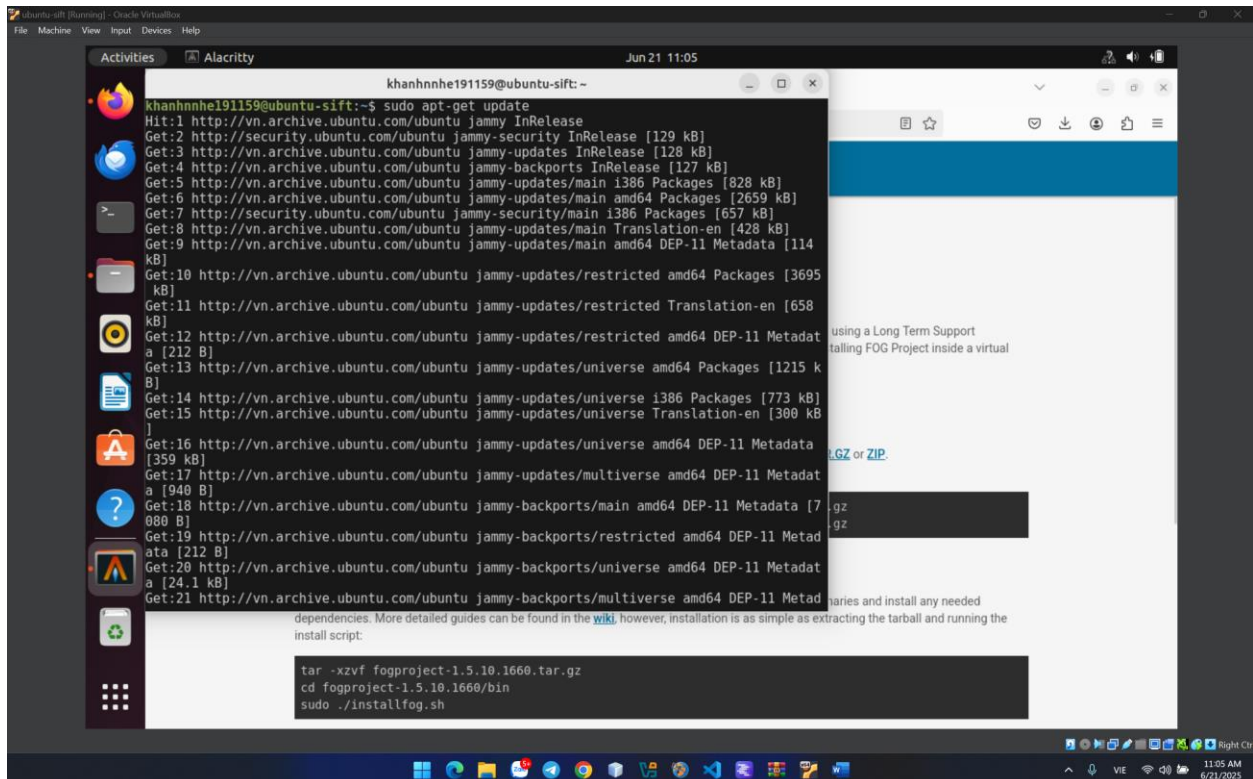


Nguyen Nam Khanh – HE191159 – IA1902 – IAM302

LAB 11: Using FOG for Cloning and Imaging Disks



The screenshot shows a virtual machine environment with the Ubuntu desktop. An Alacritty terminal window is open, displaying the output of the command `sudo apt-get update`. The output lists various packages being updated from the Ubuntu archive, including `jammy InRelease`, `jammy-security InRelease`, `jammy-updates InRelease`, `jammy-backports InRelease`, `jammy-updates/main i386 Packages`, `jammy-updates/main amd64 Packages`, `jammy-security/main i386 Packages`, `jammy-updates/main Translation-en`, `jammy-updates/main amd64 DEP-11 Metadata`, `jammy-updates/restricted amd64 Packages`, `jammy-updates/restricted Translation-en`, `jammy-updates/restricted amd64 DEP-11 Metadata`, `jammy-updates/universe amd64 Packages`, `jammy-updates/universe i386 Packages`, `jammy-updates/universe Translation-en`, `jammy-updates/universe amd64 DEP-11 Metadata`, `jammy-updates/multiverse amd64 DEP-11 Metadata`, `jammy-backports/main amd64 DEP-11 Metadata`, `jammy-backports/restricted amd64 DEP-11 Metadata`, `jammy-backports/universe amd64 DEP-11 Metadata`, and `jammy-backports/multiverse amd64 DEP-11 Metadata`. Below the update output, there is a section titled "dependencies. More detailed guides can be found in the [wiki](#), however, installation is as simple as extracting the tarball and running the install script:" followed by the commands `tar -xzf fogproject-1.5.10.1660.tar.gz`, `cd fogproject-1.5.10.1660/bin`, and `sudo ./installfog.sh`. To the right of the terminal, a web browser window is partially visible, showing a page with the text "using a Long Term Support" and "talling FOG Project inside a virtual".

```
khanhnnhe191159@ubuntu-sift:~$ sudo apt-get update
Hit:1 http://vn.archive.ubuntu.com/ubuntu jammy InRelease [129 kB]
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [128 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu jammy-updates InRelease [127 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:5 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [828 kB]
Get:6 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2659 kB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [657 kB]
Get:8 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [428 kB]
Get:9 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [114 kB]
Get:10 http://vn.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [3695 kB]
Get:11 http://vn.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [658 kB]
Get:12 http://vn.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 DEP-11 Metadata [212 B]
Get:13 http://vn.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1215 kB]
Get:14 http://vn.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Packages [773 kB]
Get:15 http://vn.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [300 kB]
Get:16 http://vn.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 DEP-11 Metadata [359 kB]
Get:17 http://vn.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 DEP-11 Metadata [940 B]
Get:18 http://vn.archive.ubuntu.com/ubuntu jammy-backports/main amd64 DEP-11 Metadata [7080 B]
Get:19 http://vn.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 DEP-11 Metadata [212 B]
Get:20 http://vn.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 DEP-11 Metadata [24.1 kB]
Get:21 http://vn.archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 DEP-11 Metadata [24.1 kB]
dependencies. More detailed guides can be found in the wiki, however, installation is as simple as extracting the tarball and running the install script:
tar -xzf fogproject-1.5.10.1660.tar.gz
cd fogproject-1.5.10.1660/bin
sudo ./installfog.sh
```

```
khanhnnhe191159@ubuntu-sift:~$ sudo apt-get install software-properties-common
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
software-properties-common is already the newest version (0.99.22.9).
software-properties-common set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 149 not upgraded.
khanhnnhe191159@ubuntu-sift:~$ sudo apt-get install python-software-properties
```


