

Forensic Investigation Tutorial Using DEFT

September 25, 2015 By Raj Chandel

DEFT (acronym for Digital Evidence & Forensics Toolkit) is a distribution made for Computer Forensics, with the purpose of running live on systems without tampering or corrupting devices (hard disks, pen drives, etc...) connected to the PC where the boot process takes place.

The DEFT system is based on GNU Linux; it can run live (via DVDROM or USB pen drive), installed or run as a Virtual Appliance on VMware or Virtual box. DEFT employs LXDE as desktop environment and WINE for executing Windows tools under Linux. It features a comfortable mount manager for device management.

First Download ISO image of deft Linux from [here](#)

After having started the DEFT boot loader, you will see a screen with several boot options. Now click on **Install DEFT Linux 8**



Now click on **continue**

Language

- Prepare
- Disk Setup
- Timezone
- Keyboard
- User Info
- Install

Welcome

Please choose the language to use for the install process. This language will be the default language for this computer.

English



www.hackingarticles.in

You may wish to [update this installer](#).

[Quit](#)

[Back](#)

[Continue](#)

Now Select the **third party software** option and click on **continue**.

Language

Prepare

Disk Setup

Timezone

Keyboard

User Info

Install

Preparing to install DEFT

For best results, please ensure that this computer:

has at least 8.6 GB available drive space

is connected to the Internet

DEFT uses third-party software to play Flash, MP3 and other media, and to work with some graphics and wi-fi hardware. Some of this software is proprietary. The software is subject to license terms included with its documentation.

Install this third-party software

Download updates while installing

[Quit](#)

[Back](#)

[Continue](#)

Select Guided-use entire disk and click on **install now**

DEFT 8

installation process

Language

Prepare

Disk Setup

Timezone

Keyboard

User Info

Install

Installation type

Where would you like to install Kubuntu?

- Guided - use entire disk
- Guided - use entire disk and set up LVM
- Guided - use entire disk and set up encrypted LVM
- Manual

SCSI33 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S

Before:

After:

DEFT
100.0% (1.0 B)

Quit

Back

Install Now

Now select your time zone and click ok

Language

Prepare

Disk Setup

Timezone

Keyboard

User Info

Install

Where are you?

Select your location, so that the system can use appropriate display conventions for your country, fetch updates from sites close to you, and set the clock to the correct local time.



Now fill your personal Details and select Continue. Click on Restart Now.

DEFT 8

installation process

Copying files... 37%

Language

Prepare

Disk Setup

Timezone

Keyboard

User Info

Install

Who are you?

Your name:

RAJ CHANDEL

Pick a username:

raj

www.hackingarticles.in

If more than one person will use this computer, you can set up multiple accounts after installation.

Choose a password:

Enter the same password twice, so that it can be checked for typing errors.

Your computer's name:

raj-virtual-machine

The name it uses when it talks to other computers.

