Turning Telemetry and Forensic Artifacts Into Information

Who Am I

- Blue Team Village Lead
- @OMENScan or OMENScan@Gmail.com
- FOSS Creator
  - OMENS, OMENSApp
  - AChoir, AChReport
- Incident Responder, CSIRT Architect & Director
- I Do Security Stuff

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.

What Are We Gonna Do Today

1. Understand, Install, Run AChoir
    - Discuss Modes (Local, Remote, Server)
    - Discuss Types (Live Response, Dead Box)

2. Get immediate information from AchReport

3. Create Self-Extracting Executables

4. Automate Memory Analysis

5. TimeLine Artifacts

6. Ingest TimeLine Data into ELK

Collection types

1. Full Forensic Imaging
   - Collect Memory
   - Full Forensic Image of Disk(s)
   - Great to Have Everything Possible
   - Litigation?
   - Not Scalable
   - Difficult Over the Wire – Best Locally

2. Specific Pre-Parsed Artifacts
   - Good at Scale
   - Good Over the Wire
   - When You Know What You Are Looking For
   - Good for Frequency Analysis (Stacking)

Collection types

3. General Raw Artifact Collection (Triage)

- Collect Memory
- Collect Raw Artifacts (Registry, Logs, etc...)
- Good For Investigating the Unknown
- Requires Post-Processing and Analysis
- Semi-Scalable
- Practical Over the Wire / Remote
- Can Lead to Full or Pre-Parsed Collection

This is what we will be looking at today

Collection Considerations

1. Predetermining what to collect
    - Memory, $MFT, Registry, Event Logs, etc...

2. Building the tool
    - There is no single forensics tool to do everything

3. Getting the tool onto the endpoint & executing it
    - Packaging, Delivering, Executing

4. Monitoring progress & storing logs
    - Local Console, Remote Console, Syslog

Collection Considerations

5. Storing the Telemetry and Artifacts
    - Local USB, Remote Server
    - RFC1918, Internet, VPN
    - SMB, SCP, SFTP, HTTP, S3

6. Converting raw Telemetry into Information
    - What are we looking for?
    - How do we get there faster?

7. What about Dead Box analysis?
    - Mounting a Forensic Image

8. Searching and correlating data
    - SIEM, Splunk, ELK

Let's Install AChoir

- HTTPS://Github.com/Omenscan

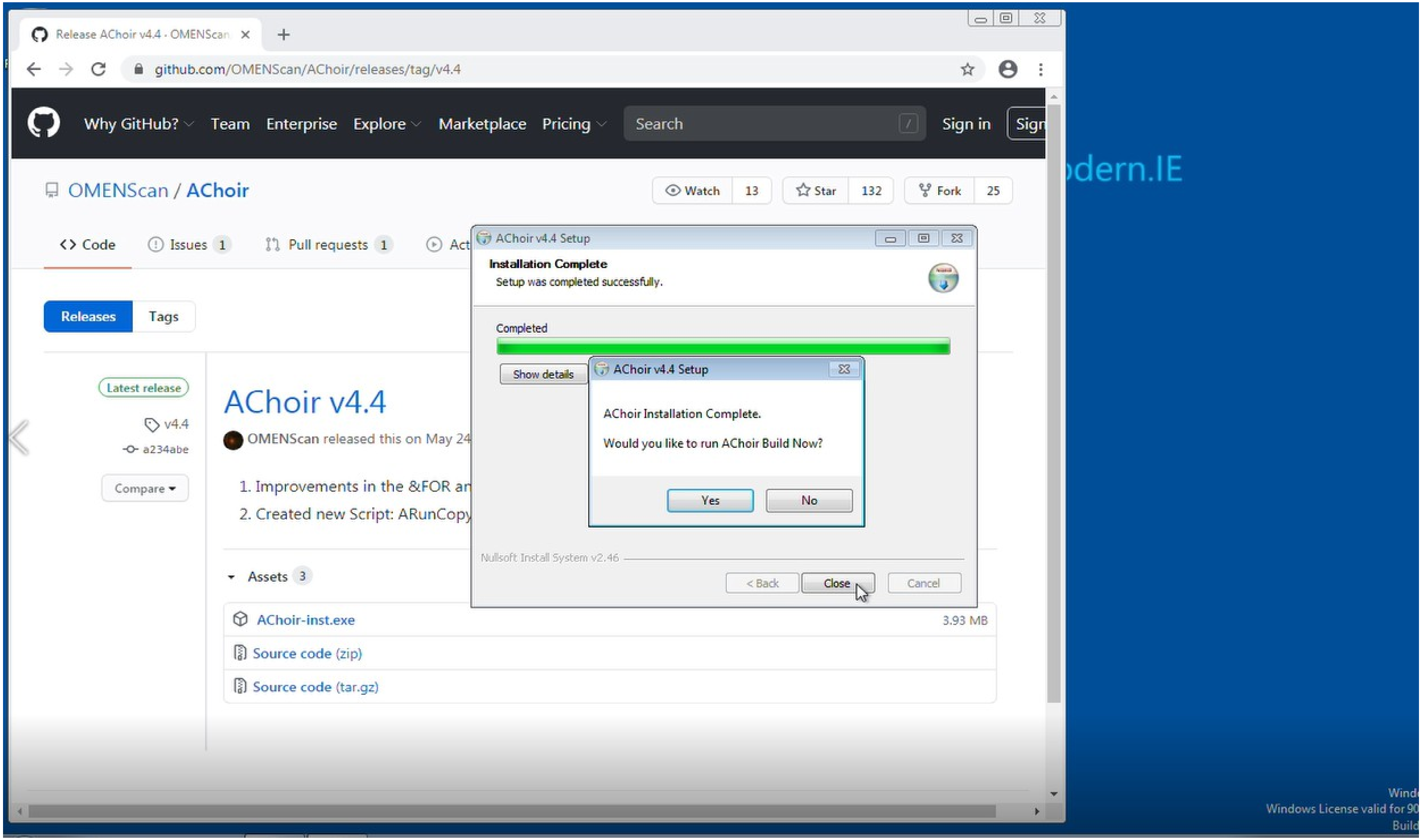
- Achoir-Inst.exe
  - I recommend copying it to a USB drive and running it from there.

