PYTHON NATION

A PUBLICATION OF PYTHON FORENSICS

Fall 2019 www.Python-Forensics.org Issue #1

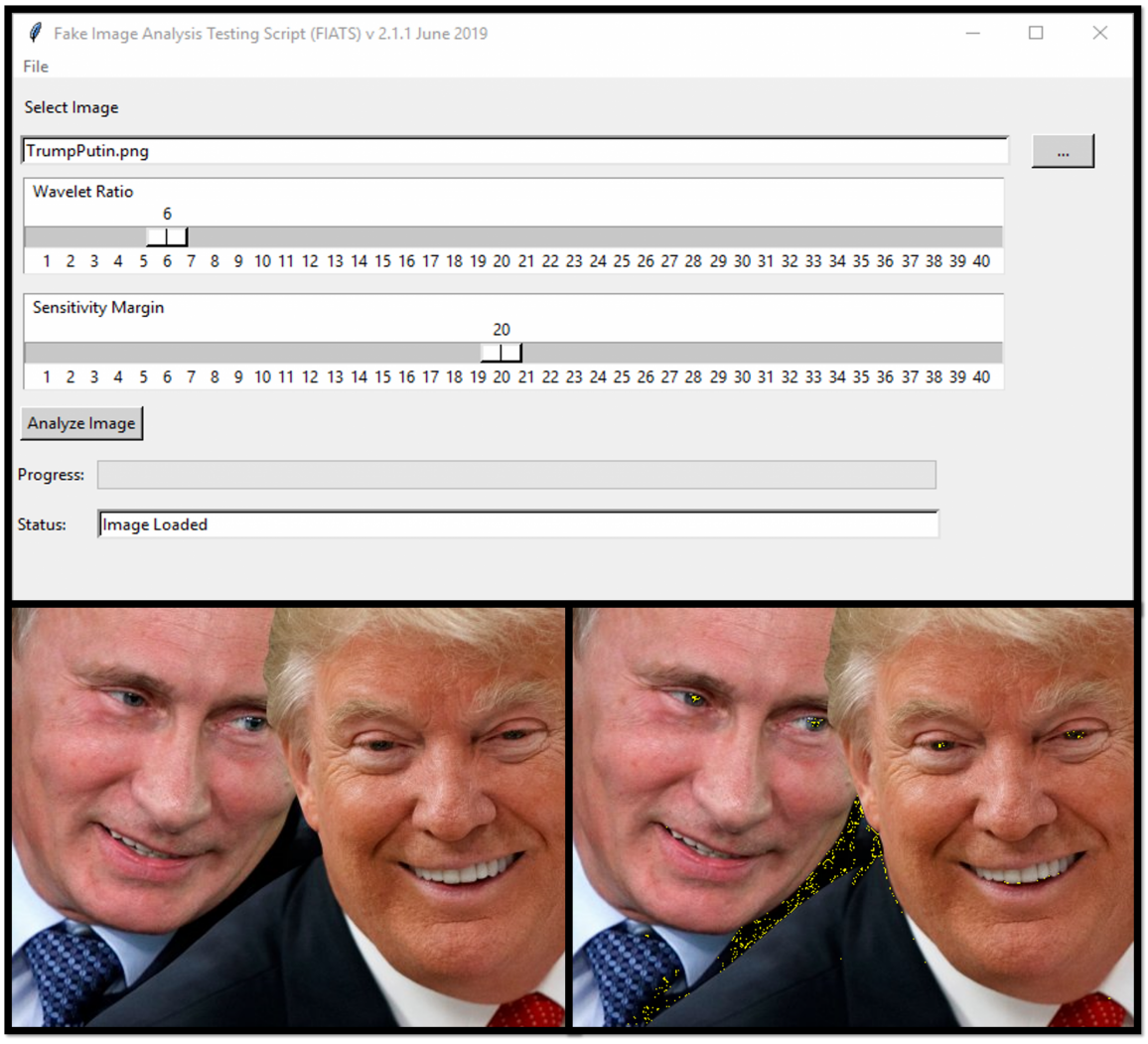
Investigating Fake Photos

The global impact resulting from the distribution of doctored digital photographs has reached epidemic proportions. These digitally altered photos are distributed via social media, news outlets, traditional web resources and are currently making their way into mainstream media. The impact these photos make can dramatically change the way people think, act, react, and believe - and can potentially cause harm. At the simplest level, they represent visual fraud.

