Forensic Investigation Tutorial Using DEFT

September 25, 2015 By Raj Chandel

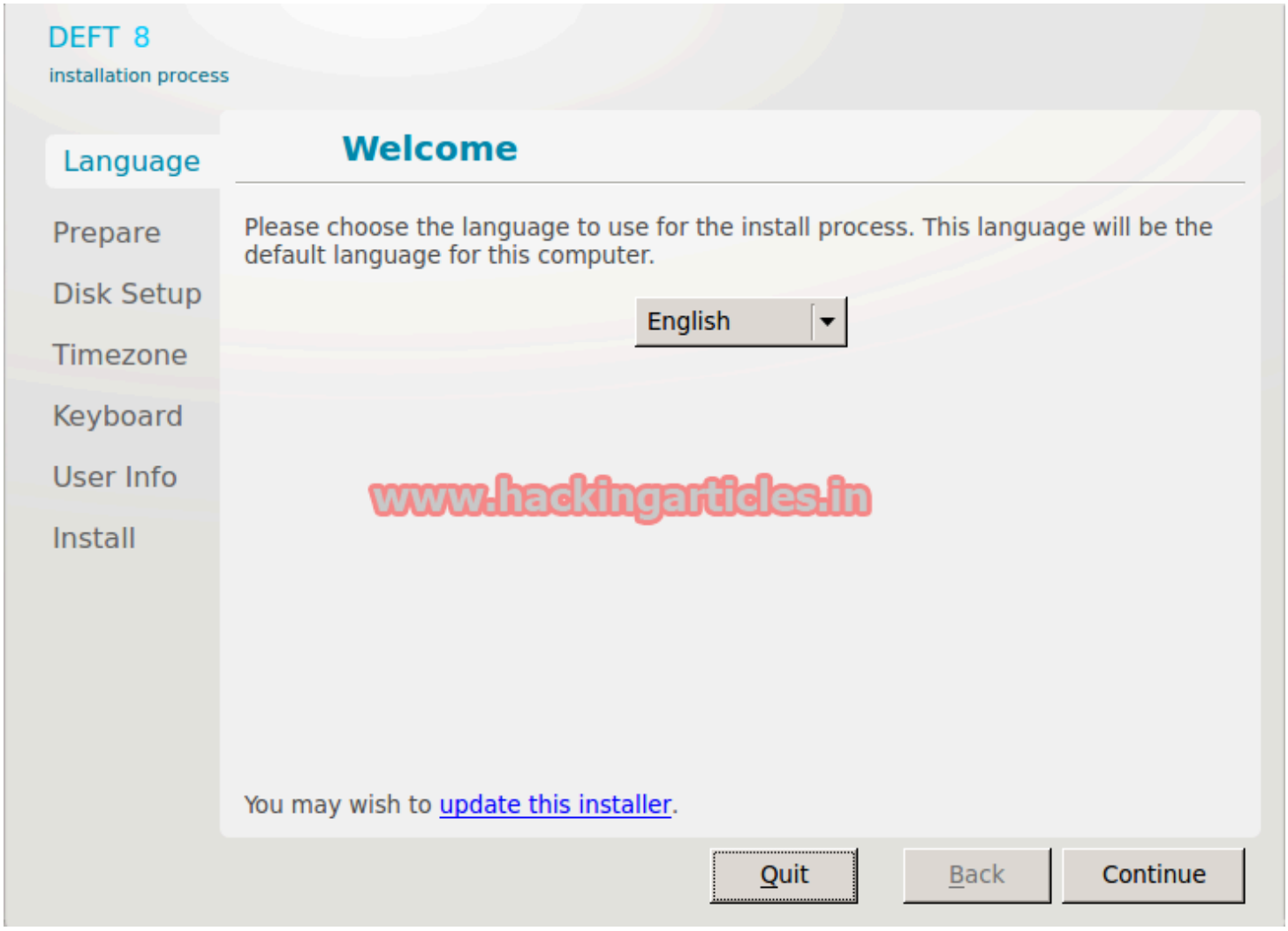
DEFT (acronym for Digital Evidence & Forensics Toolkit) is a distribution made for Computer Forensics, with the purpose of running live on systems without tampering or corrupting devices (hard disks, pen drives, etc…) connected to the PC where the boot process takes place.