After reboot

[illegible]

```

khanhnhe191159@ubuntu-sift: ~/Downloads/FOGProject-fogproject-49456fa/bin

3. FOG Version (1.5.9, 1.6, etc....)

What is this information used for?
We would like to simply track the common types of OS
being used, along with the OS Version, and the various
versions of FOG being used.

Are you ok with sending this information? [Y/n] Y

#####
# FOG now has everything it needs for this setup, but please #
# understand that this script will overwrite any setting you may #
# have setup for services like DHCP, apache, pxe, tftp, and NFS. #
#####
# It is not recommended that you install this on a production system #
# as this script modifies many of your system settings. #
#####
# This script should be run by the root user. #
# It will prepend the running with sudo if root is not set #
#####
# Please see our wiki for more information at: #
#####
# https://wiki.fogproject.org/wiki/index.php #
#####

* Here are the settings FOG will use:
* Base Linux: Debian
* Detected Linux Distribution: Ubuntu
* Interface: enp0s3
* Server IP Address: 10.0.2.15
* Server Subnet Mask: 255.255.255.0
* Hostname: ubuntu-sift.myguest.virtualbox.org
* Installation Type: Normal Server
* Internationalization: No
* Image Storage Location: /images
* Using FOG DHCP: Yes
* DHCP router Address: 10.0.2.2
* Send OS Name, OS Version, and FOG Version: Yes

* Are you sure you wish to continue (Y/N)
  
