Defend what you create

User Manual

Dr.Web® LiveCD
Version 6.0.0
User Manual
17.01.2011

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Refer to the official web site for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web® information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards. State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of Contents

1. Introduction

Dr.Web® LiveCD is a software product based on the standard **Dr. Web** anti-virus scanner. It allows to restore the system when loading a computer from a hard drive is impossible due to high virus activity. Using the emergency anti-virus assistance disk, you can not only clean your computer from infected and suspicious files, but also attempt to cure infected objects.

Dr.Web LiveCD is distributed as a boot disk with a portable Linux-based operating system and inbuilt software intended to facilitate computer scanning and curing, working with the file system, viewing and editing text files, viewing web pages, and sending and receiving e-mail messages.

Thus **Dr.Web LiveCD** provides access to computer resources both when it is impossible to load the system from a hard drive, and when there exists a need in a convenient customizable interface (for details about this variant of usage, see Creating Boot Flash Drives for **Dr.Web LiveCD**).

You can load **Dr.Web LiveCD** in one of the following modes:

- standard GUI mode;
- advanced mode with the command-line interface (Console Scanner).

The standard mode is preferable because of its user-friendly interface and improved functionality. The bigger part of this manual describes working in this GUI mode. The advanced mode is intended for experienced users familiar with Unix-based operating systems and is used when the GUI fails to load. Working with the console shell is described in the last part of this manual.

1.1. Dr.Web Anti-Virus Protection

Dr.Web® LiveCD is an anti-virus solution designed to restore the system after it was crippled as a result of virus or malware activity.

To protect the system from such situations, it is necessary to have constant reliable protection using the most advanced anti-virus technologies.

The **Dr.Web** cutting-edge technologies provide solid anti-virus protection for your home computer, office network, and large corporate networks. The **Dr.Web** solutions are distinguished for their low system requirements, compactness, operation speed and reliability in detection of all types of malware.

Doctor Web company offers the following solutions for constant protection against viruses, malware and spam:

- Protection of corporate networks (**Dr.Web Enterprise Security Suite**)
- Protection of workstations (**Dr.Web Security Space 6.0**, **Dr.Web for Windows 6.0**, **Dr.Web for Linux**, **Dr.Web Console Scanners**);
- Protection of file servers (**Dr.Web for Windows**, **Dr.Web for Unix**, **Dr.Web for Novell NetWare**);
- Protection of mail (**Dr.Web for MS Exchange**, **Dr.Web for IBM Lotus Domino**, **Dr.Web for MIMEsweeper**);
- Protection of SMTP gateways (**Dr.Web Mail Gateway**);
- Protection of Internet gateways (**Dr.Web for Unix**);
- Protection of mobile devices (**Dr.Web for Windows Mobile**)
- Internet-service for providers (**Dr.Web AV-Desk**).

For more information about company products, visit the **Dr.Web** official web site.

1.2. System Requirements

Minimum system requirements to start the **Dr.Web LiveCD** anti-virus solution:

- i386 processor
- Minimum 256 MB of RAM (512 MB if virtual memory on hard drive can not be used)
- a CD-ROM, DVD-ROM or flash drive with minimum 200 MB of

free space

1.3. Launching Dr.Web LiveCD

Make sure that your computer is set up to boot from the CD drive, in which the disk with **Dr.Web LiveCD** is inserted, or from any other data carrier, on which **Dr.Web LiveCD** is stored. At start a menu is displayed from which you can select the load mode.

Using the arrow keys on your keyboard select one of the following options and press ENTER:

- To launch the GUI version of **Dr.Web LiveCD**, select **Dr. Web-LiveCD (Default)**.
- To launch the command line version, select **DrWeb-LiveCD (Advanced)**.
- To boot your computer from the hard drive without launching **Dr.Web LiveCD**, select **Start Local HDD** (cancel launching of **Dr.Web LiveCD**, launch the system from the 0 partition of the 0 drive (hd0,0)).
- To test memory (for example, when you computer is extremely unstable and restarts at random), select **Testing Memory**.

Press TAB to edit each option manually.

2. Dr.Web LiveCD Graphic Shell

The **Dr.Web® LiveCD** software includes a graphic shell with a window-based interface similar to the Linux operating system GUI. See Figure 1.

By default, the desktop with the **Dr.Web** trademark for the background contains icons of applications included in **Dr.Web LiveCD**.