- Build the Tool Kit
  - Running the Install from USB will build the Tool Kit on that drive

  - Running the Tool Kit from USB will gather Telemetry and Artifacts to that drive

Note: Unfortunately some of the Tools that AChoir uses are detected by A/V

Install, Build, Run Exercise



AChoir v4.4

OMENScan released this on May 24

1. Improvements in the &FOR an
2. Created new Script: ARunCopy

AChoir-inst.exe	3.93 MB
Source code (zip)	
Source code (tar.gz)	

AChoir v4.4 Setup

Installation Complete

Setup was completed successfully.

Completed

AChoir v4.4 Setup

AChoir Installation Complete.

Would you like to run AChoir Build Now?

Wind
Windows License valid for 90
Build

Some Options Worth Noting

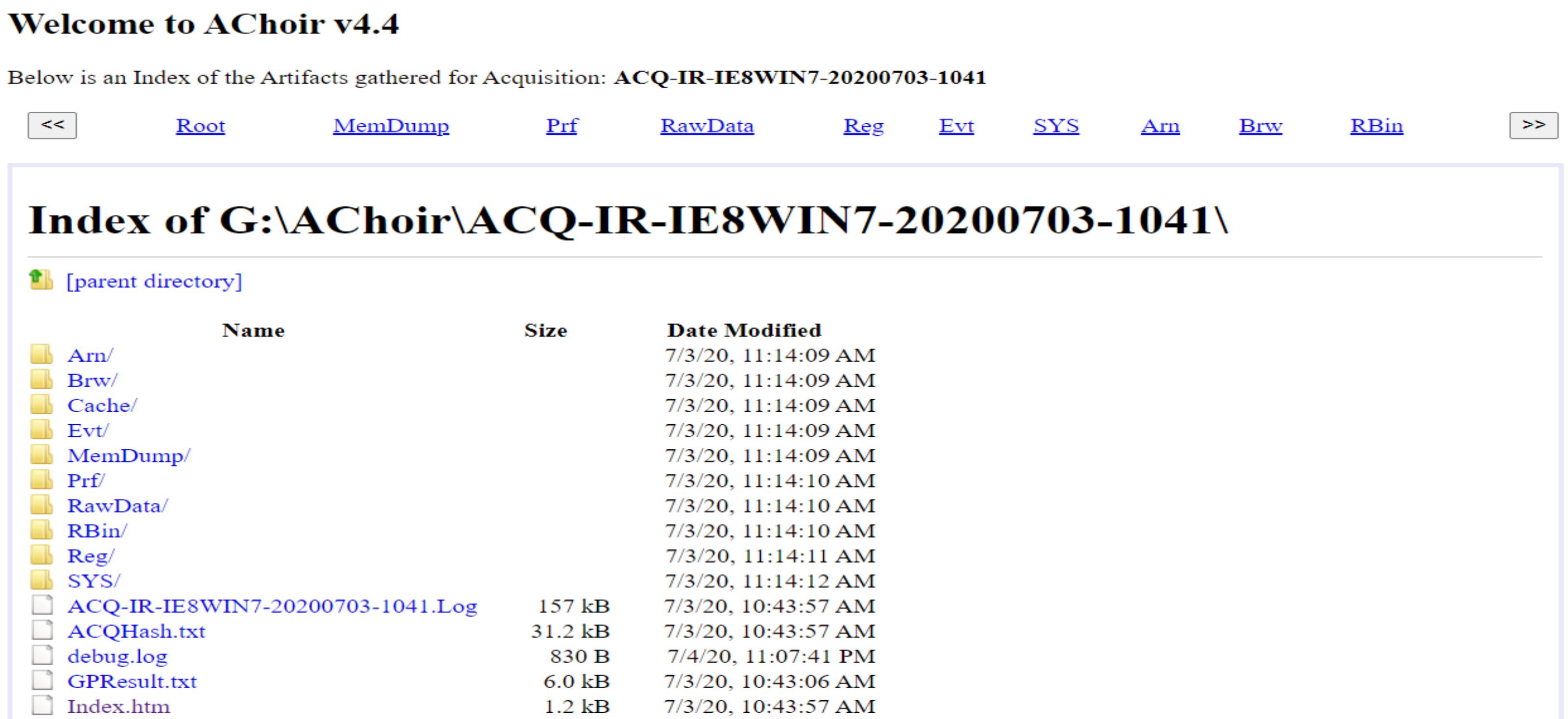
- Console Mode
  - AChoir /con
- Recognizes File and Registry Redirection
- Fully Scriptable
- Raw NTFS File Copy
- Local or Remote Collection
- SMB, SCP, SFTP, S3, whatever...
- Builtin File Parsing
  - i.e Run Autoruns, Parse, copy out all the exes

Some Options Worth Noting

- Builtin File Parsing
