

# Forum: [Hack Forums](#)

Thread: [\[Tutorial\] Buscador - Linux build for Private & Online Investigators \[NOOB FRIENDLY\]](#)

Malicious` - January 20, 2018, 4:21 am

Introduction A friend of mine recently recommended me to use an OS made specifically designed for online investigations. I was doing some research but didn't find much until I stumbled on a website some of you may know, [IntelTechniques](#). Most visitors use the website for their free online investigation tools found [here](#), but apparently they also made their very own OS, Buscador. Buscador, Spanish for Search Engine, is based on Ubuntu Linux and the build is designed to run on a Virtual Machine.

Why should I use Buscador? If you are not used to using a Linux build this one is perfect for you. Unlike traditional Linux builds where most tools are ran by using commands in the Terminal, Buscador has a UI for every tool pre-installed on the build. Your options when it comes to pentesting will be limited though. If you are a pentester I strongly recommend using a different Linux build.

Technical information

Version: v1.1

Release date: 07/05/2017

ETA on v1.2: end of January 2018. This tutorial will be updated when Buscador has been updated.

Beta Version: v1.2

Release date: 01/30/2018

Installation First decide what Virtual Machine you want to run Buscador on. VirtualBox is free and will be discussed in this tutorial, while VMWare is a premium service. Although Buscador was designed to run on a VM you can also find an experimental USB Boot on IntelTechnique's website.

Downloading Buscador v1.1 Virtualbox:

[google.com/open?id=0B7-htCcMAiX-OVdJSVB0dVZRVWM](https://www.google.com/open?id=0B7-htCcMAiX-OVdJSVB0dVZRVWM) Click to download!

(MD5: 52bd85e7037c7523f85728761039d1ae) VMWare:

[google.com/open?id=0B7-htCcMAiX-Mkt5SWZVbWJweE0](https://www.google.com/open?id=0B7-htCcMAiX-Mkt5SWZVbWJweE0) Click to download! (MD5:

0e4a4d1a2c731fa2d3f7a24dde99460b) ISO (experimental USB Live Boot):

[google.com/open?id=0B7-htCcMAiX-U3N6c0RjY2dBTGc](https://www.google.com/open?id=0B7-htCcMAiX-U3N6c0RjY2dBTGc) Click to download!

(MD5: 255fdf5e562d25a9cccad97d5a83473)

Downloading Buscador v1.2 (BETA) VirtualBox:

[google.com/uc?id=1fFRmh4CBNriXgOl9utRFGApCly3GwdW&export=download](https://www.google.com/uc?id=1fFRmh4CBNriXgOl9utRFGApCly3GwdW&export=download) Click to download!

(fbc34c2b0234bc872498885c13859f77) VMWare:

[google.com/open?id=1UR-eb5-9CPBeajl8l4pbkc-i9IMJspk5](https://www.google.com/open?id=1UR-eb5-9CPBeajl8l4pbkc-i9IMJspk5) Click to download!

(18b26fe84cf00fd4403f52367534c58d) ISO:

[google.com/open?id=1vu3tuiAXVnfSkeYImGfSgTjDi5c6TpN7](https://www.google.com/open?id=1vu3tuiAXVnfSkeYImGfSgTjDi5c6TpN7) Click to download!

(7ad64fe13444c785c17f9566b3f72b63)

Installation & Configuration In this tutorial we'll be showing you how to install Buscador in Virtualbox. Configuring Buscador is very straight-forward but to make things even easier I have added pictures for some steps in the installation process.

Download Virtualbox & Buscador

Launch Virtualbox, Under the 'File...' tab, click the 'Import' button and import the OVA file you

downloaded. This process should only take a few minutes. ([Image](#))

Before launching the VM, we'll have to edit some settings. Highlight the machine and click the 'Settings' button. If you want you can change the name of the machine now. ([Image](#))

Under 'General' go to 'Advanced' and change the 'Shared Clipboard' setting to bi-directional. This way you can easily copy information from your VM to your computer and vice versa.

Under 'System' > 'Motherboard' increase the RAM to half of your computer's capacity. ([Image](#))

Under 'Display' > 'Screen' increase Video Memory to 128 MB.

Under 'Storage' add a new optical drive. You can do this by right-clicking the plus icon on the left. Choose 'Add optical drive' & 'Leave empty' option.

Now go to 'Shared folders' and click the plus icon on the right. Choose the folder to collect evidence on and select 'Auto-Mount'. ([Image](#))

We can now launch the machine! Default username is 'osint'. Default password is 'osint'

Configuration is not completely done yet though. In the VirtualBox menu select 'Devices' > 'Insert Guest Additions CD Image'

Let the Image be installed and reboot your system. This may take a few minutes to complete. ([Image](#))

Open up the Terminal and type the following command: `sudo adduser osint vboxsf`

Reboot your system and configuration is done!

If you plan on running Buscador in VMWare or by USB Live boot, check out the installation guide found [here](#)!