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.

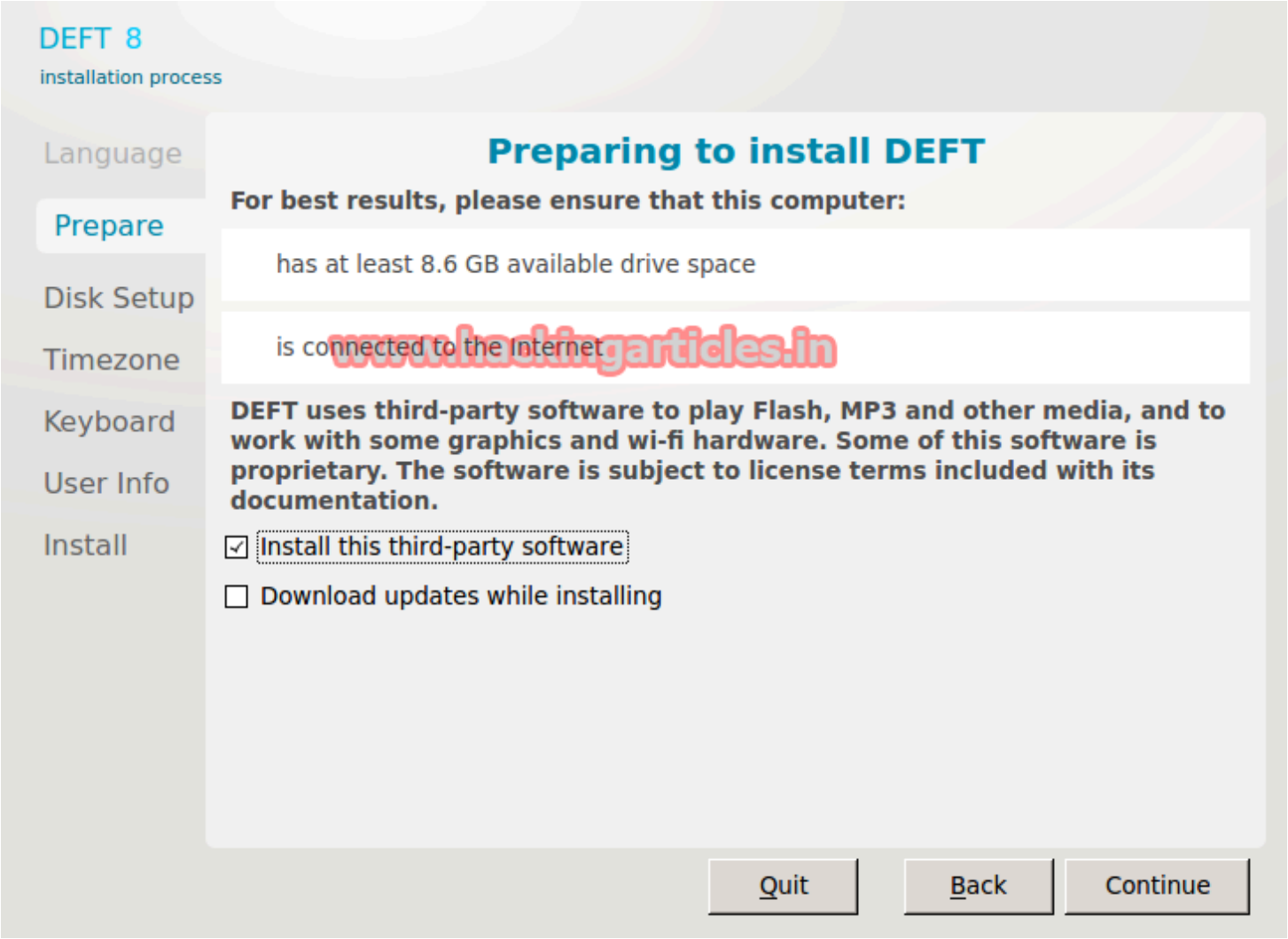
First Download ISO image of deft Linux from **here**

