eForensics Magazine

Preview

MAGAZINE

DIGITAL FORENSIC TOOLS

HOW TO IDENTIFY MALWARE ACTIVITIES IN THE WINDOWS SYSTEM

MEMORY ANALYSIS USING VOLATILITY FRAMEWORK

HOW TO START IN DIGITAL FORENSICS

SOCMINT WITH SHERLOCK

TRACKING USERNAMES ACROSS THE INTERNET WITH MAIGRET

PROCESSING iOS DEVICES FOR DIGITAL FORENSICS

VOL.10 NO.09
ISSUE 09/2022 (125) SEPTEMBER
ISSN 2300 6986

EDITOR'S WORDS

Dear Readers,

I hope everything is going well for you. In my dream, I imagined you eagerly awaiting the next issue of eForensics Magazine. The idea of this issue was to present as many digital forensics tools as our authors, reviewers, the Internet ;) and I found for you.

I hope you find them useful in your daily work. I hope that I managed this task. However, I think you will find more interesting topics.

Inside the issue, there are many technical details about the tools itself. You will find articles that were created to introduce not only the tools but you will also find articles into which you will dive deeply in the areas of digital forensics matters. I know that we have only "a few" pages this time so that we selected and mentioned, e.g., Kali Linux: a great distro focused mainly on PT, but used by investigators, but I hope that we will soon cover forensic distros, like Tsurugi or Caine, specifically created for forensic purposes.

There are a lot of topics out there so if you have any ideas for the articles that should be mentioned in our magazine, please feel free to contact me (email below). As one of my dearest reviewers said: mobile forensics (the most relevant part of the job today) is rarely talked about, and there is a lot more in the field – live forensics, network forensics, cloud forensics. I really enjoyed reading about the forensic investigation process, especially how the investigators work at the crime scene and register all the necessary documents.

Perhaps someone who reads these words at this moment wants and can share their own knowledge about it. Feel free to contact me. I am also working on the next issue and planning the next topic. Some of you read my email about it. However, I would like to remind you what the editorial schedule for the next three months looks like: Corporate Forensic Investigations, Advanced Digital Forensic Analysis, Mobile Device Forensics. I am searching for the next catchy and most-wanted topics. Of course, you are always welcome to share your own ideas and thoughts.

Now, let's have a glimpse of what our experts prepared for you.

My kindest regards,

Ewa & eForensics Mag Team

ewa.dudzic@eforensicsmag.com

TABLE OF CONTENTS

Memory Analysis Using Volatility Framework To Identify Malware Activities In The Windows Systems

Adalberto Batista da Silva

Enizaldo Severino da Silva Filho

Paulo Henrique Pereira

Regis Proença Picanço

Rodrigo Ferreira Marques

What you should know...

- ***Basics of memory analysis.***
- ***Basics of digital forenscis.***

What you will learn...

- ***Memory Capture and Live Analysis.***
- ***How to use Volatility framework.***
- ***How to identify malware activities.***

Introducing FTK Central: Helping to Transform Digital Forensics at West Midlands Police

Jon Cook, International Training Instructor, Exterro

Forensics toolkits have come a long way in a relatively short period. At the turn of the millennium, we were still navigating the early days of Windows, where small computer hard drives of around 150 megabytes were the norm. Back then, law enforcement digital forensics was in its infancy. Forensic toolkits were used to support the recovery of deleted files, but a lot was still done manually and relied heavily on the knowledge of examiners.

Fast forward to the late 2010s and now 2020s, and the technologies and capabilities of forensic toolkits have come on leaps and bounds. Indeed, these toolsets have now grown to be comprehensive and intelligent forensic processing engines that are pivotal to the success of law enforcement agencies.

Today, forensic toolkits are now able to extract both present and deleted artefacts and effectively recover available data of interest. They provide digital forensics professionals an improved means of accessing information that's hidden within a computer system.

The success of many law enforcement agencies hinges on the abilities of forensic toolkits. Criminals today leave lengthy trails of digital evidence in the form of increasingly large data sets and new types and forms of data stored on a variety of devices and platforms.

