPFS
- Windows NT/2000 FS
- *BSD disklabels
- Solaris/x86 disklabels
- Minix FS
- Reiser FS
- Linux LVM physical volume module (LVM by Heinz Mauelshagen)
- SGI XFS on Linux
- BeOS filesystem
- QNX 4.x filesystem

Download

Current gpart source:	gpart-0.1h.tar.gz
Statically linked Linux binary (265364 Bytes):	gpart.linux

Page loaded.

losetup to the rescue!

- losetup is usually used for loopback encryption.
- But it can be used to create a device which is an offset into another device!
- `losetup -o 8225280 /dev/loop0 /dev/sdb`
- You can now mount the partition by mounting the loop back device.
- `mount -r /dev/loop0 /mnt`
- Now you can deal with the files and directories like any other mounted device.

Windows loves to overwrite the MBR!



- windoze likes to overwrite the master boot record. (note to all you dual boot people.)
- some Distros do not like to share the MBR! (if you install multiple distros on different partitions.
- So you need a boot floppy, or boot CD!

Boot floppy with filesystem is most flexible.



- Grub manual describes a different method.
- filesystem method allows you to easily change the menu, device map.
- extra space available for additional info.

Boot floppy with filesystem: Step 1



- make filesystem on floppy.
- `# mke2fs /dev/fd0`
- eliminate filesystem checks.
- `# tune2fs -c 0 /dev/fd0`
- `# tune2fs -c 0 /dev/fd0`

Boot floppy with filesystem: Step 2



- mount the filesystem, copy the grub files.
- `# mount /dev/fd0 /mnt`
- `# mkdir -p /mnt/boot/grub`
- `# for x in \`
- `/usr/lib/grub/*;do`
- `cp $x /mnt/boot/grub;`
- `done`

Boot floppy with filesystem: Step 3



- Setup the grub floppy
- # grub
- grub> root (fd0)
- grub> setup (fd0)
- grub> quit

Now would be a good time to save our work as a floppy image!



- `#umount /mnt`
- `# dd bs=18k if=/dev/fd0 \`
`of=grubFS.flp.img`
- `# mount /dev/fd0 /mnt`

Boot floppy with filesystem: Step 4



- Copy the menu, and device map.
- #
`cp /boot/grub/menu.lst \ /mnt
/boot/grub/menu.lst`
- #
`cp /boot/grub/device.map \ /m
nt/boot/grub/device.map`
- This step can be redone for a different grub setup!

What does a menu look like?

- `# Modified by YaST2. Last modification on Sun Jun 18 11:27:22 CDT 2006`
-
- `color white/blue black/light-gray`
- `default`
- `timeout 8`
- `gfxmenu (hd0,0)/message`
-
- `###Don't change this comment - YaST2 identifier: Original name: linux###`
- `title SUSE Linux 10.1`
- `root (hd0,0)`
- `kernel /vmlinuz root=/dev/sda3 vga=0x31a resume=/dev/sda2 splash=silent \
showopts`
- `initrd /initrd`

Boot floppy with filesystem: Step 5: extra information.



- There is plenty of extra space on the floppy.
- Why not save the partition table, MBR in case we need it later?
- ```
sfdisk -d /dev/sda \
> /mnt/sda.pt
```
- ```
# dd bs=512 count=1 \  
if=/dev/sda \  
of=/mnt/sda.mbr
```

Boot floppy with filesystem: Step 6



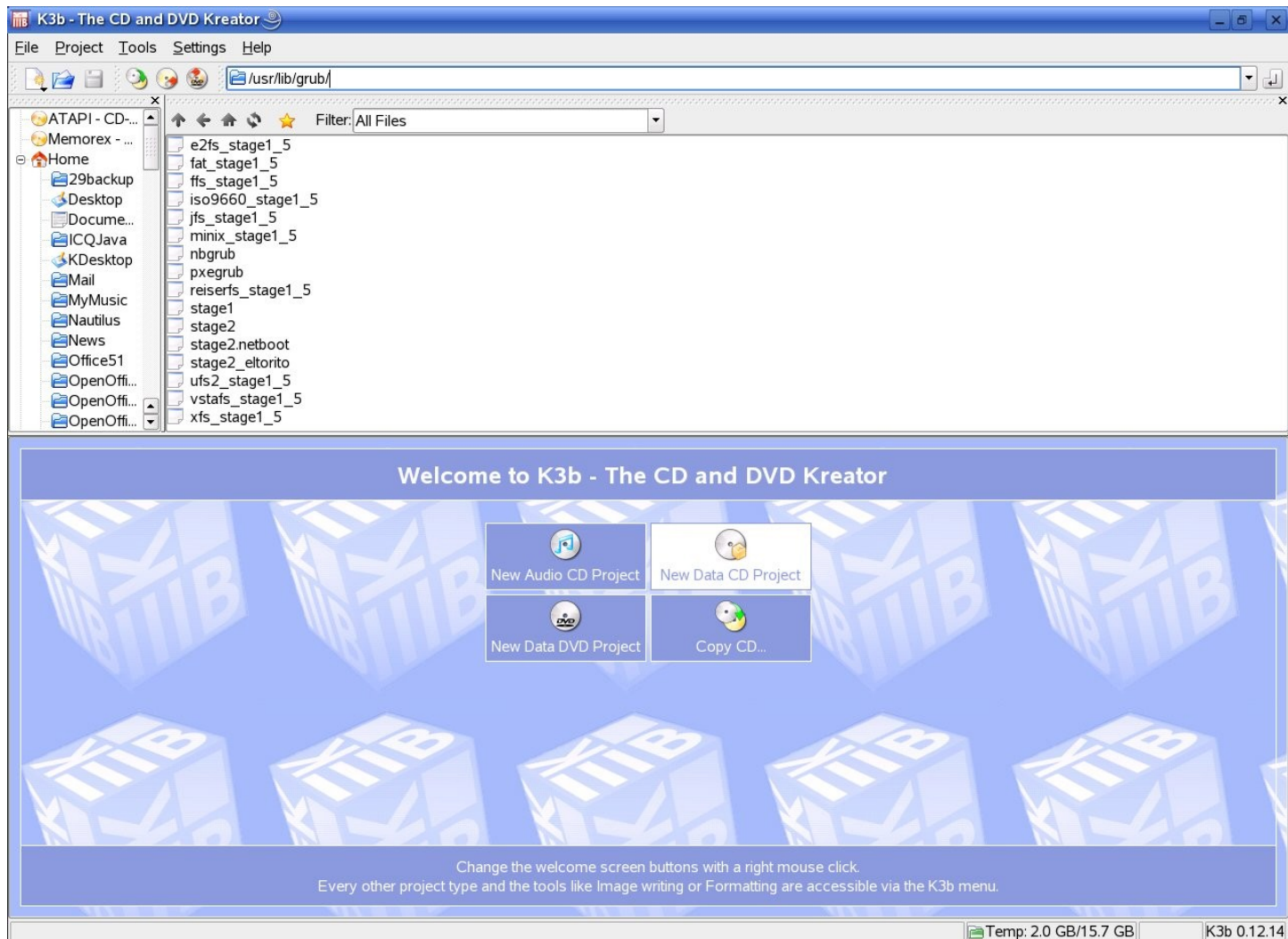
- Don't forget to unmount the filesystem before removing the floppy.
- `# umount /mnt`

Build a boot CD with K3B.