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

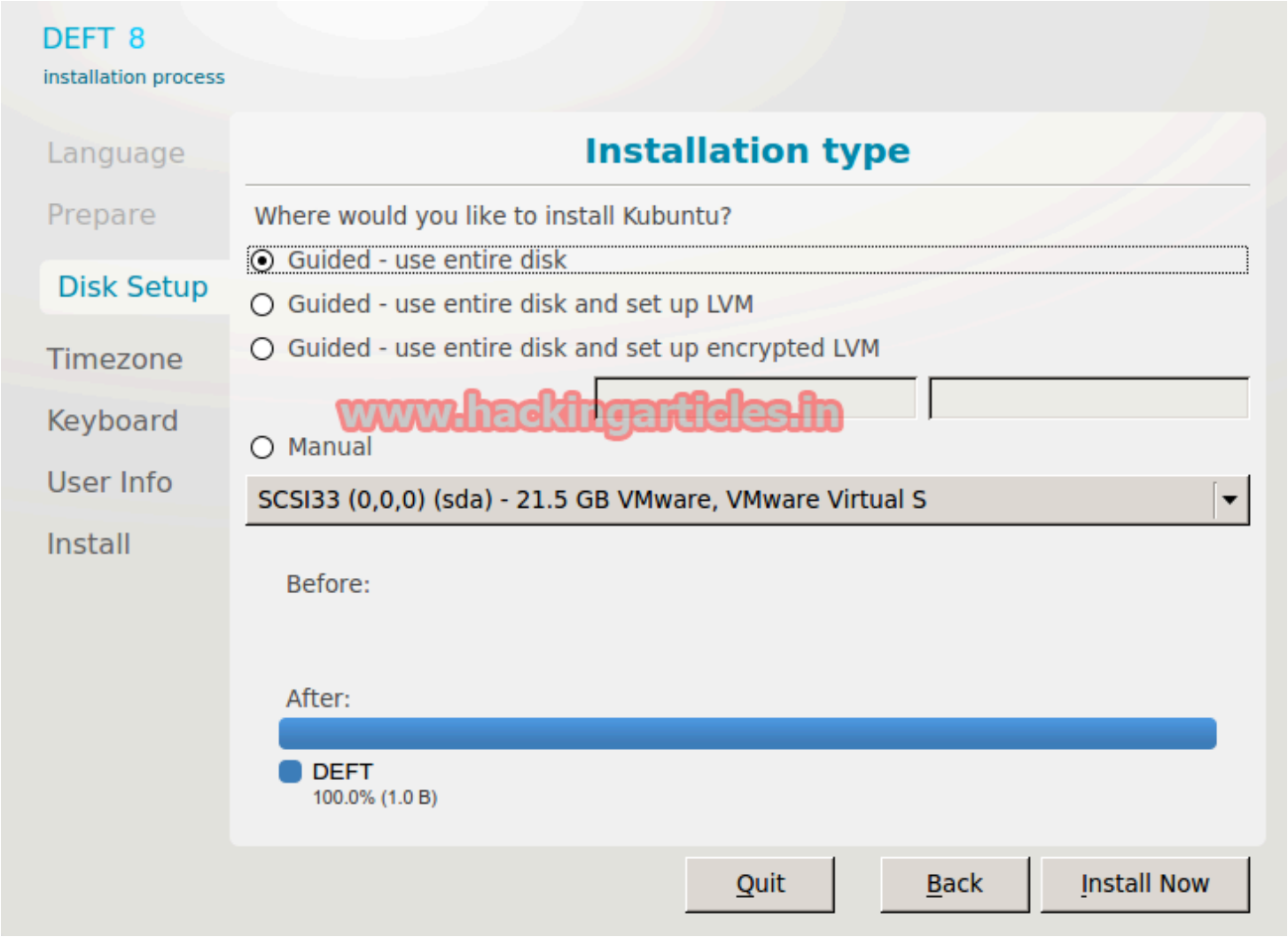
Now click on **continue**



