Linux中使用LiveCD恢复受危害的系统 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/145/2021_2022_Linux_E4_B8_AD_E4_BD_c103_145167.htm 您希望不用经过冗长的系统安装和配置过程就可以评估 Linuxreg. 平台；但由于所采用的模拟方法的不同，因此速度比一些商业化模拟器慢。另外一种商业化模拟器是 VirtualPC。 调查计算机 侵入计算机和计算机网络并在其掩护下进行严重非法活动是一种非常普遍的行为，甚至普遍到许多人都具备实现此类行为的必备技能。然而，检测并捕捉入侵者的能力却并非同样普遍。伟大的（尽管是虚构的）侦探福尔摩斯曾经说过：“ 在搜集齐所有证据之前就进行推理是一个绝大的错误。这会让判断有所偏颇。 ”从遭遇安全威胁的系统中搜集证据是计算机“ 取证 ”专家（数字时代的福尔摩斯）的工作。他们使用专门工具来搜集、研究并分析关于系统的信息。对于这种工作来说，最好的工具是开源工具，这并不奇怪。The Coroners Toolkit (TCT)、Sleuth Kit、Autopsy Forensic Browser 以及 FLAG (Forensics Log Analysis GUI) 都是非常流行的工具，不但安全专家喜欢使用这些工具，很多计算机安全课程的讲师也都很喜欢这种工具。 Helix 与很多专门 LiveCD 一样，Helix 也是应需产生的。Andrew Fahey 是 e-fense Inc. 的一位合作安全专家，他以 Knoppix 作为基础，并添加了很多日常工作中使用的工具。“ Helix 用户非常有参与意识。全世界都有 Helix 的用户，他们不断提供反馈信息。由于人们是在不同的环境中使用 Helix，因此要确保所有组件在任何情况下都可精确完成工作是一项持续不断、耗时很多的任务。所以我依靠用户的反馈改进

Helix，并修正他们所发现的故障。我还要依靠用户完成语言翻译。”Andrew 说。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com