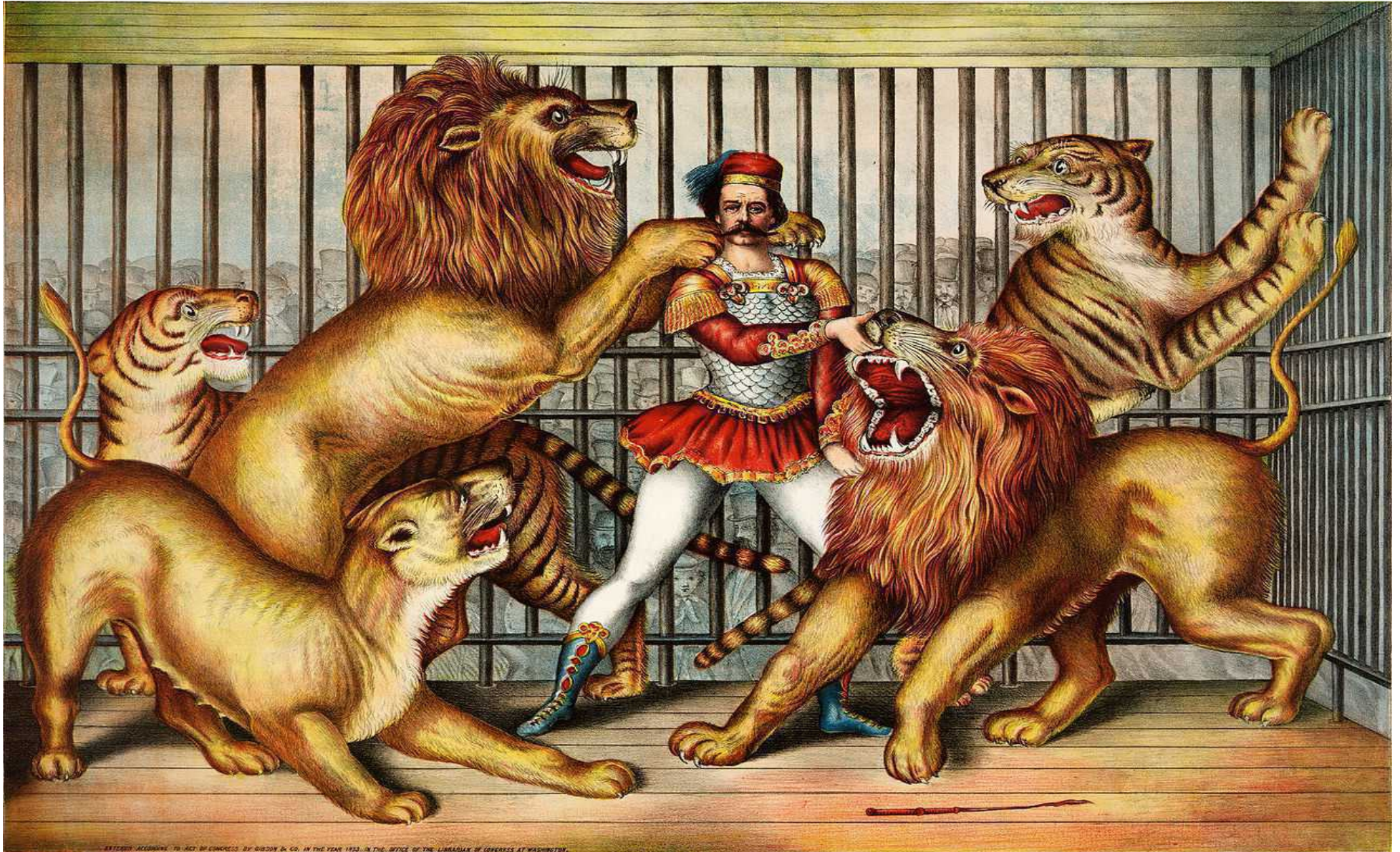


Windows Live Acquisition/Triage Using FOSS and AChoir



EXTERIOR JACOBSON TO ACT BY CONGRESS BY GIBSON & CO. IN THE YEAR 1932 IN THE OFFICE OF THE LIBRARIAN OF CONGRESS AT WASHINGTON.