It's a challenge for law enforcement to keep up, often leaving those that are unable to manage with a tidal wave of data and extensive backlogs. To avoid being left in this position, and to more effectively leverage critical data to enhance the justice process, law enforcement agencies require forensic toolkits that are collaborative, integrated and easily process data in a timely and efficient manner.

How to Start in Digital Forensics

Kharim.h Mchatta

What you should know...

- **Digital forensics basics**

What you will learn...

- **Processes involved in forensic analysis.**
- **A brief overview of forensics tools.**

In this article, we discuss the forensics processes, mainly focusing on the forensics tools used under each process. This is going to equip the reader with knowledge of not only the available tools that forensics experts use but also an understanding of where in the forensics process the tools are being used. Most of the tools discussed in this article are focused mainly on computer forensics, but you will see different tools also mentioned in this article. For this article, we will be mainly focusing on making the reader aware of the different kind of tools at their disposal. There will be a list of different kinds of tools and when they are going to be used, but for this introductory article, we will be not discussing how to specifically use the individual tools.

Introduction To Digital Forensic Tools

Digital forensics is the process of collecting and analyzing digital evidence and presenting it in a court of law. Digital forensics started to be utilized in the year 1984 as a need to combat cybercrime. The need for digital forensics was due to the desire of law enforcers to try to combat a new form of crime. Digital forensics started becoming popular in the 1990s; this also changed the way courtrooms perceived what can be considered as evidence due to the rise of digital evidence (M. G. Noblett, M. M. Pollitt & L. A. Presley, (2000) “Recovering and Examining Computer Forensic Evidence”, Forensic Science Communications, Vol. 2, No. 4.).

Reverse Engineering : Static Analysis Using Rabin2 & DnSpy

Tahaa Farooq

This is basically the process of building a program, though "Forward Engineering" is an overloaded term. The processes of building a program are as below:

1. Figure out what you want to code
2. Code it
3. Compile it
4. Run it

Information is lost at every step of forward engineering process. Most of the information are lost in the compilation process and the assemble process such as:

- Comments
- Variable Names
- Function Names
- Structure (classes, structs, etc.) data
- Sometimes, entire algorithms (optimization)

Below is a list of a few tools used in forward engineering:

- Vim/Visual Studio/Any IDE
- GCC/G++/Any Compiler Depending on the Language
- Strings
- Strip

And that's all it requires to give birth to an ELF/Windows Executable!

Reverse Engineering

Reverse engineering is the analysis of a device or program to determine its function or structure, often with the intent of re-creating or modifying it.

Malware analysis is the art of dissecting malware to understand how it works, how to identify it, and how to defeat or eliminate it. In reverse engineering, the steps are as follows:

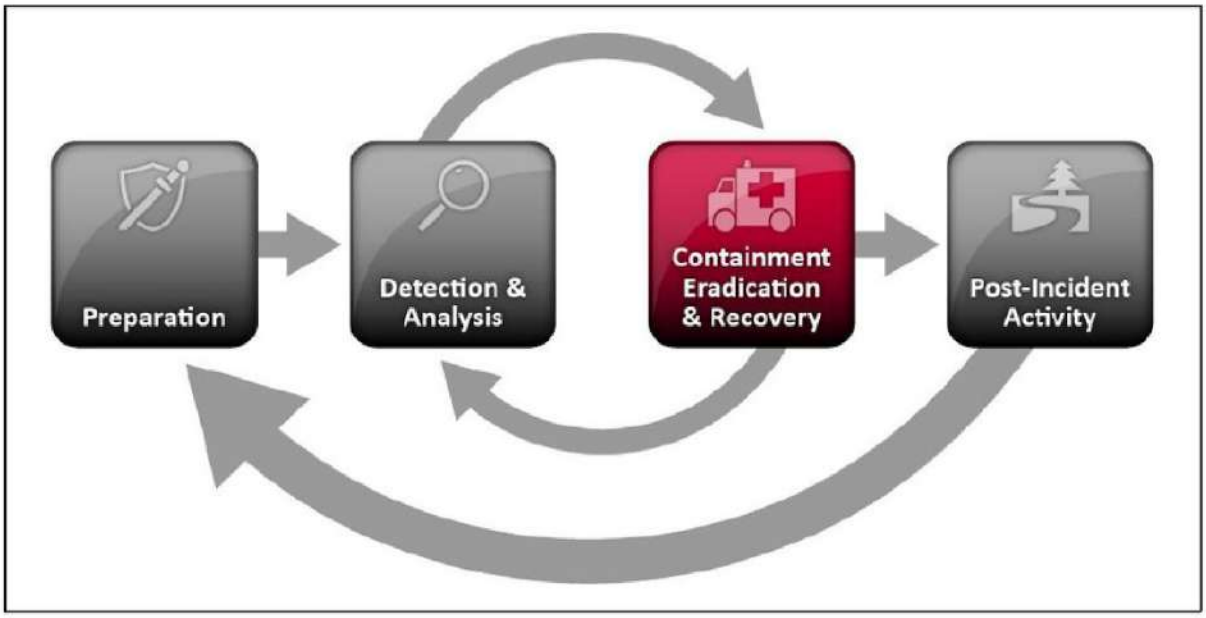
- Have the Binary (ELF/EXE)
- Disassemble
- Decompile
- Lots of thinking
- Understand

