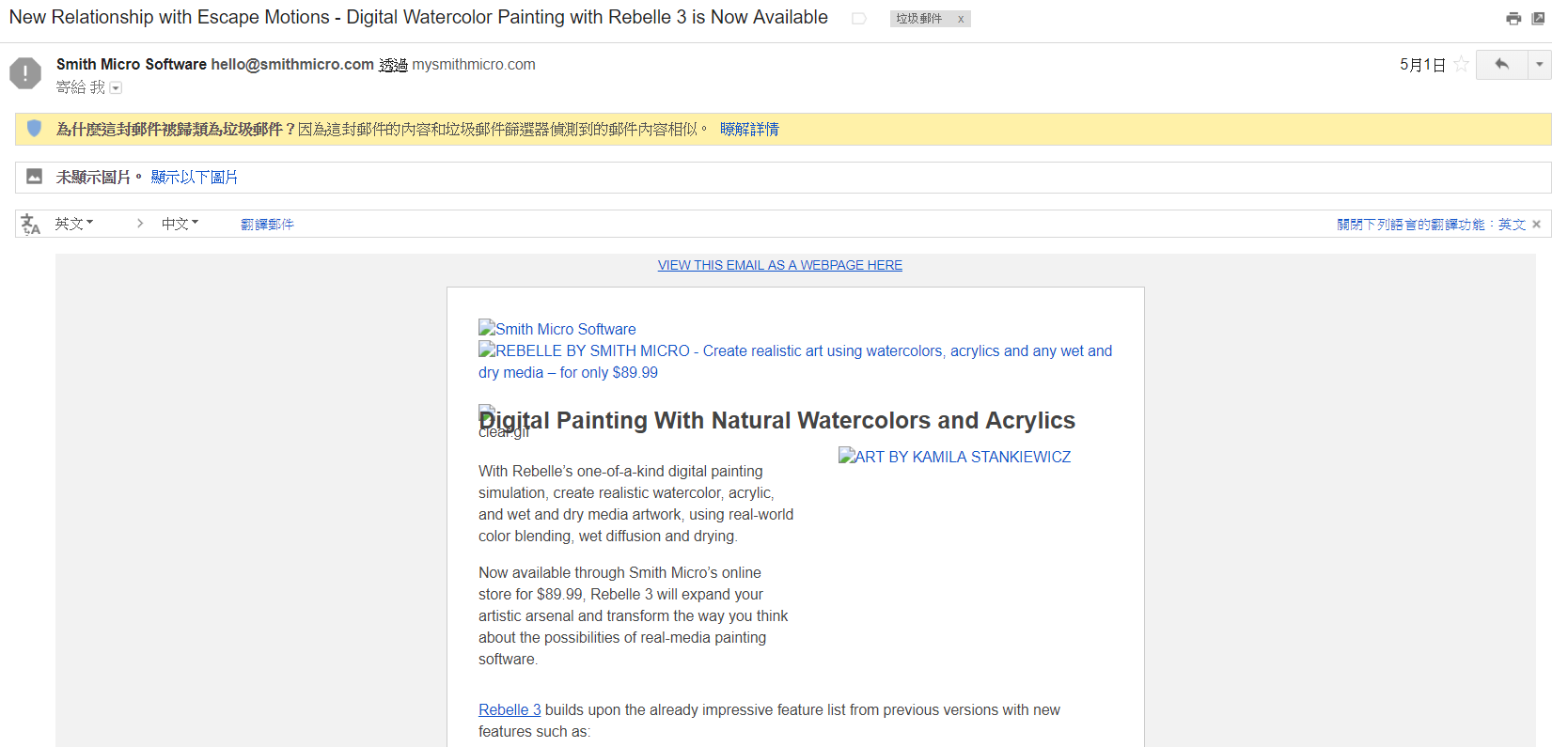
**HW03**

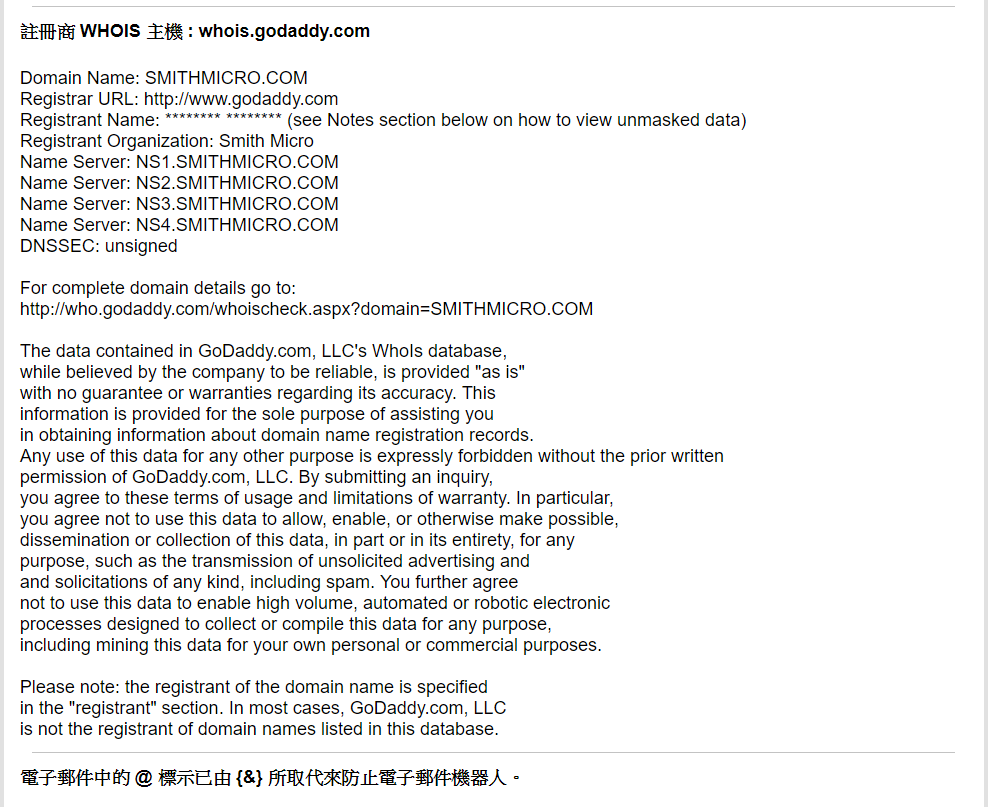
0516208-黃郁恬

1.