Who Am I

D0n Quix0te

@OMENScan or OMENScan@Gmail.com

- **Creator of OMENS, OMENSApp, AChoir**
- **Global Incident Response @ Live Nation**
- **16 Years @ NASA**
- **7 Years @ Lockheed**
- **Architecting & Defending High Value Targets**
- **Firewalls, IDS, Web Filtering**
- **Vuln Management, Security Plans, IR**

Disclaimer

ALL OPINIONS ARE MINE ALONE!

I do not speak for any past, present, or future employers or their employees, customers or clients. This talk is not endorsed, approved, or otherwise sanctioned by anybody I work for now, or have ever worked for. Ever!

In fact, these opinions are mine and mine alone. They might be wrong, and I reserve the right to change my mind at any time without prior notice.

Terms

Artifact - A digital item or remnant produced by action(s) taken on a digital device

Forensics - Identifying, extracting and analyzing evidence from digital devices

Live Acquisition - Extracting digital artifacts from a “live” (running) system

Dead-Box – Extracting digital artifacts from A system that has been shut down

STOP NOW !



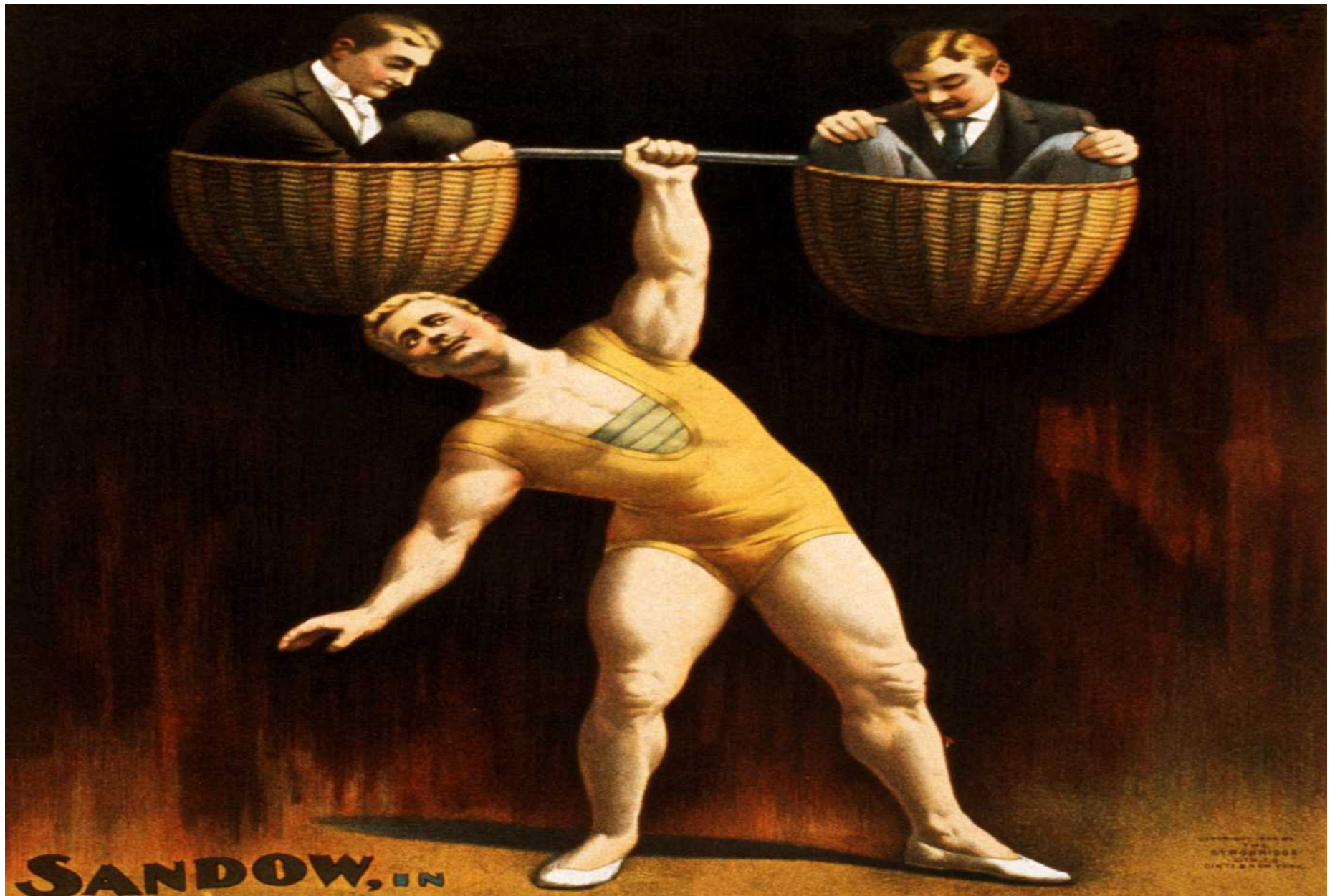
Train wreck at Montparnasse 1895 - Levy & fils

The background image is a black and white photograph of a train wreck at Montparnasse station in 1895. It shows a large, multi-story building with arched windows and a sign that reads "CHEMIN DE FER DE L'OUEST". A train is visible in the foreground, and the scene is filled with debris and smoke, indicating a major disaster.

STOP NOW !

- **If A Crime Is Suspected**
 - **Get Someone Qualified !**
 - **THIS IS IMPORTANT !**
- **Get/Have Permission**
- **This Is Not A Forensics Class**
- **This Is Not An IR Class**

Live-Box vs. Dead-Box



Live-Box vs. Dead-Box

- **Shutdown Immediately or Live Acquire**
- **Dead-Box**
 - **Image The Drive (Evidence File)**
 - **Search for Artifacts**
- **Live-Box**
 - **Dump Memory**
 - **Pull Relevant Artifacts**
 - **One Shot – Get What You Can!**


Live-Box vs. Dead-Box

- **Live-Box**
- **Volatile Artifacts**
 - **Memory, Connections, Prefetch, Etc..**
- **Many artifacts are the same... But..**
 - **Require different gathering methods**
 - **Or different scripting options / switches**
- **We Will Focus on Live Acquisition**

Free Utilities: Most Are Vertical

- **Many Good Free Win Forensic Utils**
 - Finding Them is Hard
 - Lots of Trial and Error
 - Most Are Very Specific (Vertical)
- **Downloading Them (cURL)**
<http://curl.haxx.se/>
- **Unzipping Them (Info-Zip)**
<http://www.info-zip.org/>

THE GREAT FOREPAUGH & SELLS BROTHERS SHOWS COMBINED



THE FROLICS AND AMUSING ANTICS OF TWENTY FUNNY FELT-CROWNED FOOLS. A SERIES OF COMICAL MISHAPS, LUDICROUS INCIDENTS, SIDE SPLITTING LAUGHABLE FEATS AND APT BURLESQUES ON FAMOUS HITS OF THE DAY OCCURRING CONCURRENTLY IN THE RINGS, STAGES, HIPPODROME TRACK AND AERIAL ENCLAVE.

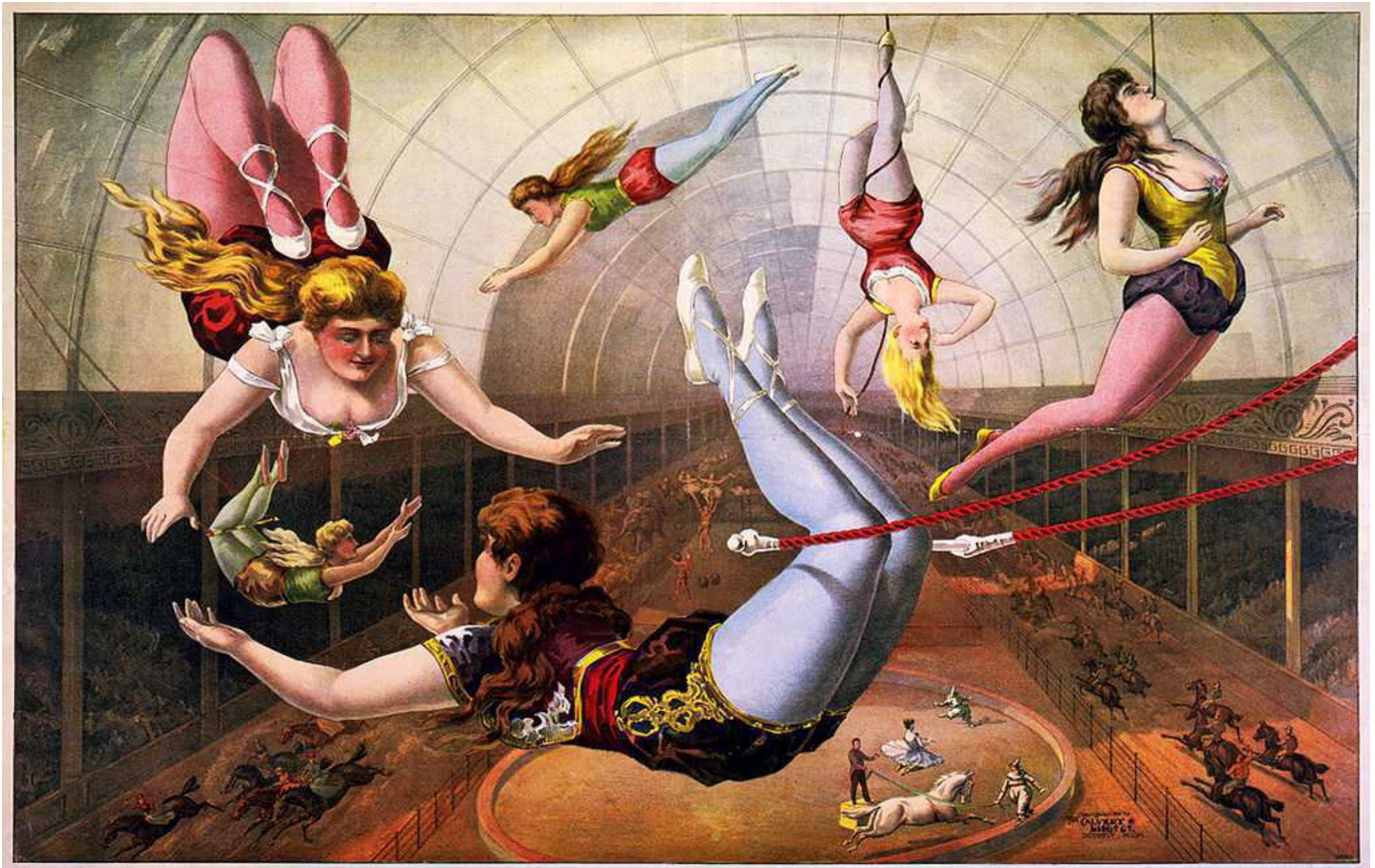
THE FROLICS AND AMUSING ANTICS OF TWENTY FUNNY FELT-CROWNED FOOLS A SERIES OF COMICAL MISHAPS, LUDICROUS INCIDENTS, SIDE SPLITTING LAUGHABLE FEATS AND APT BURLESQUES ON FAMOUS HITS OF THE DAY OCCURRING CONCURRENTLY IN THE RINGS, STAGES, HIPPODROME TRACK AND AERIAL ENCLAVE.

Script All The Things

- **Observer's Paradox**
 - **Gathering Artifacts AFFECTS System**
 - **Minimizing Impact (Memory, Disk)**
 - **Order Of Volatility**
- **I Usually Grab Everything I Can...**
 - **Time Available**
 - **Disk Space Available**
 - **What Will I Likely Need**

THE FROLICS AND AMUSING ANTICS OF TWENTY FUNNY FELT-CROWNED FOOLS. A SERIES OF COMICAL MISHAPS, LUDICROUS INCIDENTS, SIDE SPLITTING LAUGHABLE FEATS AND APT BURLESQUES ON FAMOUS HITS OF THE DAY OCCURRING CONCURRENTLY IN THE RINGS, STAGES, HIPPODROME TRACK AND AERIAL ENCLAVE.

Artifacts: Memory



Artifacts: Memory

- **WinPMem (Github/Google/Rekall)**
 - **My Favorite – Easily Scriptable**
 - **Easily Downloaded via Script**
- **Memoryze (Mandiant)**
 - **Works Consistently Well**
 - **Some idiosyncracies**
- **A Few Others – But Those Are My Favs**

Note: Volatility is Excellent For Memory Dump Analysis

Artifacts: Disk



Artifacts: Disk (Raw)

- **Some Data Isn't Meant To Be Copied**
- **Rawcopy (Github/Jschicht)**
 - **Raw Copies Data using \$MFT Index**
 - **\$MFT – An Index Of Files and Dirs**
 - **\$LogFile – File Activity Journal**
- **ExtractUSNJrnl (Github/Jschicht)**
 - **Parses the \$USNJrnl:\$J**

*Note1: Triforce ANJP \$MFT+\$LogFile+\$USNJrnl analysis
(Free/noncommercial use)*

Note2: Jschicht == Joakim Schicht



Artifacts: Disk (Parse)

- **MFTDump (The Malware Hunters)**
 - **Parses Raw \$MFT**
 - **INCREDIBLY USEFUL!**
- **FSUtil (Native DOS Utility)**
 - **Parses the \$USNJrnl:\$J**

Artifacts: System Info



Artifacts: System Info

- **Sysinternals PSTools – 'Nuff Said**
 - **PSInfo – System Info**
 - **PSList – Running Process Info**
 - **Handle – Open File Handles**
- **Native DOS Utilities**
 - **SC Query – Services Info**
 - **TaskList – Running Process & Service**
 - **Netstat – Network Connections**
 - **WMIC qfe list – List Patches**

Artifacts: Registry



Artifacts: Registry TomFoolery

- **User Entries vs. System Entries**
 - **HKCU – User Profiles: NTUSER.DAT**
 - **HKLM – System32\Config**
 - **SYSTEM, SAM, SECURITY, SOFTWARE**
- **Live Acquisition Considerations**
 - **CurrentControlSet – Only Exists Live**
 - **HKLM\SYSTEM>Select\Current**
 - **Registry Files Can't Be Copied Live**

Artifacts: Registry (Raw vs. Parse)

- **Raw – Duplicate/Copy Registry/Hives**
 - **Machine Readable**
- **Parsed – Extract Registry Data/Hives**
 - **Human Readable**
- **Meta-Data – Data About The Data**
 - **Last Write Time – EXTREMELY USEFUL**

Artifacts: Registry

- **Live Acquisition**
 - **Reg Save (Native DOS Utility)**
 - **Copies Live Registry Hive**
- **Reg Export (Native DOS Utility)**
 - **Parses Live Registry Hive**
- **Dead-Box / Post Process Reg Save**
 - **RegFileExport (Nirsoft) – Parse Hive**
 - **RegRipper (Harlan Carvey) – Last Write**

Artifacts: Event Logs



Artifacts: Event Logs

- **DOS Copy (*.evtx)**
 - **System32\winevt\Logs Directory**
 - **Sysnative\winevt\Logs Directory (64 bit)**
- **Parsing Event Logs**
 - **PSLoglist (Sysinternals)**

Artifacts: Other Stuff



Artifacts: Other Cool Stuff

- **Winaudit (Parmavex Services)**
 - **Hardware & Software Audit**
- **Nirsoft:**
 - **WinPrefetchView -Parse Prefetch Files**
 - **LastActivityView – Activity from Registry, Event Logs, Prefetch, Etc...**
 - **UserAssistView – Last Time, Count**
 - **BrowsingHistoryView – IE, FF, Chrome, Safari**

AChoir



AChoir

- **The Problem(s)**
 - **Scripting Utilities (.Bat, .WSH, .PS1, ???)**
 - **Script The Toolkit BUILD Process**
- **AChoir - Started Life as Two Batch Files**
- **Create Common Framework**
- **A Scripting Utility Built for Live Acquisition**

AChoir

- **Built-in Common Needs**
 - **Hashing (Programs & Data)**
 - **Logging (With Hashing)**
 - **Local and Remote Acquisition**
 - **Sets Artifacts to R/O**
- **Focus on Order of Volatility**
- **Hash Programs on Download AND Run**
- **Open Source**
- **Compiled (GCC)**

AChoir

- **Does Dead-Box Too**
 - **Automate Common Artifacts Extract**
 - **DeadBox.Acq script**
 - **EWFF32/EWFF64.Acq Scripts**
 - **OSFmount (PassMark Software)**
- **Automate Other Artifacts Extraction**
 - **MediaDump.Acq Script**
 - **DocDump.Acq Script**

AChoir

- **Build The Toolkit Option (/BLD)**
 - **Build.Acq - Downloads & Extracts Utils**
 - **Hashes The Toolkit**
- **Simple Menu Creation (/MNU)**
 - **Menu.Acq**
- **Architecture 32 & 64 bit**
 - **Conditional Execution**
- **Are We Admin ?**
 - **Check or FORCE**

AChoir

- **Map To Remote (SMB) Share**
 - **/Map and Map:**
- **Loop Through Files**
 - **FOR:, &FOR, &FNM, &NUM**

Example:

FOR:C:\Users\NTUSER.DAT

CPY:"&For" "&Acq\&Fnm(&Num)"

AChoir

- **Internal Copy Routine**
 - **CPY:**
 - **Hashes Files & Checks MetaData (Dates)**
 - **Size, CTime, ATime, MTime**

Cpy: C:\Users\Default\NTUSER.DAT

C:\AChoir\ACQ-IR-MUSICLAPTOP-20160303-1858\Reg\NTUSER.DAT(3)

Inf: Source File MD5.....: 9c259fbc4ef5657c8ac5e066dbf49df0

Inf: Source MetaData.....: 262144-1446186510-1454208138-1454208138

Inf: Destination File MD5: 9c259fbc4ef5657c8ac5e066dbf49df0

Inf: Destination MetaData: 262144-1446186510-1454208138-1454208138

AChoir

- **Extract Autorun Programs in Run Key**
 - **ARN:**
 - **BOTH 32 AND 64 Bit RunKeys**
 - **BOTH 32 AND 64 Bit Directories**
- **Write Protect USB**
 - **USB: Protect or Enable**
- **Run a Program on Exit**
 - **XIT:**
 - **For Instance – Zip To Archive**

AChoir

- **Hash Everything!**
- **Create A Browsable Index**
 - **Index.html**
- **Archive, Compress, Password Protect**
 - **AChoirZ.Acq – Uses ZPAQ**

AChoir

- **Github**
 - **OMENScan/AChoir**
 - **v0.40 Complete**
 - **Download It, Test It, And...**
- **Come Help Me Make It Better!**
 - **Repository Model**

Questions ?



Questions ?

Thanks for taking time to hear me talk!

Don Quixote

Twitter: @OMENScan

Email: OMENScan@GMail.com

www: MuSecTech.com