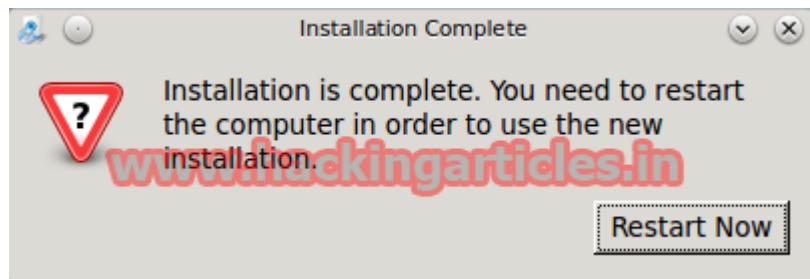
Require my password to log in

Log in automatically

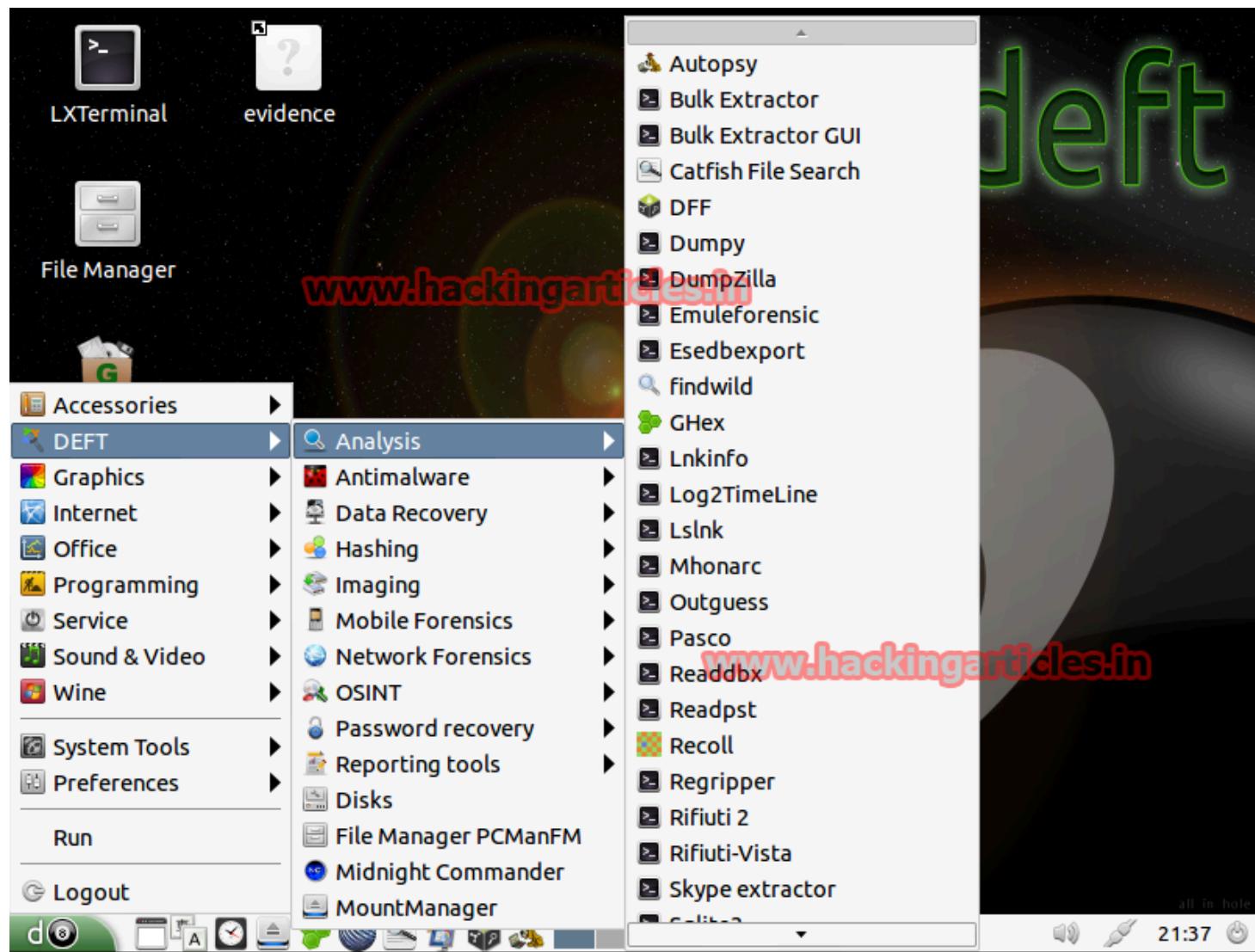
Encrypt my home folder

[Back](#)