```

```
ubuntu-sift [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Activities Alacrity Jun 21 11:51
khanhnhhe191159@ubuntu-sift: ~/Downloads/FOGProject-fogproject-49456fa/bin

* Adjusting repository (can take a long time for cleanup).....OK
* Preparing Package Manager.....OK
* Packages to be installed:

  apache2 bc build-essential cpp curl g++ gawk gcc gcc-aarch64-linux-gnu genisoimage git gzip htmldoc isc-dhcp-server isolinux l
ftp libapache2-mod-php libc6 libcurl4t64 liblzma-dev m4 mariadb-client mariadb-server net-tools nfs-kernel-server openssh-server php p
hp-bcmath php-cli php-curl php-fpm php-gd php-json php-ldap php-mbstring php-mysql php-mysqld tar tftp-hpa tftpd-hpa unzip vsftpd wge
t zlib1g

* Installing package: apache2.....OK
* Skipping package: bc.....(Already Installed)
* Installing package: build-essential.....OK
* Skipping package: cpp.....(Already Installed)
* Installing package: curl.....OK
* Skipping package: g++.....(Already Installed)
* Installing package: gawk.....OK
* Skipping package: gcc.....(Already Installed)
* Installing package: gcc-aarch64-linux-gnu.....OK
* Skipping package: genisoimage.....(Already Installed)
* Skipping package: git.....(Already Installed)
* Skipping package: gzip.....(Already Installed)
* Installing package: htmldoc.....OK
* Installing package: isc-dhcp-server.....OK
* Installing package: isolinux.....OK
* Installing package: lftp.....OK
* Installing package: libapache2-mod-php.....OK
* Skipping package: libc6.....(Already Installed)
* Skipping package: libcurl4t64.....(Does not exist)
* Installing package: liblzma-dev.....OK
* Installing package: m4.....OK
* Installing package: mariadb-client.....OK
* Installing package: mariadb-server.....OK
* Skipping package: net-tools.....(Already Installed)
* Installing package: nfs-kernel-server.....OK
* Installing package: openssh-server.....OK
* Installing package: php.....OK
* Installing package: php-bcmath.....OK
* Installing package: php-cli.....OK
* Installing package: php-curl.....OK
```

```
ubuntu-sift [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Activities Alacrity Jun 21 11:52
khanhnhhe191159@ubuntu-sift: ~/Downloads/FOGProject-fogproject-49456fa/bin

* Installing package: php-mbstring.....OK
* Installing package: php-mysql.....OK
* Skipping package: php-mysql.....(Already Installed)
* Skipping package: tar.....(Already Installed)
* Installing package: tftp-hpa.....OK
