Virtual Appliance:

A virtual Appliance is a Virtual Machine (VM) image file consisting of a pre-configured OS environment. It is deployed on virtualization technology (in this case we're using Oracle VirtualBox).

Instructions to install and configure the Virtual Appliance:

What you need to download:

1. Oracle VM VirtualBox
   You can download it here: https://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html
2. Practical Forensics 101 - .vmdk file provided on the website

W**hat is required:**

Atleast 20GB Memory should be available for allocation on your machine.

Steps for Setup:

1. Open Oracle VM VirtualBox
2. Click on "New".
3. Input the name of the machine as "Practical Forensics 101" and select Linux OS.
4. Set the amount of memory as 2GB RAM = 2048 MB.
5. Now you will be prompted to create a virtual hard disk. This is an important step in running your .vmdk file. Select the option 'Use existing hard disk' and click the "Choose a virtual hard disk file ….' button.
6. In the file selection window that opens up browse and select the Practical Forensics 101.vmdk file.
7. Click Open.
8. Now the 'Use existing hard disk' option will have the .vmdk file you selected. Click Next.

9. Click ‘Create’ to finish the process.
10. Now the VirtualBox Manager will have the new virtual machine listed. Click ‘Start’ to run the Practical Forensics 101 VM.

SETUP COMPLETE!

Looking for required information:

1. When you open the VM, you will see a folder on the desktop named “Practical Forensics 101”
2. Open the folder.
3. There are 2 folders named “Complex Case” and “Practice”.
4. The Complex Case folder contains the evidence, scenario required for the game and its solution manual.
5. The Practice folder consists of yet 3 more folders namely “System Forensics Practice Case”, “Network Forensics Practice Case” and “Email Forensics Practice Case”. These folders contain evidence and scenario required for each in their respective folders with the solution manuals.

Digital Forensic Tools:

All the tools you require are already embedded into the system. Just type them in the search box and you will find them.

Tools you require:

1) Wireshark

2) Bulk Extractor

3) Autopsy