The taskbar (a horizontal bar in the bottom) contains

- System menu button
- Quick Launch icons for inbuilt applications
- Desktop switching icons
- Icons of currently used applications
- System clock (in the right corner)

Dr.Web LiveCD includes the following basic applications:

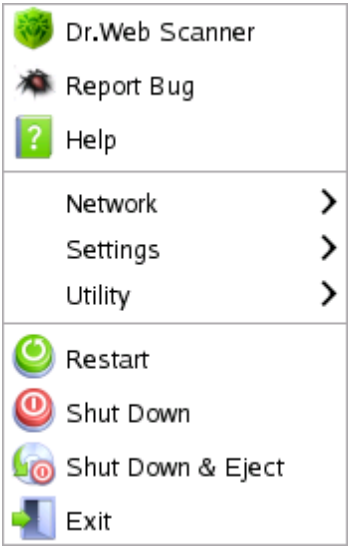
- **Dr.Web Scanner for Linux**;
- **Firefox** browser;
- **Sylpheed** mail client;
- **Midnight Commander** file manager;
- command-line terminal to work directly from under the graphic shell;
- **Leafpad** text editor.

Figure 1. Graphical User Interface

You can start the main components by

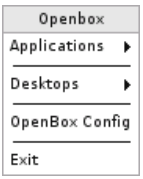
- double-clicking the icon of the respective component on the desktop (by default, basic components are represented on the desktop);
- clicking the icon of the respective component in the taskbar (except for the file manager and **Dr.Web Scanner for Linux**).
- selecting the respective component on the system menu.

To open the system menu, click the system menu button in the taskbar.



Click a command for info

You can access the desktop context menu named **Openbox** by right-clicking the desktop.



Click an area for info

2.1. Dr.Web Antivirus

When you boot **Dr.Web LiveCD** in default (GUI) mode, **Dr.Web Control Center for Linux** will be started automatically. See

Figure 2.

With **Dr.Web Control Center** you can

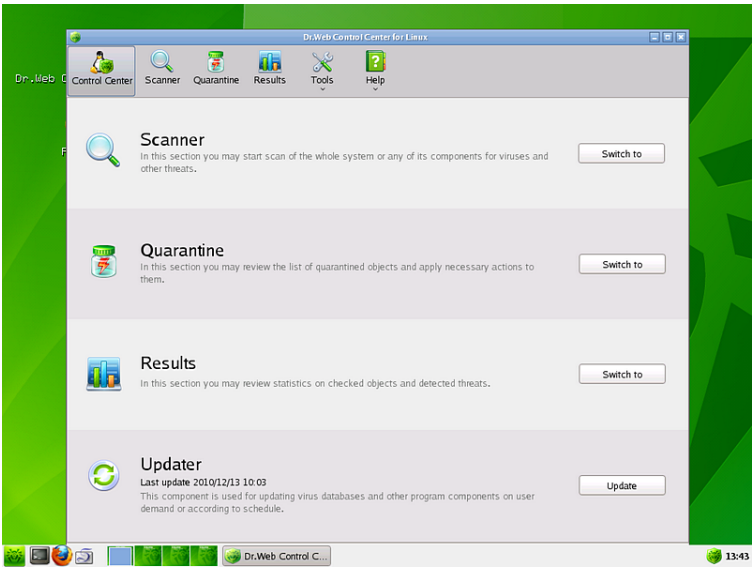
- scan you system with **Dr.Web Scanner**;
- eliminate detected threats or isolate suspicious files in **Quarantine**;
- change scanning and automatic threat processing settings;
- update virus databases;
- view full report on scanning of your system.

SpIDer Guard, notifications and simultaneous use by multiple users features are not supported in this version.

To learn more about using **Dr.Web Antivirus for Linux** consult the program help.

To ensure maximum scanning effectiveness virus databases are updated automatically. Please note that Internet connection is required for updating databases. Information on how to set up connection can be found in Network connection chapter.

Figure 2. Dr.Web Control Center for Linux



2.1. Settings

The **Dr.Web LiveCD** settings are available through the **Settings** item of the system menu and include the following options:

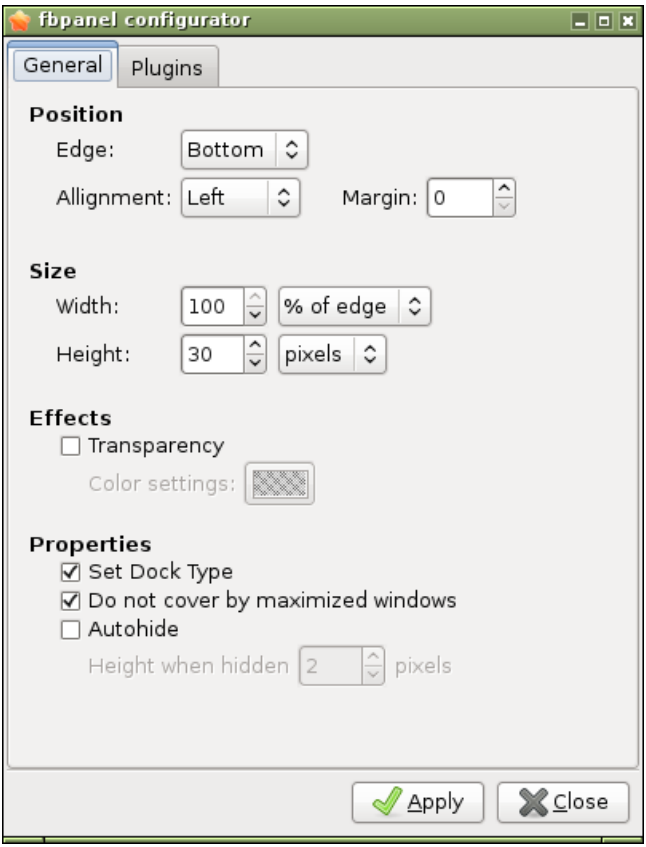
- Menu Configuration which allows you to configure appearance of the taskbar
- NetWorks Configuration which allows you to configure network
- Openbox Configuration Manager which allows you to configure the GUI
- Xorg Configuration which allows to configure the X Window System

To configure settings, select a corresponding item in the menu.

2.1.1. Taskbar Configuration

This windows allows you to configure the position, size, and special effects in appearance of the taskbar (on the **General** tab) as well as configure installed GUI plugins (on the **Plugins** tab). See Figure 3.

Figure 3. Taskbar configuration



Setting	Description
Position	Specify values for the following parameters: • the taskbar position on the screen (**Edge**) • alignment of the taskbar elements (**Alignment**) • the taskbar margine (**Margine**)
Size	Adjust the the taskbar width **Width** and **Height**.
Effects	Adjust the taskbar **Transparency** and **Color** settings.
Properties	Specify values for other parameters: • type of the taskbar (**Set Dock Type**) • taskbar covering options (**Do not cover by maximized windows**) • hiding options (**Autohide**)

2.1.2. NetWorks Configuration

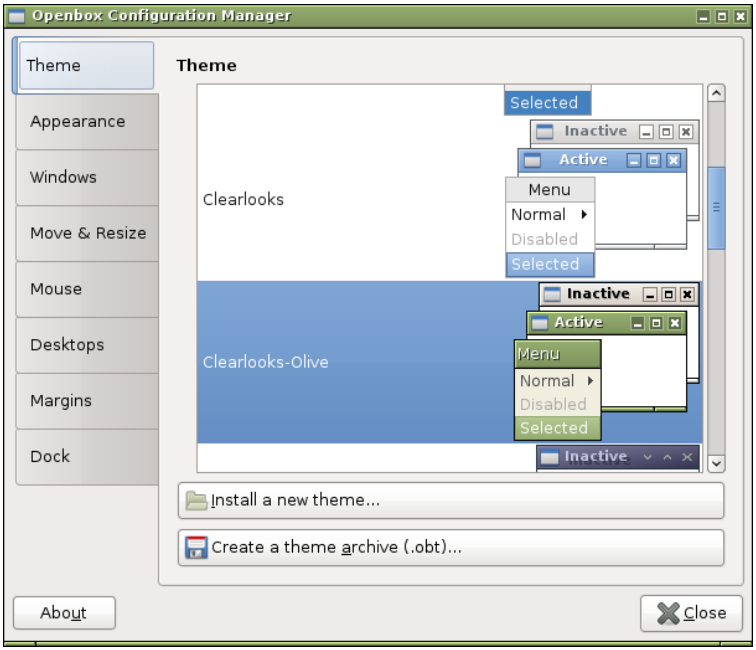
This window allows you to configure IP protocol settings manually or receive them via DHCP. See Figure 4.

Figure 4. Network configuration

2.1.3. Openbox Configuration Manager

This window allows you to configure the Openbox GUI including colour schemes, desktop parameters etc. See Figure 5.

Figure 5. Openbox configuration



2.1.4. X Window Configuration

This window allows you to configure the X Window system (screen resolution, type of the video driver and the mouse, keys for shifting the keyboard layout). See Figure 6.

