1 Introduction

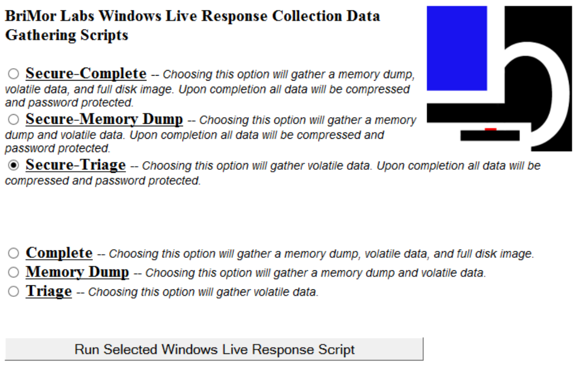
Live Response Collection (LRC) is a collection of forensic tools that can be used to gather information from a machine under investigation. LRC can be run on Windows, Linux, and Mac OSX by choosing the appropriate script and running it with administrative rights. To tamper evidence as little as possible, it is strongly recommended to run the script from a USB stick or a network share that can be mounted from the target machine. The output of the LRC script will be saved on the partition from which LRC was run and the size of this output can be several hundreds of MB, hence it is important to choose a partition with enough free space.

2 Preparation (on separate machine)

1. Obtain Live Response Collection. This tool can be downloaded for free from official website https://www.brimorlabs.com/tools/.
2. Depending on whether target machine has a physical USB port or not, either:
   a. Unzip file on USB stick.
   b. Unzip file on network share that can be mounted on target machine.

3 Information capture (on **Windows** target machine)

1. Mount the network share where LRC was unzipped or connect USB stick to target machine.
2. Open in Explorer USB/Network share and go to folder “LiveResponse\Windows_Live_Response”
3. Right-click on “Windows Live Response Collection.exe” and select “Run as administrator”
4. In the GUI that opens, select option “Secure Triage”

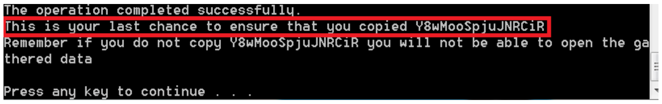


BriMor Labs Windows Live Response Collection Data Gathering Scripts

○ **Secure-Complete** -- *Choosing this option will gather a memory dump, volatile data, and full disk image. Upon completion all data will be compressed and password protected.*
○ **Secure-Memory Dump** -- *Choosing this option will gather a memory dump and volatile data. Upon completion all data will be compressed and password protected.*
● **Secure-Triage** -- *Choosing this option will gather volatile data. Upon completion all data will be compressed and password protected.*

○ **Complete** -- *Choosing this option will gather a memory dump, volatile data, and full disk image.*
○ **Memory Dump** -- *Choosing this option will gather a memory dump and volatile data.*
○ **Triage** -- *Choosing this option will gather volatile data.*

5. Click on “Run Selected Windows Live Response Script”. A terminal window will open where progress of the script can be followed.
6. At the end of the gathering process, after a message attesting successful completion, the script will pause and print a randomly generated password. Make sure to write down this password otherwise it will be impossible to open the gathered data.



```
The operation completed successfully.
This is your last chance to ensure that you copied Y8wMooSpjuJNRCiR
Remember if you do not copy Y8wMooSpjuJNRCiR you will not be able to open the ga
thered data

Press any key to continue . . .
```

7. Press any key to continue and close the terminal.
8. The data gathered by LRC will be found in the folder LiveResponse\Windows_Live_Response, the format of the name of this file will be <hostname>_YYYYMMDD_HHMMSS.7z. This file is ready to be sent to IBM Security X-Force IR.
9. Use method approved within your organization to securely erase LRC output folder.

Note: On an average Windows system, the LRC script takes 30-60 minutes to complete.

4 Information capture (on **Linux** target machine)

1. Mount the network share where LRC was unzipped or connect USB stick to target machine.
2. Open terminal and gain root privileges, depending on Linux distribution, this can be done either by running a command:
   `$ sudo su`
   on distributions using sudo (e.g. Ubuntu), or
   `$ su –`
   on other distributions (e.g. Debian, CentOS, RHEL)
3. Navigate to folder LiveResponse\nix_Live_Response
4. Run command:

```
# sh nix_Live_Response.sh
```

5. When the script finishes, a folder whose name has the format <hostname>_YYYYMMDDHHMMSS will be created in LiveResponse\nix_Live_Response.
6. Compress folder containing results using:

```
# tar –cvzf <hostname>.tar.gz
<hostname_YYYYMMDDHHMMSS>
```

7. Encrypt created archive with complex password (16 characters, mixed case letters, numbers, and special symbols):

   ```
   # gpg --symmetric --cipher-algo AES256
   <hostname>.tar.gz
   ```

   This output file with *.gpg extension is ready to be sent to IBM Security X-Force IR.
8. Use method approved within your organization to securely erase LRC output folder and unencrypted tar.gz archive.

Note: On an average Linux system, the LRC script takes just a few minutes to complete.

5 Delivering files to IBM Security X-Force IR

1. Compressed, encrypted archive is ready for delivery to IBM Security X-Force IR team via agreed method of delivery.
2. Share complex password used to for encryption with IBM Security X-Force IR team using different communication channel then used to share forensic image.