Memory Acquisition on Windows and Linux

Ricardo Alves da Silva

This article will discuss how to perform memory collection procedures in Windows and Linux operating systems. Following the incident response lifecycle defined by NIST 800–61r2, the evidence collection and treatment process begins in the "Containment, Eradication, and Recovery" phase.

This is a crucial phase, as it is necessary to measure the actual and potential impacts of a particular incident and, above all, to understand its root cause, so that it is possible to carry out the necessary containment effectively and definitively eradicate the environment.



In certain types of incidents, it may be necessary to present evidence in court, and it is extremely important to follow all good practices to ensure the integrity and reliability of the evidence collected.

Processing iOS Devices for Digital Forensics

Amber Schroader, CEO & Founder Paraben Corporation

As Apple devices have soared in popularity, the frequency that they are involved in a digital forensic investigation has increased. These devices have remained high on personal information protection, causing them to be incapable of bypassing options without the licensing and purchase of specialized tools for bypass of encryption locks. Those technology items, that can be in the tens of thousands, can afford you options for processing. However, a locked device is not always a barrier and other options are available for imaging.

The imaging process for most iOS devices is logical imaging. Physical imaging of these devices is only available once a device has gone through the Jailbreak process. That process will unlock the limitations of the file system from access, and standard forensic tools can then image the device physically. For this workflow, the logical process and evaluation will be reviewed with common issues that can cause pitfalls to get a proper logical image.

First, let's start with a tool selection. As mentioned, there are specialized tools for unlocking devices, but most standard forensic tools will be able to do a logical image. In our workflow, the use of the Paraben E3 Forensic Platform will be doing the imaging example. Logical images can be made by the forensic tool itself or through the processing of an iTunes backup. Both methods to capture the data will yield the same data results.

With either method, the standard operating procedure for any version of iOS 12 and higher is to also do an encrypted backup to be able to capture more data. The encrypted backup that is done through either iTunes or your digital forensic tools allows for the collection of data known as Apple keychain data and can contain valuable insight into the device's location, and use. The encryption can be done with known passwords and, if done with a digital forensic tool, typically the password used is removed after the acquisition process is complete.

After plugging in the iOS device and opening the E3 Forensic Platform software, you will select the Acquire Device option from the E3 welcome screen. It is important to note that all iOS devices will automatically power on once they have been plugged in. Protection from signals should be maintained through proper Faraday equipment or using Airplane mode with manual turn off of the additional signal options such as Wi-Fi, Bluetooth, and NFC.

Tracking Usernames Across the Internet with Maigret

Jeff Minakata

What you should know...

- **A basic understanding of digital forensics.**

What you will learn...

- **How to install Maigret onto Linux (CSI Linux).**
- **How to scan a username along with verifying the results.**
- **How to install Maigret onto a Linux (CSI Linux) system.**

Do you need to find different sites that use a particular username? I have the perfect tool for you to use. In situations such as this, one of the programs that I turn to is Maigret. A fork of the popular tool Sherlock, Maigret has proven to be a valuable time saver that has helped me on several occasions when performing OSINT searches (also very useful for pentesting). In this article, I will be detailing how to install Maigret onto a Linux (CSI Linux) system (Debian, Mint, Tracelabs Linux, Kali Linux, etc., will all install the same way) and also show an example of scanning a username along with verifying the results.