Figure 6. X Window configuration

2.2. Inbuilt Applications

This section describes applications available within the **Dr.Web LiveCD** anti-virus solution. Access to these applications can be gained via **Network** and **Utility** options of the system menu.

The **Utility** option on the system menu opens the drop-down list:

- Create Live USB - create boot flash drive;
- **Leafpad** - open the inbuilt text editor (notepad);
- Midnight Commander - open the file manager;
- **Terminal** - open the command-line terminal.

The **Network** option on the system menu opens the drop-down list:

- Firefox - open the inbuilt browser;
- Sylpheed - open the inbuilt mail client.

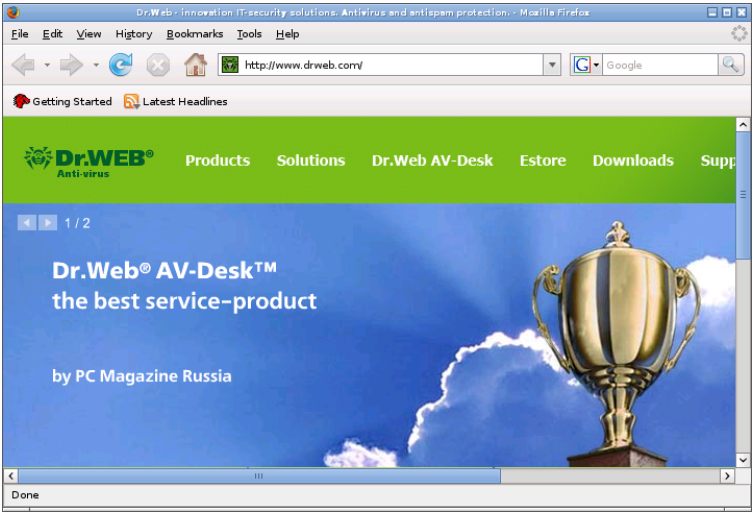
2.2.1. Browser

Even though your computer cannot be loaded from the hard drive, the Mozilla Firefox web browser included in **Dr.Web LiveCD** will allow you to view web sites and save the pages. See Figure 7. You will be able to view the saved pages after the OS is fully restored and loaded.

An Internet connection via the Local Area Network is required to access the web pages with the inbuilt browser.

The browser default start page is the **Doctor Web** official web site.

Figure 7. Inbuilt Browser



2.2.2. Mail Client

The inbuilt **Sylpheed** mail client will enable you to carry on e-mail correspondence in full volume. See Figure 8.

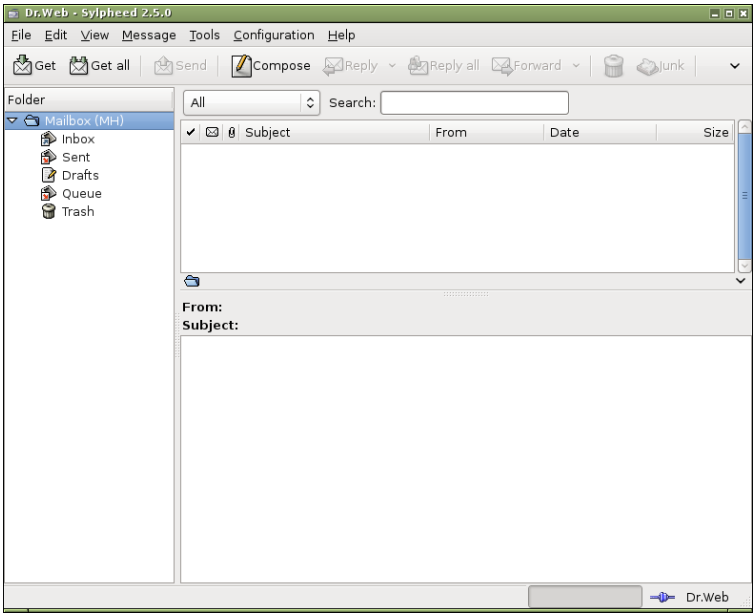
An account at the `mail.drweb.com` server is preinstalled in the **Sylpheed** mail client to enable user send messages. You can create additional accounts to maintain correspondence.

To create a new account, select **Configuration** menu -> **Create new account**. Enter all information necessary to enable mail transfer, such as sender's e-mail address, mail sending and receiving parameters (SMTP and POP3 protocols respectively), and

accompanying information.

To work with several accounts, you can create separate mailboxes. To do this, select **File** menu -> **Mailbox** -> **Add mailbox**. In the e-mail box properties specify what account is to be used: on the context menu of the mailbox select **Properties** -> **Compose** tab -> **Account** drop-down list -> specify the account.