* Installing package: tftpd-hpa.....OK
* Skipping package: unzip.....(Already Installed)
* Installing package: vsftpd.....OK
* Skipping package: wget.....(Already Installed)
* Skipping package: zlib1g.....(Already Installed)
* Updating packages as needed.....OK

* Confirming package installation

* Checking package: apache2.....OK
* Checking package: bc.....OK
* Checking package: build-essential.....OK
* Checking package: cpp.....OK
* Checking package: curl.....OK
* Checking package: g++.....OK
* Checking package: gawk.....OK
* Checking package: gcc.....OK
* Checking package: gcc-aarch64-linux-gnu.....OK
* Checking package: genisoimage.....OK
* Checking package: git.....OK
* Checking package: gzip.....OK
* Checking package: htmldoc.....OK
* Checking package: isc-dhcp-server.....OK
* Checking package: isolinux.....OK
* Checking package: lftp.....OK
* Checking package: libapache2-mod-php.....OK
* Checking package: libc6.....OK
* Checking package: liblzma-dev.....OK
* Checking package: m4.....OK
* Checking package: mariadb-client.....OK
* Checking package: mariadb-server.....OK
* Checking package: net-tools.....OK
* Checking package: nfs-kernel-server.....OK
* Checking package: openssh-server.....OK
* Checking package: php.....OK
* Checking package: php-bcmath.....OK
```



```
ubuntu-sift [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Activities Alacritty Jun 21 11:52
khanhnhhe191159@ubuntu-sift: ~/Downloads/FOGProject-fogproject-49456fa/bin

* Configuring services
* Setting up fogproject user.....OK
* Locking fogproject as a system account.....OK
* Setting fogproject password.....OK
* Stopping FOGMulticastManager.service Service.....OK
* Stopping FOGImageReplicator.service Service.....OK
* Stopping FOGSnapinReplicator.service Service.....OK
* Stopping FOGScheduler.service Service.....OK
* Stopping FOGPingHosts.service Service.....OK
* Stopping FOGSnapinHash.service Service.....OK
* Stopping FOGImageSize.service Service.....OK
* Setting up and starting MySQL.....OK
* Setting up MySQL user and database.....OK
* Backing up user reports.....Done
* Stopping web service.....OK
* Setting up Apache and PHP files.....OK
* Testing and removing symbolic links if found.....OK
* Backing up old data.....OK
* Copying new files to web folder.....OK
* Creating config file.....OK
* Creating redirection index file.....OK
* Downloading kernel, init and fog-client binaries.....Done
* Copying binaries to destination paths.....OK
