# Linux Forensics Workshop

Hello and welcome to the Digital Forensic Research Workshop (DFRWS) USA 2022 Linux Forensics Workshop. PLEASE make sure you read this document so you know what to expect.

**Important Notes:**

1. This workshop does not assume you have experience in Linux, but if you do, then that's an advantage.
2. Some of the instructions that will be covered are for educational purposes, there are so many other ways to solve this case, but we are showing how to do that using very simple commands and trying our best not to make things complicated.
3. Anything in the manual document referenced in red is a **command**, while those in blue are referencing either a **file** or **directory**.

**Workshop Preparation:**

Before starting the workshop, we would like to ask you to prepare your workstation so you can follow the instructions and apply them yourself. We prefer learning by doing, so we will assume you have a working workstation or virtual machine ready for the workshop. To help you get prepared, we recommend you do the following:

1. Please watch this short video explaining the files that have been shared with you and which one to choose from. The decision is totally up to you, but at least check what these files are, so you do not download the files twice.

2. Download the **Tsurugi Linux** VM, from the URLs below. This is an OVA file which is for Virtual Machines. All you need to do is download the OVA file and the other files that are part of the VM and then import it or open it using your hypervisor.

3. **Workshop Files:** There are a number of different locations where you can download the files that will be used for our Linux Forensics Workshop. All the URLs to the files needed can be found below. We also recommend you check our recorded video explaining the workshop files that have been shared with you. The video can be found here.

**3.1. Option #1 - Google Drive**

| | | |
|---|---|---|
| 3.1.1. | Video explaining the workshop files | here |
| 3.1.2. | Tsurugi Linux VM Preloaded with Evidence | here |
| 3.1.3. | Evidence used in the workshop can be found | here |
| 3.1.4. | Tsurugi Linux VM without any Evidence | here |

**3.2. Option #2 - Archive.org**

| | | |
|---|---|---|
| 3.2.1. | Main Directory | here |
| 3.2.2. | E01 file | here |
| 3.2.3. | Timeline CSV | here |
| 3.2.4. | Hashes | here |

**3.3.** If you prefer to download and install the **Tsurugi Linux** distribution for this workshop, then please visit the download URL here to download the ISO file for **Tsurugi Linux**.

**3.4.** You are also welcome to use any other Linux distro or install the required tools needed; that's up to you.

4. After downloading the VM, import it into your hypervisor (VMWare, Virtualbox, Hyper-V, etc) and then power it up.
5. The default user and password for **Tsurugi Linux** is: **tsurugi**
6. If you didn't download the preloaded VM, then make sure to copy the forensic image for this workshop to your newly prepared **Tsurugi Linux** or whatever Linux distro you are using.
7. Setup the language and the display as preferred.