Figure 8. Mail client



Sylpheed provides a secure connection to the mail server through the SSL and TLS protocols.

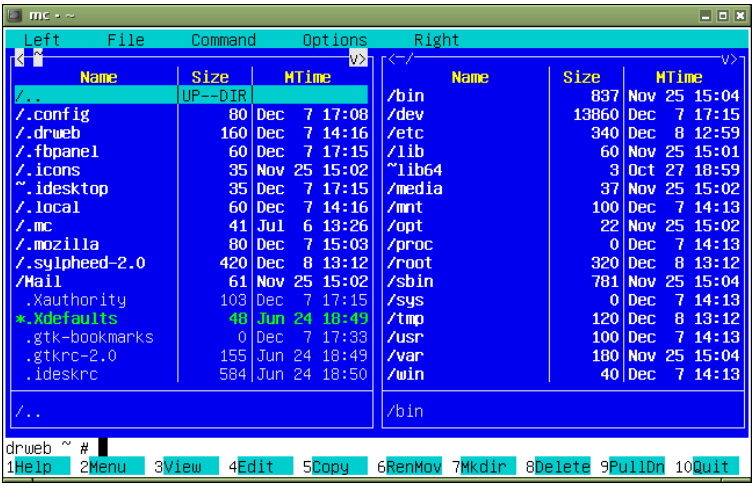
When your OS is damaged and you cannot use your customary tools, this mail client included in **Dr.Web LiveCD** will allow you to keep up a correspondence through your registered e-mail account until the problem is solved.

2.2.3. File Manager

The inbuilt **Midnight Commander** file manager is similar to the Norton Commander file manager. See Figure 9. By using full screen display mode it provides intuitive user interface to the operating system and serves as a useful tool for operations with files, suitable for users with any level of experience, from a newbie to a guru.

Homepage: http://www.ibiblio.org/mc/.

Figure 9. File manager



3. Advanced mode

You can use advanced mode to scan your system in command line if you do not want or unable to use GUI. Command line interface provides better performance and allows you to use snapshots.

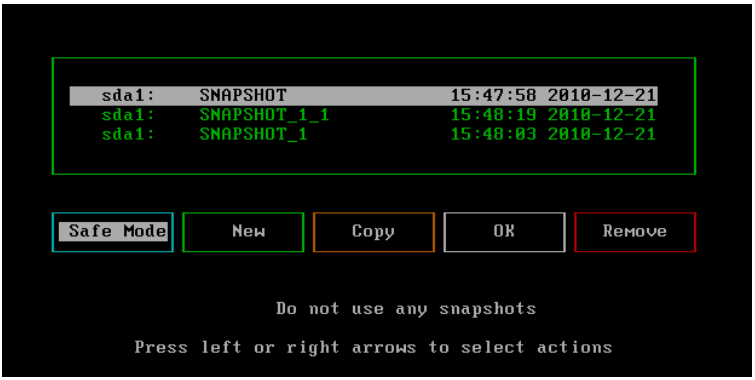
3.1. Snapshots

You can use snapshot to save all changes, log files and temporary files created during scanning on local disks or flash drives. Using snapshot reduces memory footprint and helps avoid program failures when scanning large archives.

By default snapshots are not used and **Dr.Web LiveCD** saves all its settings and temporary files only in RAM.

When booting LiveCD in advanced mode all available drives will be automatically scanned for existing snapshots and you will be offered to select a snapshot to use or create a new one. See Figure 10.

Figure 10. Snapshot list



Use UP ARROW and DOWN ARROW keys to select snapshot. Use LEFT ARROW and RIGHT ARROW keys to select options. Available options are

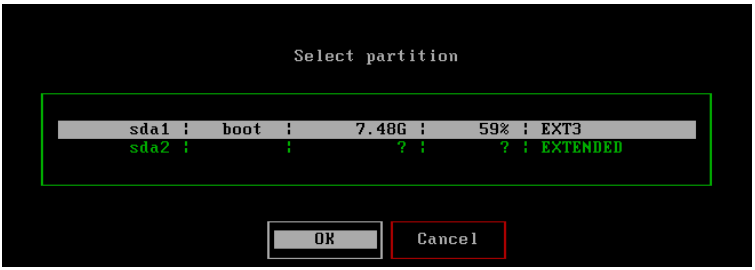
- **Safe Mode** - boot in safe mode without snapshot support;
- **New** - create new snaphot;
- **Copy** - copy selected snapshot to a different partition;
- **OK** - boot using selected snaphot;
- **Remove** - remove selected snaphot;

If no available partitions or flash drives have been found, snapshot list will not be displayed and LiveCD will be booted in safe mode without snapshot support.