* Enabling apache and fpm services on boot.....OK
* Creating SSL CA.....OK
* Creating SSL Private Key.....OK
* Creating SSL Certificate.....OK
* Creating auth pub key and cert.....OK
* Resetting SSL Permissions.....OK
* Setting up Apache virtual host (no SSL).....OK
* Starting and checking status of web services.....OK
* Changing permissions on apache log files.....OK
* Backing up database.....Done

* You still need to install/update your database schema.
* This can be done by opening a web browser and going to:
http://10.0.2.15/fog/management
* Press [Enter] key when database is updated/installed.
```

```
ubuntu-sift [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Activities Alacritty Jun 21 12:44
khanhnhhe191159@ubuntu-sift: ~/Downloads/FOGProject-fogproject-49456fa/bin

* Setting permissions on FOGImageSize.service script.....OK
* Enabling FOGImageSize.service Service.....OK
* Setting up FOG Services.....OK
* Starting FOGMulticastManager.service Service.....OK
* Starting FOGImageReplicator.service Service.....OK
* Starting FOGSnapinReplicator.service Service.....OK
* Starting FOGScheduler.service Service.....OK
* Starting FOGPingHosts.service Service.....OK
* Starting FOGSnapinHash.service Service.....OK
* Starting FOGImageSize.service Service.....OK
* Setting up NFS configuration file.....OK
* Setting up exports file.....OK
* Setting up and starting RPCBind.....OK
* Setting up and starting NFS Server.....OK
* Linking FOG Logs to Linux Logs.....OK
* Linking FOG Service config /etc.....OK
* Ensuring node username and passwords match.....Done
* Setting up FOG External Reporting.....Done

* Setup complete

You can now login to the FOG Management Portal using
the information listed below. The login information
is only if this is the first install.

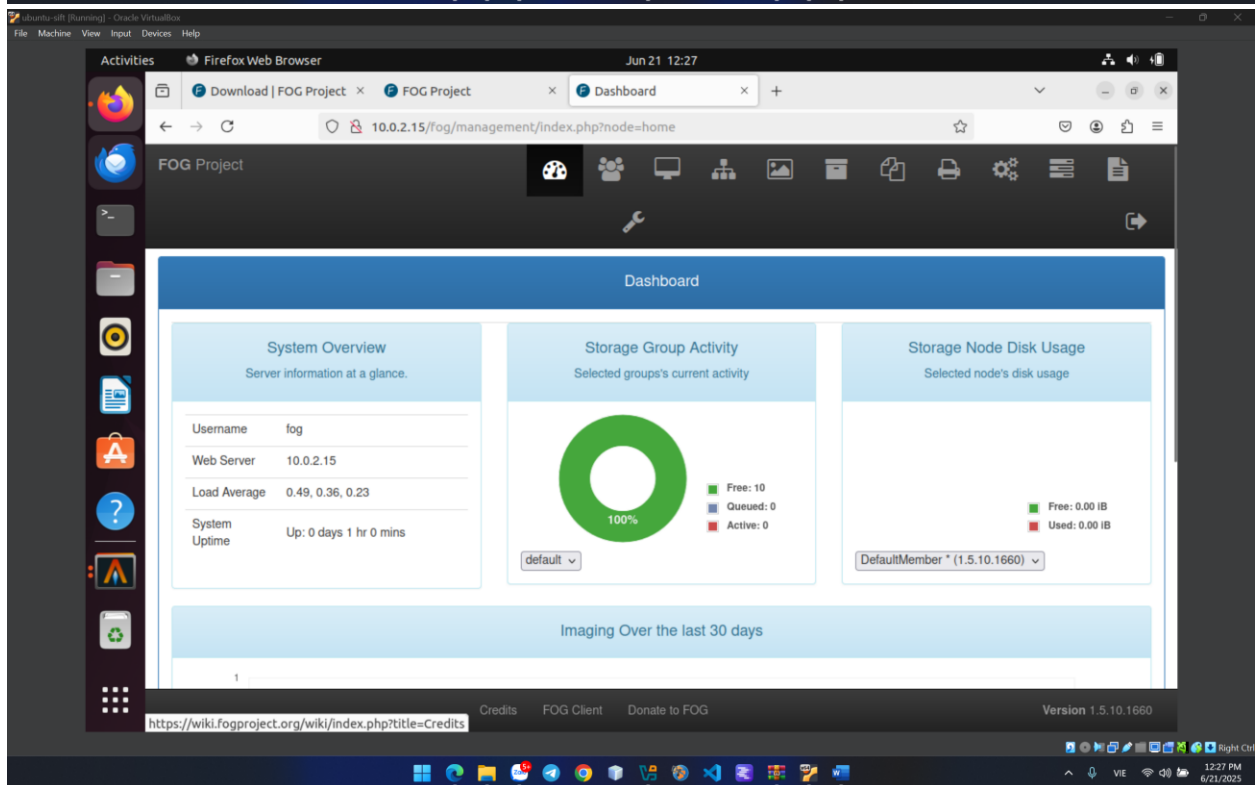
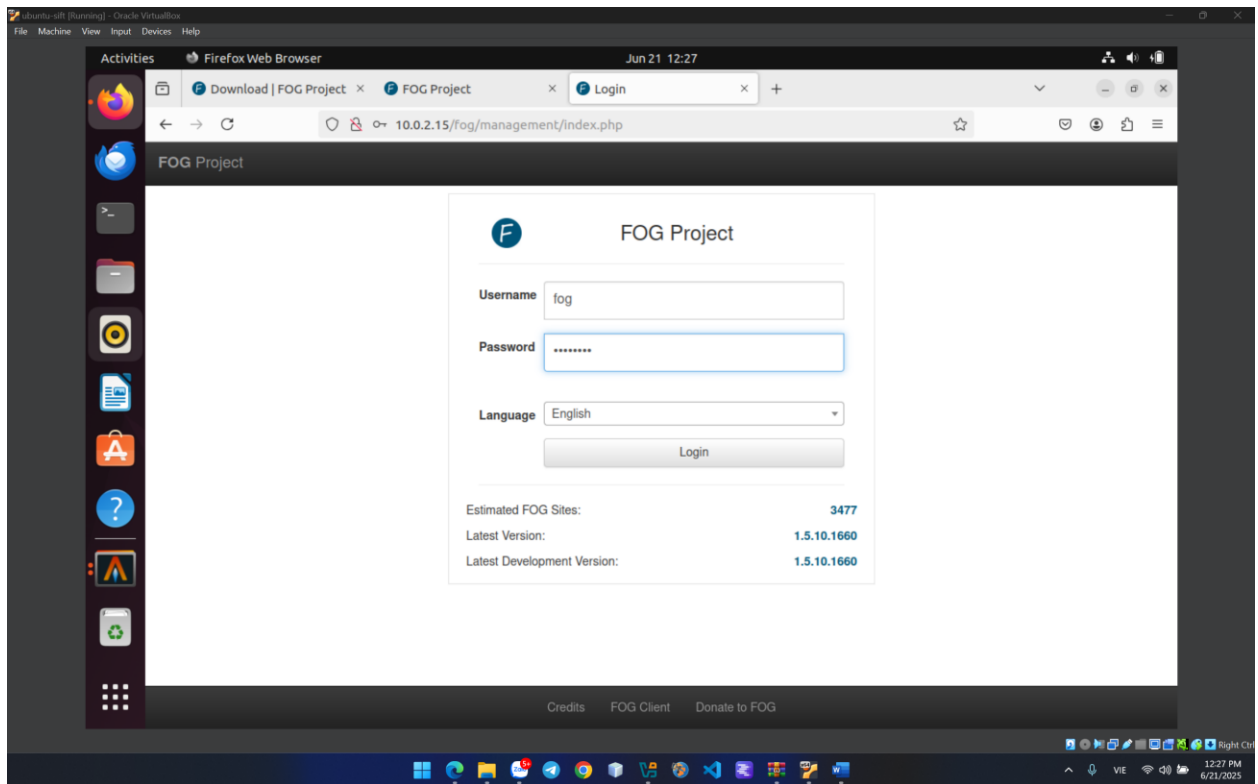
This can be done by opening a web browser and going to:
http://10.0.2.15/fog/management

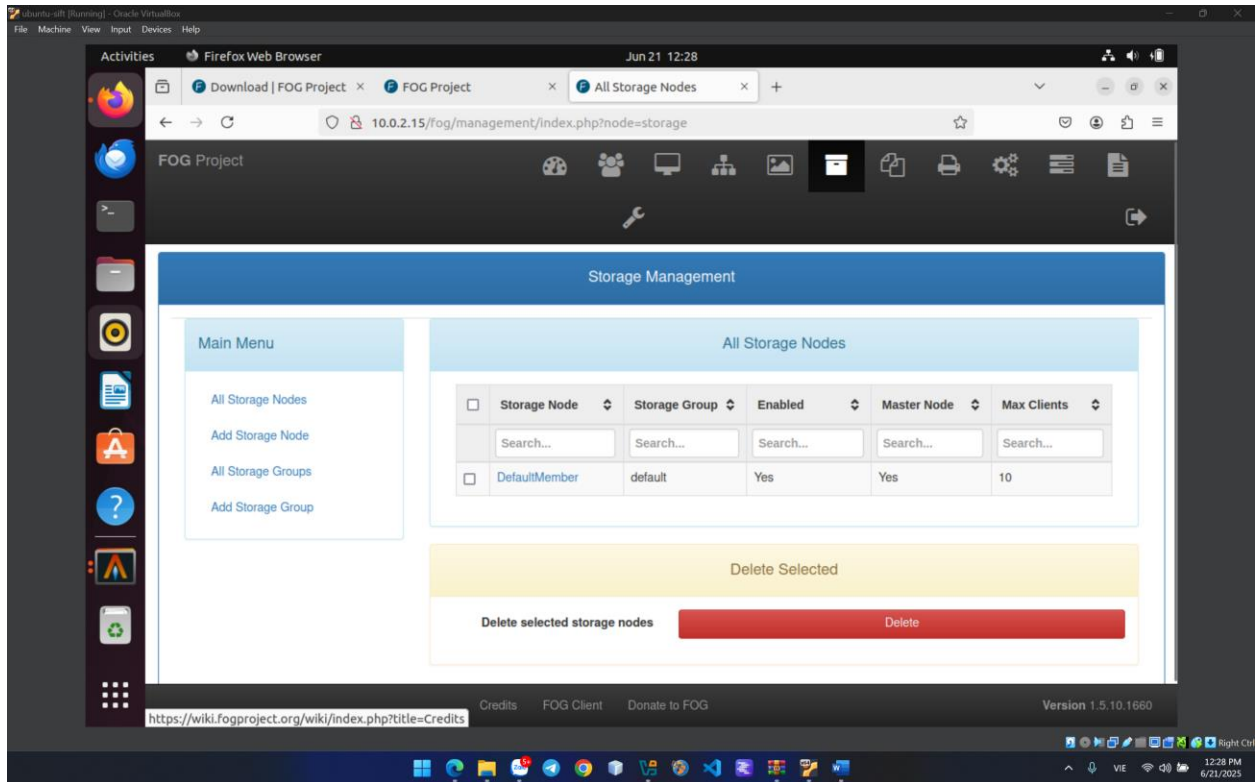
Default User Information
Username: fog
Password: password

* Changed configurations:

The FOG installer changed configuration files and created the
following backup files from your original files:
* /etc/vsftpd.conf <=> /etc/vsftpd.conf.1750484535
* /etc/exports <=> /etc/exports.1750484535

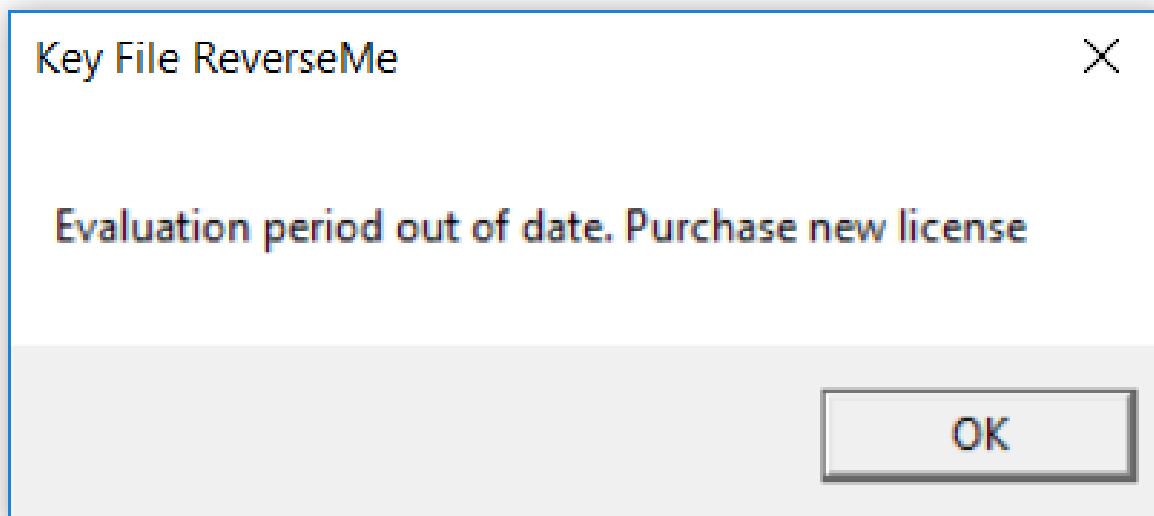
khanhnhhe191159@ubuntu-sift:~/Downloads/FOGProject-fogproject-49456fa/bin$
```