Figure 1: Maigret logo

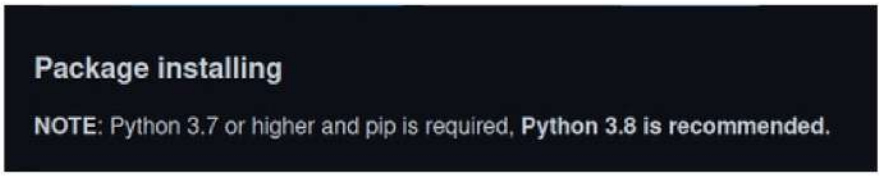


Figure 2: Python requirement

Before you begin, you will want to make sure that you have both Python 3.7 (or higher) and pip installed. If you are installing to CSI Linux, TraceLabx Linux, or the current version of Kali Linux, this should already be installed.

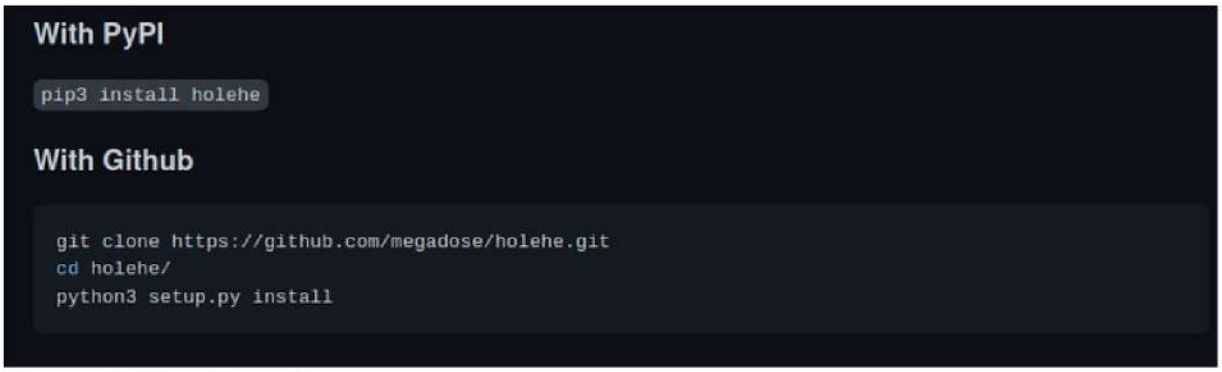


Figure 3: Github install instructions

For the installation, you can install it with PyPI (if installed) or through the git clone command (which we will be using for this tutorial). To check your version of Python, you can enter the following command in the terminal: *python --version and pip -- version*

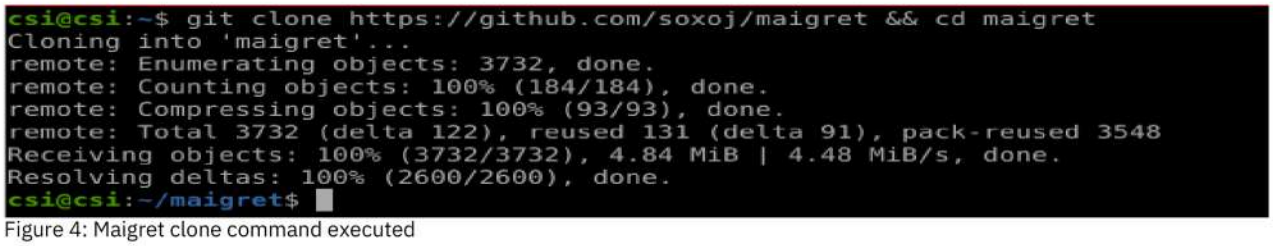


Figure 4: Maigret clone command executed

From the terminal, we want to clone the repo for Maigret. To do so, we can enter the following command in the terminal: git clone *https://github.com/soxoj/maigret* && cd maigret.