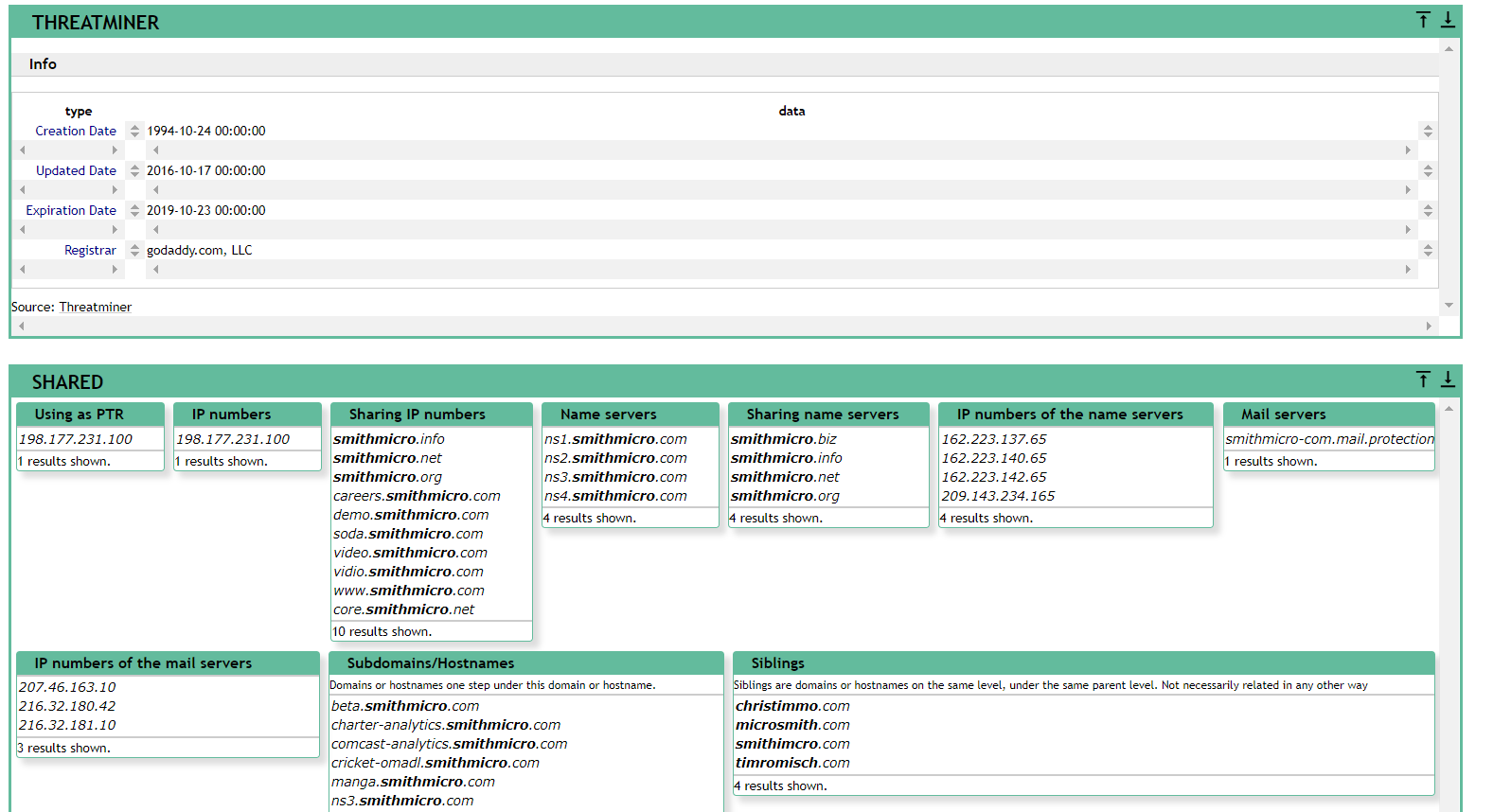
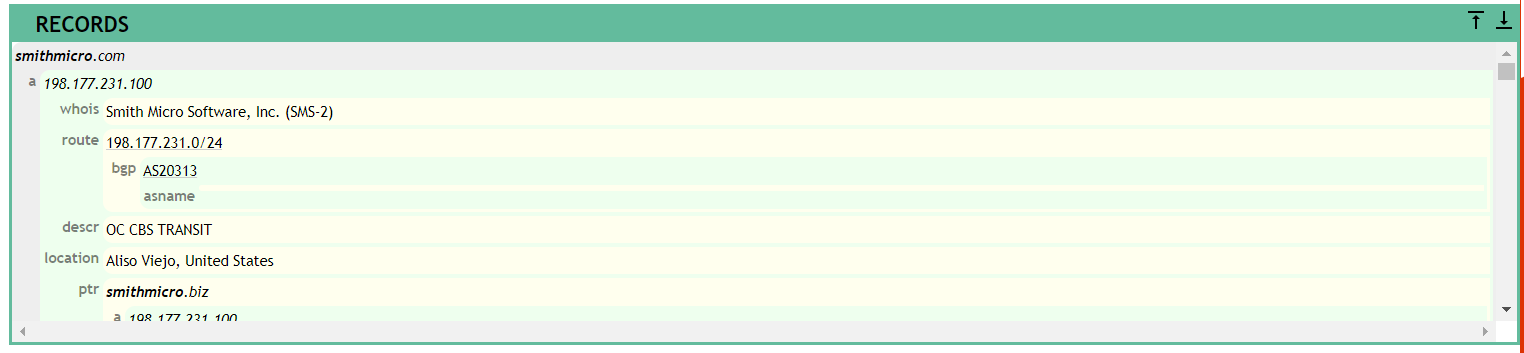