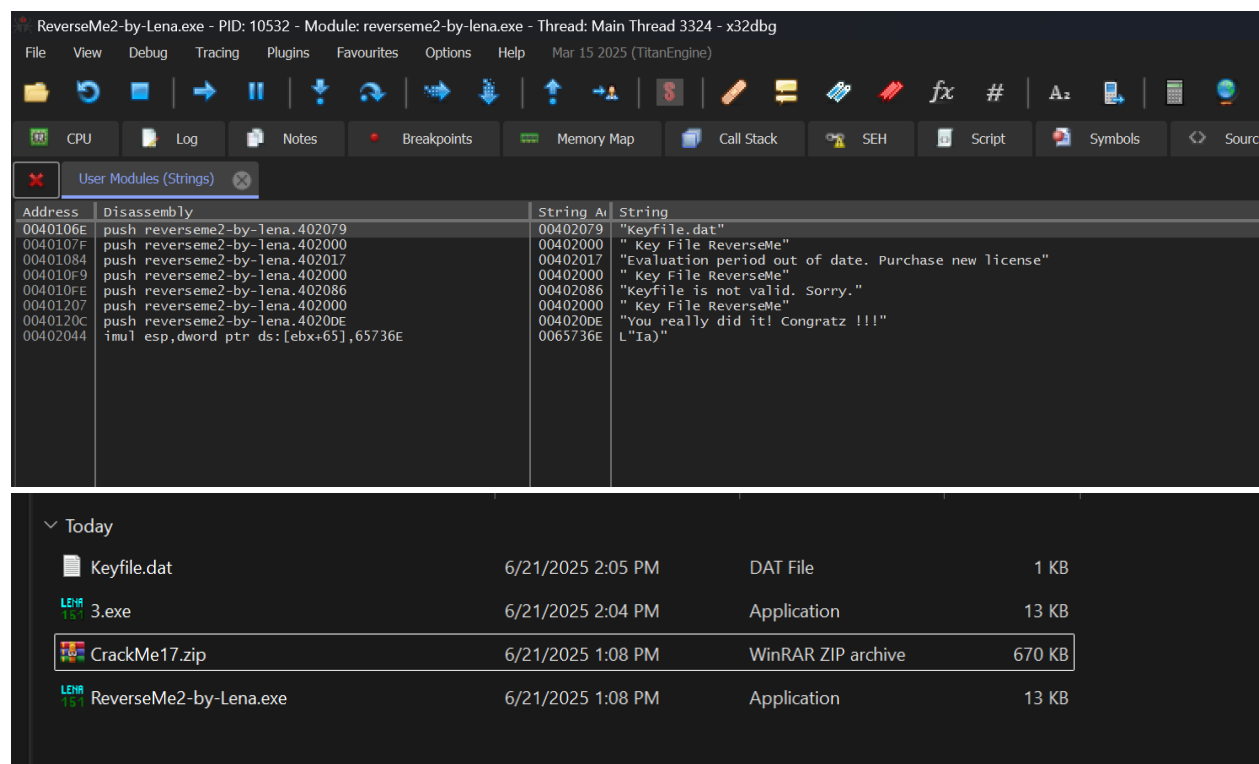
CRACK ME 10

This reverseme is written by Lena and is one of the classic reverseme's used to learn reversing. Use this in conjunction with xAnalyzer plugin for x64dbg to practice serial key fishing.



First, go to String references and see that, we have a keyfile.dat

So i create keyfile.dat on the same folder with file .exe



The top screenshot shows the x64dbg interface with the 'User Modules (Strings)' window open. It displays a list of strings and their addresses. The string 'keyfile.dat' is highlighted.

Address	Disassembly	String Address	String
0040106E	push reverseme2-by-lena.402079	00402079	"keyfile.dat"
0040107F	push reverseme2-by-lena.402000	00402000	" Key File ReverseMe"
00401084	push reverseme2-by-lena.402017	00402017	"Evaluation period out of date. Purchase new license"
004010F9	push reverseme2-by-lena.402000	00402000	" Key File ReverseMe"
004010FE	push reverseme2-by-lena.402086	00402086	"keyfile is not valid. Sorry."
00401207	push reverseme2-by-lena.402000	00402000	" Key File ReverseMe"
0040120C	push reverseme2-by-lena.4020DE	004020DE	"You really did it! Congratz !!!"
00402044	1mul esp,dword ptr ds:[ebx+65],65736E	0065736E	L"Ta"

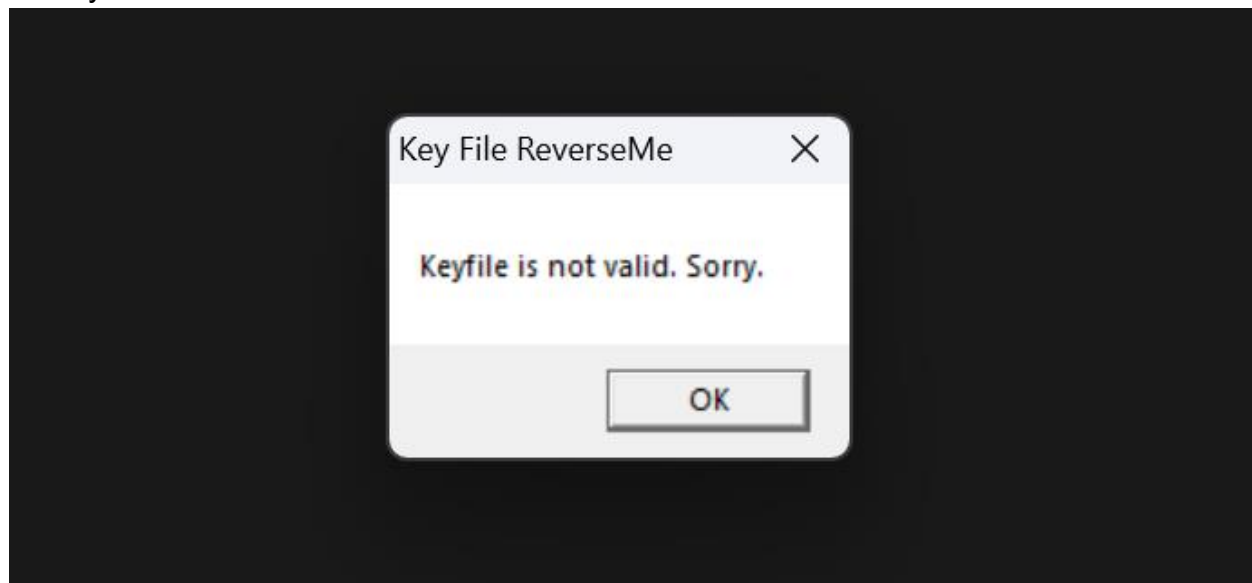
The bottom screenshot shows a file explorer view of the 'Today' folder. It lists several files, including 'keyfile.dat', '3.exe', 'CrackMe17.zip', and 'ReverseMe2-by-Lena.exe'.