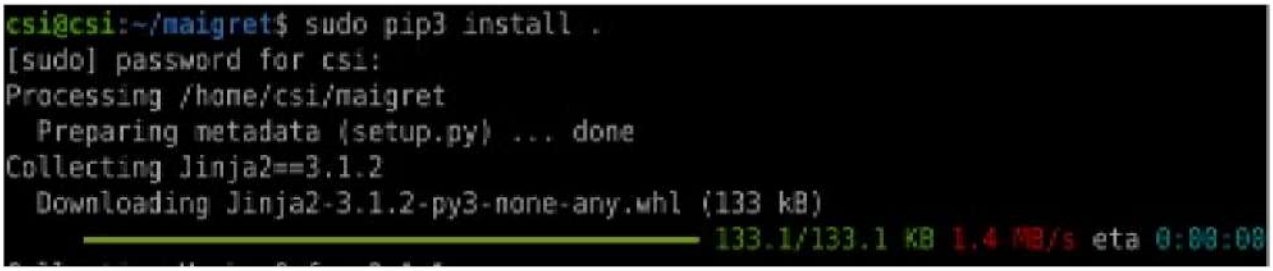


Figure 5: Installing Maigret

With the repository cloned and we are not in the maigret folder, it's time to install. The instructions on the page simply say to install, you can do a *pip3 install .* (do not forget the ***space*** "." in the command) command, however, I prefer using a sudo command when doing this. Using sudo during an install tends to avoid quirky install issues.

Figure 6: Using Maigret to find “snipersmurfdh”

After the program is installed, running the program is simple. In this example, we are searching for the username ***snipersmurfdh*** by entering the following command: **./maigret.py snipersmurfdh** we can just as easily search for any other user by entering ./**maigret.py** ***#the username of the target that we wish to search for***.

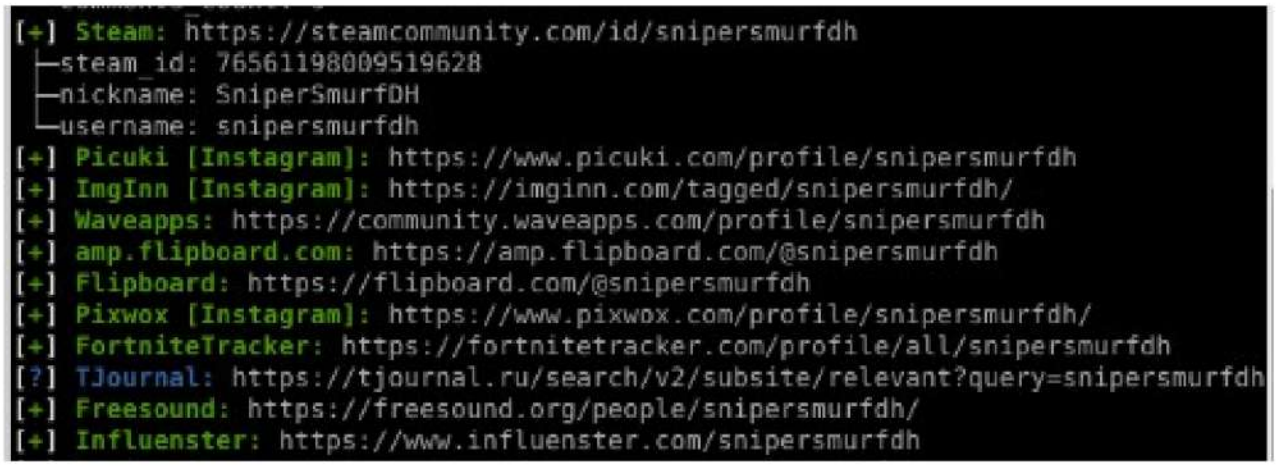


Figure 7: Initial search results

Maigret works surprisingly fast, searching through a number of sites for the username that we entered. In this example, we can see various potential matches to our search query highlighted in green with a + indicator, along with the site and link to the profile.