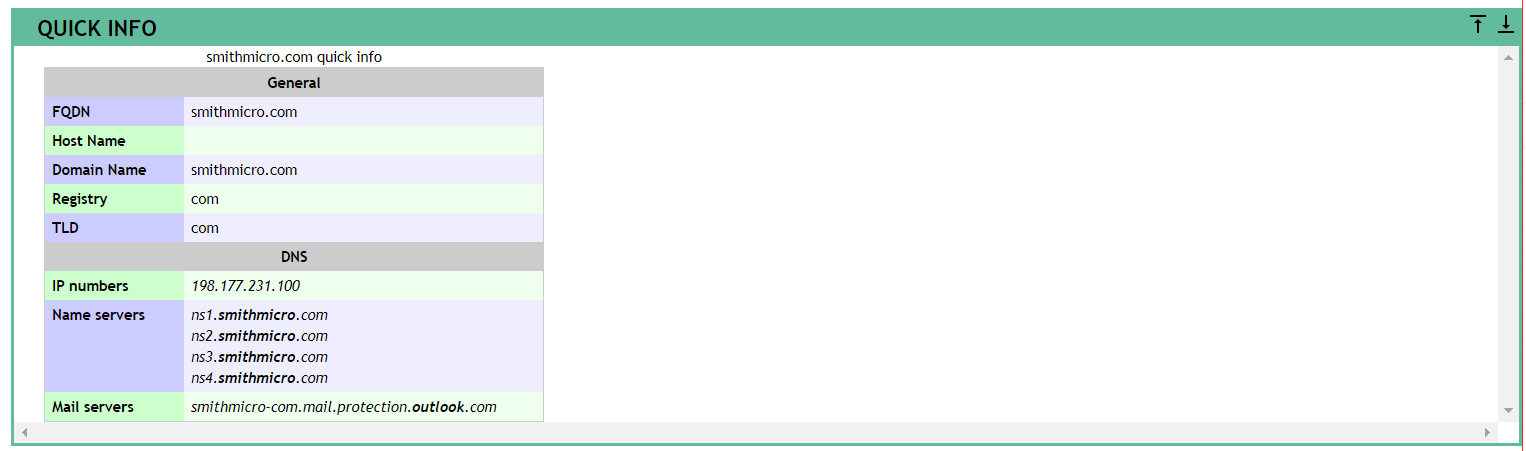
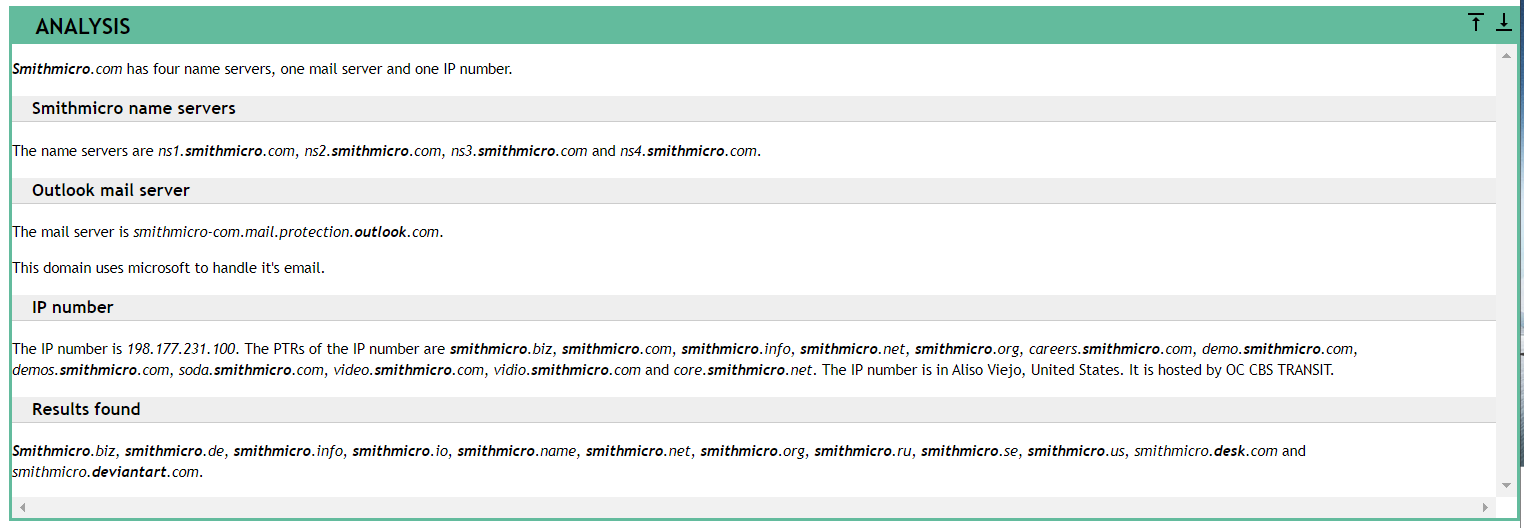
我從gmail垃圾郵件中挑選一封作為測試