File Name	Date/Time	File Type	Size
keyfile.dat	6/21/2025 2:05 PM	DAT File	1 KB
3.exe	6/21/2025 2:04 PM	Application	13 KB
CrackMe17.zip	6/21/2025 1:08 PM	WinRAR ZIP archive	670 KB
ReverseMe2-by-Lena.exe	6/21/2025 1:08 PM	Application	13 KB

Next inspect to the assembly code of this string.

0040106E	68 79204000	push reverseme2-by-lena.402079	402079:"KeyFile.dat"
00401073	E8 0B020000	call <JMP.&CreateFileA>	
00401078	83F8 FF	cmp eax,FFFFFFFF	
0040107B	75 1D	jne reverseme2-by-lena.40109A	
0040107D	6A 00	push 0	
0040107F	68 00204000	push reverseme2-by-lena.402000	402000:" Key File ReverseMe"
00401084	68 17204000	push reverseme2-by-lena.402017	402017:"Evaluation period out of date. Purchase new license"
00401089	6A 00	push 0	
0040108B	E8 D7020000	call <JMP.&MessageBoxA>	
00401090	E8 24020000	call <JMP.&ExitProcess>	
00401095	E9 83010000	jmp reverseme2-by-lena.40121D	
0040109A	6A 00	push 0	
0040109C	68 73214000	push reverseme2-by-lena.402173	
004010A1	6A 46	push 46	
004010A3	68 1A214000	push reverseme2-by-lena.40211A	
004010A8	50	push eax	
004010A9	E8 2F020000	call <JMP.&ReadFile>	
004010AE	85C0	test eax,eax	
004010B0	75 02	jne reverseme2-by-lena.4010B4	
004010B2	EB 43	jmp reverseme2-by-lena.4010F7	
004010B4	33DB	xor ebx,ebx	
004010B6	33F6	xor esi,esi	
004010B8	833D 73214000 10	cmp dword ptr ds:[402173],10	
004010BF	7C 36	j1 reverseme2-by-lena.4010F7	
004010C1	8A83 1A214000	mov al,byte ptr ds:[ebx+40211A]	
004010C7	3C 00	cmp al,0	
004010C9	74 08	je reverseme2-by-lena.4010D3	
004010CB	3C 47	cmp al,47	47:'G'
004010CD	75 01	jne reverseme2-by-lena.4010D0	

Notice the note "47:'G'". May be this is the value of the string. So i type only one word G on keyfile.dat and receive this result.



So i continue to analyze next code:

004010B6	33F6	xor esi,esi	
004010B8	833D 73214000 10	cmp dword ptr ds:[402173],10	
004010BF	7C 36	j1 reverseme2-by-lena.4010F7	
004010C1	8A83 1A214000	mov al,byte ptr ds:[ebx+40211A]	
004010C7	3C 00	cmp al,0	
004010C9	74 08	je reverseme2-by-lena.4010D3	
004010CB	3C 47	cmp al,47	47:'G'
004010CD	75 01	jne reverseme2-by-lena.4010D0	
004010CF	46	inc esi	
004010D0	43	inc ebx	
004010D1	EB EE	jmp reverseme2-by-lena.4010C1	
004010D3	83FE 08	cmp esi,8	
004010D6	7C 1F	j1 reverseme2-by-lena.4010F7	
004010D8	E9 28010000	jmp reverseme2-by-lena.401205	
004010DD	0000	add byte ptr ds:[eax],al	
004010DF	0000	add byte ptr ds:[eax],al	
004010E1	0000	add byte ptr ds:[eax],al	
004010E3	0000	add byte ptr ds:[eax],al	
004010E5	0000	add byte ptr ds:[eax],al	
004010E7	0000	add byte ptr ds:[eax],al	
004010E9	0000	add byte ptr ds:[eax],al	
004010EB	0000	add byte ptr ds:[eax],al	
004010ED	0000	add byte ptr ds:[eax],al	
004010EF	0000	add byte ptr ds:[eax],al	
004010F1	0000	add byte ptr ds:[eax],al	
004010F3	0000	add byte ptr ds:[eax],al	
004010F5	EB 00	jmp reverseme2-by-lena.4010F7	
004010F7	6A 00	push 0	
004010F9	68 00204000	push reverseme2-by-lena.402000	402000:" Key File ReverseMe"
004010FE	68 86204000	push reverseme2-by-lena.402086	402086:"Keyfile is not valid. Sorry."
00401103	6A 00	push 0	
00401105	E8 5D020000	call <JMP.&MessageBoxA>	
0040110A	E8 A4010000	call <JMP.&ExitProcess>	
0040110F	E9 09010000	jmp reverseme2-by-lena.40121D	

We have the CMP and JL.

Jump Low means if the ptr ds:[402173] lower than 10, program will jump to the status "Keyfile is not valid. Sorry."

So i inspect to the DUMP of address 00402173 and see that these address contain value 0 so i change the CMP of this address with 0 to ignore JL command.

