Lab Requirements

Download data file from:

https://drive.google.com/file/d/15rupTZ6sRDiQOHJCK54O1JTU56Hk4keg/view

You'll need something to uncompress an encrypted 7z file.

- Password: Brunos2Pizza & Test data file: https://github.com/markjx/oldcurrent/raw/main/test.7z
- If you can work with test.7z, then you can work with this lab

You'll need approximately 13GB of disk space for the uncompressed data set

Linux environment (WSL, Virtual Machine, whatever)

For the most recent copy of information about this presentation, please reference:
https://github.com/markjx/oldcurrent/

Link to download access.log.7z:
https://drive.google.com/file/d/15rupTZ6sRDiQOHJCK54O1JTU56Hk4keg/view

Setup for Lab. Please complete these before the start of the Presentation.

1. You'll need a Linux environment for this lab. I tested with Fedora and Ubuntu, but anything should work. It should work under WSL (Windows Subsystem for Linux), a VM (Virtual Machine under Vmware, VirtualBox, KVM/QEMU, Proxmox, etc), or on hardware.
2. You may need root access to install tools. You'll need a tool that can handle password-protected 7z files. To install:
    1. On Fedora: `sudo dnf install -y p7zip`
    2. On Ubuntu: `sudo apt install -y p7zip` or `sudo apt install -y p7zip-full`
    3. If you want to try on high difficulty, feel free to use something like John the Ripper or hashcat instead. ☺ This is **not** recommended.
3. Download the data file from

https://drive.google.com/file/d/15rupTZ6sRDiQOHJCK54O1JTU56Hk4keg/view You'll need approximately 13GB of disk space to uncompress it. You'll get the password for this, at the same time as everyone else, during the presentation ☺

4. If you want to make sure that you're all setup to work with the real data file, I created https://github.com/markjx/oldcurrent/raw/main/test.7z The password is above (the password isn't "above". The password is on the slide, which is above this sentence ☺). If you're able to uncompress this, then you're ready for the real one.
    1. Command to uncompress the test.7z file:
       `7z x test.7z`
       Then enter the password when prompted.
5. You should now be ready for the lab!

All testing was done on x86 / x86_64 systems. But, this should all work from an Apple Mac with an M1/M2/M3 CPU. It would probably work under IRIX with a MIPS CPU. And, it's probably work on a Sun SparcStation under Solaris. AIX on Power and HP-UX would probably work fine too. There's no way it'd work under OS/2, but it'd be fun to write the analysis in REXX…

If you want to attempt on a MacOS system, you may need an additional tool to uncompress the password-protected 7z file.

- Some have had good luck with Keka at https://www.keka.io/en/
- Others used `brew install p7zip` from homebrew at https://brew.sh/

NOTE: Your antivirus scanner *may* flag the test.7z file as a virus. (Specifically Windows Defender may flag it as Trojan:Script/Wacatac.B!ml) It is not a virus. Viruses have to be executable code. This is a password-protected 7zip file. No big deal. There's no executable code.