  - I.e Run Autoruns, Parse, copy out all the exes
- Syslogging to your SIEM
- TimeLining with Plaso
- Copy by Magic Number
- Conditional Logic
  - Windows Version, 64/32 bit, File Existence, Numbers, Strings, etc...

Let's Run AChoir

- AChoir, A-AChoir, Achoir64, A-AChoir64
  - Unique Directory for each collection
  - Contains an Index.htm for navigation
  - For many analysts this would enough



Welcome to AChoir v4.4

Below is an Index of the Artifacts gathered for Acquisition: **ACQ-IR-IE8WIN7-20200703-1041**

Index of G:\AChoir\ACQ-IR-IE8WIN7-20200703-1041\

[parent directory]

Name	Size	Date Modified
Arn/		7/3/20, 11:14:09 AM
Brw/		7/3/20, 11:14:09 AM
Cache/		7/3/20, 11:14:09 AM
Evt/		7/3/20, 11:14:09 AM
MemDump/		7/3/20, 11:14:09 AM
Prf/		7/3/20, 11:14:10 AM
RawData/		7/3/20, 11:14:10 AM
RBin/		7/3/20, 11:14:10 AM
Reg/		7/3/20, 11:14:11 AM
SYS/		7/3/20, 11:14:12 AM
ACQ-IR-IE8WIN7-20200703-1041.Log	157 kB	7/3/20, 10:43:57 AM
ACQHash.txt	31.2 kB	7/3/20, 10:43:57 AM
debug.log	830 B	7/4/20, 11:07:41 PM
GPResult.txt	6.0 kB	7/3/20, 10:43:06 AM
Index.htm	1.2 kB	7/3/20, 10:43:57 AM