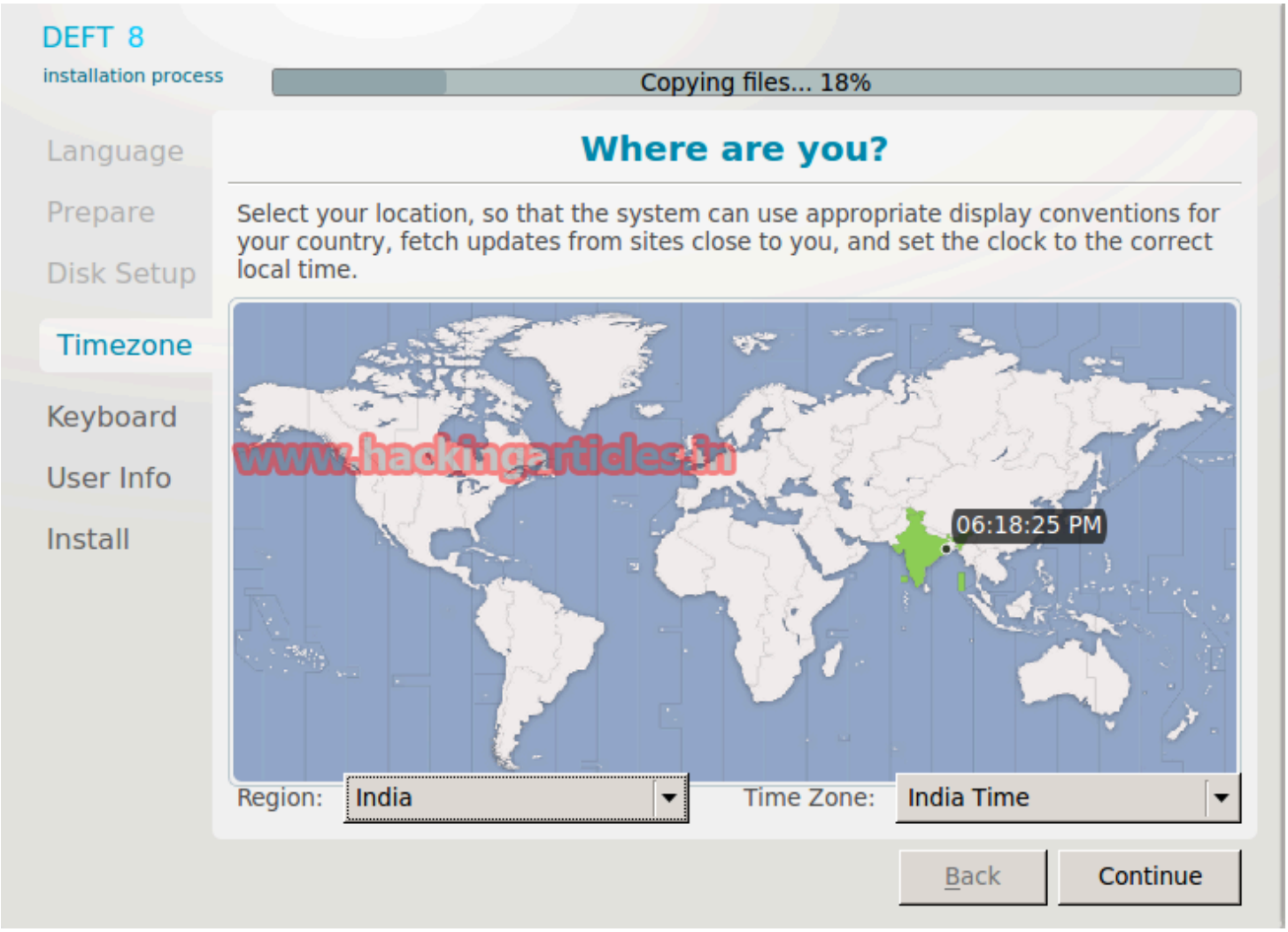
Now Select the **third party software** option and click on **continue.**