To create a new snapshot

- Boot **Dr.Web LiveCD** in advanced mode.
- Select **New** option in the snapshot list menu.
- Select partition where snapshot will be stored. See Figure 11.

Figure 11. Selecting partition



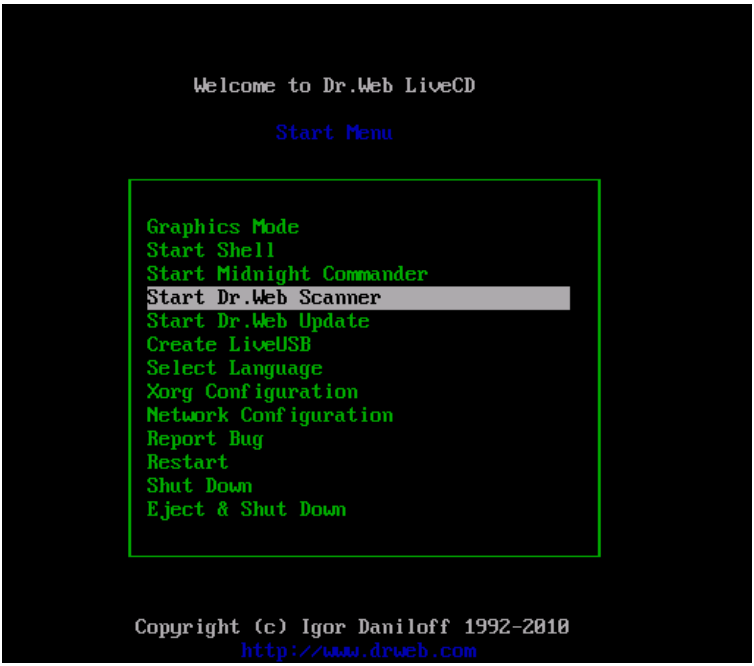
- Specify name of the new snapshot. See Figure 12.

Figure 12. Snapshot name

3.2. Scanning

When **Dr.Web LiveCD** is booted in advanced mode **Start Menu** will appear. See Figure 13.

Figure 13. Start Menu



Using the arrow keys, select one of the following items from the menu and press **ENTER**:

- **Graphics mode** - to launch the GUI version of the **Scanner**;
- **Start Shell** - to bring up the command line;
- **Start Midnight Commander** - to launch the inbuilt file manager;
- **Start Dr.Web Scanner** - to start scanning all hard disk partitions with default settings;
- **Start Dr.Web Update** - to update the virus databases;
- **Select Language** - to change the interface language;
- **Xorg Configuration** - to adjust parameters of the X Window system, if it was not configured automatically;
- **Network Configuration** - to adjust network parameters, if

the network was not configured automatically;

- **Report Bug** - to send information about a bug in the product to the developers;
- **Restart** - to reboot the computer;
- **Shut Down** - to shut down the computer without ejecting the disk;
- **Eject & Shut Down** - to eject the disk and shut down the computer.

If you want to start scanning with special options, select **Start Shell**. This will bring up the command line in the bottom of the screen. To run console **Scanner** you can use the following command:

```
$ /opt/drweb/
drweb <path> [command line parameters]
```

where <path> - is the path to scanned directory or the mask for checked files.

When **Scanner** is started only with `<path>` argument without any parameters specified, it scans the specified directory using the default set of parameters. In the following example drive **C:** is being checked:

```
$ /opt/drweb/drweb /mnt/disk/sda1
```

Log files are located in `/var/drweb/log/` directory:

- `drweb.log` - **Scanner** log file;
- `updater.log` - log file of utility used for updating virus databases;

3.3. Scanner Command Line Parameters

Dr.Web Scanner supports numerous command line parameters. They are separated from specified path by white space and are prefixed by hyphen "-". To get complete list of parameters, run `drweb` with `-?`, `-h` or `-help` parameters.

Main program parameters can be classified in the following way:

- scan area parameters;
- diagnostics parameters;
- actions parameters;
- interface parameters.

Scan area parameters determine where the virus check must be performed. They include:

- `path` — specify path for scan. Several paths can be specified in one parameter;
- `@[+]<file>` — check objects listed in the specified file. Plus «+» instructs Scanner not to delete files from the list of objects after scan is completed. List file may contain paths to directories that must be scanned regularly, or list of files to be checked only once;
- `sd` — recursive search and scan of files in subdirectories starting from the current directory;
- `fl` — follow links, both to files and directories. Links causing loops are ignored;
- `mask` — ignore masks for file names.