To counter this threat, Python Forensics has been researching and developing new tools to examine and identify these fakes. The example shown here is an image depicting our Fake Image Analysis Testing Script (FIATS), which was written in Python. The technology is an outgrowth of the over two decades of work surrounding the detection and analysis of steganography within images and multimedia content.

Steganography *is the art of making slight changes to images, audio, video, and network protocols (typically referred to as the carrier) to conceal hidden content, or to covertly communicate information (typically referred to as the payload). Steganography differs from encryption where the goal of steganography is to hide the mere existence of hidden data or the message, while encryption is used to keep the content of the information private. Many steganography programs first encrypt the message content, then hide the data into the carrier, thus providing multiple layers of disguise.*

The methods and techniques used for fake photo identification differ, but rely on similar deep analysis of digital images.



The image on the left is the original fake image of President Trump and President Putin. The image on the right depicts the analysis and annotation delivered by FIATS. This shows the detection of where the photos were merged together. In addition, you can see the indications of the changes in President Putin's eyes. The algorithm is picking up the variations caused by the contacts that he wears to enhance the color. If you look closely at the image of President Trump, you can see the variations in his teeth which is caused by the caps that he wears to improve his appearance.

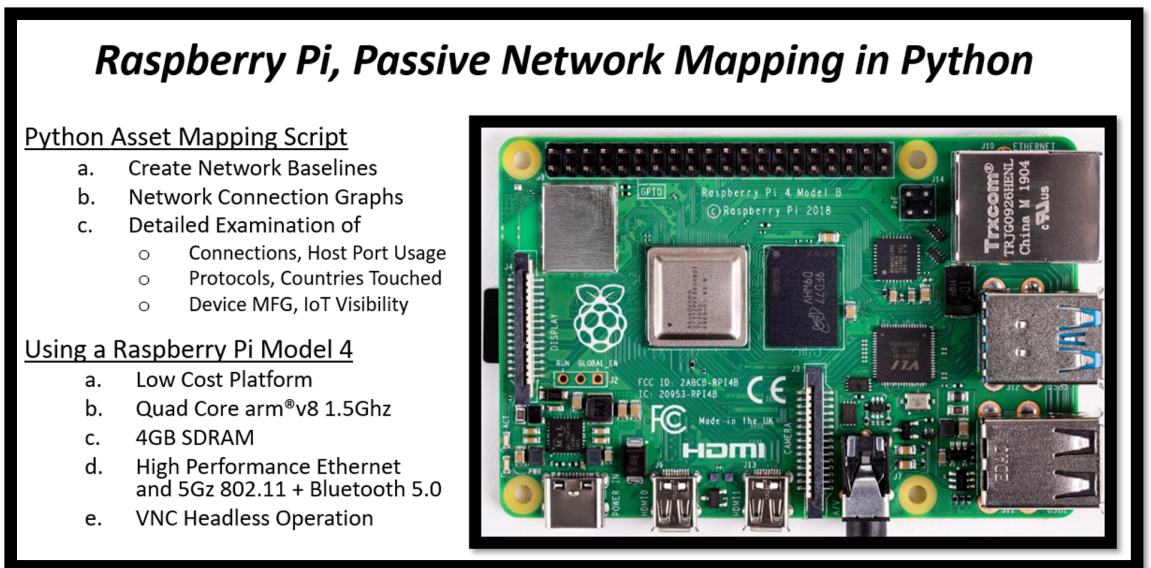
The application and continued research, development and use of this technology is an important step in combatting the proliferation of fakes and deep fakes throughout the Internet and social media.

If you would like to learn more about FIATS, Chet Hosmer, founder of Python Forensics will be presenting and demonstrating "Fake Photos" at the TechnoSecurity Conference in San Antonio, TX on Tuesday, Oct 1, 2019.