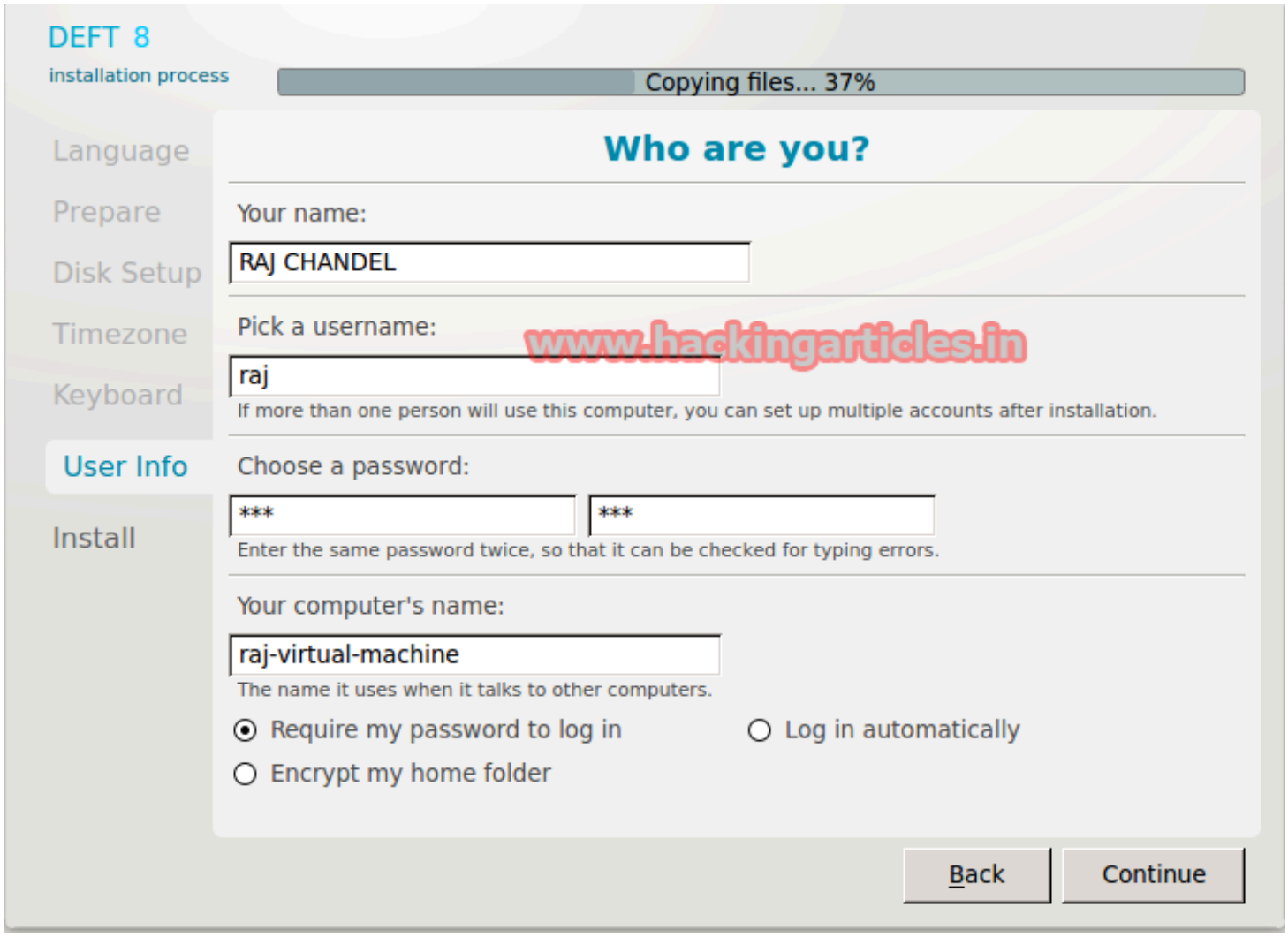
Select Guided-**use entire disk** and click on **install now**

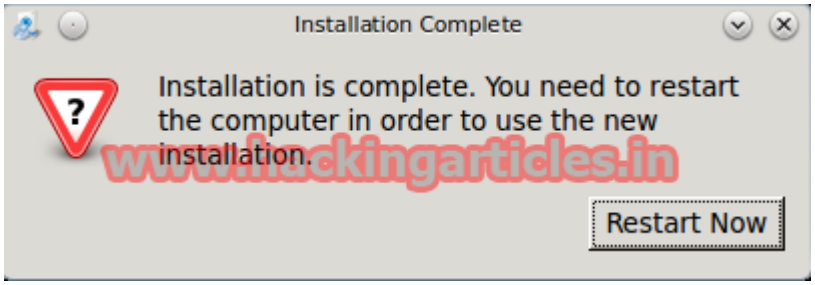


Now select your time zone and click ok

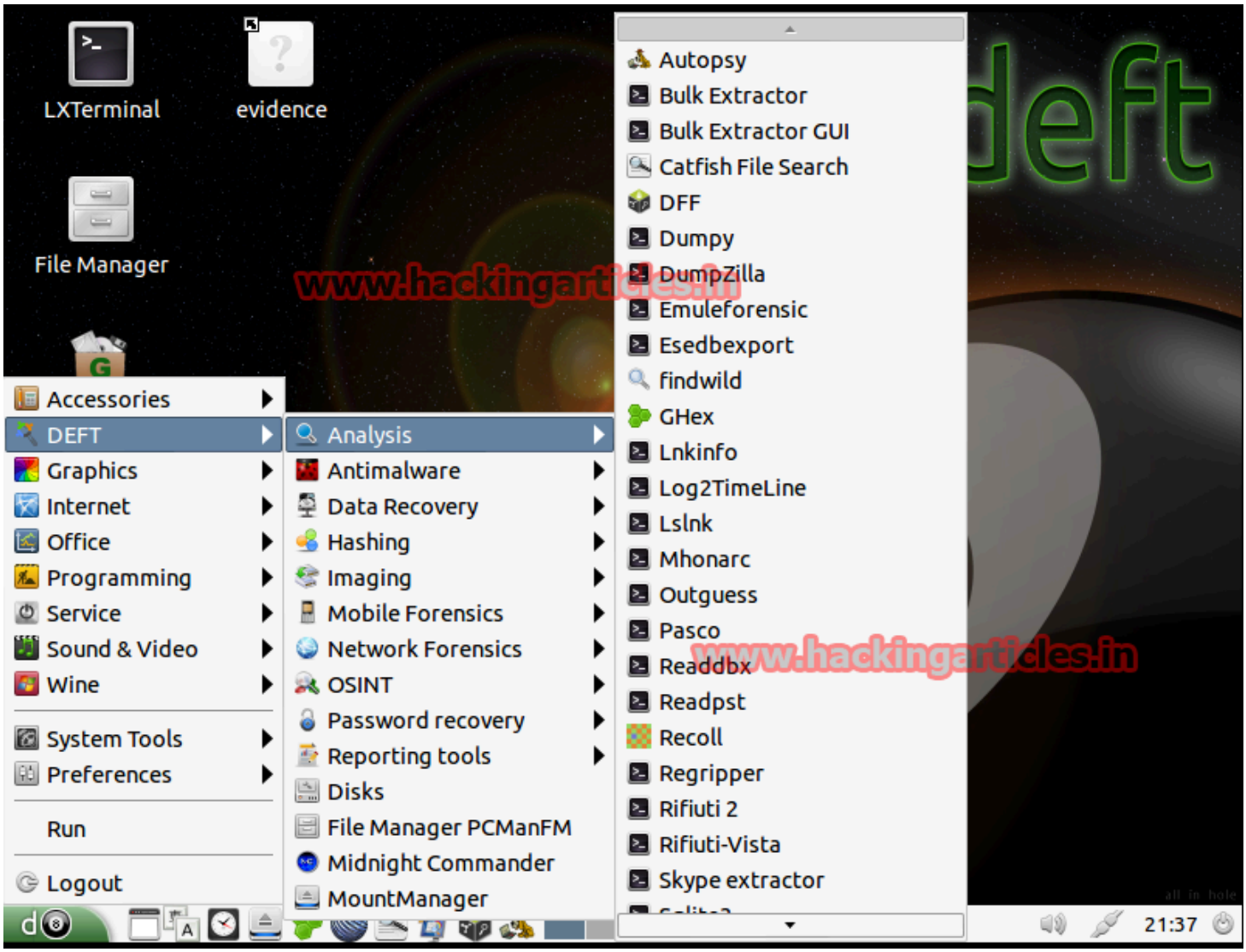


Now fill your personal Details and select Continue. Click on Restart Now.