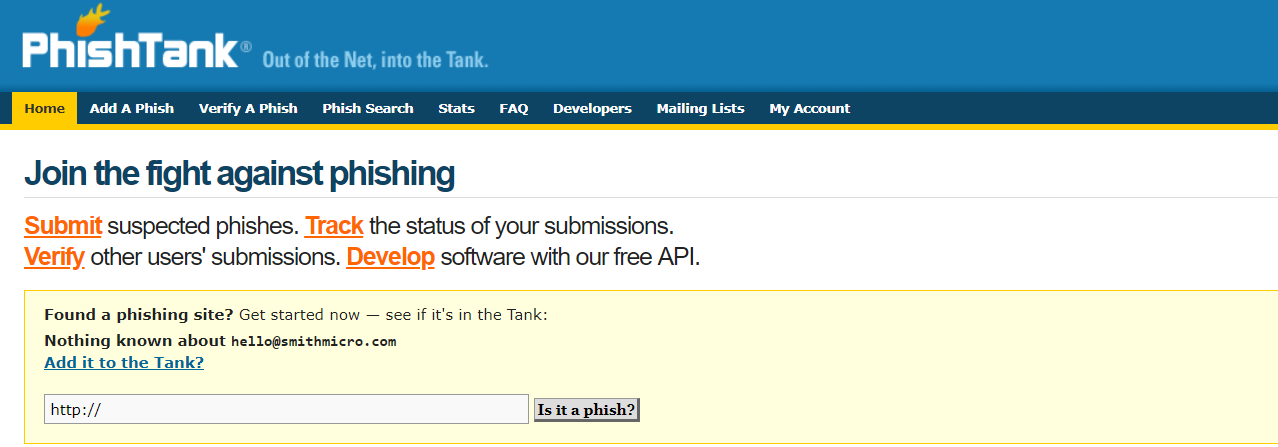
**WHOIS**



**Robtex**

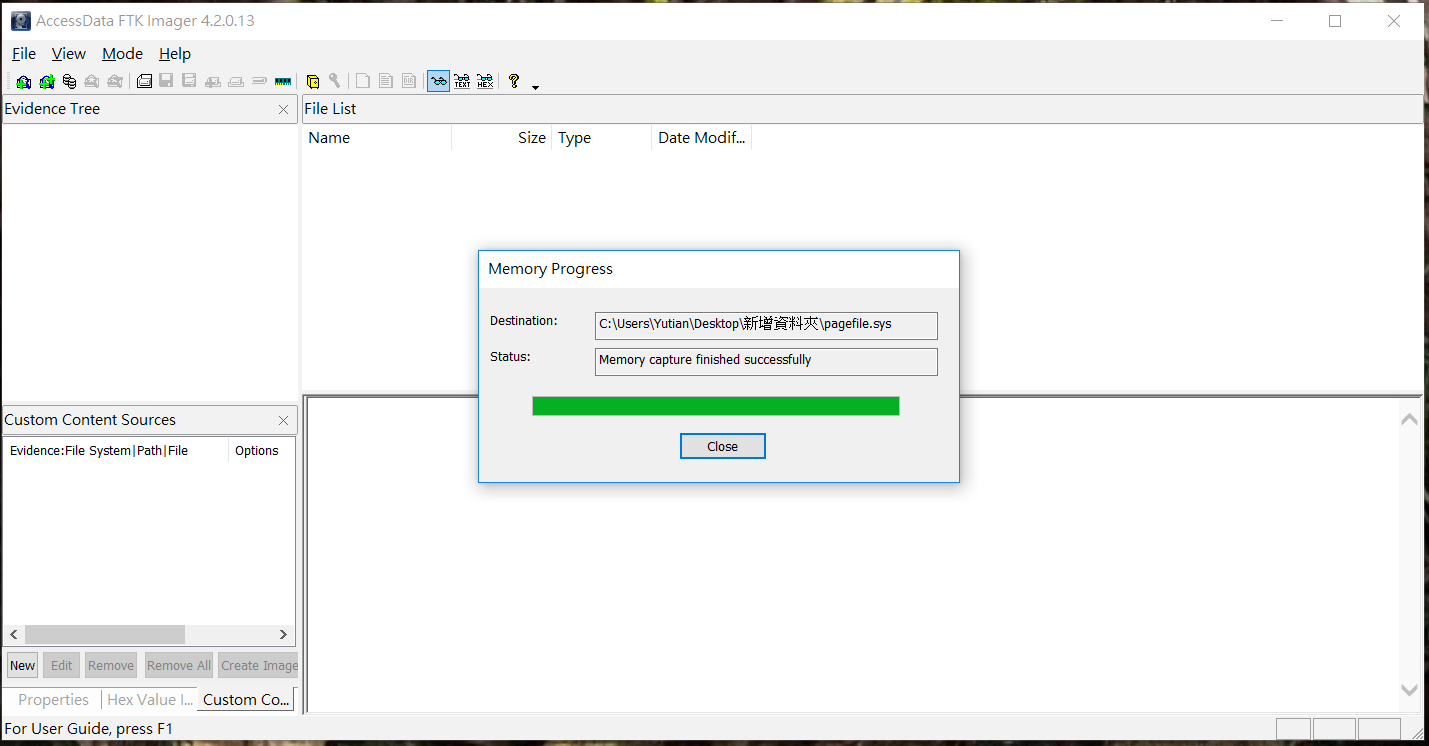


**PhishTank**

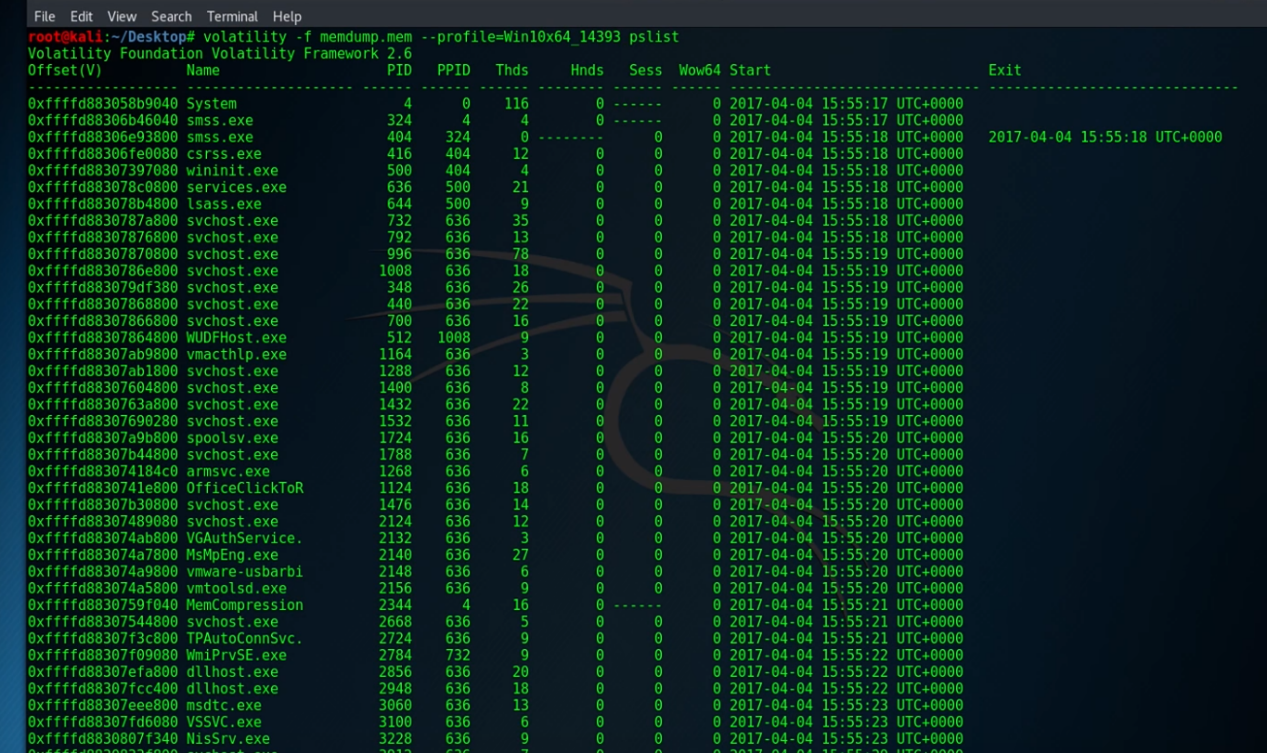


2.

use FTK Imager to dump memory(是把存在於記憶體中的資料寫在硬碟裡):



use Volatility Framework to analyze the memory dump:



3.

