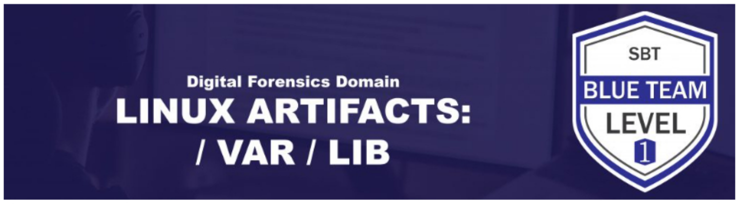
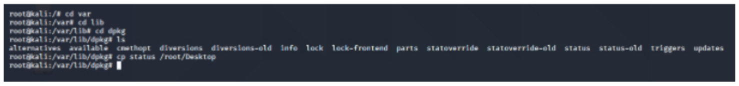
Linux Artifacts – /Var/Lib and /Var/Log



In this lesson we're going to cover two locations that may be of interest to forensic investigators, `/var/lib` and `/var/log`.

Installed Software and Packaging

On Debian-based systems, we can find a very useful file at the following location: `/var/lib/dpkg/status`. This file includes a list of all installed software packages, and can be a gold mine if you're looking to see what programs the user has installed to the system. Let's take a copy of this file and move it to our desktop, and then open it in a text editor, and see what installed applications we can find!

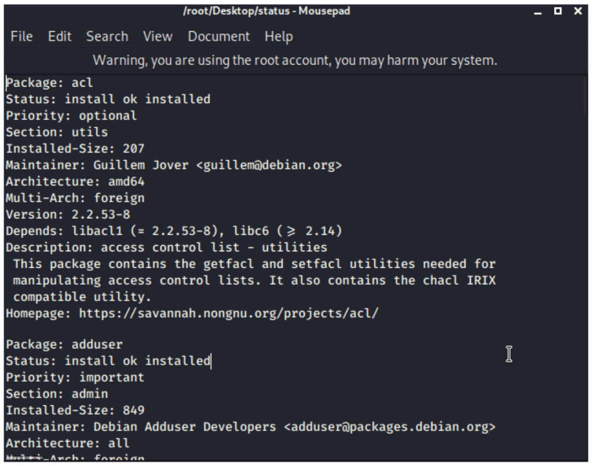


```
root@kali:/# cd var
root@kali:/var# cd lib
root@kali:/var/lib# cd dpkg
root@kali:/var/lib/dpkg# ls
alternatives  available  cmethopt  diversions  diversions-old  info  lock  lock-frontend  parts  statoverride  statoverride-old  status  status-old  triggers  updates
root@kali:/var/lib/dpkg# cp status /root/Desktop
root@kali:/var/lib/dpkg# █
```

In the below GIF you can see that we've opened the 'status' file, and searched for some different programs. We would see that this system has the following installed:

- steghide
- exiftool
- nikto

If forensic investigators or incident responders were looking for specific packages, they could use the search functionality (CTRL + F) to search for what they need.


/root/Desktop/status - Mousepad
File Edit Search View Document Help

Warning, you are using the root account, you may harm your system.

```
Package: acl
Status: install ok installed
Priority: optional
Section: utils
Installed-Size: 207
Maintainer: Guillem Jover <guillem@debian.org>
Architecture: amd64
Multi-Arch: foreign
Version: 2.2.53-8
Depends: libacl1 (= 2.2.53-8), libc6 (≥ 2.14)
Description: access control list - utilities
 This package contains the getfacl and setfacl utilities needed for
 manipulating access control lists. It also contains the chacl IRIX
 compatible utility.
Homepage: https://savannah.nongnu.org/projects/acl/

Package: adduser
Status: install ok installed
Priority: important
Section: admin
Installed-Size: 849
Maintainer: Debian Adduser Developers <adduser@packages.debian.org>
Architecture: all
Multi-Arch: foreign
```

Previous Topic

Mark Complete ✓

Next Topic

Back to Lesson