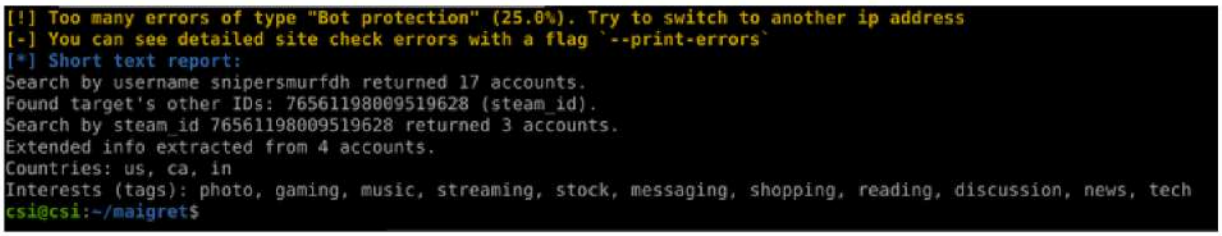


Figure 8: Additional information found

At the bottom of the Maigret results, we can see additional information including the number of extracted accounts, potential countries, and interest tags, all of which can be excellent information when profiling and learning about your target.

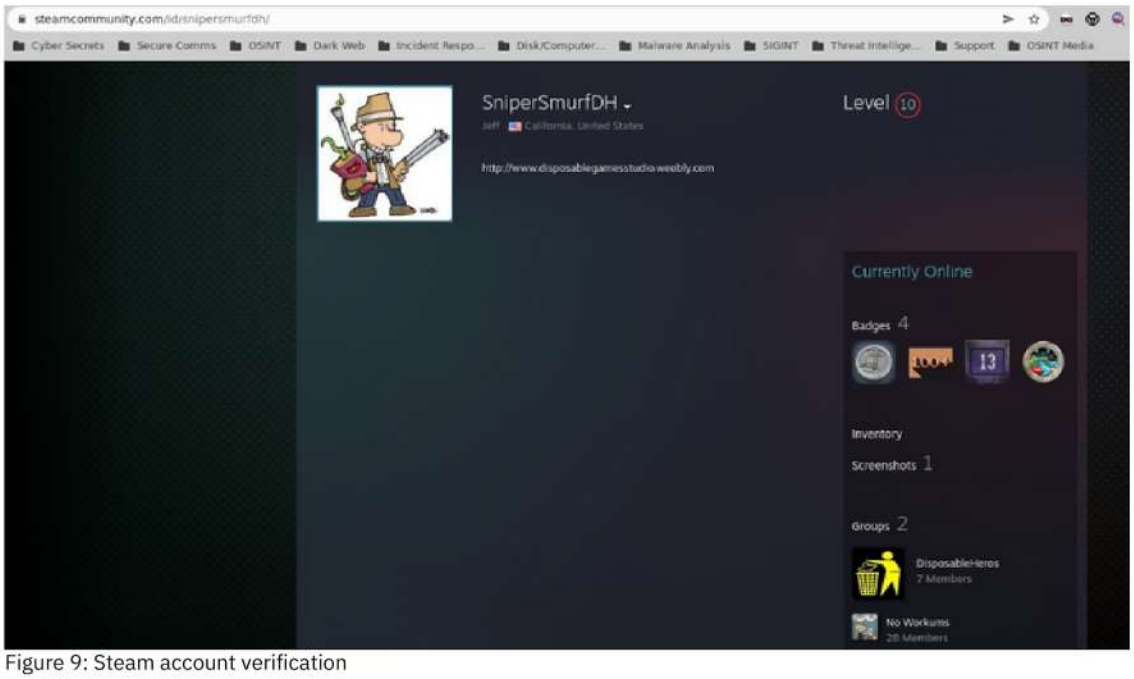


Figure 9: Steam account verification

As with any tool, it's always important to verify the results that are returned. In this example, we have a return for Steam along with the steam ID, so this is likely an accurate find. We still verify by navigating to the URL that Maigret has found; in this case, we do indeed have a positive match for Steam by correctly navigating to their Steam page. Having this confirmed information not only allows us to build a much clearer profile on our target, but also allows us to take this information and (for example) see if their accounts are part of any data breaches. From the data breach, we can take the password hash and see where else that password has been used, etc.