We Can do WAY Better

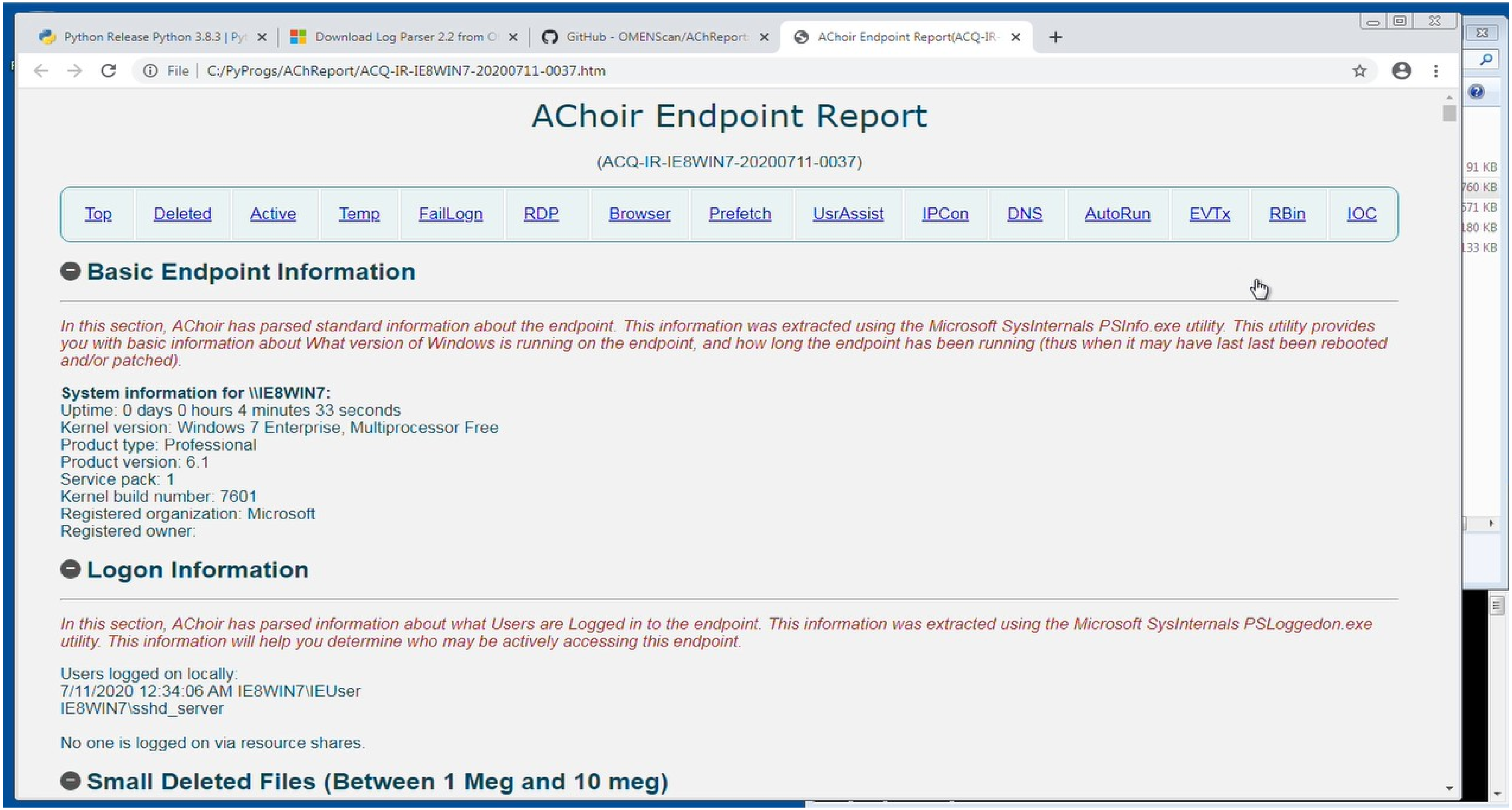
HTTPS://Github.com/Omenscan

- Download AchReport.py
  - Put AChReport.py in your Python Directory
  - Requires Python 3.7 or above
  - Must be run on Windows
  - Requires Achoir to be installed
  - Requires Microsoft Logparser

- Py AchReport.py -d <collection directory>

- Now we have information!

Installing AchReport Exercise


Python Release Python 3.8.3 | Py
Download Log Parser 2.2 from O
GitHub - OMENScan/AChReport
AChoir Endpoint Report(ACQ-IR-
File
C:/PyProgs/AChReport/ACQ-IR-IE8WIN7-20200711-0037.htm
91 KB
760 KB
571 KB
180 KB
133 KB

AChoir Endpoint Report

(ACQ-IR-IE8WIN7-20200711-0037)

Top | Deleted | Active | Temp | FailLogn | RDP | Browser | Prefetch | UsrAssist | IPCon | DNS | AutoRun | EVTx | RBin | IOC

⊖ Basic Endpoint Information

In this section, AChoir has parsed standard information about the endpoint. This information was extracted using the Microsoft SysInternals PSInfo.exe utility. This utility provides you with basic information about What version of Windows is running on the endpoint, and how long the endpoint has been running (thus when it may have last last been rebooted and/or patched).