Poison Ivy: A Remote Access Tool (RAT) that is commonly leveraged by threat actors because it is free and easy to use.  It provides a quick and feature-rich platform for controlling a compromised system. And Poison Ivy is so widely used that security professionals have a harder time tracing attacks that use the RAT to any particular attacker

**FireEye Poison Ivy** 解碼器會檢查每個 TCP 工作階段的開端是否有 PIVY 詢問/回應序列。如果有，此模組會嘗試使用一或多個以引數形式提供的密碼來驗證回應。若要使用 FireEye ChopShop 模組，您必須安裝 CamCrypt，此為 Camellia 加密程式庫的開放原始碼實作所適用的 Python 包裝函式(大部分的 PIVY功能都涵蓋於此模組中)。

註：若 PIVY 流量未對應於任何提供的密碼，則無法解碼。所幸，萬一您遭到破壞的端點感染了PIVY或PIVY伺服器程式碼，您將可輕易找出自訂 PIVY 密碼。

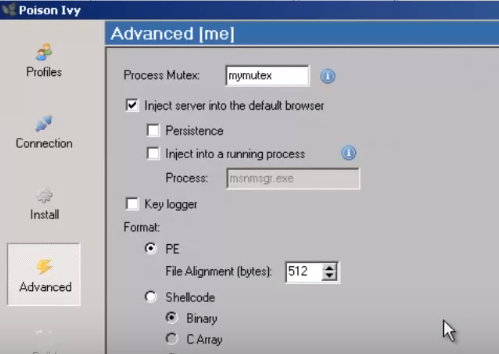
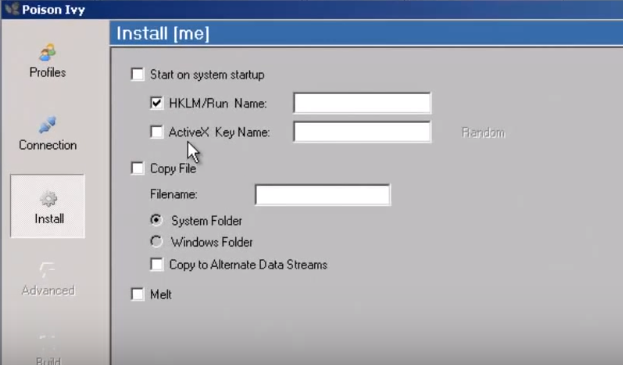
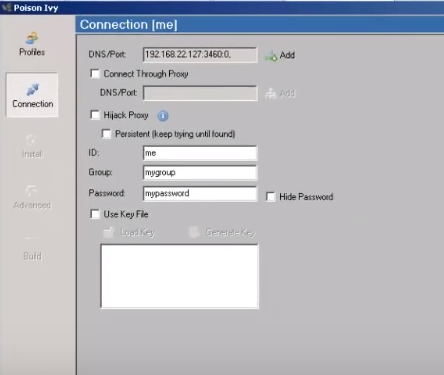
🡪 使用 **Calamine PyCommand 指令碼**找出 PIVY 密碼

有許多攻擊者會保留預設密碼“admin＂。在此情況下，您將可立即開始使用此解碼器。然而，攻擊者通常會選擇建立唯一密碼，以強化安全性。但只要能存取受PIVY感染的端點或PIVY伺服器執行檔，就能輕易擷取到密碼。

(可以透過多種方式擷取密碼，視您的環境與偏好而定)