Techno Security & Digital Forensics Conference

Scan me

Passive Network Mapping in Python with Raspberry Pi



Mapping of network assets and their behaviors is a vital step that is needed for the prevention and response to cyber-attacks. Today, active tools like NMAP are used successfully to discover network assets. However, methods like NMAP are designed to only take a momentary snapshot of network devices, whereby the discovery of rogue devices, aberrant behavior, and emerging threats is only possible using passive network mapping.

It is becoming clear that the Internet of Things (IoT) and Industrial Control Systems (ICS) require special attention from a cyber security point of view. It is a well-known and documented fact that the protocols and implementations have vulnerabilities, when exploited, that can produce considerable damage and provide an avenue for the exfiltration of data.

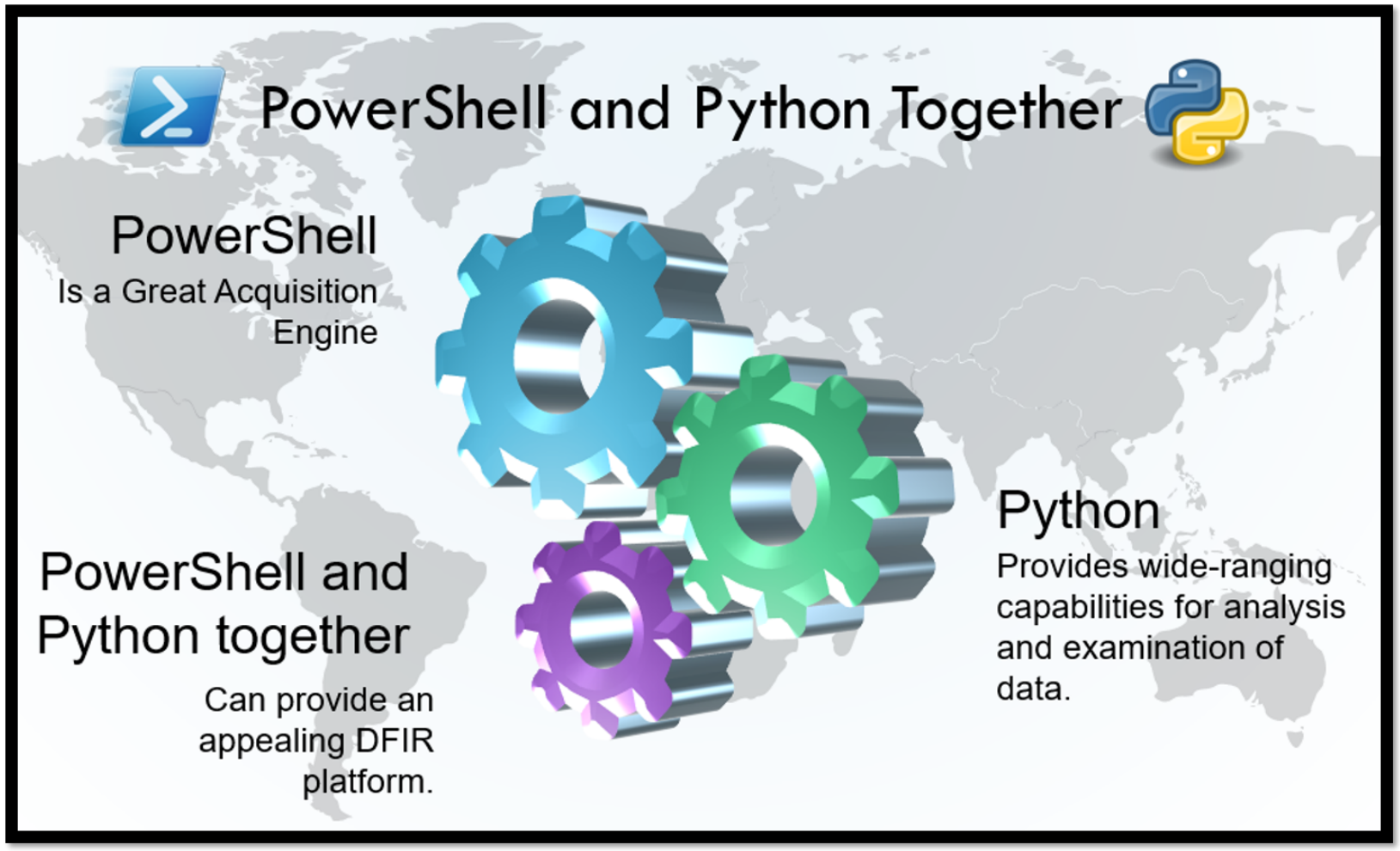
In addition, when taxed with examining these environments, due to the dynamic nature and/or critical infrastructure implications, active scanning or probing of the environment is either discouraged or ineffective. Thus, passive monitoring, (placement of the monitoring devices to provide visibility and coverage from both a wired and wireless point of view), offers insights into the behavior of the devices and the networks in which they operate. Of course there are vendor solutions offered today, however they often rely on expensive hardware and software solutions and may lack flexibility.