System information for \\IE8WIN7:
Uptime: 0 days 0 hours 4 minutes 33 seconds
Kernel version: Windows 7 Enterprise, Multiprocessor Free
Product type: Professional
Product version: 6.1
Service pack: 1
Kernel build number: 7601
Registered organization: Microsoft
Registered owner:

⊖ Logon Information

In this section, AChoir has parsed information about what Users are Logged in to the endpoint. This information was extracted using the Microsoft SysInternals PSLoggedon.exe utility. This information will help you determine who may be actively accessing this endpoint.

Users logged on locally:
7/11/2020 12:34:06 AM IE8WIN7\IEUser
IE8WIN7\sshd_server

No one is logged on via resource shares.

⊖ Small Deleted Files (Between 1 Meg and 10 meg)

Let's Look at Mine

- Review Sections
  - Expand Compress
  - Descriptions of Purpose

- Suspected Compromised Machine
  - Metasploit Suspected
  - Mimikatz Suspected

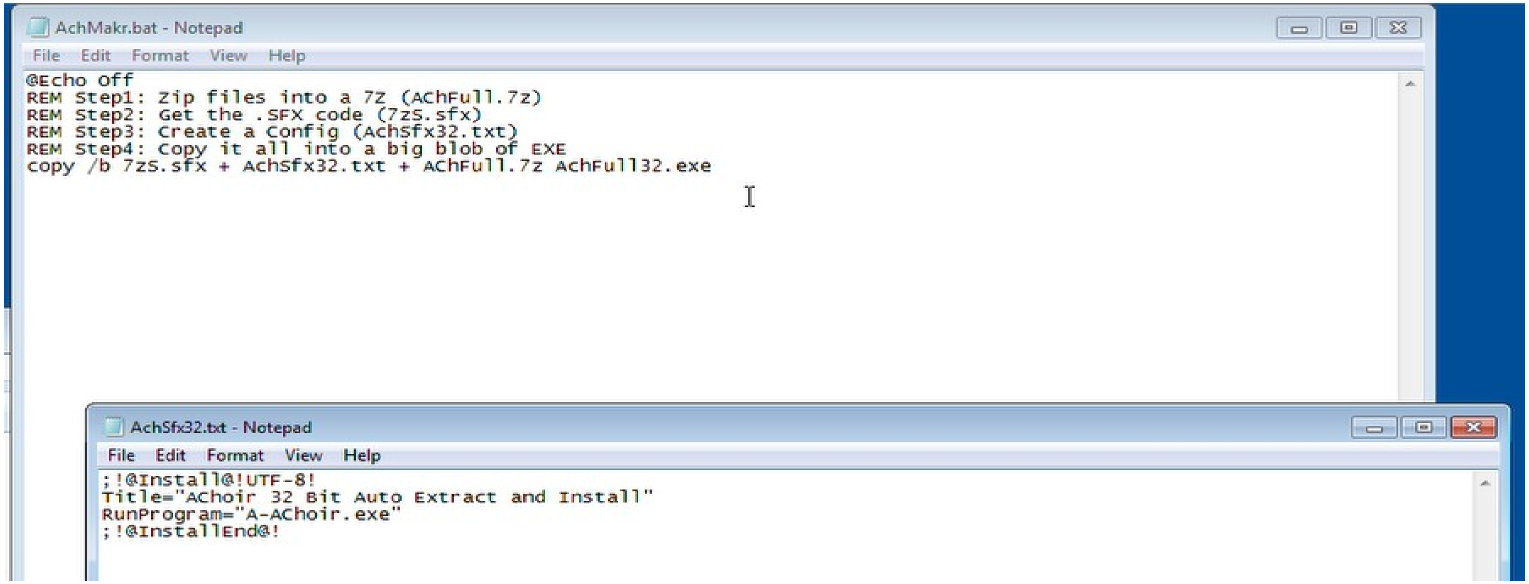
- Suspicious Indicators
  - Executables in Temp Directories
  - Success RDP (unknown ID AchBAdmin)
  - Failed Logins (RDP)