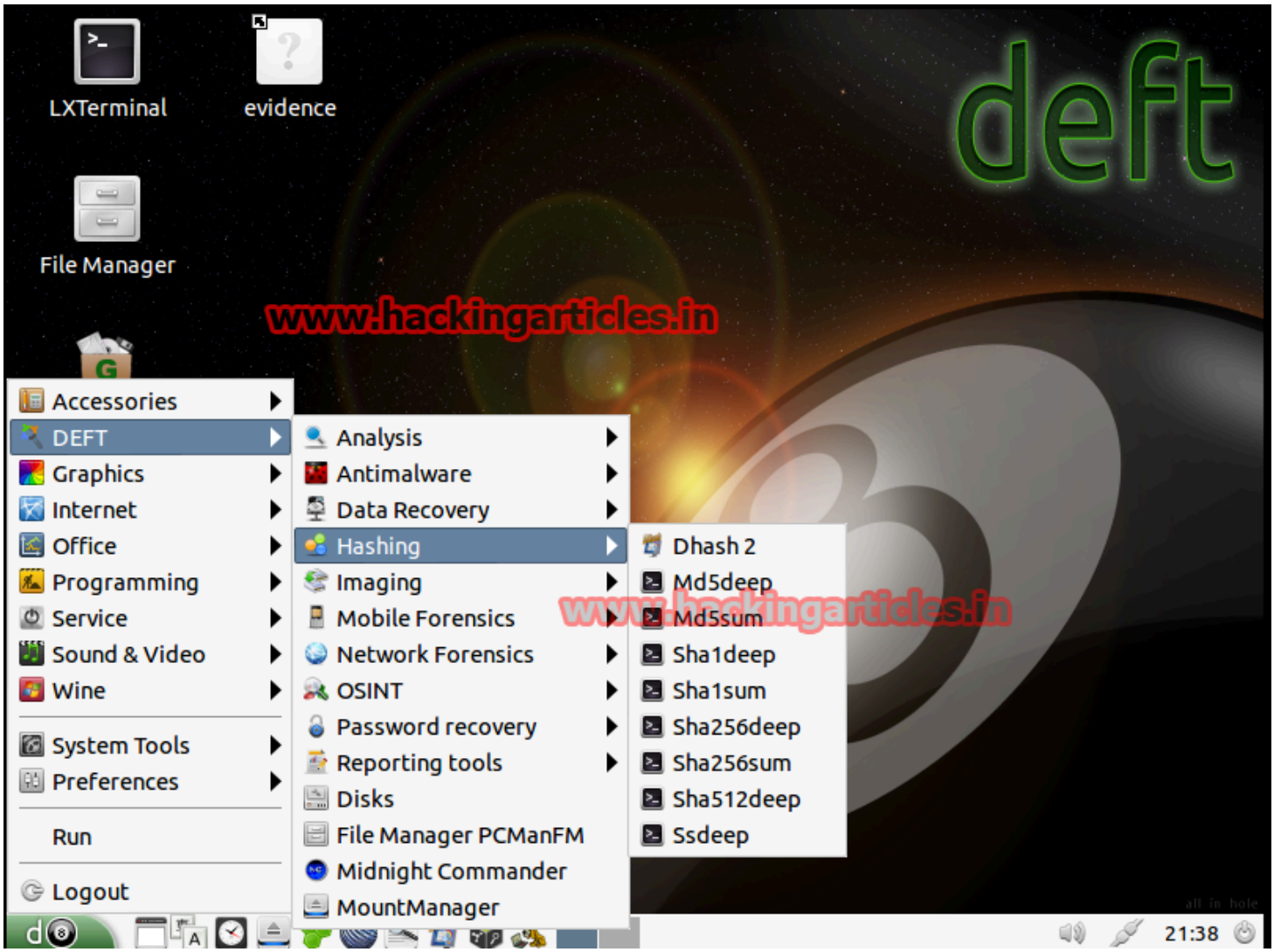
Analysis – Analysis Tools files of different types



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.


LXTerminal
evidence
File Manager
deft
www.hackingarticles.in
Accessories
DEFT
Graphics
Internet
Office
Programming
Service
Sound & Video
Wine
System Tools
Preferences
Run
Logout
Analysis
Antimalware
Data Recovery
Hashing
Imaging
Mobile Forensics
Network Forensics
OSINT
Password recovery
Reporting tools
Disks
File Manager PCManFM
Midnight Commander
MountManager
Grab screenshot
KeepNote
Mobius Forensic
RecordMyDesktop
SciTE Text Editor
VYM - View Your Mind
21:43