INVETECK GLOBAL

Forensic Investigation with Prefetch Files

Mr. Blay Abu Safian

Founder, Engineer & Lead Trainer

LinkedIn: Abu Safian Blay

Instagram: k1ngblay

www.inveteckglobal.com

profile@about-me# whoami

Mr. Blay Abu Safian

- Founder, Inveteck Global
- Former CTF Team Lead, Black Cyber Security Association (USA)
- International Offensive Security Speaker & Trainer
- Cyberforce Red Team Lead Volunteer for DOE (USA)

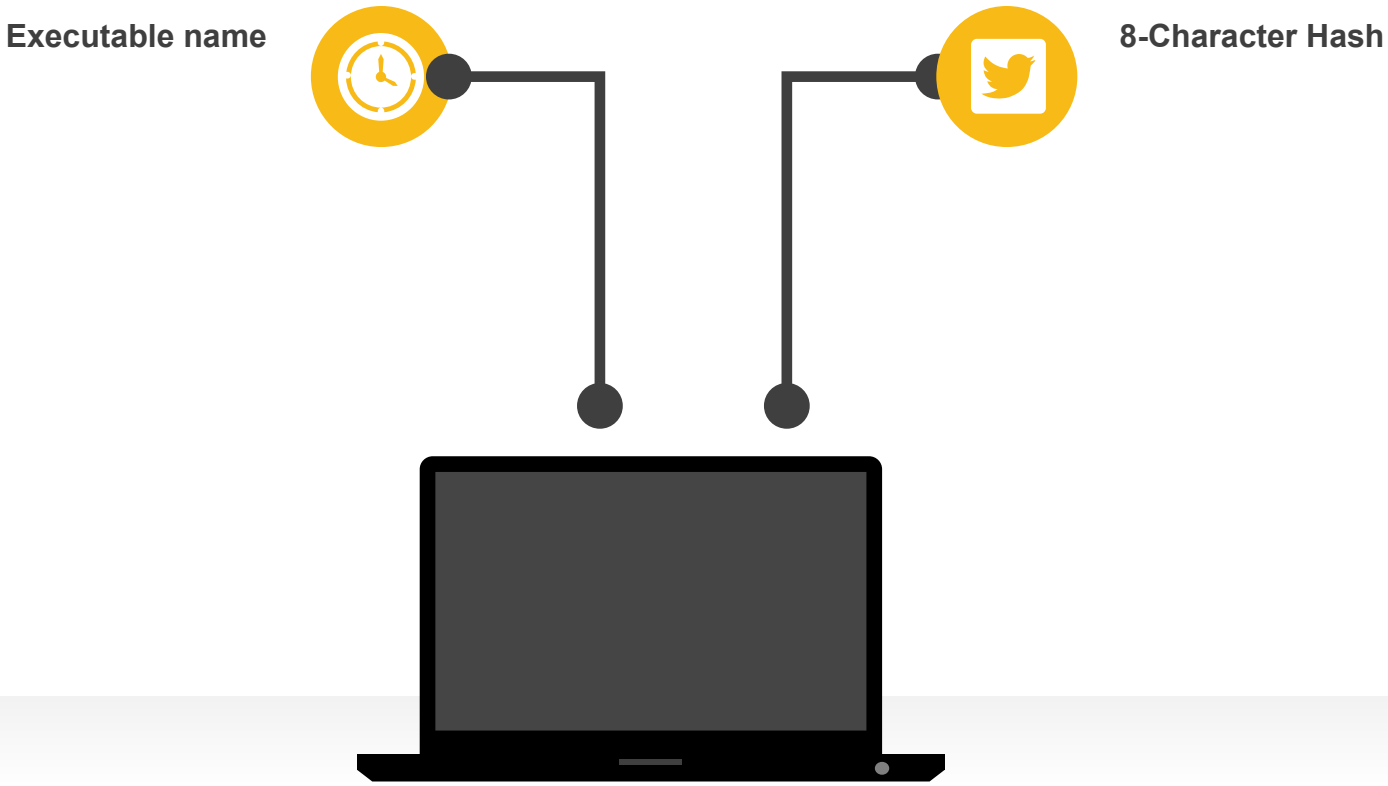
Agenda Style

Introduction to Prefetch Files

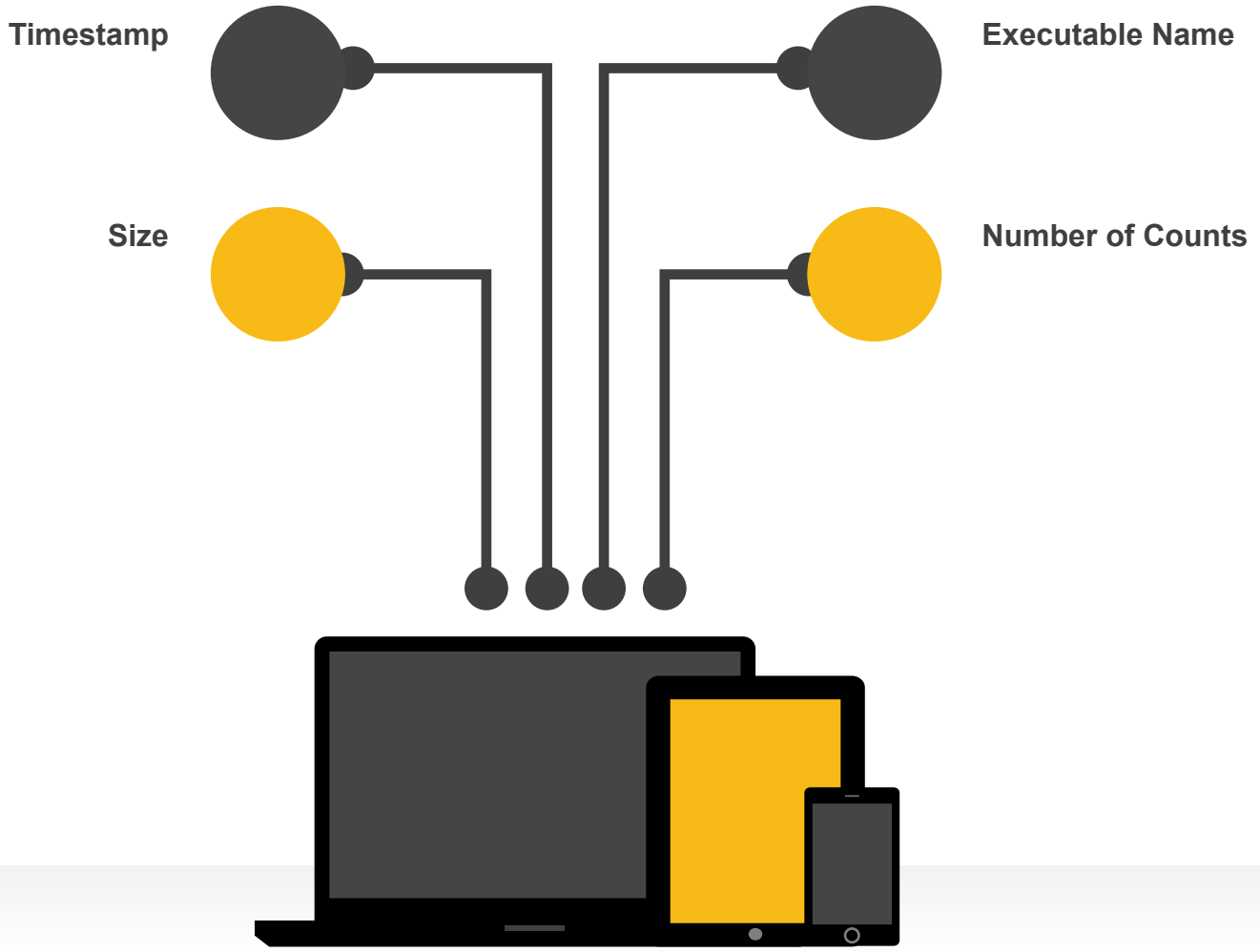
1. **Introduced in windows. Has extension of .pf**
2. **Increases speed of applications' startup processes**
3. **Helps find evidence of execution.**