Let's Look at Mine

- Suspicious Indicators (continued)
  - Prefetch
    - HackTools, PsExec, Exe from Temp
  - Autoruns
  - Wierd IP Connections
    - Port 4444
  - Installed Services (7045) – Random Names
    - TJSUUcvByfYdZ & QTVbGmcynyU
    - NUZA.exe

Let's Talk About Packaging

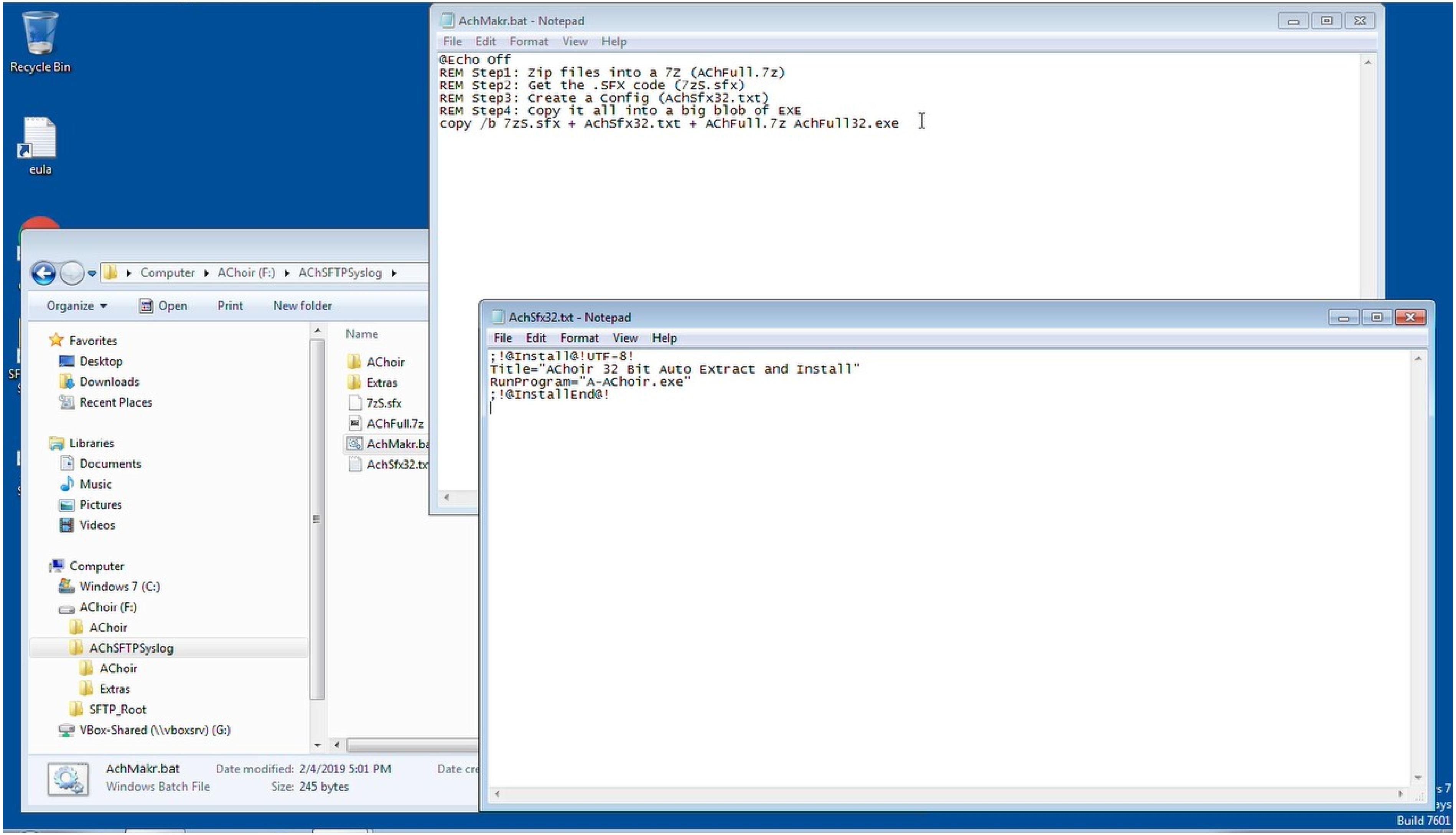
- 7Zip SFX
  - https://www.7-zip.org/download.html
  - FOSS
  - Self Extracting, Self Executing
  - Self Destructing – Probably the best part



```
@Echo Off
REM Step1: Zip files into a 7z (AChFull.7z)
REM Step2: Get the .SFX code (7zS.sfx)
REM Step3: Create a Config (AchSfx32.txt)
REM Step4: Copy it all into a big blob of EXE
copy /b 7zS.sfx + AchSfx32.txt + AChFull.7z AchFull32.exe
```

```
;!@Install@!UTF-8!
Title="AChoir 32 Bit Auto Extract and Install"
RunProgram="A-AChoir.exe"
;!@InstallEnd@!
```

