

Blue Team Level 1 Certification
(Standard)☐ TI6) Malware and Global Campaigns

6 Topics 1 Quiz

DIGITAL FORENSICS DOMAIN

☐ DF1) Introduction to Digital Forensics

5 Topics

☐ DF2) Forensics Fundamentals

10 Topics 5 Quizzes

☐ DF3) Digital Evidence Collection

8 Topics 1 Quiz

☐ DF4) Windows Investigations

3 Topics 3 Quizzes

☒ DF5) Linux Investigations

4 Topics 2 Quizzes

☐ Section Introduction, Linux Investigations☐ Linux Artifacts – Passwd and Shadow☐ Activity) Password Cracking☒ Linux Artifacts – /Var/Lib and /Var/Log☐ Linux Artifacts – User Files☐ Activity) End of Section Review, Linux Investigations☐ DF6) Volatility

3 Topics 1 Quiz

☐ DF7) Autopsy

4 Topics 1 Quiz

SECURITY INFORMATION AND EVENT
MANAGEMENT DOMAIN☐ SI1) Introduction to SIEM

7 Topics 1 Quiz

☐ SI2) Logging

6 Topics 2 Quizzes

☐ SI3) Aggregation

2 Topics 1 Quiz

☐ SI4) Correlation

6 Topics 1 Quiz

☐ SI5) Using Splunk

5 Topics 2 Quizzes

INCIDENT RESPONSE DOMAIN

☐ IR1) Introduction to Incident Response

8 Topics 1 Quiz

☐ IR2) Preparation Phase

10 Topics 2 Quizzes

☐ IR3) Detection and Analysis Phase

7 Topics 4 Quizzes

☐ IR4) Containment, Eradication, and Recovery Phase

5 Topics 1 Quiz

☐ IR5) Lessons Learned and Reporting

7 Topics

☐ IR6) MITRE ATT&CK

13 Topics 2 Quizzes

BTL1 EXAM

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

Blue Team Level 1 Certification (Standard) > DF5) Linux Investigations > Linux Artifacts – /Var/L...

IN PROGRESS



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 conchtop diversions diversions-old info lock lock-frontends parts statoverride statoverride-old status status-old triggers updates
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 ✓

Back to Lesson

Next Topic >