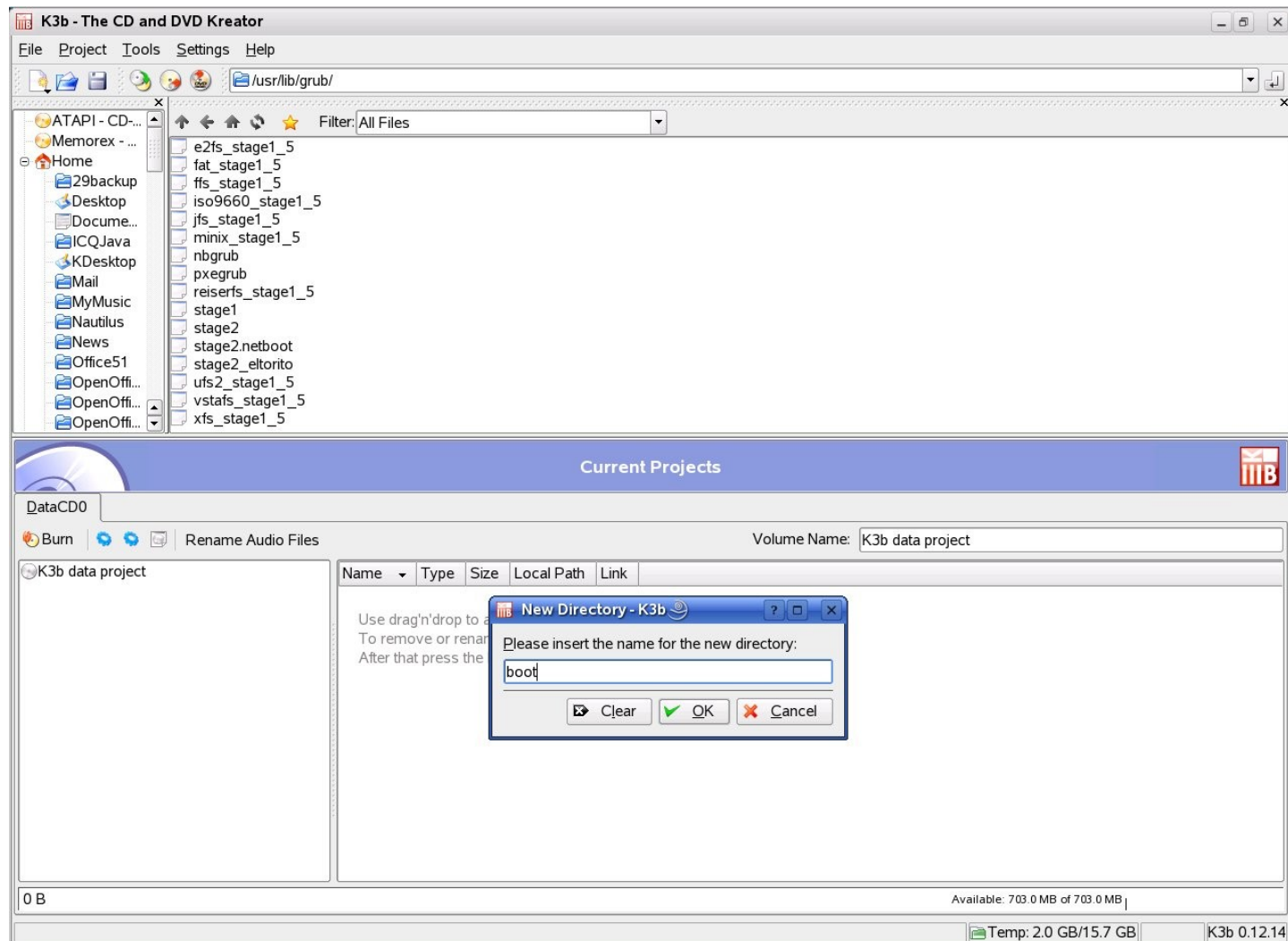


- Many newer computers have CD player but no floppy!
- Grub manual describes how to build boot CD from the command line.
 - <http://www.gnu.org/software/grub/manual/>
- We describe the point and clicky way: K3b