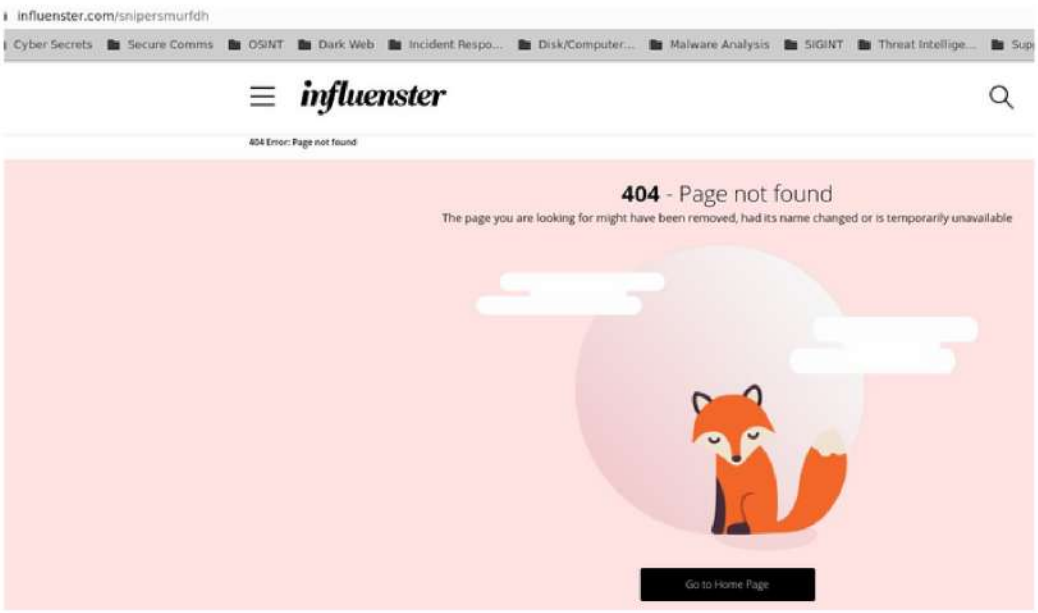


Figure 10: Influenster verification (false positive)

We also have a return for influenster, as we can see here that page has a 404 error, which indicates that this is either a false positive or the user has deleted their account here. We could potentially go a step farther by entering the URL into the Internet Archive and see if there is indeed a cached page, however, this is correctly a false positive in this case (I never made an account here). This is why it's always important to check your results.

Conclusion

Being able to quickly associate network accounts to a username is an incredible asset to a wide variety of roles allowing us to track users, unmask people, find potential security issues and more. To this end, Maigret shows that it can be a very easy to use and quick way to locate potential accounts scattered across the internet with a single, powerful command.

On the Web:

https://github.com/soxoj/maigret/blob/main/README.md https://archive.org/

About the Author

Trained in CEH8 and CEH9, CISP, Metasploit certified, Accredited Configuration Engineer (ACE), MCSI OSINT Practitioner, MCSI OSINT Practitioner, and CWA certified. Over 22 years' experience in the IT industry. Online instructor for OSINT, ethical hacking, and network security. Has contracted courses for EC-Council and has written articles for Hakin9 and eForensics magazine. To contact the author: *keyboardkomando@tutanota.com*

SOCMINT WITH SHERLOCK

Gabriel Sousa Carvalhaes

What you should know...

- **Basic knowledge of digital forensics tools.**

What you will learn...

- **How to use Sherlock.**
- **Google Cloud Shell.**

Social Media Intelligence (SOCMINT) is a type of Open-Source Intelligence (OSINT) focused on finding publicly available information on social websites. In other words, SOCMINT techniques can track the data that travels through social media. Therefore, it is important to understand that one of the best ways to gather information on social media is to keep track of accounts, and it is possible to do that through searching of usernames. Michael Bazzell, an OSINT expert who has worked for years on criminal investigations for the FBI task force, describes this process best in his book “Open-Source Intelligence Techniques”:

XProCheck: When Necessity is the Mother of Reinvention

Israel Torres

What you will learn...

- **What XProCheck is and how it benefits a macOS user forensically to identify malware activity on their local systems.**

What you should know...