Diagnostics parameters determining what types of objects must be scanned for viruses:

- `al` — scan all files on specified drive or in specified directory;
- `ar[d|m|r][n]` — scan files in archives (ARJ, CAB, GZIP, RAR, TAR, ZIP, etc.).
  `d` - delete, `m` - move, `r` - rename archives containing infected objects, `n` - archiver name output disabled.
  Archives can be in simple (`*.tar`) or compressed forms (`*.tar.bz2`, `*.tbz`);
- `cn[d|m|r][n]` — scan files in containers (HTML, RTF, PowerPoint, etc.).
  `d` - delete, `m` - move, `r` - rename containers containing infected objects, `n` - container type output disabled;
- `ml[d|m|r][n]` — scan files in mailboxes.
  `d` - delete, `m` - move, `r` - rename mailboxes, containing infected objects; `n` - mailbox type output disabled;

- `up[ n]` — scan executable files packed with LZEXE, DIET, PKLITE, EXEPACK;
  `n` - packer type output disabled;
- `ex` — diagnostics using file masks (see `FilesTypes` parameter in configuration file);
- `ha` — heuristic analysis (search for unknown viruses).

Actions parameters determine what actions must be performed if infected or suspicious files are detected. They include:

- `cu[ d| m| r]` — cure infected files: `d` - delete, `m` - move, `r` - rename infected files;
- `ic[ d| m| r]` — actions for incurable files: `d` - delete, `m` - move, `r` - rename incurable files;
- `sp[ d| m| r]` — actions for suspicious files: `d` - delete, `m` - move, `r` - rename suspicious files;
- `adw[ d| m| r| i]` — actions for files containing adware: `d` - delete, `m` - move, `r` - rename, `i` - ignore;
- `dls[ d| m| r| i]` — actions for dialers: `d` - delete, `m` - move, `r` - rename, `i` - ignore;
- `jok[ d| m| r| i]` — actions for joke programs: `d` - delete, `m` - move, `r` - rename, `i` - ignore;
- `rsk[ d| m| r| i]` — actions for potentially dangerous programs: `d` - delete, `m` - move, `r` - rename, `i` - ignore;
- `hck[ d| m| r| i]` — actions for hacktools: `d` - delete, `m` - move, `r` - rename, `i` - ignore;

Interface parameters configure **Scanner** report output:

- `v, version` – output information about product and **Engine** versions;
- `ki` – output information about key file and its owner (in UTF8 encoding only);
- `foreground[ yes| no]` – enable **Scanner** to run in foreground or in background;
- `ot` — output information to standard output (`stdout`);
- `oq` — disable information output;
- `ok` — display «`Ok`» for not infected files;

- `log=<path to file>` — logging to specified file;
- `ini=<path to file>` — path to alternative configuration file;
- `lng=<path to file>` — path to alternative language file.

You can use hyphen "-" postfix to disable the following parameters:

```
-ar -cu -ha -ic -fl -ml -ok -sd -sp
```

For example, if you start **Scanner** with the following command:

```
$ drweb <path> -ha-
```

heuristic analysis (enabled by default) will be disabled.

By default (if **Scanner** configuration was not customized and no parameters were specified) **Scanner** starts with the following parameters:

```
-ar -ha -fl- -ml -sd
```

Default **Scanner** parameters (including scan of archives, packed files and mailboxes, recursive search, heuristic analysis, etc.) is sufficient for everyday diagnostics and can be used in typical cases. You can also use hyphen "-" postfix to disable some parameters, as it was explained above.

Disabling scan of archives and packed files will significantly decrease antivirus protection level, because in archives (especially, self-extracting) enclosed in e-mail attachments viruses are distributed. Office documents potentially susceptible to infection with macro viruses (Word, Excel) are also dispatched via e-mail in archives and containers.

When you run **Scanner** with default parameters, no **cure** actions and no actions for incurable and suspicious files are taken. For these actions to be performed, you must specify corresponding command line parameters explicitly.

Set of actions parameters may vary in particular cases. We recommend the following:

- `cu` — cure infected files and system areas without deletion, moving or renaming infected files;

- `icd` — delete incurable files;
- `spm` — move suspicious files;
- `spr` — rename suspicious files.