Image of Prefetch Files

Prefetch Files Naming Conversion



Prefetch Files Metadata

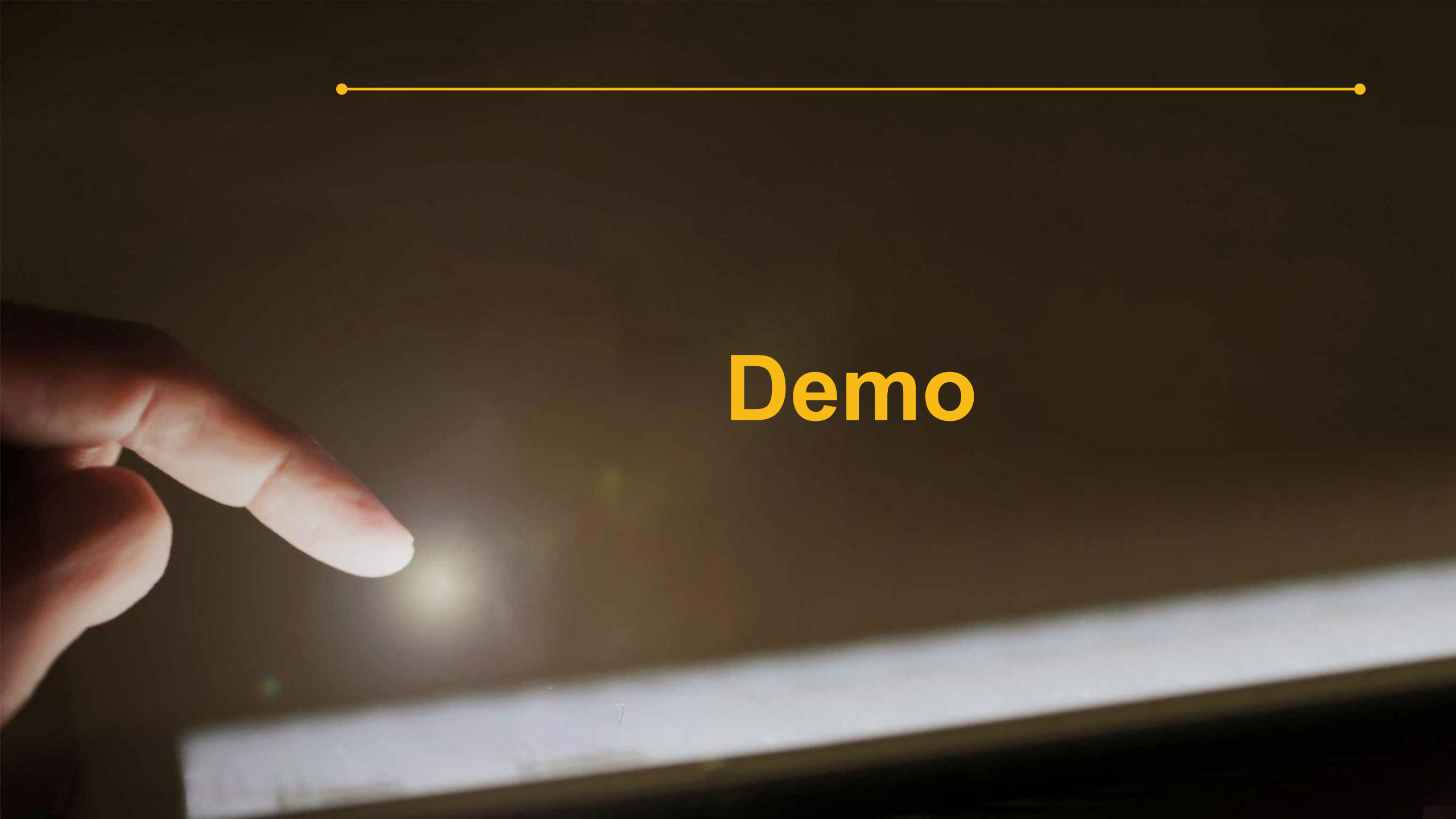


Finding Prefetch Files in Windows 10

1. Go to run
2. Open and type prefetch
3. Run as administrator
4. You are presented with the prefetch files

Open Source Tools for Prefetch Investigation

1. **WinPrefetchView - https://bit.ly/3EHYOZN**
2. **PECmd - https://bit.ly/3mIhL8M**


Demo

THANK YOU