Using a Raspberry Pi and Open Source Python software to passively monitor, detect, baseline and provide insight into these behaviors have been called “crazy” by some. However, as you will see, the Raspberry Pi, with its multicore processor, and integrated wired and wireless network components, provides the basic underpinnings necessary for a lightweight IoT/ICS sensor with a cost of less than $50 USD. Couple that flexibility with an Open Source and extensible Python software solution that dynamically reduces and records the most pertinent observations, and you have a low cost, flexible and versatile PiSensor for IoT and ICS environments.

If you would like to learn more about Passive Network Mapping using a Raspberry Pi, Chet Hosmer, founder of Python Forensics, will be participating in a Raspberry Pi “*Build Day*” at the **PFIC Conference** on September 12, in Park City Utah.

Scan me

Integrating PowerShell and Python



PowerShell provides a great acquisition engine for obtaining a vast array of information from live systems, servers, peripherals, mobile devices and data driven applications like Active Directory. Because of Microsoft's decision to open PowerShell and provide the ability to acquire information from other non-Microsoft platforms such as Mac and Linux, the breadth of information that can be accessed is virtually limitless (of course, with the proper credentials). Combine that with a plethora of built-in and 3rd Party cmdlets (pronounced Command-let) that can be filtered, sorted and piped together you have the ultimate acquisition engine.

By adding a bridge from PowerShell to Python we can now leverage the rich analytical, machine learning and deep analysis to the raw information acquired by PowerShell.

The endeavor to integrate PowerShell and Python came about a couple years ago during a training for a large chemical company, while teaching the members of the SOC, (secure operations center), how to apply Python scripts during investigations and incident response. Subsequent trainings to the SOC were requested and provided! Based on this, it was quickly realized that PowerShell was great at acquisition of information across the enterprise, and Python was a perfect partner to perform analysis of data that had been acquired by other tools such as PowerShell.

PowerShell advocates will say that PowerShell scripts can be developed to perform detailed analysis. Likewise, Python advocates will say Python scripts can be developed to perform very capable evidence acquisition. Both advocates have a point. The real question is if we combine the best of both environments, does 1 + 1 = 2 or does 1 + 1 = 11? I believe that the answer falls somewhere in the middle.

If you would like to learn more about integrating PowerShell and Python during your investigations, Chet Hosmer is presenting and demonstrating PowerShell and Python Together at the PFIC Conference on September 11. He is also presenting at the HTCIA International Conference in Chicago on Monday, September 23, and Wednesday, September 25.

Want to learn more?

Scan me

Amazon Author Page

Chet Hosmer is the Founder of Python Forensics, Inc., a non-profit organization focused on the collaborative development of open source investigative technologies utilizing Python and other popular scripting languages. Chet has been researching and developing technologies and trainings surrounding forensics, digital investigation and steganography for multiple decades. He has made numerous appearances to discuss emerging cyber threats, including interviews on National Public Radio's Kojo Nnamdi show, ABC's Primetime Thursday, and ABC News Australia. He has also been a frequent contributor to technical and news stories relating to cyber security and forensics with the IEEE, The New York Times, The Washington Post, Government Computer News, Salon.com and Wired Magazine.

Chet has currently authored seven books which are used in classrooms worldwide, and hosts a podcast series at www.pythonnation.com.

FALL CONFERENCES

PFIC
9/10 – 9/12 · Park City, UT

HTCIA
9/22 – 9/25 · Chicago, IL

TechnoSecurity
9/30 – 10/1 · San Antonio, TX

special THANK YOU to our sponsors

paraben® corporation paraben.com