**Snapshots** After doing some investigations you have the risk of your VM being cluttered with information you no longer need. Therefore I highly recommend making a snapshot of your fresh Buscador build. Shut down your VM completely and click the Snapshots button. Click the plus button and name the Snapshot whatever you want.

If you ever want to revert to your old snapshot just right-click it and click the 'Restore...' option.

**Features** The current build is 3,5 GB and includes, but isn't limited to the following resources:

Custom Firefox & Chrome install with add-ons  
Default extensions in Firefox: Copy All, Disconnect, DownThemAll, DuckDuckGo, Exif Viewer, Firegestures, Firefox, FoxyProxy, Foxyspider, gtranslate, HTTPS Everywhere, JSONView, Nimbus Screen Capture, NoScript, Self-Destructing Cookies, UA Switches, Video Downloader.

Default extensions in Google Chrome: DuckDuckGo, GNOME Shell Integration, G Docs, HTTPS Everywhere, ipinfo, JSON Viewer, Lightshot, Prophet, Proxy SwitchYOmega, Shodan, Threatpinch Lookup, uBlock Origin (+ Extra), UA Switcher, Wappalyzer, WEBRTC Leak Prevent Toggle

**Video Manipulation Utilities (FFmpeg)**

FFmpeg is a cross-platform solution to convert audio and video.

**Youtube Downloader** A simple command-line tool that downloads videos from Youtube. Comes with a UI in Buscador.

**Recon-NG**

Recon-NG is a web reconnaissance framework written in Python. Documentation can be found [here](#). Some users have reported Recon-NG does not work in Buscador v1.1. The developers are aware of the issue and will fix this in v1.2 (coming out Jan 2018)

**Maltego**

Before using Maltego you'll have to sign up for free on [Paterva](#).

**Cree.py**

This is honestly one of my favorite tools. I made a tutorial on configuring Creepy earlier, you can find that tutorial [here](#)!

**Metagoofil**

Very powerful tool for collecting meta-data from websites.

### Example output for Youtube

Code ===== /home/osint/Metagoofil/docs\_youtube.com/jp.pdf

File Name : jp.pdf

MIME Type : application/pdf

PDF Version : 1.3

Page Count : 9

Title : YouTubeNextUp2017JapanContestRulesJAPAN\_FINALV2

Producer : Mac OS X 10.12.4 Quartz PDFContext

Create Date : 2017:04:28 16:10:03Z

### Exiftool

Extracts meta-data from images. Also allows you to delete or edit meta-data too.

Example output from [this image](#) Code File Name : Priam's\_treasure.jpg

Orientation : Horizontal (normal)

Caption Writer : Susan Jane Williams

Legacy IPTC Digest : 5A29C52C2E2B7308256F9615389F5A61

Workagent : Heinrich Schliemann (German archaeologist)

Worktitle : Priam's Treasure (Gold of Troy)

Workdescription : Heinrich Schliemann (German archaeologist, 1822-1890); Priam's Treasure; Gold of Troy; partial view; 1873 (discovery) Nearly all Schliemann's material, which was in Berlin at the end of World War II, disappeared in 1945; gold, electrum, silver, and bronze

Workrights : publicDomain

Image Size : 400x600

Megapixels : 0.240

### MedialInfo

MedialInfo is another tool that is able to extract meta-data from media files.

### Harvester

'The Harvester' scans domains for emails and hosts. An example output can be seen [here. \(Large image\)](#)

### WayBack Packer

The WayBack Packer allows you to download the entire WB archive for a specific URL.

### HTTrack

HTTrack allows you to completely copy websites.

### Snapper

Another tool that lets you take snapshots of domains.

### Knock

Knock is a subdomain scanner, that scans for DNS zone transfer and tries to bypass the wildcard DNS record (if enabled). Tool is very easy to use.

### Subbrute

Very similar to Knock. It also scans for subdomains.

### Twitter Export

Exports data retrieved from Twitter profiles.

Currently does not work for everyone in v1.1

### Tinfoleak

Analyzes Twitter profiles and saves the output to a html document.

## Veracrypt

Veracrypt is a free disk encryption tool based on Truecrypt.

## Keepass

Keepass allows you to store your passwords safely.

v1.2 BETA Features (released on 1/30/2018!)

## Aquatone

Aquatone can discover subdomains on a given domain by using open sources as well as the more common subdomain dictionary brute force approach. ([Example image](#))

## EyeWitness

## Sublist3r

Similar to Aquatone it discovers subdomains. I find Aquatone to be better and more extensive.

## MAT (Metadata Anonymisation Kit)

The Metadata Anonymisation Kit is able to delete any metadata on media files.

## KeePassXC

Replaces the outdated Keypass in v1.1

You have reached the end of this tutorial. Thank you for taking the time to read this. I hope some of you have learnt something or started using Buscador thanks to this thread. I'd truly appreciate it if you left me some feedback below. I'm always eager to learn and your input will be very much appreciated!