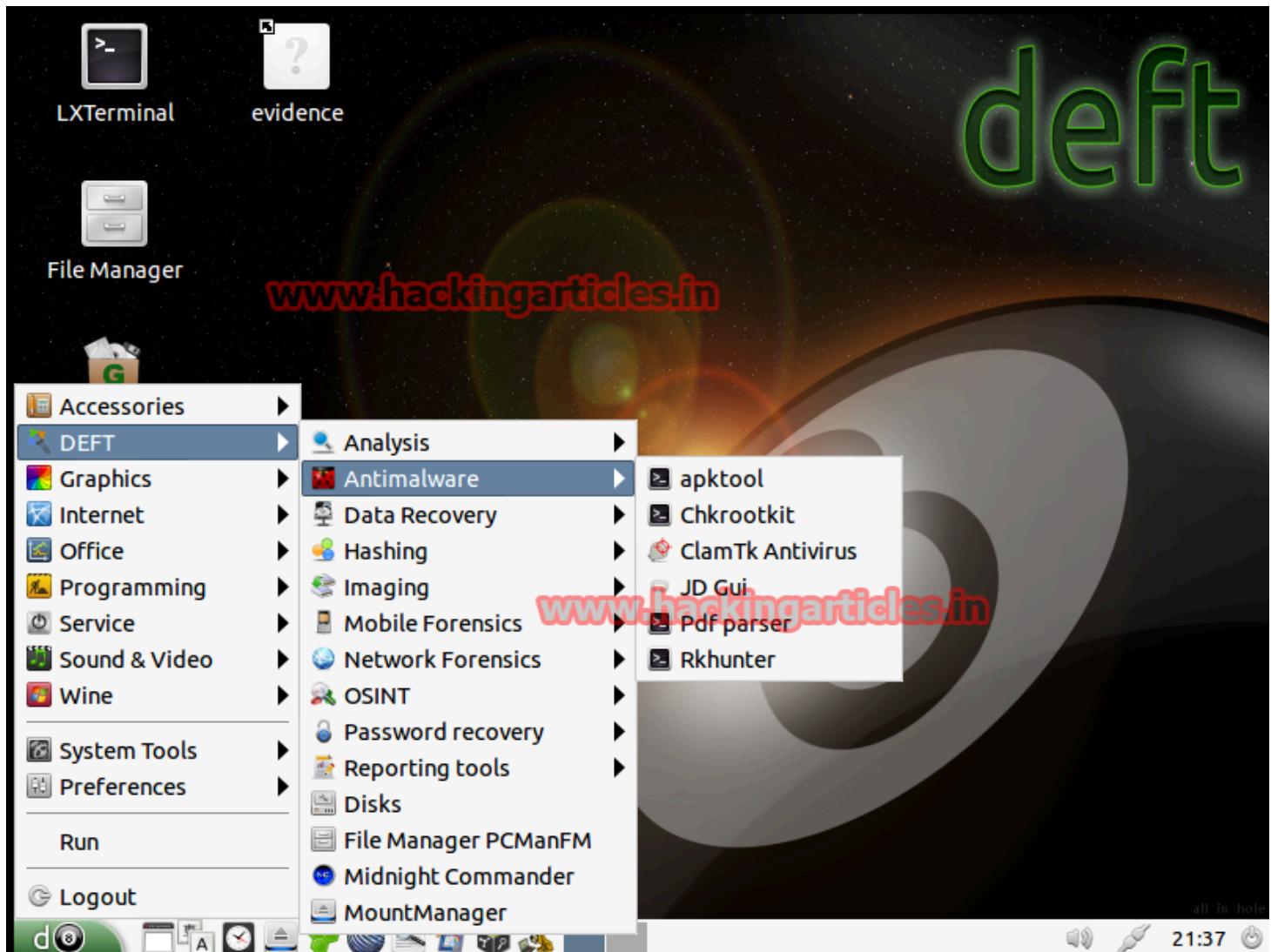
[Continue](#)



Analysis – Analysis Tools files of different types



Antimalware – Search for root kits, viruses, malware and malicious PDFs.



Data Recovery – File Recovery Software



Hashing – Scripts that allow the realization of calculating hashes of certain processes (SHA1, SHA256, MD5 ...)



Imaging – Applications that we can use to make cloned and imaging of hard drives or other sources.



Mobile Forensics – Analysis Blackberry, Android, iPhone, as well as information about typical databases SQLite mobile devices used by applications.