SFX Package, SFTP, Syslog Exercise



AchMakr.bat Date modified: 2/4/2019 5:01 PM Date cre
Windows Batch File Size: 245 bytes

AchMakr.bat - Notepad

```
@Echo Off
REM Step1: Zip files into a 7Z (AChFull.7z)
REM Step2: Get the .SFX code (7zS.sfx)
REM Step3: Create a Config (AchSfx32.txt)
REM Step4: Copy it all into a big blob of EXE
copy /b 7zS.sfx + AchSfx32.txt + AChFull.7z AchFull32.exe
```

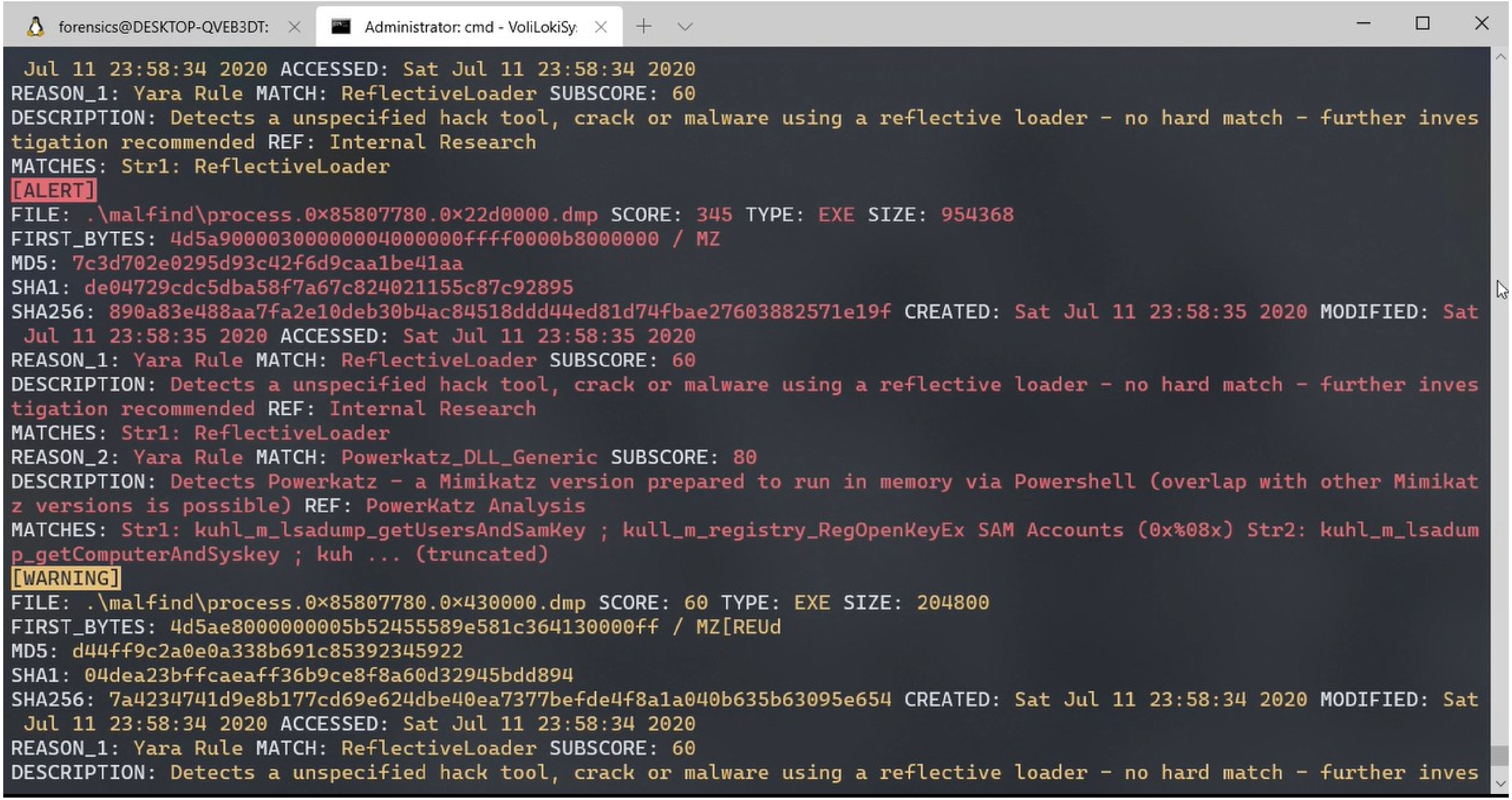
AchSfx32.txt - Notepad

```
;!@Install@!UTF-8!
Title="AChoir 32 Bit Auto Extract and Install"
RunProgram="A-AChoir.exe"
;!@InstallEnd@!
```