- **Basic usage of macOS and an understanding of malware.**

I love a good tool to help me get the information I need to complete the next step. I spend a lot of my time making my own tools as well as integrating other tools together and into my tools to help solve daily problems. To be good at this, you want to make sure you understand a number of things. Like, why was the tool built, what is the tool solving, and if there are other better tools to do the job - and if not, to start designing your own tool.

I personally don't like to rely on tools that I don't understand, which is often why I create my own tools from scratch or sometimes reverse engineer tools that don't have documentation so I can complement or supplement those tools with mine. In this specific case, I got to see this tool come to fruition and see it grow early on and always get excited when I see an update. Especially because it saves me a lot of time in having to write my own!

We'll be going over a new tool named XProCheck that gets better with each version and is being actively worked on, and rapidly. The awesome part about this tool is that it encapsulates another tool named Apple XProtect Remediator (formerly XProtect) that is embedded in the macOS system and pretty much undocumented by most standards to the public.

This means that at any time, something can change internally at Apple; say their developers decide to change their mind on something, and then change it without advertisement and bang, the tool (XProCheck) that works with the internal tool (Apple XProtect Remediator) is now broken until the developer (Howard Oakley) can poke and prod to get their tool working again.

Catching Phish with Splunk Stream

Thomas Mitchell

A network tap or span port can be used with Splunk Stream to monitor network traffic. The Splunk Stream tool acts as a network protocol "sniffer". By using the user-friendly GUI interface, you can select individual metadata fields specific to a network protocol object and add them to your Splunk indexers. It is easy now to capture all kinds of useful metadata through Splunk Stream and even limited full packet capture. SS can be used to capture DNS, DHCP, HTTP transactions, database queries, emails, and more.

Overview

This white paper provides an overview of what is required to deploy, configure, and manage Splunk Stream in a distributed environment. A deployment can consist of many Splunk Universal Forwarders running on endpoints throughout the environment. When the first Splunk Stream Technology Add-On (TA) is first installed from the central deployment server, the SS configuration is pulled from the central Splunk Stream server. You can run two Splunk roles on the same host - Deployment Server and Splunk Stream Server. This document covers common steps and requirements. Splunk Stream enables the capture, filtering, indexing, and analysis of streams of network event data.

A "stream" is a continuous flow of network events, such as network protocol and metadata attributes.

With the addition of logs, metrics, and other information, the stream flow enables you to capture and extract valuable data points. This will allow insight into network activities and determine if there is suspicious behavior across your network infrastructure landscape.

The SS usage looks like below:

- Phishing to passively capture live streams of network event data - Capture metadata and full packet streams for multiple network protocols
- Capture NetFlow protocol data
- Applying aggregation methods for statistical analysis of event data

eForensics Magazine

Editor-in-Chief
Joanna Kretowicz *joanna.kretowicz@eforensicsmag.com*

Managing Editor
Ewa Dudzic *ewa.dudzic@eforensicsmag.com*

Editors
Bartek Adach *bartek.adach@pentestmag.com*
Agata Staszelis *agata.staszelis@hakin9.org*

Reviewers
David Michaud, Gabriel Carvalhaes, Ranjitha R, J Sc, Davide Gabrini, Hammad Arshed, Jan-Tilo Kirchhoff, Dauda Sule, Yousuf Zubairi, Alex Giles

Senior Consultant/Publisher
PawełMarciniak

CEO
Joanna Kretowicz *joanna.kretowicz@eforensicsmag.com*

Marketing Director
Joanna Kretowicz *joanna.kretowicz@eforensicsmag.com*

Cover Design
Hiep Nguyen Duc

Publisher
Hakin9 Media Sp. z o.o.
02-511 Warszawa
ul. Bielawska 6/19
Phone: 1 917 338 3631
www.eforensicsmag.com

Upcoming

THE EDITORIAL SCHEDULE FOR THE NEXT 3 MONTHS LOOKS AS FOLLOWS:

CORPORATE FORENSIC INVESTIGATIONS

ADVANCED DIGITAL FORENSIC ANALYSIS

MOBILE DEVICE FORENSICS