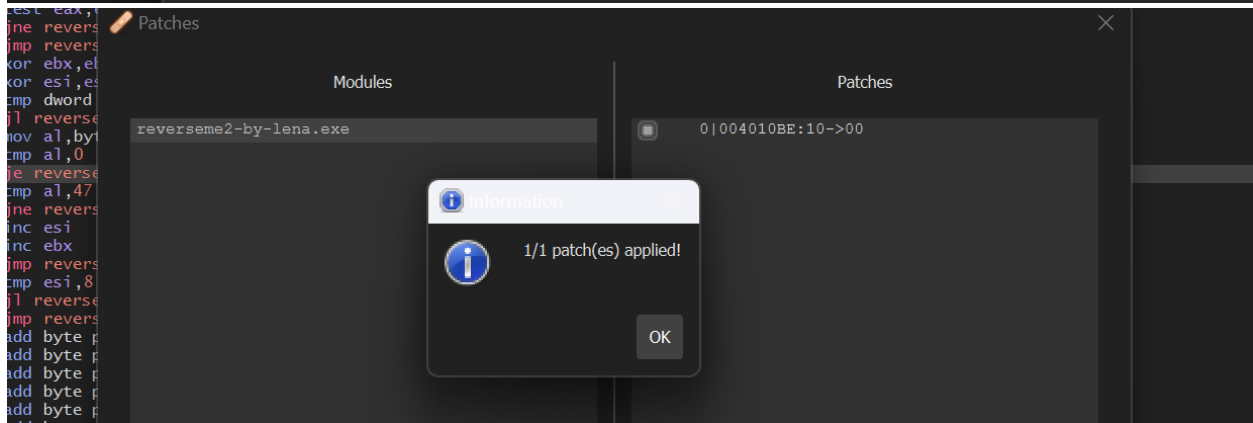
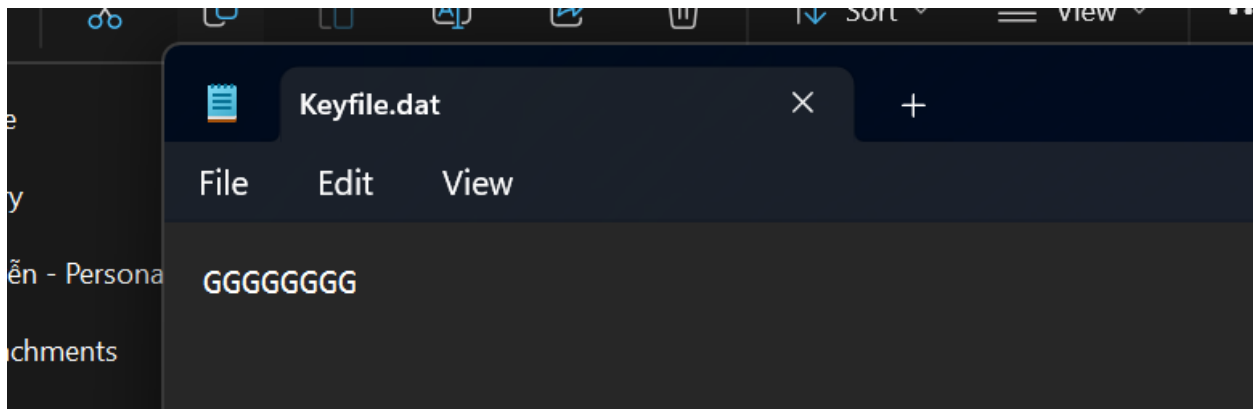
Address	Hex	ASCII
00402173	00 00 00 00
00402183	00 00 00 00
00402193	00 00 00 00
004021A3	00 [00402173] = 00000000 (User Data)
004021B3	00 00 00 00
004021C3	00 00 00 00
004021D3	00 00 00 00
004021E3	00 00 00 00
004021F3	00 00 00 00
00402203	00 00 00 00
00402213	00 00 00 00
00402223	00 00 00 00

Next we need to find the content of keyfile.dat. We see that EBX and ESI represent for each byte of content and size of content respectively.

AL is assigned by EBX, and this compare with hexa 47 (letter G). ESI compares with 8 if lower we jump to status invalid. So the length of content is 8. We have the JMP of address 004010D1 creates the loop of comparing file content with G until AL equals to 0 (nothing to compare in EBX).

004010B6	33 F6	xor esi,esi	
004010B8	83 3D 73214000 00	cmp dword ptr ds:[402173],0	
004010BF	7C 36	j1 reverseme2-by-1ena.4010F7	
004010C1	8A 83 1A214000	mov al,byte ptr ds:[ebx+40211A]	
004010C7	3C 00	cmp al,0	
004010C9	74 08	je reverseme2-by-1ena.4010D3	
004010CB	3C 47	cmp al,47	47: 'G'
004010CD	75 01	jne reverseme2-by-1ena.4010D0	
004010CF	46	inc esi	
004010D0	43	inc ebx	
004010D1	EB EE	jmp reverseme2-by-1ena.4010C1	
004010D3	83 FE 08	cmp esi,8	
004010D6	7C 1F	j1 reverseme2-by-1ena.4010F7	
004010D8	E9 28010000	jmp reverseme2-by-1ena.401205	
004010DD	00 00	add byte ptr ds:[eax],al	
004010DF	00 00	add byte ptr ds:[eax],al	
004010E1	00 00	add byte ptr ds:[eax],al	

So we guest that the conten of Keyfile.dat is 8 letters G. So i type 8 times letter G in Keyfile.dat and patch file .exe to check.



DONE!!!