**JELLY?IsH** - January 20, 2018, 6:21 am

Another great tutorial from Malicious. I heard of this before but I never used it, I'll give it a try.

Thanks!

**oRequiem** - January 20, 2018, 6:40 am

You make some good tutorials, thank you for contributing to the forum!

**The.Businessman** - January 20, 2018, 6:43 am

Great share my friend. Amazing code you have right there

**Malicious`** - January 20, 2018, 8:17 am

(Jan 20, 2018 07:21 AM)symbiø Wrote: [\[CITE\]](#) Another great tutorial from Malicious. I heard of this before but I never used it, I'll give it a try.

Thanks!

(Jan 20, 2018 07:40 AM)oRequiem Wrote: [\[CITE\]](#) You make some good tutorials, thank you for contributing to the forum!

(Jan 20, 2018 07:43 AM)The.Businessman Wrote: [\[CITE\]](#) Great share my friend. Amazing code you have right there

Thank you all for the kind words!

**Zink** - January 20, 2018, 3:35 pm

I really did enjoy reading this, bookmark this thread also for future references.

**Malicious`** - January 21, 2018, 12:21 am

(Jan 20, 2018 04:35 PM)DoctorSheep Wrote: [\[CITE\]](#) I really did enjoy reading this, bookmark this thread also for future references.

Cheers mate. English isn't my native language so expect some grammatical errors. If anyone could rewrite this slightly, that'd be amazing.

**Mad76e** - January 21, 2018, 12:24 am

I love both Reco-ng and exiftool.. this is a nice tutorial.. good work

**Malicious`** - January 21, 2018, 5:18 am

(Jan 21, 2018 01:24 AM)Mad76e Wrote: [\[CITE\]](#) I love both Reco-ng and exiftool.. this is a nice tutorial.. good work

Thanks man! ?

**JuniperHacker583** - January 26, 2018, 12:12 am

This is very useful and I didnt know about it until now. Will certainly give it a try. Thanks allot for the quality post

**Malicious`** - January 26, 2018, 6:06 am

(Jan 26, 2018 01:12 AM)JuniperHacker583 Wrote: [\[CITE\]](#) This is very useful and I didnt know about it until now. Will certainly give it a try. Thanks allot for the quality post

Thanks for checking out the tutorial! Buscador v1.2 will be released in a few days.

**Malicious`** - January 30, 2018, 2:33 am

Buscador has been updated to v1.2! I have updated the thread too.

**rockmy** - January 31, 2018, 7:01 pm

another great one had to read in between work gonna try to put it to use soon thank you

**german.p.r** - February 1, 2018, 5:24 am

Looks great man. Will try

**King Moonracer** - February 1, 2018, 8:41 am

Thanks for the recommendation ! In that vein, I found this:

[//github.com/arismelachroinos/lscript](https://github.com/arismelachroinos/lscript)

"Why should I use Buscador?

If you are not used to using a Linux build this one is perfect for you. Unlike traditional Linux builds where most tools are ran by using commands in the Terminal, Buscador has a UI for every tool pre-installed on the build"

**Malicious`** - February 1, 2018, 11:54 pm

(Feb 1, 2018 09:41 AM)King Moonracer Wrote: [\[CITE\]](#) Thanks for the recommendation ! In that vein, I found this:

[//github.com/arismelachroinos/lscript](https://github.com/arismelachroinos/lscript)

"Why should I use Buscador?

If you are not used to using a Linux build this one is perfect for you. Unlike traditional Linux builds where most tools are ran by using commands in the Terminal, Buscador has a UI for every tool pre-installed on the build"

The Lazy Script is very useful when you are investigating a website indeed.

**Malicious`** - June 12, 2018, 1:05 pm

This tutorial will be updated within the next 7 days as some issues are popping up.

The main issue is a FF add-on injecting ads on websites, but there are other things malfunctioning. This will all be discussed in the thread update soon.

**?C???I?x???** - June 13, 2018, 9:31 am

Incredible high-quality tutorial Malicious my man, guarantee this will come in handy for a lot of new users.

**Narcist** - June 14, 2018, 1:18 am

<https://hackforums.net/showthread.php?tid=5842557>

scammed me

**guaddegoop** - June 20, 2018, 8:26 am

Very helpful. I was having trouble with the virtual machine part but you explained it well.

**Delhi** - June 20, 2018, 8:34 am

Really interesting read and surprisingly informative. Thanks for sharing this with the forum, I will definitely be looking into this and I'll get back to you if I have any questions or concerns!

**JoshEight** - April 29, 2019, 5:47 am

Hey I've been doxing for awhile and this sounds really cool I'll check it out thanks man.

**AlphaMagic** - April 29, 2019, 2:34 pm

Nice tutorial, fella. Thanks!

**fqllexangel** - May 3, 2019, 11:26 am

do u still have the iso file link ??