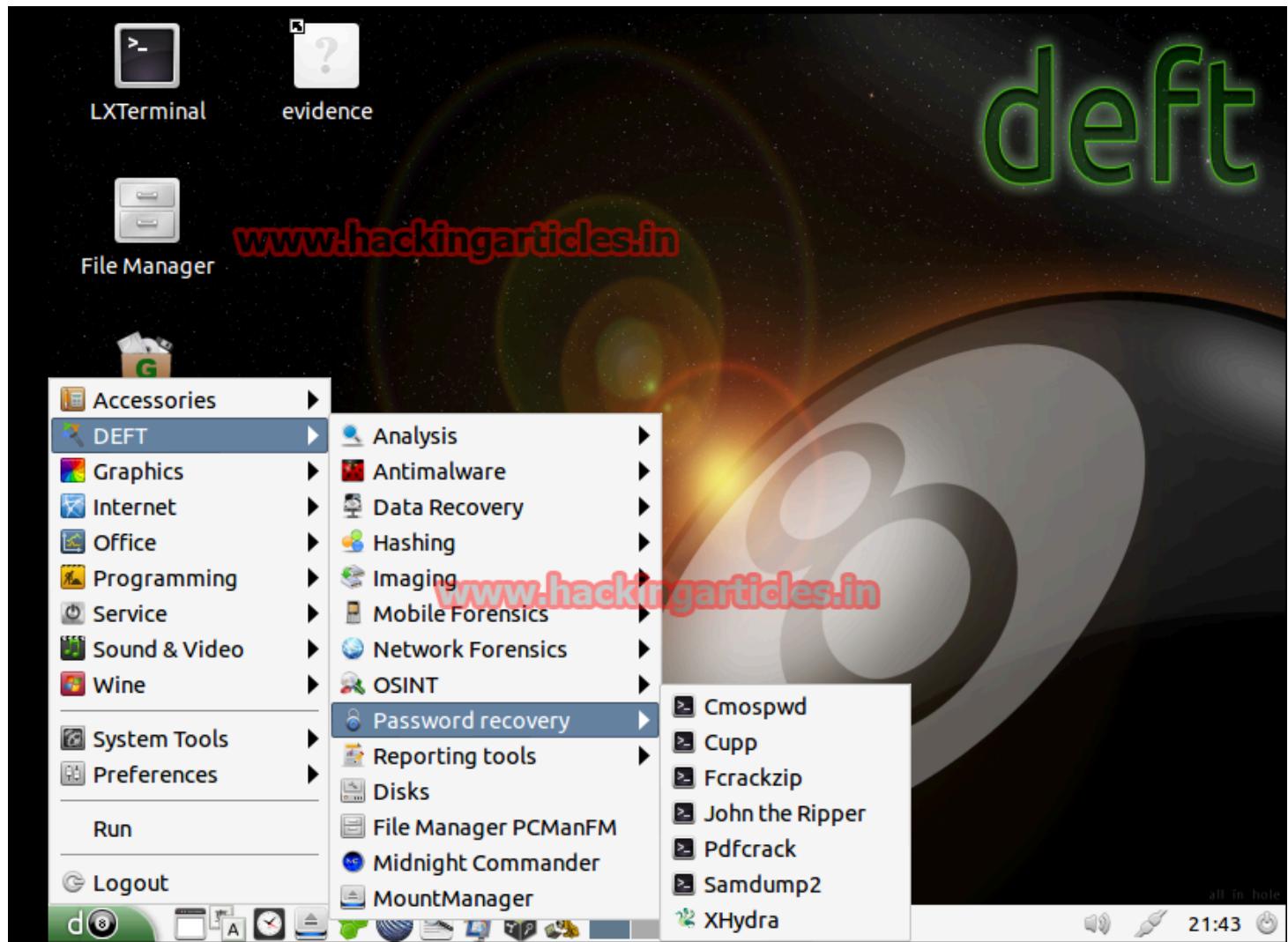
Network Forensics – Tools for processing information stored in network



OSINT – Applications that facilitate obtaining information associated with users and their activity.



Password recovery – Recovery BIOS passwords, compressed files, office, brute force, etc.



Reporting tools – Finally, within this section you will find tools that will facilitate the task of reporting and obtaining evidence that will serve to document forensics. Screen capture, collection of notes, desktop activity log, etc.

