Kernel Modules for memory acquisition:

For better security, the Linux systems restrict the access of /dev/mem device file to a limited memory range. Therefore, sophisticated memory acquisition kernel modules are required to access the complete memory range from the kernel space.

Loadable kernel modules (LKMs) are object files that extend the kernel functionality.
Some useful Loadable Kernel Modules for memory acquisition are fmem, SecondLook and Linux Memory Extractor (LiME).

LiME:
LiME allows volatile memory acquisition from Linux and Linux-based devices. It supports acquiring memory either to the file system of the device or over the network.

LiME can also be used for full memory captures from Android devices.

Using LiME:

Download the source code from: https://github.com/504ensicsLabs/LiME

Move to the src directory of extracted file and run make:

```
$src make
```

The produced LiME object (e.g. lime.ko) file can be saved in your trusted tool kit for incident response.

On the subject system, load object file using insmod (loads the kernel modules) utility.

Command:

```
insmod ./lime.ko "path=<outfile> format=<raw|padded|lime>"
```

`path` (required): outfile ~ name of file to write to on local system

`format` (required):
- `raw` ~ concatenates all System RAM ranges
- `padded` ~ pads all non-System RAM ranges with 0s
- `lime` ~ each range prepended with fixed-size header containing address space info.

Additional arguments can be provided to acquire memory over network.

Remove the LiME kernel module after acquisition is complete:

```
$rmmod lime
```