When **Scanner** is started with **Cure** action specified, it will try to restore the previous state of infected object. It is possible only if detected virus is known virus, and cure instructions for it are available in virus database, though even in this case cure attempt may fail if infected file is seriously damaged by virus.

If infected files are found inside archives they will not be cured, deleted, moved or renamed. To cure such files you must manually unpack archives to the separate directory and instruct **Scanner** to check it.

When **Scanner** is started with action **Delete** specified, it will delete all infected files from disk. This option is suitable for incurable (irreversibly damaged by virus) files.

Action **Rename** makes **Scanner** replace file extension with a certain specified extension ("`*.#??`" by default, i.e. first extension symbol is replaced with "`#`" character). Enable this parameter for files of other OS (e.g., DOS/Windows) detected heuristically as suspicious. Renaming helps to avoid accidental startup of executable files in these OS and therefore prevents infection by possible virus and its further expansion.

With action **Move** enabled **Scanner** will move infected or suspicious files to the quarantine directory.

4. Creating Boot Flash Drive

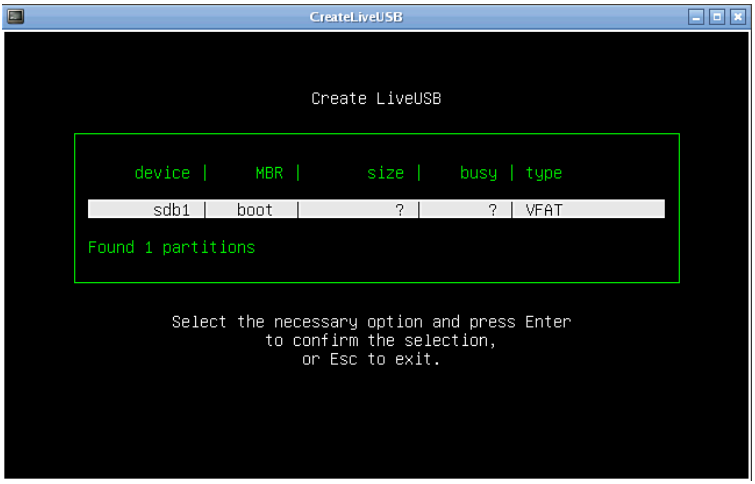
Dr.Web LiveCD may be used as a portable operating system customized according to the certain user needs to enable access to data on any computer regardless of the OS and software installed. To save and reuse individual settings created during a session in **Dr.Web LiveCD** it is necessary to write **Dr.Web LiveCD** files to a flash memory. For this purpose the `CreateLiveUSB` command is used.

In spite of the fact that `CreateLiveUSB` does not change or delete the content of devices, it is recommended to save the files from the flash drive you are going to use to another data carrier, before running the command.

To enable load of **Dr.Web LiveCD** it is not required to write the product to a CD disk and have a CD drive available. You may use a virtual machine with a CD drive emulator instead.

All **Dr.Web LiveCD** files are written to the `/boot` directory. `CreateLiveUSB` may change the configuration of the partitions of the flash drive, if necessary; the original configuration is saved to the `/boot/partition.backup` file. `CreateLiveUSB` copies the MBR on the flash drive; the original master boot record is saved to the `/boot/mbr.backup` file. See Figure 14.

Figure 14. Create LiveUSB



To create a boot flash automatically

1. Connect the flash drive. It takes maximum ten seconds for a connection to be registered.
2. In the graphic shell, double-click the **Create Live USB** icon on the desktop, or run `create_usb` command in the console.
3. **CreateLiveUSB** will detect all available partitions automatically.
4. Select the suitable partition and press ENTER.
5. Files will start to copy automatically.

5. Reporting a bug

If you use graphic shell, then to send a report about some bug in program operation you must do the following:

- pass to the main options section of the **Scanner** using the **Options** button  on the toolbar or using the menu in the **Scanner** main window: **Settings** -> **Options**;
- in the main options section select **Support** tab;
- press the **Bug report** button on this tab;
- after that an inbuilt mail client will be started with the message template already opened;
- in the **Subject** field give a brief description of the problem encountered, and in the message body describe the problem in every detail, including the steps to be made to reproduce it;
- send the message using the default e-mail account.

If you use console, then to send a report about a bug use the following algorithm:

- using the arrow keys, select the **Report Bug** items from the **Start Menu** and press **ENTER**;
- a console text editor (nano) will open, where you can describe the encountered problem;
- after finishing the description, press **CTRL+X** to exit the text editor;
- before exit you will be prompted to make a decision whether you want to send the bug report or not, and press the corresponding key (**Y** - to send a report, **N** - to discard it).