

Installing Ubuntu/Caine

The base system for creating a forensic workstation is Ubuntu. Starting with 4buntu version 8.04-004, the recommended Ubuntu platform is Caine, which is based on Ubuntu 8.04. Although the 4buntu script will run and install the software on a plain Ubuntu 8.04, the preferred platform for a forensic workstation is a Caine system. Caine is specifically configured for digital forensic work. Caine also includes a number of digital forensic tools. The 4buntu script installs additional forensic tools to Caine to make it a powerful forensic workstation.

You will need a computer with plenty of disk space and ram to install Caine. Since Caine is based on Ubuntu 8.04, it has the same system requirements. Also, please note that digital forensic work requires large disk space to be able to handle the data for analysis. Some of the programs used in forensic work require additional CPU and RAM resources in order to do the work in less time. Once you have adequate hardware, you can install Caine as follows:

WARNING: It is recommended to have a dedicated system to build a forensic workstation since 4buntu will customize the system, including the **root** account. If you can't dedicate a system for forensic work, consider using a virtual machine. From the procedural point of view a dedicated system also reduces the risk of cross contaminating the digital evidence.

1- Download the Caine Live CD (iso image) and burn it to a CD. The Caine CD is located at <http://www.caine-live.net> .

2- Boot from the Caine Live CD

3- Click the Install icon on the Caine Desktop. Follow the on-screen instructions to complete the installation.

After a successful installation of Caine, you must verify that network connectivity is properly configured and the computer has access to the Internet. The Caine installation defaults to the Italian keyboard layout (Caine was developed in Italy). If necessary change the keyboard layout to your native keyboard with the following menu picks Main->System->Preferences->Keyboard->Layouts->Add.

Downloading and running 4buntu

Follow these steps run the 4buntu script:

Step 1:

Start your new Caine system and login with the account created during the installation.

Step 2:

From the 4buntu Download page determine the latest available version of 4buntu. The commands below indicate version **8.04-XXX**. You will need replace XXX for the actual release number with is a given by three digits. The latest release should be in the 4buntu Download web page.

Step 3:

From the Caine Desktop follow these clicks to get a Terminal; **Main Menu->Accessories->Terminal**

Use the 4buntu version determined in **Step 2** for the wget command below. In the terminal issue the following commands:

```
wget "http://downloads.sourceforge.net/four-buntu/4buntu-8.04-XXX.tar.gz?use\_mirror=0"
```

```
tar xzf 4buntu-8.04-XXX.tar.gz
```

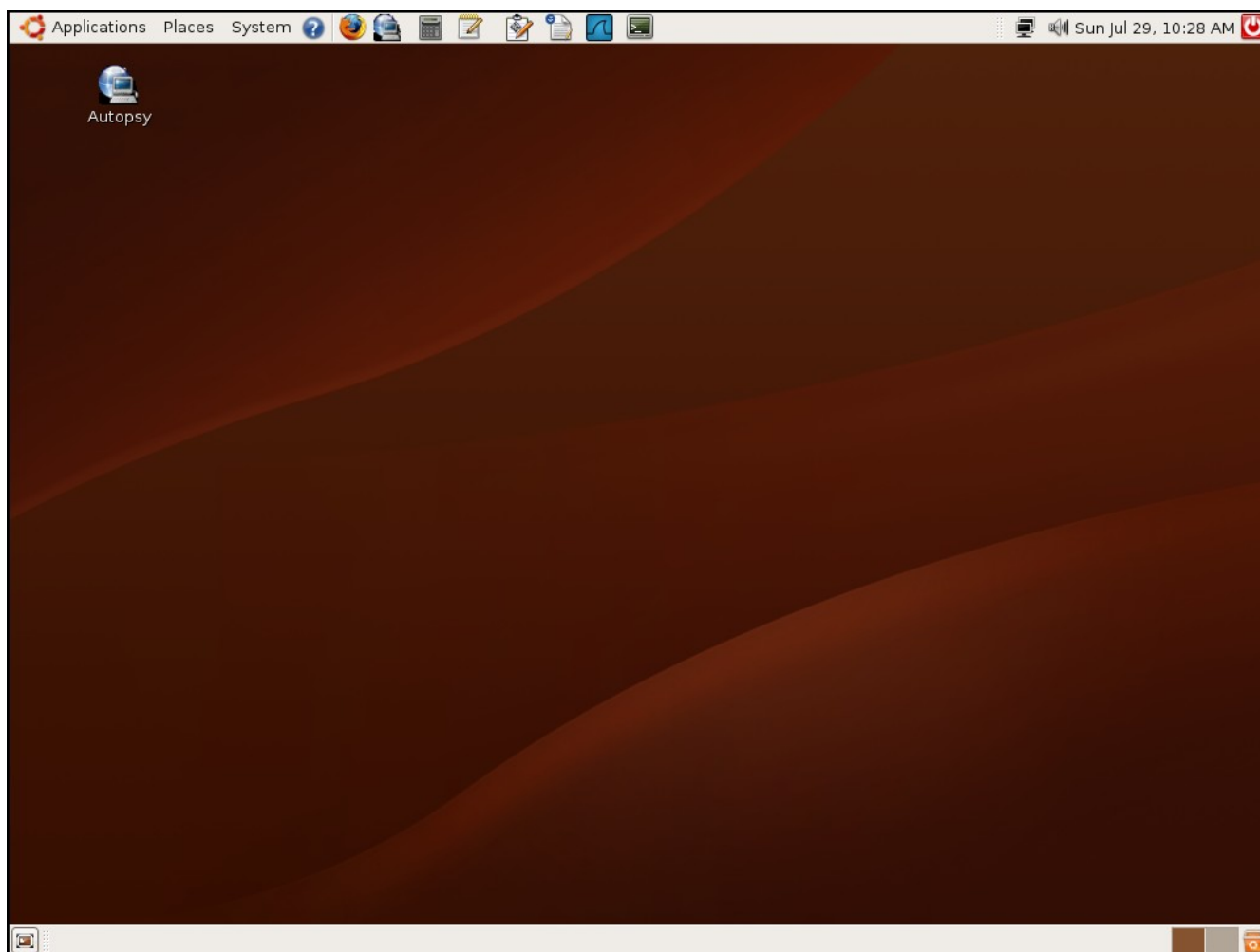
```
cd 4buntu-8.04-XXX
```

```
sudo sh 4buntu
```

After the last command, follow the on-screen instructions. At the end, the script will produce a report of the main packages that were installed or detected, by marking them as OK. You will be prompted to hit enter to continue with a re-start the login session.

Step 4:

From the Caine login screen, proceed to login with the **root** account. Use the root password that you set in Step 4 above. After login the desktop should like like this:



You have a complete digital forensic analysis workstation.