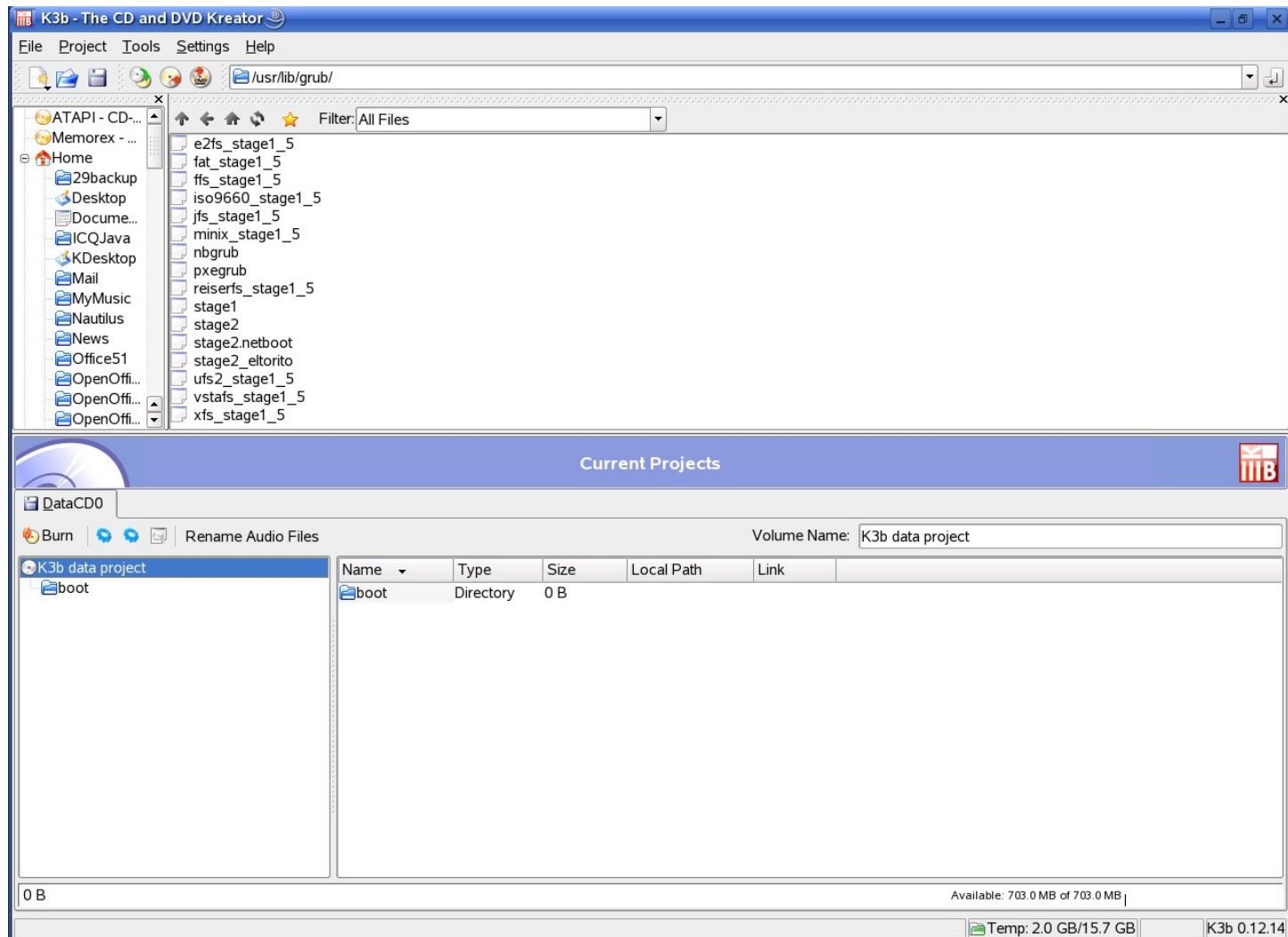
K3b: New Data CD project



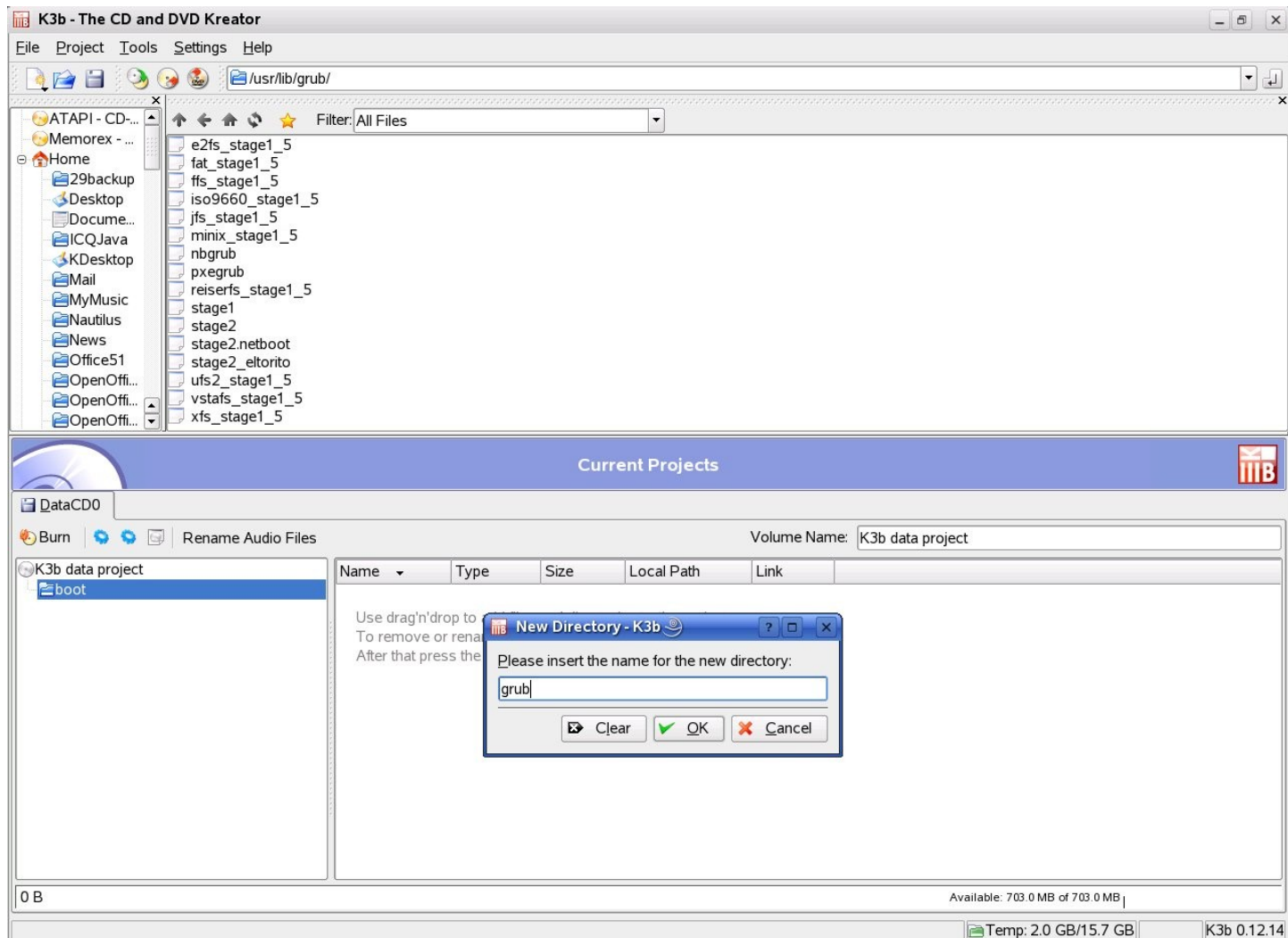
K3b: Right click, New directory to create /boot directory on the CD.



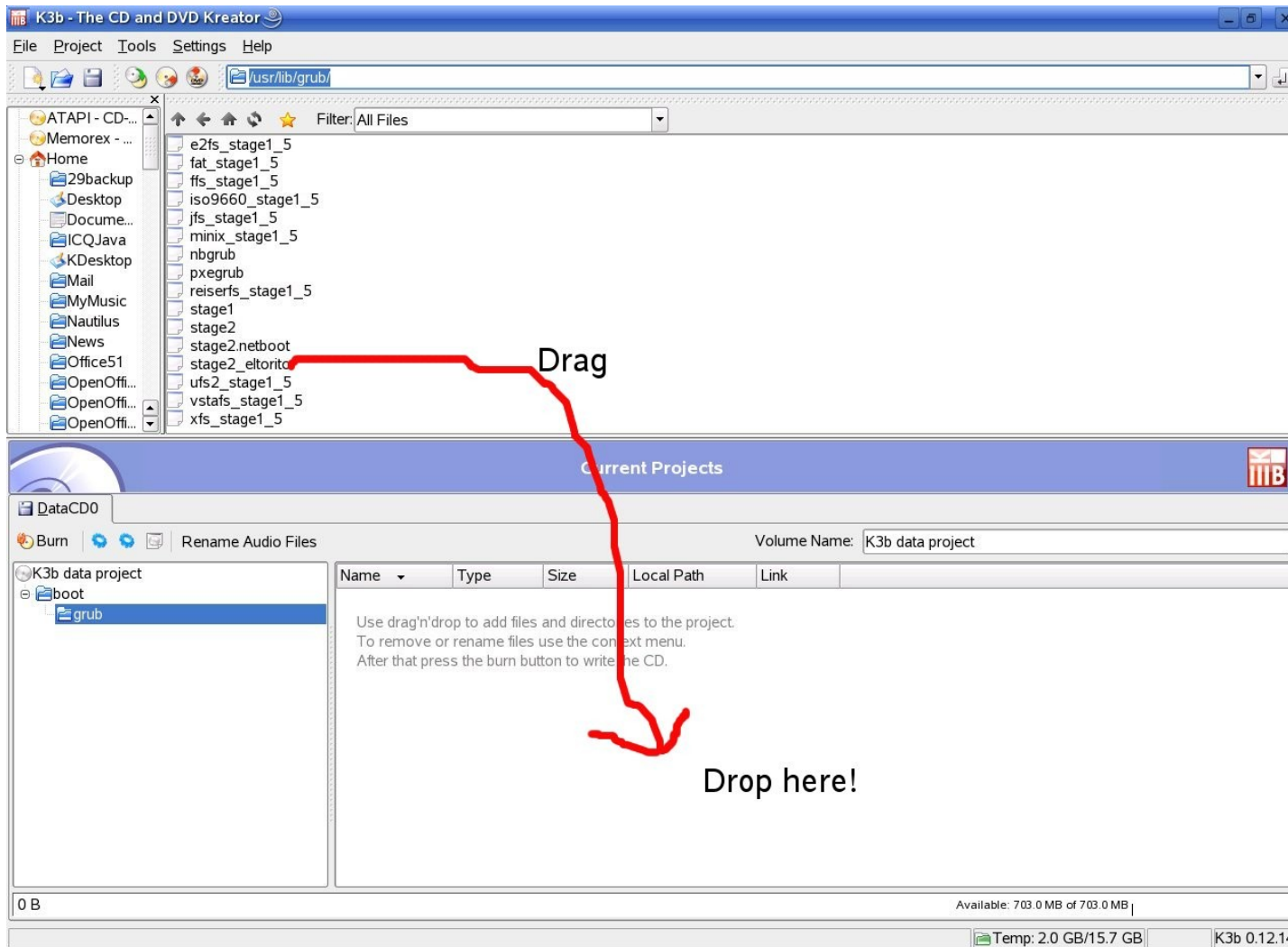
K3b: click on boot directory to enter it.



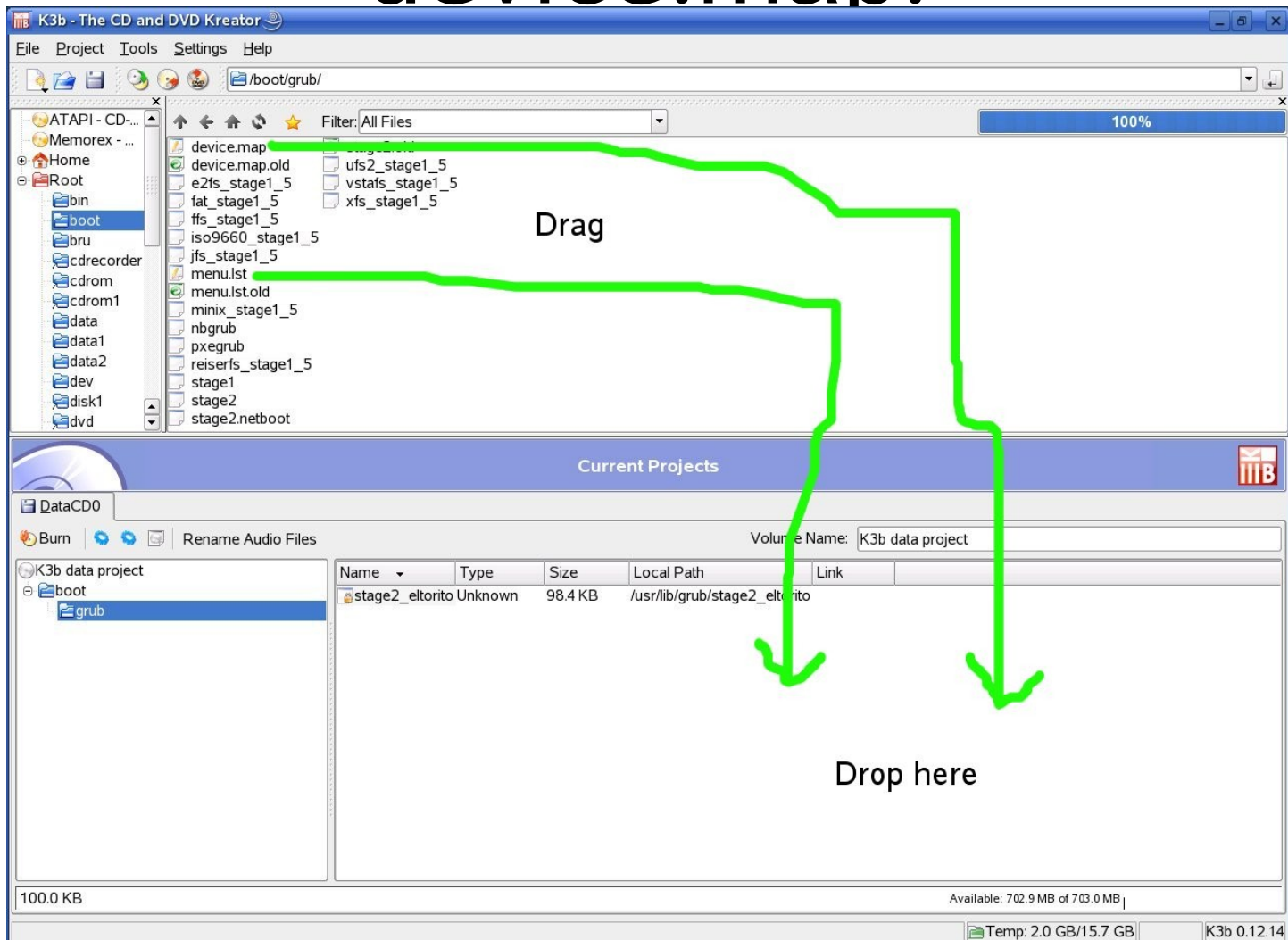
as before, create grub subdirectory within /boot and enter it.



Drag /usr/lib/grub/stage2_eltorito into /boot/grub on the CD.



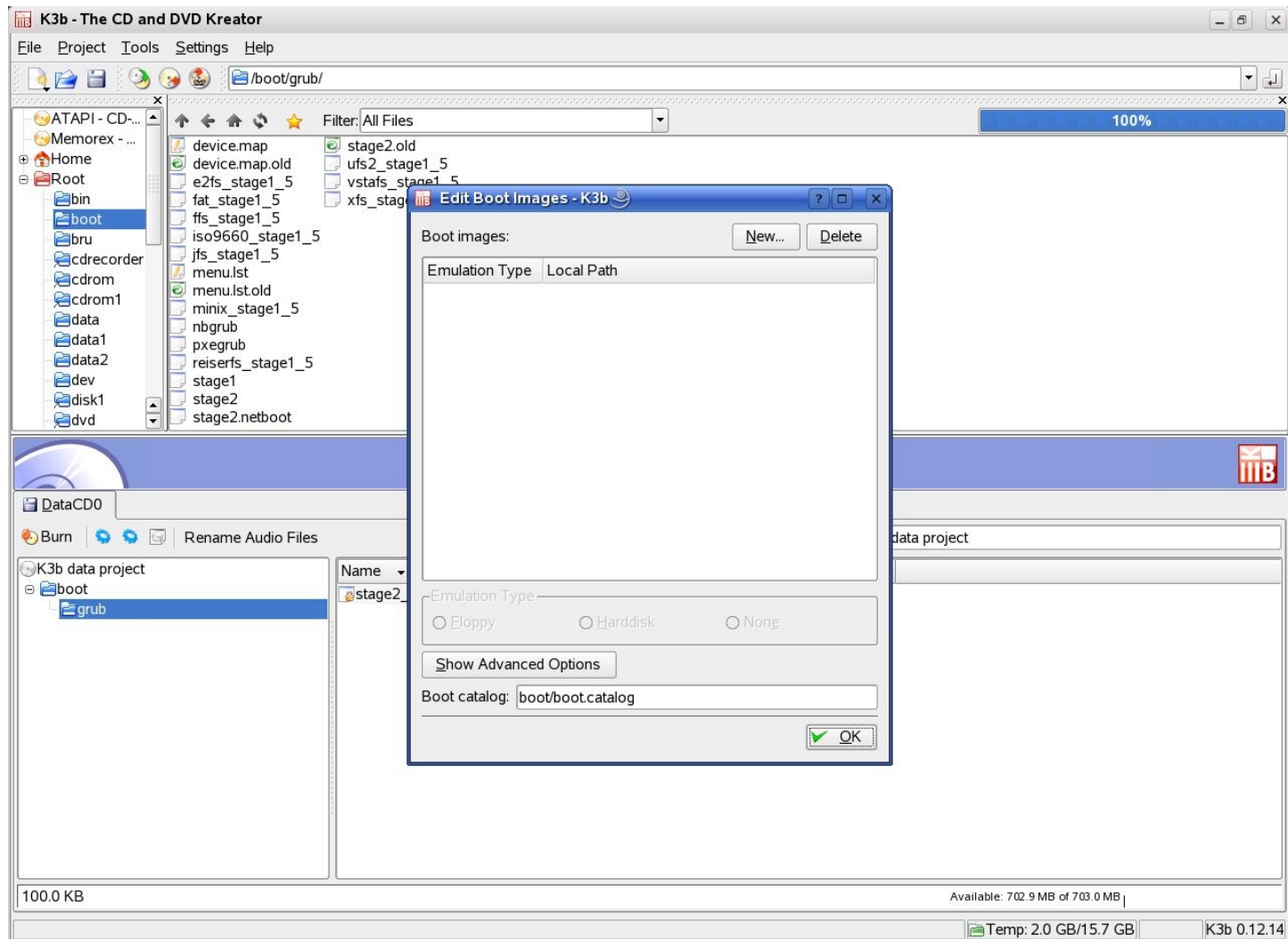
In the same way drag /boot/grub/menu.lst and device.map.



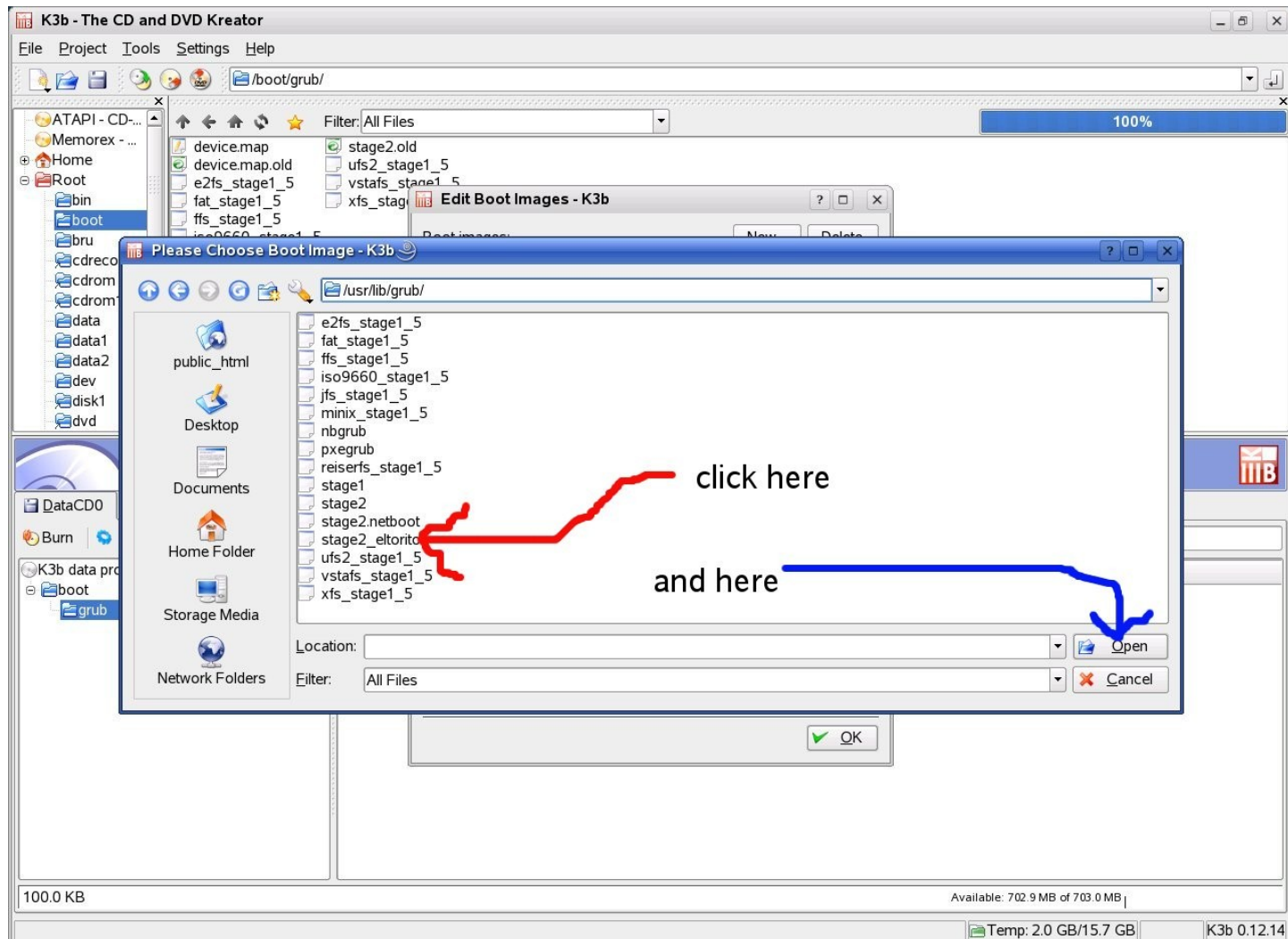
At this point we could add any additional info to the CD.

- like the partition table info and the MBR info, like we did for the floppy.
- In the interests of brevity, we will skip this step.

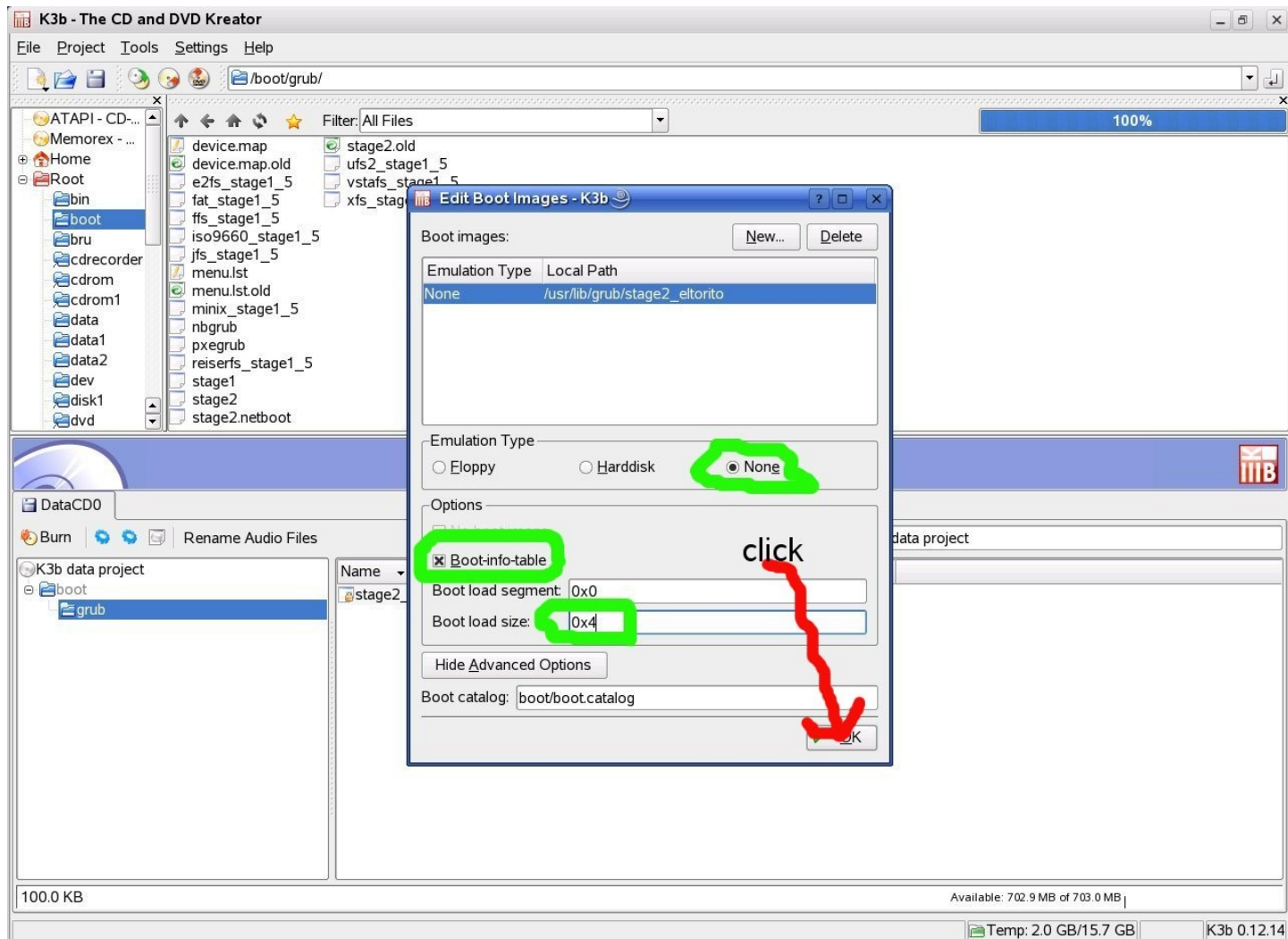
Now click on Project\Edit Boot Images...



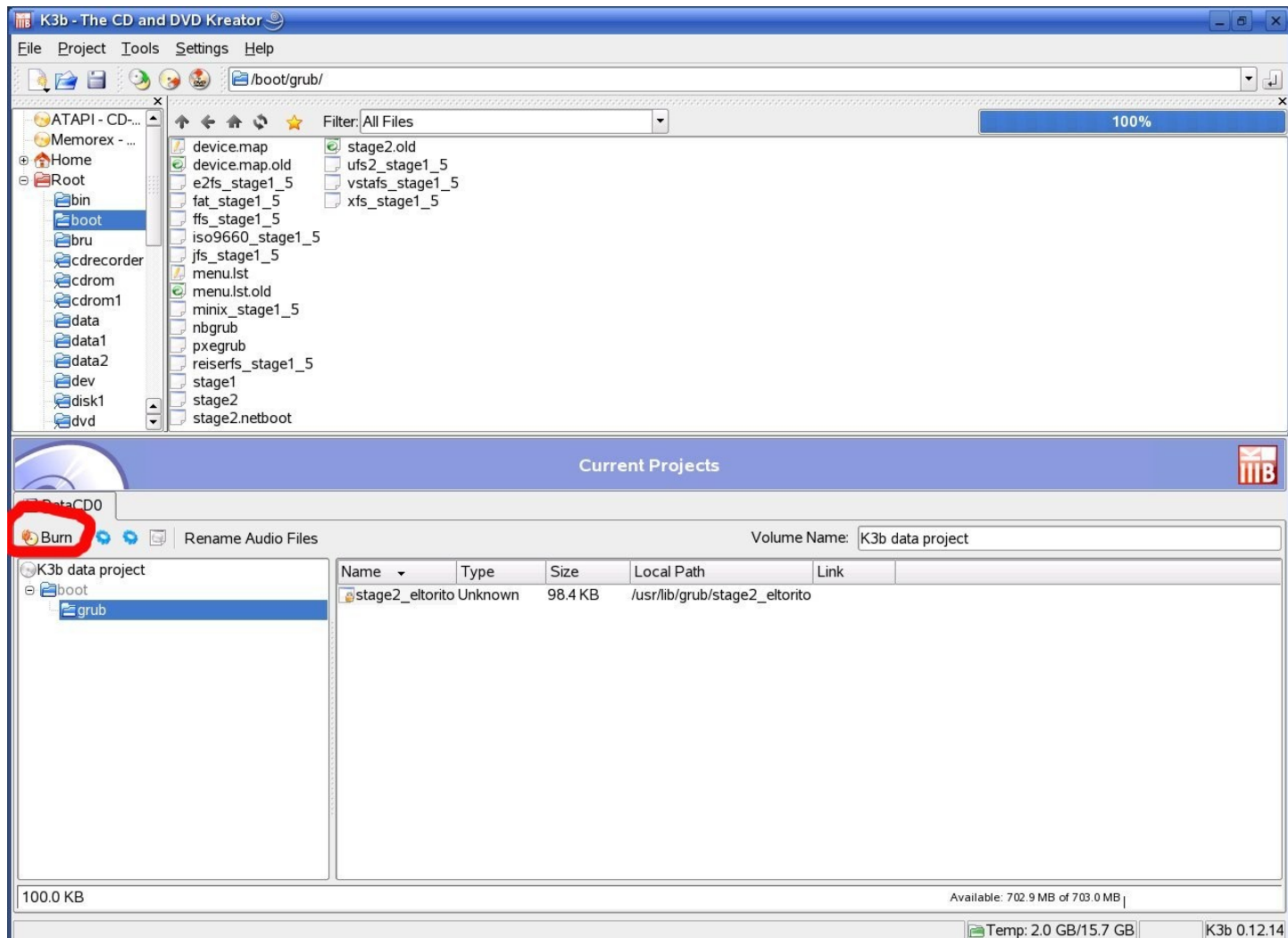
Click on Advanced options and New and open stage2_eltorito



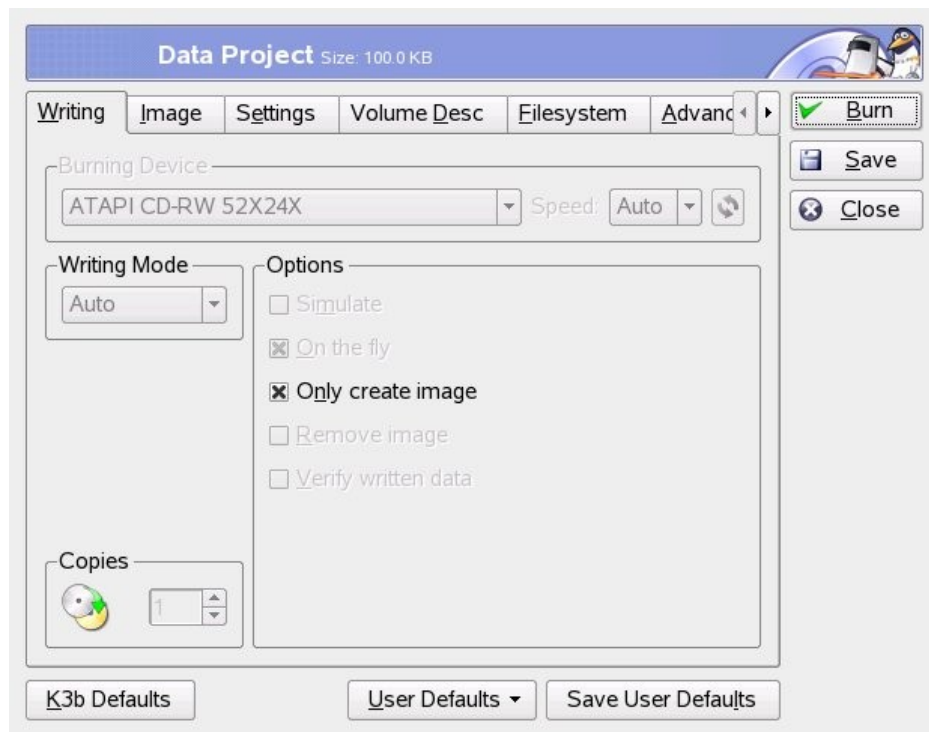
click on none, boot-info-table and set boot load size to 0x4



Almost done, click burn



Click on “Only Create Image”



- For some reason, direct burning does not work.
- If the local computer does not have a CD burner, the iso can be transferred to one that does.
- Use tools\Burn CD Image... to burn iso.

Note to all distro authors.

- The grub manual describes command line procedure, to create Boot CDs.
- Many new computers do not have floppy.
- All distros should have a “point and clicky” option to create boot a CD, just like the one to create a boot floppy.
- This code should be fairly easy to write.

use fetchmail with openssl!



- If you connect to your ISP's imap via modem or the ISP's cable line you probably don't need any encryption.
- Modem conversations are almost impossible to decypher.
- If cable line is insecure, then ISP's host probably is insecure too.

But if sometimes you connect to your ISP via the open Internet....



- then you can worry.
- You don't want to have your password moving in the clear over the open Internet!
- Solution: use ssl with fetchmail!
- ssl encrypts passwords and prevents man-in-the-middle attacks!

Step1: run fetchmail -v

- check that you do not already have an ssl command in .fetchmailrc
- fetchmail -v
- look for the first line that starts like this:
- fetchmail: IMAP< * OK [CAPABILITY
- check for the capability “STARTTLS” in this line.
- If not there, you are out of luck, your imap server does not support ssl. Otherwise, goto next step.

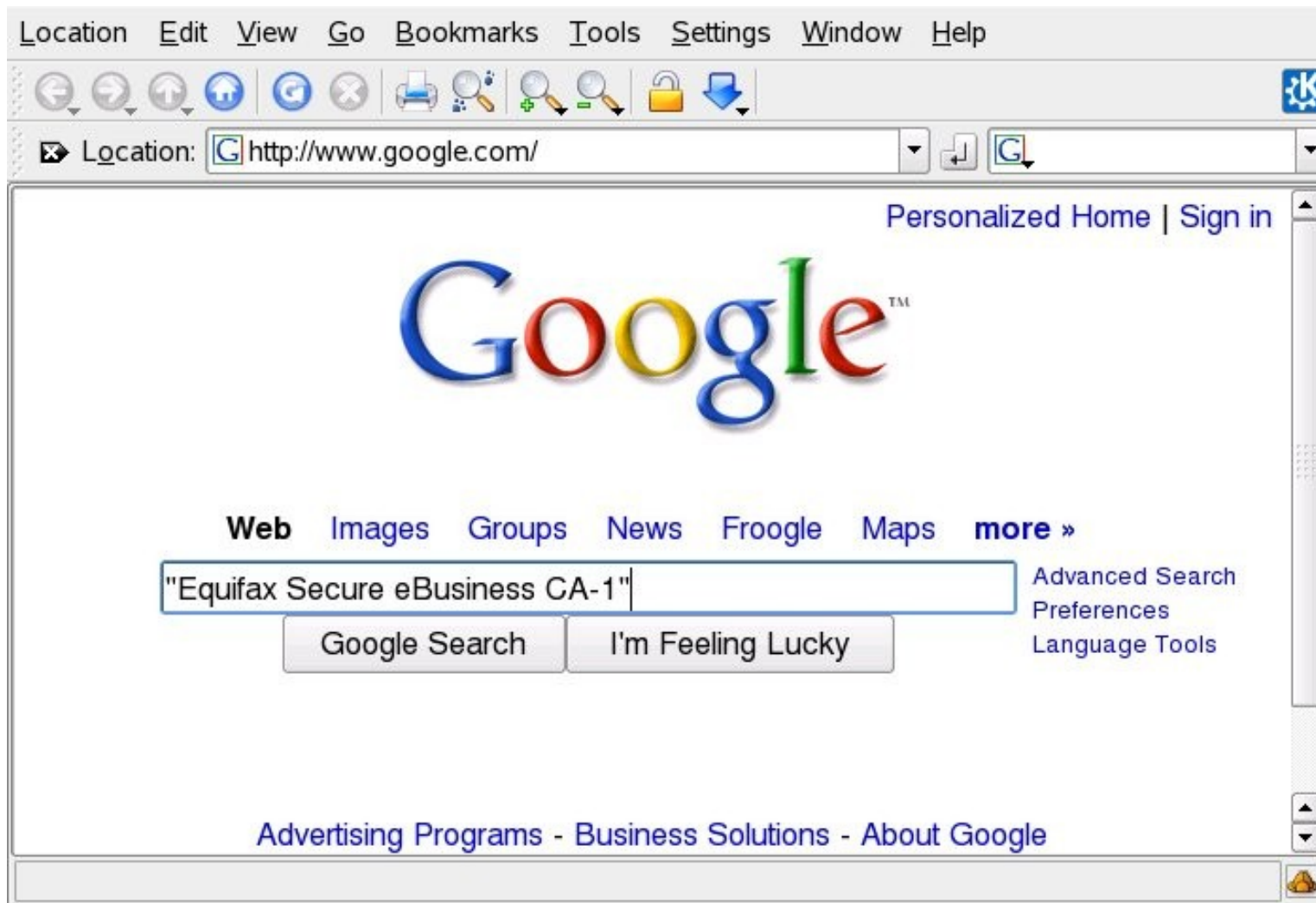
Step2: run `fetchmail -v --ssl`

- look for errors that look like this:
- `fetchmail: Server certificate verification error: unable to get local issuer certificate`
- `fetchmail: Server certificate verification error: certificate not trusted`
- `fetchmail: Server certificate verification error: unable to verify the first certificate`
- no errors: done, add ssl to `.fetchmailrc`
- otherwise continue to step 3

Step3: run fetchmail -v --ssl

- look for a line that looks like this:
- `fetchmail: Issuer CommonName: Equifax Secure eBusiness CA-1`
- Search the net for the CommonName.

step4:Find the place to download the certificate.



We have found it!

The image shows a screenshot of a web browser displaying Google search results. The search query is "Equifax Secure eBusiness CA-1". The results page shows several links, with a red arrow pointing to the second result: "GeoTrust: SSL Certificate, SSL, Server Certificates, Web Server ...". The arrow points to the text "Here it is." written in green. The browser's address bar shows the search URL: "http://www.google.com/search?hl=en&q=%22Equifax+Secure+eBusiness+CA-1%22&btnG=Google+Search". The browser's menu bar includes "Location", "Edit", "View", "Go", "Bookmarks", "Tools", "Settings", "Window", and "Help". The browser's toolbar includes navigation buttons (back, forward, home, stop, refresh) and search, print, and zoom icons. The search results page includes the Google logo, navigation tabs (Web, Images, Groups, News, Froogle, Maps, more), and a search box containing the query. The results are categorized under "Web" and show "Results 1 - 10 of about 409 for 'Equifax Secure eBusiness CA-1'. (0.66 seconds)". The first result is a sponsored link for "Equifax - Official Site". The second result is the one highlighted by the red arrow. The third result is another sponsored link for "Internet Security Suite". The fourth result is a PDF report from GeoTrust. The fifth result is a technical error message from noreply.org. The sixth result is a link to "NTT DoCoMo - SSL Specifications".

Location Edit View Go Bookmarks Tools Settings Window Help

Location: <http://www.google.com/search?hl=en&q=%22Equifax+Secure+eBusiness+CA-1%22&btnG=Google+Search>

Sign in

Google Web Images Groups News Froogle Maps more »

"Equifax Secure eBusiness CA-1" Search Advanced Search Preferences

Web Results 1 - 10 of about 409 for "Equifax Secure eBusiness CA-1". (0.66 seconds)

Equifax - Official Site Sponsored Link
www.equifax.com Order Your Personalized Credit Report Instantly and Securely

GeoTrust: SSL Certificate, SSL, Server Certificates, Web Server ...
Download - **Equifax Secure eBusiness CA-1** (DER encoded X.509) Download - **Equifax Secure eBusiness CA-1** (Certified PDF - Base-64 encoded X.509). Organization: ...
www.geotrust.com/resources/root_certificates/index.asp - 50k - Cached - Similar pages

Secure Certificates - SSL FAQs
RapidSSL.com's ChainedSSL Wildcard product uses an intermediate certificate issued by the **Equifax Secure eBusiness CA-1** root, making it the only stable ...
diswebhost.com/securecertfaqs.shtml - 27k - Cached - Similar pages

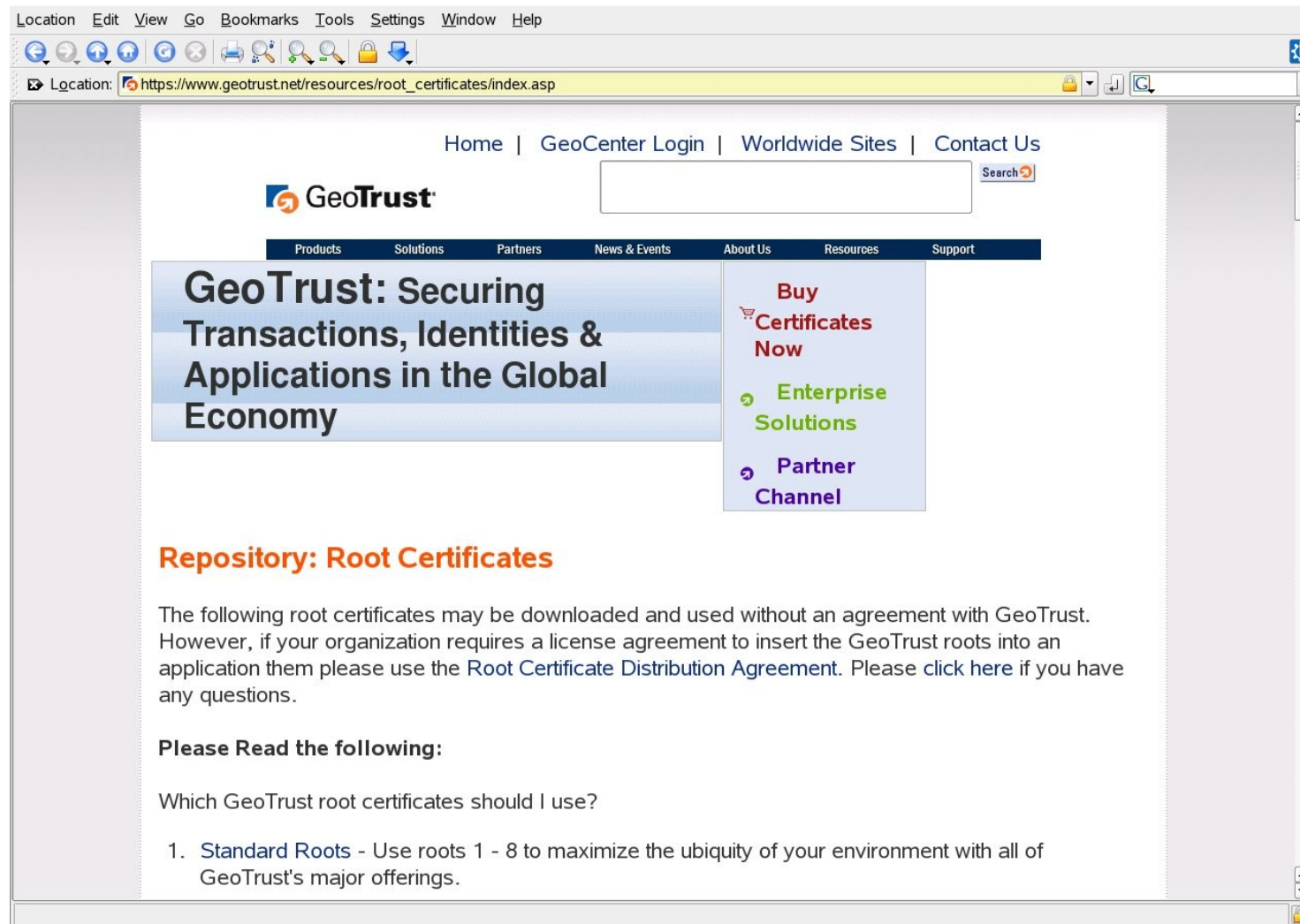
Report of Independent Accountants To the Management of GeoTrust ...
File Format: PDF/Adobe Acrobat - View as HTML
Equifax Secure eBusiness CA-1,. Equifax Secure eBusiness CA-2,. Equifax Secure Global eBusiness CA-1,. GeoTrust Global CA,. ChainedSSL CA, ...
<https://cert.webtrust.org/SealFile?seal=431&file=pdf> - Similar pages

depth=1 /C=US/O=Equifax Secure Inc./CN=**Equifax Secure eBusiness CA** ...
depth=1 /C=US/O=Equifax Secure Inc./CN=**Equifax Secure eBusiness CA-1** verify
error:num=19:self signed certificate in certificate chain verify return:0 ...
www.noreply.org/tls/cert-mail.cyberiad.it.txt - 4k - Cached - Similar pages

NTT DoCoMo - SSL Specifications
Equifax Secure eBusiness CA-1 · GeoTrust Global CA · Terminals compatible with SSL

Here it is.

We have found it! Check that it is the true respectable site.



Location Edit View Go Bookmarks Tools Settings Window Help

Location: https://www.geotrust.net/resources/root_certificates/index.asp

Home | [GeoCenter Login](#) | [Worldwide Sites](#) | [Contact Us](#)

GeoTrust

Products Solutions Partners News & Events About Us Resources Support

GeoTrust: Securing Transactions, Identities & Applications in the Global Economy

- Buy Certificates Now
- Enterprise Solutions
- Partner Channel

Repository: Root Certificates

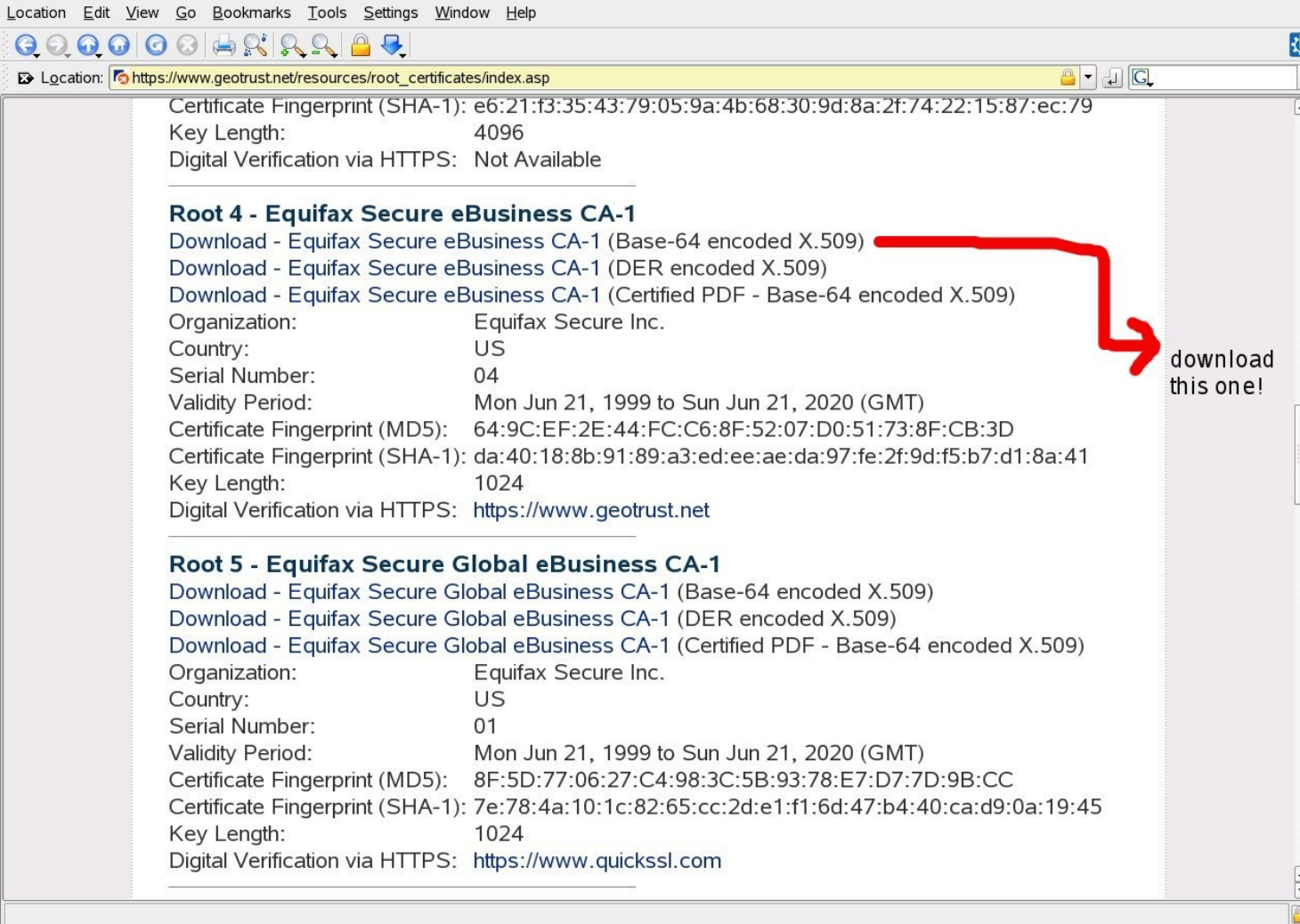
The following root certificates may be downloaded and used without an agreement with GeoTrust. However, if your organization requires a license agreement to insert the GeoTrust roots into an application them please use the [Root Certificate Distribution Agreement](#). Please [click here](#) if you have any questions.

Please Read the following:

Which GeoTrust root certificates should I use?

1. **Standard Roots** - Use roots 1 - 8 to maximize the ubiquity of your environment with all of GeoTrust's major offerings.


step5: Download the base64 version of the certificate.



Location Edit View Go Bookmarks Tools Settings Window Help

Location: https://www.geotrust.net/resources/root_certificates/index.asp

Certificate Fingerprint (SHA-1): e6:21:f3:35:43:79:05:9a:4b:68:30:9d:8a:2f:74:22:15:87:ec:79
Key Length: 4096
Digital Verification via HTTPS: Not Available

Root 4 - Equifax Secure eBusiness CA-1
Download - Equifax Secure eBusiness CA-1 (Base-64 encoded X.509) 
Download - Equifax Secure eBusiness CA-1 (DER encoded X.509)
Download - Equifax Secure eBusiness CA-1 (Certified PDF - Base-64 encoded X.509)
Organization: Equifax Secure Inc.
Country: US
Serial Number: 04
Validity Period: Mon Jun 21, 1999 to Sun Jun 21, 2020 (GMT)
Certificate Fingerprint (MD5): 64:9C:EF:2E:44:FC:C6:8F:52:07:D0:51:73:8F:CB:3D
Certificate Fingerprint (SHA-1): da:40:18:8b:91:89:a3:ed:ee:ae:da:97:fe:2f:9d:f5:b7:d1:8a:41
Key Length: 1024
Digital Verification via HTTPS: <https://www.geotrust.net>

Root 5 - Equifax Secure Global eBusiness CA-1
Download - Equifax Secure Global eBusiness CA-1 (Base-64 encoded X.509)
Download - Equifax Secure Global eBusiness CA-1 (DER encoded X.509)
Download - Equifax Secure Global eBusiness CA-1 (Certified PDF - Base-64 encoded X.509)
Organization: Equifax Secure Inc.
Country: US
Serial Number: 01
Validity Period: Mon Jun 21, 1999 to Sun Jun 21, 2020 (GMT)
Certificate Fingerprint (MD5): 8F:5D:77:06:27:C4:98:3C:5B:93:78:E7:D7:7D:9B:CC
Certificate Fingerprint (SHA-1): 7e:78:4a:10:1c:82:65:cc:2d:e1:f1:6d:47:b4:40:ca:d9:0a:19:45
Key Length: 1024
Digital Verification via HTTPS: <https://www.quickssl.com>

download this one!

step 6: Find the place openssl keeps all its certificates!

- There will be a lot of files of type “.pem” there.
- On my system it is: /etc/ssl/certs
- logon to root, copy the certificate you downloaded there, renaming the type to “.pem”.
- Then do a “c_rehash” on the directory.
Example:
- `# c_rehash /etc/ssl/certs`

step7: fetchmail -v --ssl again!

- This time check that the error messages we encountered before about: `Server certificate verification error:` has gone away!
- OK, good we have verified that ssl works!

Step8: edit .fetchmailrc

- add “ssl” and “sslcertck” to the user line.
- Mine looks like this:
 - `set postmaster "pelliott"`
 - `set bouncemail`
 - `set no spambounce`
 - `set properties ""`
 - `poll mail.io.com with proto IMAP`
 - `user 'pelliott' there with password 'XXXXXX' is \`
`'pelliott' here ssl sslcertck`

Success.



- From now on whenever we use fetchmail, it will use openssl to encrypt our password and protect us from man-in-the-middle attacks!
- Done.

Do you know 3 or 4 Miscellaneous Linux Tricks?



- Perhaps you can compile your favorite Linux Tricks into a presentation for ALG?
- ALG can use some internally generated presentations.