Let's Look at Memory

- AChoir captured Memory
  - Automate Volatility to parse out both processes AND Indicators (IP Addresses, File Names, Etc)
- Then Run Loki Against Them
  - Send the Telemetry to Syslog for your SIEM
  - Once Automated, these are quick wins
- Extra Credit – Import into Sof-Elk

Volatility Loki Demo



```
 Jul 11 23:58:34 2020 ACCESSED: Sat Jul 11 23:58:34 2020
REASON_1: Yara Rule MATCH: ReflectiveLoader SUBSCORE: 60
DESCRIPTION: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further inves
tigation recommended REF: Internal Research
MATCHES: Str1: ReflectiveLoader
[ALERT]
FILE: .\malfind\process.0x85807780.0x22d0000.dmp SCORE: 345 TYPE: EXE SIZE: 954368
FIRST_BYTES: 4d5a90000300000004000000ffff0000b8000000 / MZ
MD5: 7c3d702e0295d93c42f6d9caa1be41aa
SHA1: de04729cdc5dba58f7a67c824021155c87c92895
SHA256: 890a83e488aa7fa2e10deb30b4ac84518ddd44ed81d74fbae27603882571e19f CREATED: Sat Jul 11 23:58:35 2020 MODIFIED: Sat
 Jul 11 23:58:35 2020 ACCESSED: Sat Jul 11 23:58:35 2020
REASON_1: Yara Rule MATCH: ReflectiveLoader SUBSCORE: 60
DESCRIPTION: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further inves
tigation recommended REF: Internal Research
MATCHES: Str1: ReflectiveLoader
REASON_2: Yara Rule MATCH: Powerkatz_DLL_Generic SUBSCORE: 80
DESCRIPTION: Detects Powerkatz - a Mimikatz version prepared to run in memory via Powershell (overlap with other Mimikat
z versions is possible) REF: PowerKatz Analysis
MATCHES: Str1: kuhl_m_lsadump_getUsersAndSamKey ; kull_m_registry_RegOpenKeyEx SAM Accounts (0x%08x) Str2: kuhl_m_lsadum
p_getComputerAndSyskey ; kuh ... (truncated)
[WARNING]
FILE: .\malfind\process.0x85807780.0x430000.dmp SCORE: 60 TYPE: EXE SIZE: 204800
FIRST_BYTES: 4d5ae8000000005b52455589e581c364130000ff / MZ[REUd
MD5: d44ff9c2a0e0a338b691c85392345922
SHA1: 04dea23bffcaeaff36b9ce8f8a60d32945bdd894
SHA256: 7a4234741d9e8b177cd69e624dbe40ea7377befde4f8a1a040b635b63095e654 CREATED: Sat Jul 11 23:58:34 2020 MODIFIED: Sat
 Jul 11 23:58:34 2020 ACCESSED: Sat Jul 11 23:58:34 2020
REASON_1: Yara Rule MATCH: ReflectiveLoader SUBSCORE: 60
DESCRIPTION: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further inves
```

Let's TimeLine it with Plaso

- **AChoir already has a Script for that**
  - **AChoir /ini:Plaso.acq**
  - **Downloads Plaso automatically and does all the magic**

  - **Process using your favorite TimeLine software**

  - **Sof-Elk**

Questions ?

Thanks For Hanging Out !

Twitter: @OMENScan

Email: OMENScan@GMail.com

Web: www: MuSecTech.com