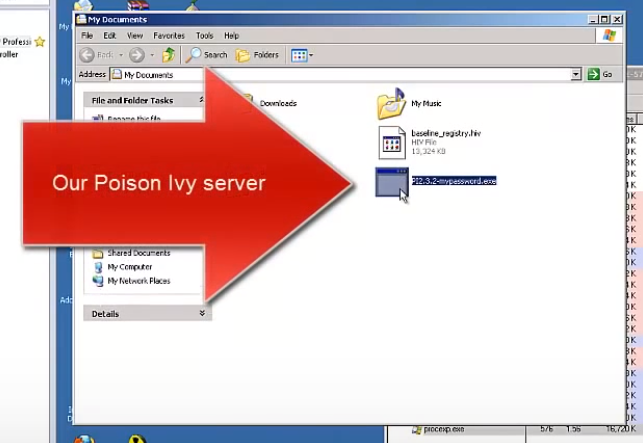
🡪

Reference: <https://www.youtube.com/watch?v=jL6nc14_NO8>

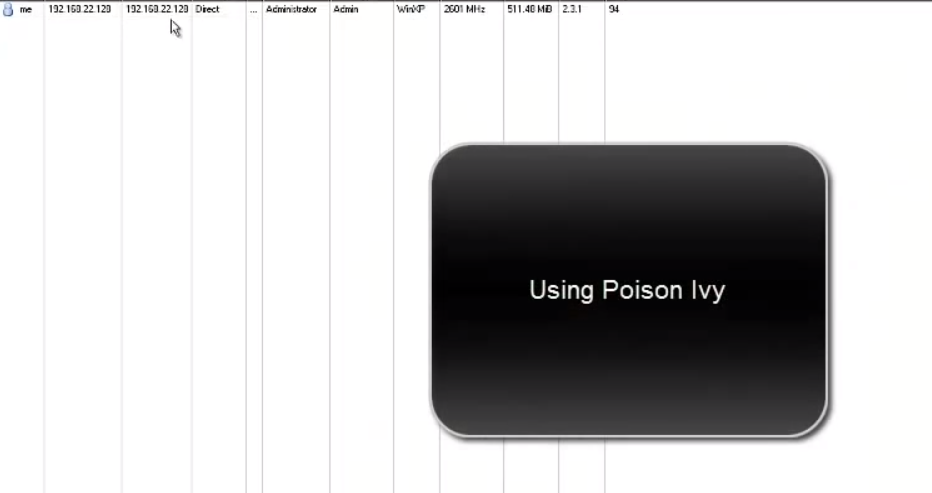


Deliver server to victom

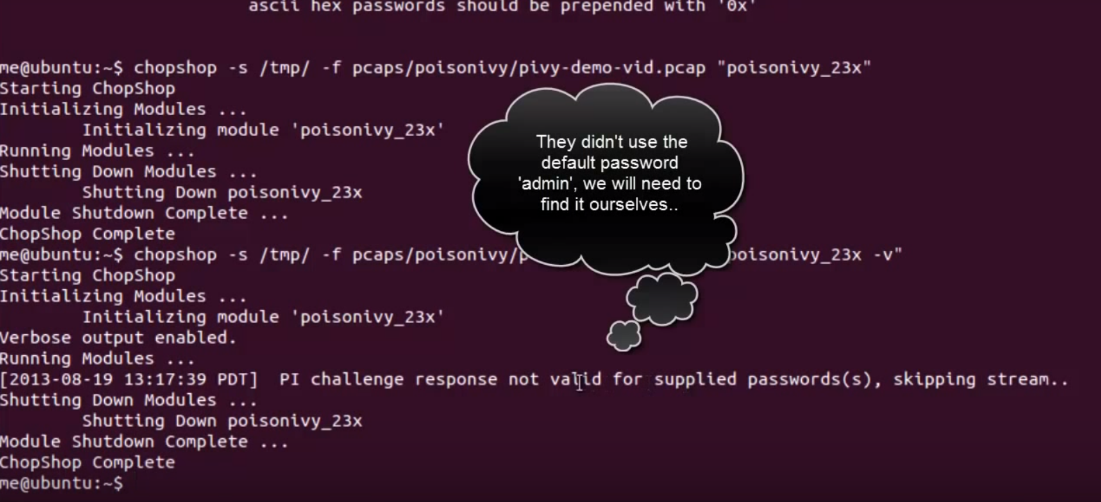
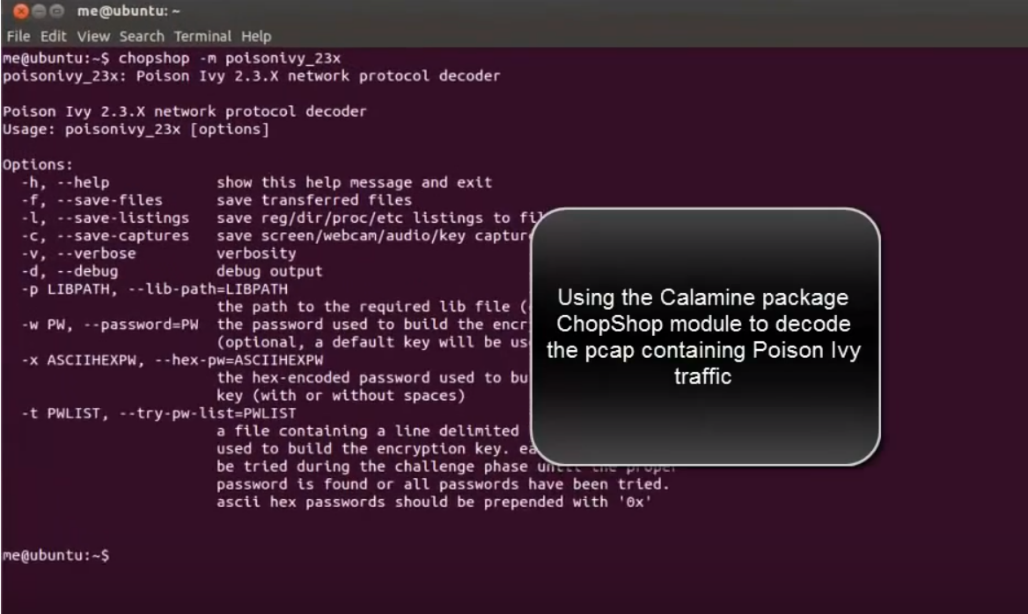
The following is the poison IVY server



Using poison IVY

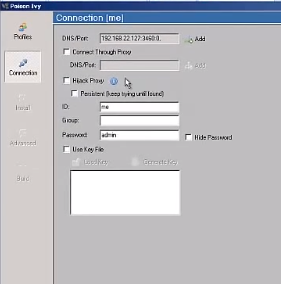
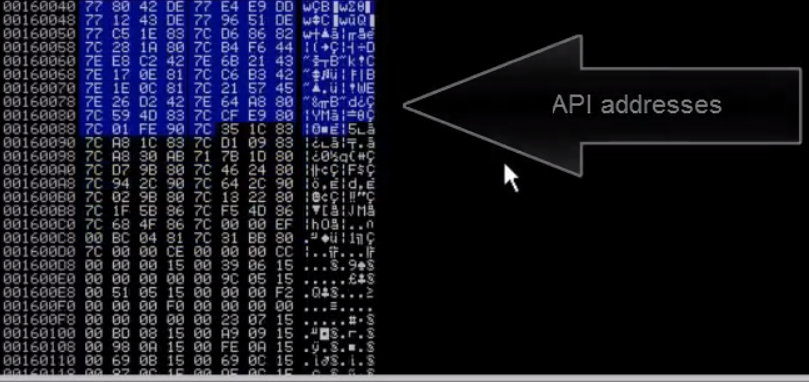


Using the Calamine package ChopShop module to decode the pcap containing Poison Ivy traffic.



Using the Calamine package PyCommand to dump the Poison Ivy configuration details.

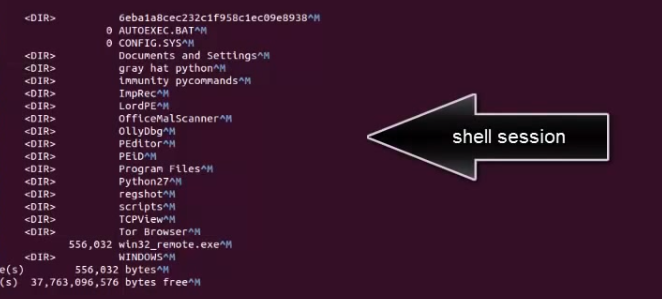
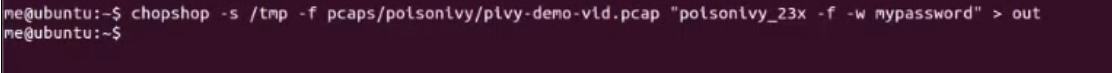
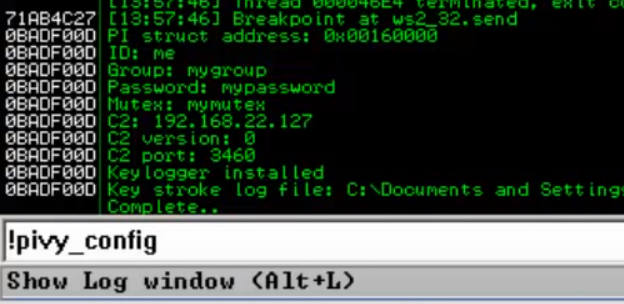
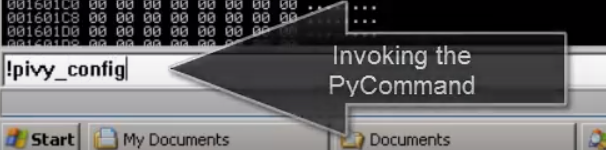
API addresses:



Password:

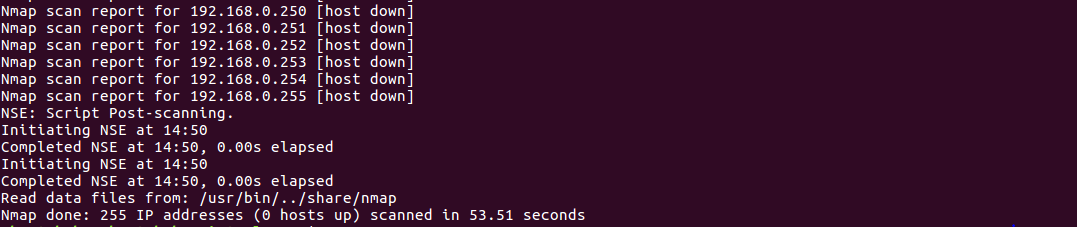
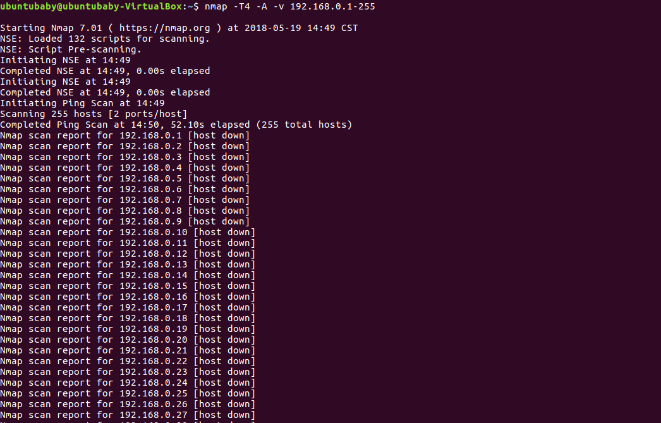


Invoking the Pycommand:



4.

Nmap:



NTA Monitor:

IKEProbe:

5.

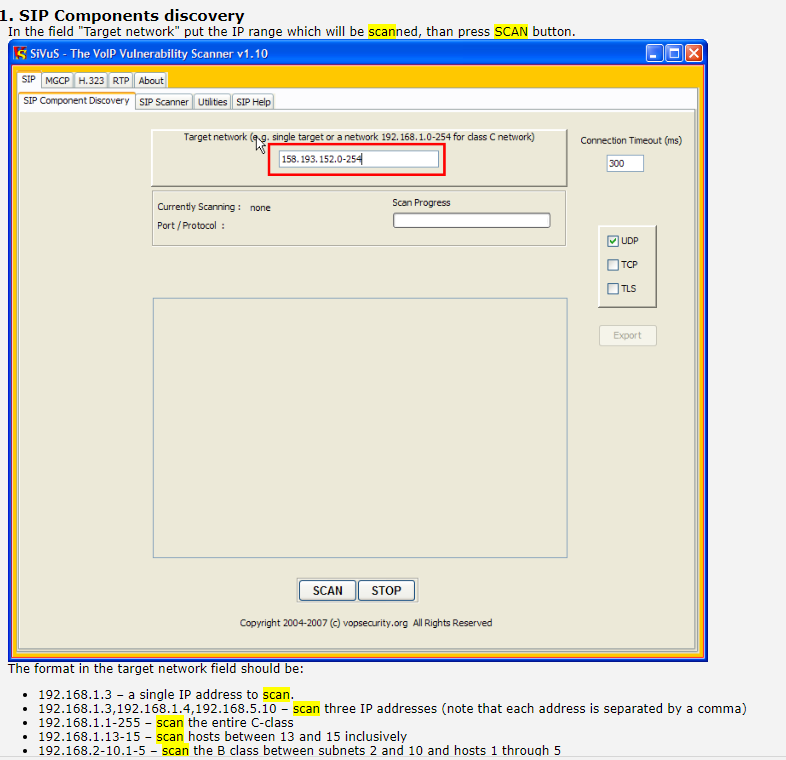
Because SiVuS and SIPVicious are too old to download, I do not download and test it.

But I can list their usages and explain:

**SiVus**

Reference: <http://nil.uniza.sk/sip/tools/sivus-voip-vulnerability-scanner>

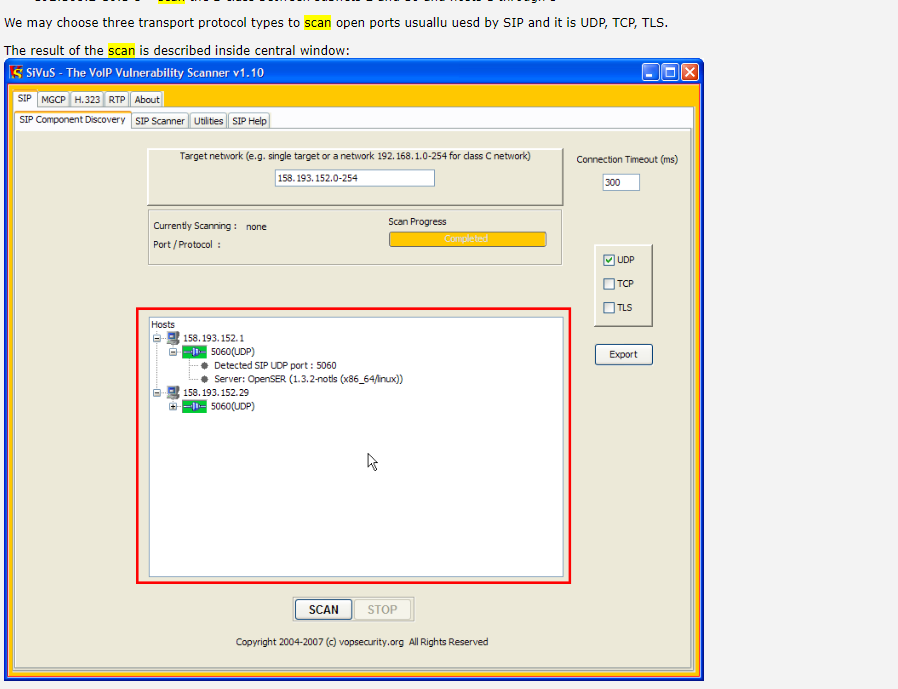
1. SIP Components discovery



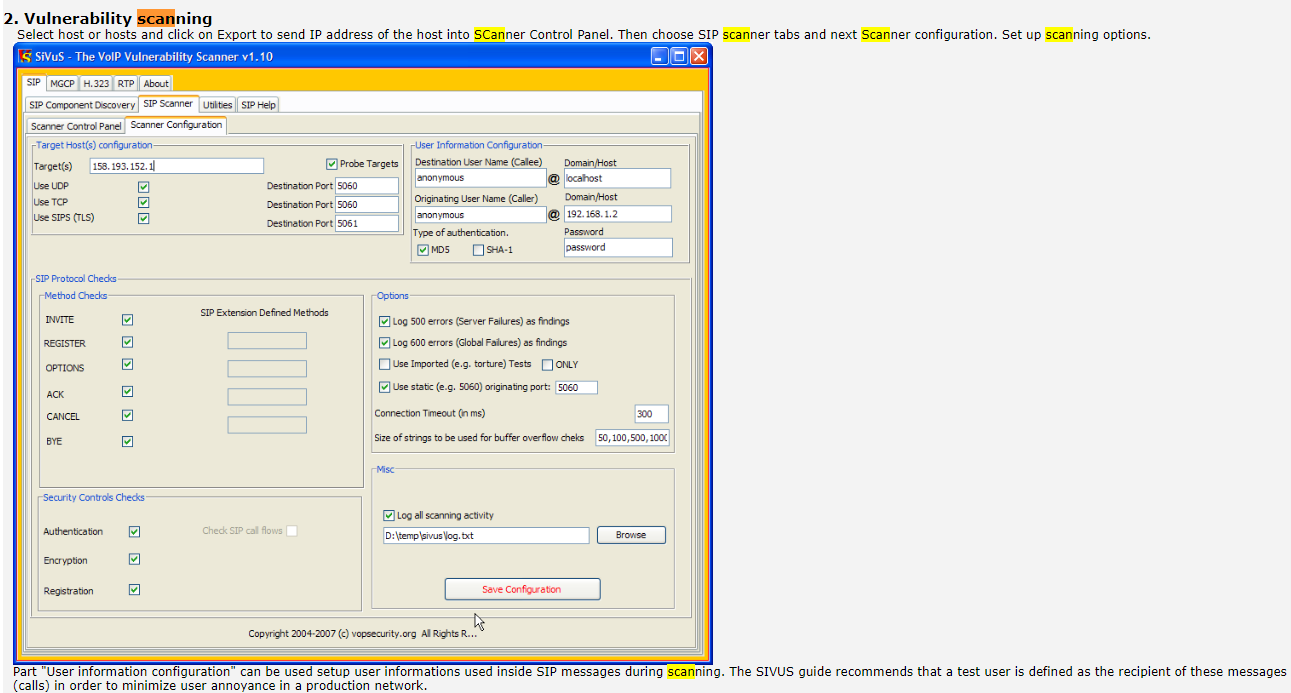
The format in the target network field should be:

* 192.168.1.3 – a single IP address to scan.
* 192.168.1.3,192.168.1.4,192.168.5.10 – scan three IP addresses (note that each address is separated by a comma)
* 192.168.1.1-255 – scan the entire C-class
* 192.168.1.13-15 – scan hosts between 13 and 15 inclusively
* 192.168.2-10.1-5 – scan the B class between subnets 2 and 10 and hosts 1 through 5
* We may choose three transport protocol types to scan open ports usually used by SIP and it is UDP, TCP, TLS.

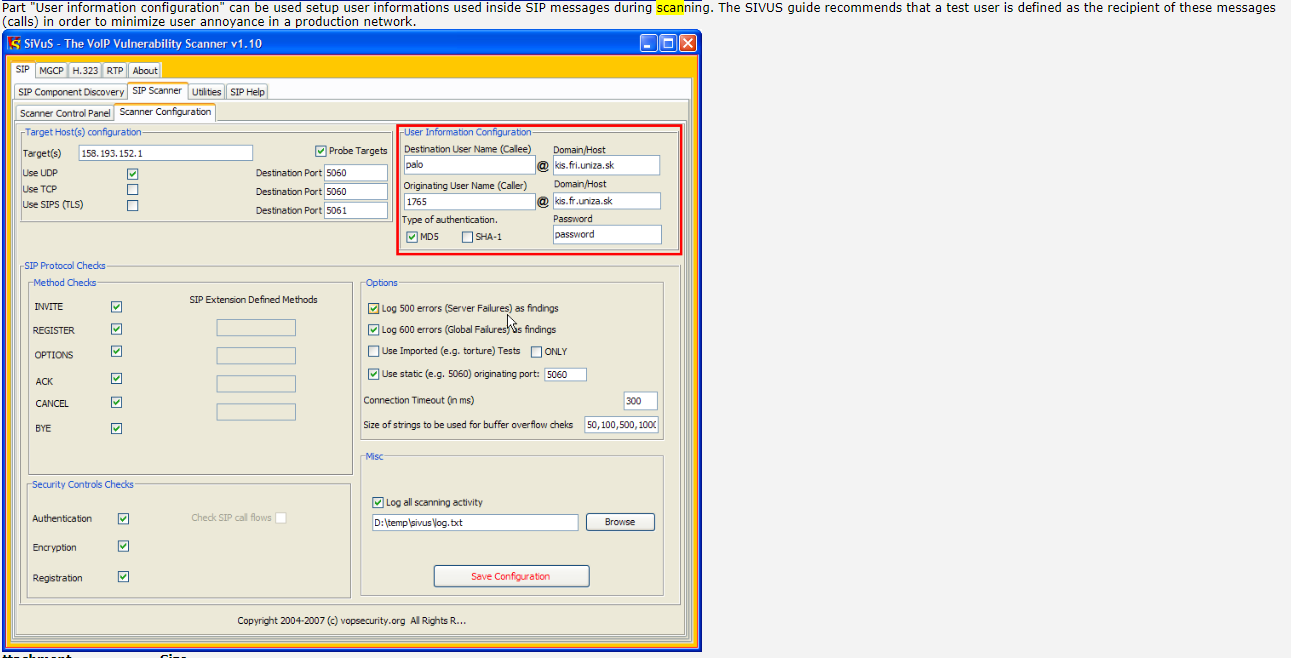
The result of the scan is described inside central window:



1. Vulnerability scanning



The "User information configuration" part can be used to setup user information which is used inside SIP messages while scanning. The SIVUS guide recommends that a test user is defined as the recipient of these messages (calls) to minimize users’ annoyance in a production network.



**SIPVicious**

Reference: <https://www.aldeid.com/wiki/SIPVicious/svmap>

svmap – Lists SIP devices found on an IP range

* Usage: svmap [options] host1 host2 hostrange
* Scans for SIP devices on a given network

Example:

