

# Opdracht Security Advanced – Blue Teaming aspect: Vulnerability Analysis / Forensics

## Inhoud

<b>Level C requirements .....</b>	2
Voorbereiding .....	2
Installeren VM met Kali.....	2
Installeren Nessus Essentials op Kali.....	2
Installeren van nmap op Kali.....	2
Installeren van OWASP ZAP op Kali .....	3
Downloaden en installeren van 2 VMs: SimpleWin en Server16 .....	3
Scanning en Analyses.....	4
Scan en analyse targets met Nessus.....	4
Scan targets en analyse met nmap .....	9
Scan en analyse targets met OWASP ZAP .....	13
<b>Level B requirements .....</b>	15
Voorbereiding .....	15
Download Volatility source code van github .....	15
Scanning van de dump van het werkgeheugen.....	15
Profile finding.....	15
Process Listing.....	16
Andere nuttige commands .....	18
Analyse van de dump van het werkgeheugen .....	18
Opdracht 1: Recover het windows wachtwoord .....	18
Opdracht 2 : Vind ‘important.rar’ en toon de inhoud .....	20
Opdracht 3: Terughalen tekening MSPaint.....	23
<b>Level A(+) requirements .....</b>	27
Voorbereiding .....	27
Installeren Autopsy op Kali .....	27
Start nieuwe Autopsy Case .....	27
Analyse.....	34
Onderzoeken van Discord .....	35
Onderzoek van deleted files in the Recycle bin.....	36
Onderzoek naar “cloud”-toepassingen.....	37

## Level C requirements

## Voorbereiding

## Installeren VM met Kali

## Download van Kali voor VMWare via

<https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>

Run Virtual machine and type in terminal:

> sudo passwd (to change)

> su - (to activate root)

## Installeren Nessus Essentials op Kali

Download Nessus Essentials van <https://www.tenable.com/downloads/nessus?loginAttempted=true>  
(in dit geval de versie voor Debian 9, 10 / Kali Linux 1, 2017.3, 2018, 2019, 2020 AMD64 )

```
>sudo apt install Nessus-8.14.0-debian6_amd64.deb
```

> /bin/systemctl start nessusd.service (om de Nessus Scanner te starten)

Dan via de webbrowser naar <https://kali:8834/> om de activatiecode en dergelijke in te kunnen geven (verkregen via studentenregistratie op <https://www.tenable.com/tenable-for-education/nessus-essentials?edu=true>)

## Installeer nmap op Kali

Installatie was al gebeurd in de VM gedownload van Offensive Security.

Nmap is the most powerful network mapping tool.

Nmap komt met een GUI, Zenmap genaamd. Deze is niet standaard geïnstalleerd in onze Kali.

#### **Procedure:**

Download zenmap van <https://nmap.org/download.html>

Installeer Alien om het redhat package om te zetten in een Debian package file

> sudo apt-get install alien

```
Converteer file zenmap-7.91-1.noarch.rpm  
>sudo alien zenmap*.rpm  
zenmap_7.91-2_all.deb generated  
Installeer zenmap  
>sudo dpkg -i zenmap*.deb  
Zenmap gebruikt Python GTK als GUI => afhalen package  
>wget http://archive.ubuntu.com/ubuntu/pool/universe/p/pygtk/python-gtk2\_2.24.0-5.1ubuntu2\_amd64.deb  
Installeren Python GTK  
>sudo apt install ./python-gtk2_2.24.0-5.1ubuntu2_amd64.deb  
Start zenmap GUI (met elevated rights)  
>sudo zenmap
```

#### Installeren van OWASP ZAP op Kali

Installatie was al gebeurd in de VM gedownload van Offensive Security => versie 2.10.0

Downloaden en installeren van 2 VMs: SimpleWin en Server16

Importeren met Network connection Bridged, zodat iedere VM zijn eigen IP-Adres krijgt.

## Scanning en Analyses

### Scan en analyse targets met Nessus

Werkwijze gebaseerd op PluralSight courses:

<https://app.pluralsight.com/library/courses/nessus-vulnerability-analysis/table-of-contents>

<https://app.pluralsight.com/library/courses/discover-network-weaknesses-nessus/table-of-contents>

#### Scan

1. Start Nessus in een browser via <https://kali:8834>
2. Insert hostnames to scan (IP addresses gevonden via een snelle nmap scan)

Welcome to Nessus Essentials ×

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

**Targets**

192.168.1.27, 192.168.1.57

Close Submit

My Host Discovery Scan Results ×

Nessus found the following hosts listed below from your list of targets (192.168.1.27, 192.168.1.57).

To launch your first basic network scan, select the hosts you want to scan. These hosts count towards the 16 host limit on your license.

<input type="checkbox"/> IP	DNS
<input type="checkbox"/> 192.168.1.27	Jon-PC.lan
<input type="checkbox"/> 192.168.1.57	RetroWeb.lan

Discovering Hosts... Back Run Scan

3. Run scans

## My Basic Network Scan

[Back to My Scans](#)

Configure Audit Trail Launch Report E:

Hosts [2] Vulnerabilities [30] VPR Top Threats [ ] History [1]

Filter Search Hosts 2 Hosts

Host	Vulnerabilities
192.168.1.27	2 Critical, 1 High, 2 Medium, 34 Low
192.168.1.57	1 Critical, 4 Medium, 29 Low

Scan Details

Policy: Basic Network Scan  
 Status: Completed  
 Severity Base: CVSS v3.0  
 Scanner: Local Scanner  
 Start: Today at 7:19 AM  
 End: Today at 7:26 AM  
 Elapsed: 7 minutes

Vulnerabilities

Critical: 2, High: 1, Medium: 2, Low: 34, Info: 30

### Analyse Jon-PC

#### 4. Analyse kwetsbaarheden Jon-PC

##### My Basic Network Scan / 192.168.1.27

[Back to Hosts](#)

Configure Audit Trail Launch Report Export

Vulnerabilities [21]

Filter Search Vulnerabilities 21 Vulnerabilities

Sev	Name	Family	Count
MIXED	Microsoft Windows (Multiple Issues)	Windows	5
MEDIUM	SMB Signing not required	Misc.	1
INFO	SMB (Multiple Issues)	Windows	7
INFO	DCE Services Enumeration	Windows	7
INFO	Nessus SYN scanner	Port scanners	3
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Ethernet MAC Addresses	General	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1

Host: 192.168.1.27

Host Details

IP: 192.168.1.27  
 DNS: Jon-PC.lan  
 MAC: 00:0C:29:7F:A6:11  
 OS: Microsoft Windows 7 Professional  
 Start: Today at 7:19 AM  
 End: Today at 7:21 AM  
 Elapsed: 2 minutes  
 KB: Download

Vulnerabilities

Critical: 2, High: 1, Medium: 2, Low: 34, Info: 30

##### My Basic Network Scan / 192.168.1.27 / Microsoft Windows (Multiple Issues)

[Back to Vulnerabilities](#)

Configure Audit Trail

Vulnerabilities [21]

Search Vulnerabilities 5 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)	Windows	1
CRITICAL	Unsupported Windows OS (remote)	Windows	1
HIGH	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMA...)	Windows	1
MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	Windows	1
INFO	WMI Not Available	Windows	1

### Threat 1 en oplossing

CRITICAL1 : CVSS (Common Vulnerability Scoring System) van 10.0. Dit is de hoogst mogelijke score!

Windows DNS client processes Link-local Multicast Name Resolution queries laten het toe remotely code uit te voeren.

## Oplossing: Windows heeft patches klaar.

My Basic Network Scan / Plugin #53514

< Back to Vulnerability Group

Configure Audit Trail Launch Report Export

Vulnerabilities 21

CRITICAL MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

### Description

A flaw in the way the installed Windows DNS client processes Link-local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.

Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

### Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

### See Also

<https://www.nessus.org/u?361871b1>

### Output

No output recorded.

Port	Hosts
5355 / udp / llmnr	192.168.1.27

### Plugin Details

Severity: Critical  
ID: 53514  
Version: 1.18  
Type: remote  
Family: Windows  
Published: April 21, 2011  
Modified: August 5, 2020

### Risk Information

Risk Factor: Critical  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Temporal Score: 8.3  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I/C:A/C  
CVSS v2.0 Temporal Vector: CVSS2#E/F/RL/OF/RC/C  
IAVM Severity: I

### Vulnerability Information

CPE: cpe:/o:microsoft:windows  
Exploit Available: true  
Exploit Ease: Exploits are available

## Threat 2 en oplossing

### CRITICAL2 : CVSS van 9.8

Het OS “Windows 7 Professional” wordt niet meer ondersteund door Microsoft.

## Oplossing: upgrade van het OS.

My Basic Network Scan / Plugin #108797

< Back to Vulnerability Group

Configure Audit Trail Launch Report Export

Vulnerabilities 21

CRITICAL Unsupported Windows OS (remote)

### Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

### Solution

Upgrade to a supported service pack or operating system

### See Also

<https://support.microsoft.com/en-us/lifecycle>

### Output

The following Windows version is installed and not supported:  
Microsoft Windows 7 Professional

Port	Hosts
N/A	192.168.1.27

### Plugin Details

Severity: Critical  
ID: 108797  
Version: 1.11  
Type: remote  
Family: Windows  
Published: April 3, 2018  
Modified: September 22, 2020

### Risk Information

Risk Factor: Critical  
**CVSS v2.0 Base Score 9.8**  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/I/U/N/S:U/H:H/A:H  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I/C:A/C

### Vulnerability Information

CPE: cpe:/o:microsoft:windows  
Unsupported by vendor: true

## Threat 3 en oplossing

### HIGH : CVSS van 8.1

Het Server Message Block of Common Internet File System netwerkprotocol (dat gebruikt wordt om bestandsuitwisseling tussen meerdere computers mogelijk maakt) bevat kwetsbaarheden waardoor remote code uitgevoerd kan worden. Een zeer bekende ransomware dat hier gebruik van maakt is WannaCry.

Oplossing: patches van Windows bestaan. Nieuwere Windows versies gebruiken SMBv2 of hoger.

## My Basic Network Scan / Plugin #97833

< Back to Vulnerability Group

Configure Audit Trail Launch Report Export

Vulnerabilities 21

HIGH MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALRO...

### Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNTERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

### Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

See Also

### Plugin Details

Severity: High  
ID: 97833  
Version: 1.24  
Type: remote  
Family: Windows  
Published: March 20, 2017  
Modified: October 15, 2020

### Risk Information

Risk Factor: High  
**CVSS v3.0 Base Score 8.1**  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/  
UI:N/S:UC:H/H:A:H  
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/  
RL:O/RC:C  
CVSS v2.0 Temporal Score: 7.7  
CVSS v2.0 Base Score: 9.3  
CVSS v2.0 Temporal Score: 8.1  
CVSS v2.0 Vector: CVSS:2#AV:N/AC:M/Au:N/C:  
I/L/A:C  
CVSS v2.0 Temporal Vector:  
CVSS:2#E:H/RL:O/RC:C  
IAVM Severity: I

## Threat 4 en oplossing

### MEDIUM1: CVSS van 6.8

**SAM (Security Account Manager) en LSAD (Local Security Authority Domain) protocols laten man-in-the-middle aanvallen toe wanneer via RPC (Remote Procedure Call) gecommuniceerd wordt door onvolledige controle van de credentials.**

### Oplossing: Microsoft heeft patches voorzien

## My Basic Network Scan / Plugin #90510

< Back to Vulnerability Group

Configure Audit Trail Launch Report Export

Vulnerabilities 21

MEDIUM MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (unauthenticated check)

### Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

### Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

### See Also

<http://www.nessus.org/u?52ade1e9>  
<http://badlock.org/>

### Output

No output recorded.

Port Hosts

49156 / tcp / dce-rpc 192.168.1.27

### Plugin Details

Severity: Medium  
ID: 90510  
Version: 1.9  
Type: remote  
Family: Windows  
Published: April 13, 2016  
Modified: July 23, 2019

### Risk Information

Risk Factor: Medium  
**CVSS v3.0 Base Score 6.8**  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/  
UI:R/S:UC:H/H:A:N  
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/  
RL:O/RC:C  
CVSS v3.0 Temporal Score: 5.9  
CVSS v2.0 Base Score: 5.8  
CVSS v2.0 Temporal Score: 4.3  
CVSS v2.0 Vector: CVSS:2#AV:N/AC:M/Au:N/C:P/  
I/P/A:N  
CVSS v2.0 Temporal Vector:  
CVSS:2#E:URL:O/RC:C  
IAVM Severity: I

## Threat 5 en oplossing

### MEDIUM2: CVSS van 5.3

Gelinkt met "HIGH" hierboven. Het SMB-protocol laat ook nog eens man-in-the-middle aanvallen toe van niet-geautenticeerde, remote aanvallers op de SMB server

### Oplossing: Verplicht digital "signing" via de settings op de host.

My Basic Network Scan / Plugin #57608

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

[Back to Vulnerabilities](#)

**Vulnerabilities** 21

**MEDIUM** SMB Signing not required

**Description**  
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

**Solution**  
Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

**See Also**  
<http://www.nessus.org/u?df39b8b3>  
<http://technet.microsoft.com/en-us/library/cc731957.aspx>  
<http://www.nessus.org/u?774b80723>  
<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>  
<http://www.nessus.org/u?a3cac4ea>

**Output**  
No output recorded.

Port	Hosts
445 / tcp / cifs	192.168.1.27

**Plugin Details**

Severity: Medium  
ID: 57608  
Version: 1.19  
Type: remote  
Family: Misc.  
Published: January 19, 2012  
Modified: March 15, 2021

**Risk Information**

Risk Factor: Medium  
**CVSS v3.0 Base Score 5.3**  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UF:N/U:C:N/L:A/N  
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/R:CC  
CVSS v3.0 Temporal Score: 4.6  
CVSS v2.0 Base Score: 5.0  
CVSS v2.0 Temporal Score: 3.7  
CVSS v2.0 Vector: CVSS2:AV:N/AC:L/Au:N/C:N/I:P/A:N  
CVSS v2.0 Temporal Vector: CVSS2:E:U/RL:O/R:CC

## Analyse RetroWeb-PC

### 5. Analyse kwetsbaarheden RetroWeb-PC

My Basic Network Scan / 192.168.1.57

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Exp](#)

[Back to Hosts](#)

**Vulnerabilities** 21

**Filter**  Search Vulnerabilities

21 Vulnerabilities

Sev	Name	Family	Count	Actions
MIXED	SSL (Multiple Issues)	General	9	
MIXED	TLS (Multiple Issues)	Service detection	3	
INFO	HTTP (Multiple Issues)	Web Servers	3	
INFO	Nessus SYN scanner	Port scanners	2	
INFO	Additional DNS Hostnames	General	1	
INFO	Common Platform Enumeration (CPE)	General	1	
INFO	Device Type	General	1	
INFO	Ethernet Card Manufacturer Detection	Misc.	1	
INFO	Ethernet MAC Addresses	General	1	
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1	

**Host** 192.168.1.57

**Host Details**

IP: 192.168.1.57  
DNS: RetroWeb.Ian  
MAC: 00:0C:29:E5:C5:54  
OS: Microsoft Windows 10  
Start: Today at 7:19 AM  
End: Today at 7:26 AM  
Elapsed: 7 minutes  
KB: Download

**Vulnerabilities**

My Basic Network Scan / 192.168.1.57 / SSL (Multiple Issues)

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Exp](#)

[Back to Vulnerabilities](#)

**Vulnerabilities** 9

**Search Vulnerabilities**

9 Vulnerabilities

Sev	Name	Family	Count	Actions
HIGH	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	1	
MEDIUM	SSL Certificate Cannot Be Trusted	General	1	
MEDIUM	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General	1	
MEDIUM	SSL Self-Signed Certificate	General	1	
INFO	SSL Certificate Information	General	1	
INFO	SSL Cipher Block Chaining Cipher Suites Supported	General	1	
INFO	SSL Cipher Suites Supported	General	1	
INFO	SSL Perfect Forward Secrecy Cipher Suites Supported	General	1	

**Scan Details**

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 7:19 AM  
End: Today at 7:26 AM  
Elapsed: 7 minutes

**Vulnerabilities**

## Threats en oplossingen

### SSL-kwetsbaarheden:

1. SSL ciphers van medium strength zijn toegelaten (keylengtes tussen 64 en 112 bits of 3DES) die gemakkelijk te omzeilen zijn wanneer een aanvaller op hetzelfde fysieke netwerk zit.  
Oplossing: Herconfigureer en verstreng de encryptie
2. Het SSL certificaat van de server is onbetrouwbaar  
Oplossing: Koop of genereer een correct SSL certificaat voor deze service
3. RC4 Cipher suites worden ondersteund. Deze Cipher wordt als zwak beschreven, zeker wanneer er herhaaldelijk plaintexts geencrypteerd worden en een aanvaller deze kan bemachtigen.  
Oplossing: Herconfigureer en verstreng de encryptie (bij voorkeur TLS1.2)
4. Self-Signed SSL Certificaat. Idem punt 2

TLS-kwetsbaarheid: Transport Layer Security Protocol 1.0 wordt nog geaccepteerd.

Oplossing : enable support voor TLS 1.2 en 1.3 en disable TLS 1.0

#### Scan targets en analyse met nmap

Werkwijze gebaseerd op 2 PluralSight courses:

<https://app.pluralsight.com/library/courses/nmap-getting-started/table-of-contents> en  
<https://app.pluralsight.com/library/courses/scanning-vulnerabilities-nse/table-of-contents>

\*

Scanning het netwerk met command “***sudo nmap -sn 192.168.1.0/24***” (discover network machines in mijn lokaal netwerk (range 192.168.1.0 tem 192.168.1.255)) -ook wel pingscan genoemd- toont de volgende twee netwerkmachines, belangrijk voor onze testen:

Nmap scan report for Jon-PC.lan (192.168.1.27)  
Host is up (0.0067s latency).  
MAC Address: 00:0C:29:7F:A6:11 (VMware)

Nmap scan report for RetroWeb.lan (192.168.1.57)  
Host is up (0.0012s latency).  
MAC Address: 00:0C:29:E5:C5:54 (VMware)

\*

***sudo nmap -sS -p80 192.168.1.0/24*** (scan alle devices op status van poort 80):

PORt STATE SERVICE  
80/tcp closed http  
MAC Address: 00:0C:29:7F:A6:11 (VMware)

PORt STATE SERVICE  
80/tcp open http  
MAC Address: 00:0C:29:E5:C5:54 (VMware)

\*

Om legaal te kunnen werken, kunnen we best ons te scannen netwerk en/of hosts oplijsten. Dit kunnen we doen door de ip-adressen in een file te zetten en de file op te roepen via “***sudo nmap -sL -iL ./Downloads/wbcscanlist***”

```
[kali㉿kali)-[~]
└$ sudo nmap -sn -iL ./Downloads/wbcscanlist
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 11:26 EDT
Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.00021s latency).
MAC Address: 00:0C:29:7F:A6:11 (VMware)
Nmap scan report for RetroWeb.lan (192.168.1.57)
Host is up (0.00069s latency).
MAC Address: 00:0C:29:E5:C5:54 (VMware)
Nmap done: 2 IP addresses (2 hosts up) scanned in 0.15 seconds
```

\*

Verdedigen tegen PingScans kan door de firewall zo te configureren dat ICMP traffic geblokkeerd wordt of dat TCP packets op poorten 80 en 443 te blokkeren wanneer deze niet nodig zijn.

Poort scanning is belangrijk om outdated of kwetsbare of onnodige services te detecteren en kwetbare applications of hosts die niet gevonden worden met een ping te vinden.

>**sudo nmap -p1-1023 -iL ./Downloads/wbcscanlist** (scan poorten 1 tem 1023 van de hosts in te file) of

>**sudo nmap -iL ./Downloads/wbcscanlist** (scan de 1000 meest voorkomende poorten)

Om ALLE poorten te scannen dienen we

>**sudo nmap -p1-1023,[1024-] -iL ./Downloads/wbcscanlist** uit te voeren, waarbij [1024-] enkel poorten gescanned zullen worden die geregistreerd zijn in nmap services (dus nmap weet dat een poort toegewezen is aan een specifieke service)

```
[kali㉿kali)-[~]
└$ sudo nmap -p1-1023,[1024-] -iL ./Downloads/wbcscanlist
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 16:26 EDT
Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.0013s latency).
Not shown: 8366 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
MAC Address: 00:0C:29:7F:A6:11 (VMware)

Nmap scan report for RetroWeb.lan (192.168.1.57)
Host is up (0.0014s latency).
Not shown: 8371 filtered ports
PORT      STATE SERVICE
80/tcp     open  http
3389/tcp   open  ms-wbt-server
5985/tcp   open  wsman
MAC Address: 00:0C:29:E5:C5:54 (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 22.08 seconds
```

Enkele opmerkingen:

80/tcp draait nog over http en is dus clear text. Recomendatie is eerder om hier https te gebruiken (gebruikelijk over poort 443)

Het is gebruikelijk om alle niet gebruikte poorten te sluiten.

Een extra veiligheid is IDS en IPS op te zetten.

\*

Service and Application version detection

> sudo nmap -sV -T4 -iL ./Downloads/wbcscanlist

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV -T4 -iL ./Downloads/wbcscanlist
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 16:41 EDT
Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.0022s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:7F:A6:11 (VMware)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for RetroWeb.lan (192.168.1.57)
Host is up (0.0014s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http          Microsoft IIS httpd 10.0
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:0C:29:E5:C5:54 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 64.37 seconds
```

\*

OS Detection

> sudo nmap -sV -T4 -iL ./Downloads/wbcscanlist

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV -T4 -iL ./Downloads/wbcscanlist
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 16:52 EDT
Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.0022s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
MAC Address: 00:0C:29:7F:A6:11 (VMware)
Device type: general purpose
Running: Microsoft Windows 7 [2008] 8.1
OS CPE: cpe:/o:microsoft:windows_7:::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

Nmap scan report for Retroweb.lan (192.168.1.57)
Host is up (0.0018s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
3389/tcp  open  ms-wbt-server
MAC Address: 00:0C:29:E5:C5:54 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 7.00 seconds
```

Voor de 2 laatste punten is de beste remedie steeds update naar de laatste versie en security patches, zowel voor services, applications als operating systems. Bovenstaande testen maken duidelijk dat het Windows 7 OS zo snel mogelijk ge-upgrade dient te worden.

\*

Nmap NSE scripting om authentication controls te testen (scripting taal = Lua)

VB: test of http default accounts heeft geactiveerd (authentication script):

```
(kali㉿kali)-[~]
$ sudo nmap --script=http-default-accounts -iL ./Downloads/wbcscanlist
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 17:31 EDT
Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.0012s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
MAC Address: 00:0C:29:7F:A6:11 (VMware)

Nmap scan report for RetroWeb.lan (192.168.1.57)
Host is up (0.00087s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp     open  http
3389/tcp   open  ms-wbt-server
MAC Address: 00:0C:29:E5:C5:54 (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 5.32 seconds
```

In bovenstaande geval hebben beide geen default accounts.

Of een brute force script op de IIS service waarbij gebruik gemaakt werd van een tilde als mogelijke vulnerability:

```
(kali㉿kali)-[~]
$ sudo nmap -p80 --script=http-iis-short-name-brute -iL ./Downloads/wbcsanlist
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 17:41 EDT
Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.00081s latency).

PORT      STATE SERVICE
80/tcp     closed http
MAC Address: 00:0C:29:7F:A6:11 (VMware)

Nmap scan report for RetroWeb.lan (192.168.1.57)
Host is up (0.00086s latency).

PORT      STATE SERVICE
80/tcp     open  http
MAC Address: 00:0C:29:E5:C5:54 (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.70 seconds
```

De IIS service op RetroWeb heeft hier geen last van en behoeft geen aanpassing.

Idem voor Cross Side Reference Forgery.

```
[kali㉿kali)-[~]WARNING **: 11:05:33.790: invalid source position
$ sudo nmap -p80 --script=http-csrf -iL ./Downloads/wbcscanlist
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 17:50 EDT
Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.00039s latency). 11:05:33.790: invalid source position

PORT      STATE SERVICE
80/tcp    closed http
MAC Address: 00:0C:29:7F:A6:11 (VMware) 11:05:33.791: invalid source position

Nmap scan report for RetroWeb.lan (192.168.1.57)
Host is up (0.00072s latency).
* (zenmap:41244): WARNING **: 11:05:33.825: invalid source position
PORT      STATE SERVICE
80/tcp    open  http  WARNING **: 11:05:33.860: invalid source position
|_http-csrf: Couldn't find any CSRF vulnerabilities.
MAC Address: 00:0C:29:E5:C5:54 (VMware) 11:05:33.826: invalid source position

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.58 seconds
```

Idem voor SQL-injection

```
[kali㉿kali)-[~]
$ sudo nmap -p80 --script=http-sql-injection -iL ./Downloads/wbcscanlist
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 17:52 EDT
Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.00047s latency).

PORT      STATE SERVICE
80/tcp    closed http
MAC Address: 00:0C:29:7F:A6:11 (VMware)

Nmap scan report for RetroWeb.lan (192.168.1.57)
Host is up (0.00057s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:E5:C5:54 (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

\*

Fuzzer (ingave van ongeldige en onverwachte data) en DoS (Denial of Service) scripts niet getest, maar zijn mogelijk om als Blue team uit te voeren.

### Scan en analyse targets met OWASP ZAP

Werkwijze gebaseerd op PluralSight course <https://app.pluralsight.com/library/courses/owasp-zap-web-app-pentesting/table-of-contents>

Aangezien OWASP ZAP een beveiligingsscanner voor webtoepassingen is en we via nmap hebben vastgesteld dat er 1 webserver is, nl RetroWeb, zullen we onze scan ook enkel op deze server uitvoeren.

>Start an automated scan on URL http://192.168.1.57

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack: http://192.168.1.57

Use traditional spider:

Use ajax spider:  with Firefox Headless

**Attack** **Stop**

Progress: Attack complete - see the Alerts tab for details of any issues found

Dit resulteert in 3 alerts:

1. X-Frame-Options Header Not Set, waardoor de webserver vatbaar wordt tegen "ClickJacking" attacks  
Oplossing: Zorg voor ondersteuning van de X-Frame-Options HTTP header voor alle webpagina's

**X-Frame-Options Header Not Set**

URL: http://192.168.1.57

Risk: Medium

Confidence: Medium

Parameter: X-Frame-Options

Attack:

Evidence:

CWE ID: 16

WASC ID: 15

Source: Passive (10020 - X-Frame-Options Header)

Description:

X-Frame-Options header is not included in the HTTP response to protect against 'Clickjacking' attacks.

Other Info:

2. X-Content-Type-Options Header Missing, waardoor er nog steeds sniffing mogelijk is.

Oplossing: Zet de Anti-MIME-Sniffing header X-content-type-option op 'nosniff' voor alle webpagina's

**X-Content-Type-Options Header Missing**

URL: http://192.168.1.57

Risk: Low

Confidence: Medium

Parameter: X-Content-Type-Options

Attack:

Evidence:

CWE ID: 16

WASC ID: 15

Source: Passive (10021 - X-Content-Type-Options Header Missing)

Description:

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Other Info:

This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.  
At 'High' threshold this scan rule will not alert on client or server error responses.

Solution:

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  
If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

Reference:

<http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx>  
[https://owasp.org/www-community/Security\\_Headers](https://owasp.org/www-community/Security_Headers)

3. Idem het vorige voorbeeld

**X-Content-Type-Options Header Missing**

URL: http://192.168.1.57

Risk: Low

Confidence: Medium

Parameter: X-Content-Type-Options

Attack:

Evidence:

CWE ID: 16

WASC ID: 15

Source: Passive (10021 - X-Content-Type-Options Header Missing)

Description:

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Other Info:

This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.  
At 'High' threshold this scan rule will not alert on client or server error responses.

Solution:

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  
If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

Reference:

<http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx>  
[https://owasp.org/www-community/Security\\_Headers](https://owasp.org/www-community/Security_Headers)

Aangezien sniffing nog mogelijk is, kan er via tools als gobuster naar webpagina's gezocht worden, die op hun beurt dan weer op kwetsbaarheden gescanned kunnen worden, maar dat brengt ons te ver van ons initiële doel.

## Level B requirements

Werkwijze gebaseerd op PluralSight course <https://app.pluralsight.com/library/courses/getting-started-memory-forensics-volatility/table-of-contents>

Extra documentatie uit:

Volatility officiële website: <https://www.volatilityfoundation.org/>

Handige volatility commands en Plugins:

<https://atalaysblog.wordpress.com/2019/07/13/useful-volatility-commands-plugins/>

Volatility github and Kali Command reference:

<https://github.com/volatilityfoundation/volatility/wiki/Command-Reference>

<https://tools.kali.org/forensics/volatility>

*De Kali VM van Offensive Security uit de level A testen zal ook gebruikt worden voor het Level B forensisch onderzoek.*

## Voorbereiding

Download Volatility source code van github

```
(kali㉿kali)-[~/Downloads]
└─$ git clone https://github.com/volatilityfoundation/volatility.git
Cloning into 'volatility'...
remote: Enumerating objects: 27411, done.
remote: Total 27411 (delta 0), reused 0 (delta 0), pack-reused 27411
Receiving objects: 100% (27411/27411), 21.10 MiB | 4.20 MiB/s, done.
Resolving deltas: 100% (19758/19758), done.
```

Met >**sudo python vol.py --info** kunnen wij zien welke profiles, Address Spaces, Scanner Checks en Plugins default meegekomen zijn in de Volatility tool

## Scanning van de dump van het werkgeheugen

### Profile finding

\* Algemene informatie memdump via plugin imageinfo:

```
(kali㉿kali)-[~/Downloads/volatility]
└─$ sudo python vol.py -f ..\Alissas-PC.raw imageinfo
Volatility Foundation 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search ...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/kali/Downloads/Alissas-PC.raw)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf800028100a0L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff80002811d00L 6.32 Likewise you cannot build a profile for a Debian 2.6.32 system to analyze a memory dump from
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2019-12-11 14:38:00 UTC+0000
Image local date and time : 2019-12-11 20:08:00 +0530 UTC+0000
```

Hier kunnen we al nuttige info uithalen zoals welk profile we kunnen proberen met de volatility-tool om meer gerichte analyses te doen.

\* Een uitbreiding hierop is >**sudo python vol.py -f ..\Alissas-PC.raw kdbgscan** dat meer accurate informatie toont over het te gebruiken profiel. Deze plugin is extreem belangrijk om memory images te analyseren omdat ze informatie bevat over het systeem, de pointers naar de start van de lijst met actieve processen en de kernel modules

```

[kali㉿kali)-[~/Downloads/volatility]
$ sudo python vol.py -f ../../Alissas-PC.raw kdbgscan
Volatility Foundation Volatility Framework 2.6.1
*****
Instantiating KDBG using: /home/kali/Downloads/Alissas-PC.raw WinXPSP2x86 (5.1.0 32bit)
Offset (P) : 0x28100a0
KDBG owner tag check : True
Profile suggestion (KDBGHeader): Win7SP1x64
PsActiveProcessHead : 0x2846b90
PsLoadedModuleList : 0x2864e90
KernelBase : 0xfffff8000261f000

*****
Instantiating KDBG using: /home/kali/Downloads/Alissas-PC.raw WinXPSP2x86 (5.1.0 32bit)
Offset (P) : 0x28100a0
KDBG owner tag check : True
Profile suggestion (KDBGHeader): Win2008R2SP1x64
PsActiveProcessHead : 0x2846b90
PsLoadedModuleList : 0x2864e90
KernelBase : 0xfffff8000261f000

```

Hier wordt duidelijk dat het OS WinXP met SP2 is.

## Process Listing

\* pslist lijst alle processen van een systeem op, op het moment van de geheugendump.

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0xfffffa8000ca0040	System	4	0	80	570	—	0	2019-12-11 13:41:25 UTC+0000	
0xfffffa800148f040	smss.exe	248	4	3	37	—	0	2019-12-11 13:41:25 UTC+0000	
0xfffffa800154f740	csrss.exe	320	10	312	9	457	0	2019-12-11 13:41:32 UTC+0000	
0xfffffa8000ca81e0	csrss.exe	368	360	—	199	1	0	2019-12-11 13:41:33 UTC+0000	
0xfffffa8001c45060	psxss.exe	376	248	18	786	0	0	2019-12-11 13:41:33 UTC+0000	
0xfffffa8001c5f060	winlogon.exe	416	360	4	118	1	0	2019-12-11 13:41:34 UTC+0000	
0xfffffa8001c5f630	wininit.exe	424	312	30	75	0	0	2019-12-11 13:41:34 UTC+0000	
0xfffffa8001c98530	services.exe	484	424	13	219	0	0	2019-12-11 13:41:35 UTC+0000	
0xfffffa8001ca0580	lsass.exe	492	424	9	764	0	0	2019-12-11 13:41:35 UTC+0000	
0xfffffa8001ca4b30	lsm.exe	500	424	11	185	0	0	2019-12-11 13:41:35 UTC+0000	
0xfffffa8001cf4b30	svchost.exe	588	484	11	358	0	0	2019-12-11 13:41:39 UTC+0000	
0xfffffa8001d327c0	VBoxService.exe	652	484	13	137	0	0	2019-12-11 13:41:40 UTC+0000	
0xfffffa8001d49b30	svchost.exe	720	484	8	279	0	0	2019-12-11 13:41:41 UTC+0000	
0xfffffa8001d8c420	svchost.exe	816	484	23	569	0	0	2019-12-11 13:41:42 UTC+0000	
0xfffffa8001da5b30	svchost.exe	852	484	28	542	0	0	2019-12-11 13:41:43 UTC+0000	
0xfffffa8001da96c0	svchost.exe	876	484	32	941	0	0	2019-12-11 13:41:43 UTC+0000	
0xfffffa8001eb3b30	svchost.exe	472	484	19	476	0	0	2019-12-11 13:41:47 UTC+0000	
0xfffffa8001e50b30	svchost.exe	1044	484	14	366	0	0	2019-12-11 13:41:48 UTC+0000	
0xfffffa8001eba230	spoolsv.exe	1208	484	13	282	0	0	2019-12-11 13:41:51 UTC+0000	
0xfffffa8001eda060	svchost.exe	1248	484	19	313	0	0	2019-12-11 13:41:52 UTC+0000	
0xfffffa8001f58890	svchost.exe	1372	484	22	295	0	0	2019-12-11 13:41:54 UTC+0000	
0xfffffa8001f91b30	TCPVCS.EXE	1416	484	4	97	0	0	2019-12-11 13:41:55 UTC+0000	
0xfffffa8000d3c400	sppsvc.exe	1508	484	4	141	0	0	2019-12-11 14:16:06 UTC+0000	
0xfffffa8001c38580	svchost.exe	948	484	13	322	0	0	2019-12-11 14:16:07 UTC+0000	
0xfffffa8002170630	wmpnetwk.exe	1856	484	16	451	0	0	2019-12-11 14:16:08 UTC+0000	
0xfffffa8001d376f0	SearchIndexer.exe	480	484	14	701	0	0	2019-12-11 14:16:09 UTC+0000	
0xfffffa8001eb47f0	taskhost.exe	296	484	8	151	1	0	2019-12-11 14:32:24 UTC+0000	
0xfffffa8001dfa910	dwm.exe	1988	852	5	72	1	0	2019-12-11 14:32:25 UTC+0000	
0xfffffa8002046960	explorer.exe	604	2016	33	927	1	0	2019-12-11 14:32:25 UTC+0000	
0xfffffa80021c75d0	VBoxTray.exe	1844	604	11	140	1	0	2019-12-11 14:32:35 UTC+0000	
0xfffffa80021da060	audiogd.exe	2064	816	6	131	0	0	2019-12-11 14:32:37 UTC+0000	
0xfffffa80022199e0	svchost.exe	2368	484	9	365	0	0	2019-12-11 14:32:51 UTC+0000	
0xfffffa800222780	cmd.exe	1984	604	1	21	1	0	2019-12-11 14:34:54 UTC+0000	
0xfffffa8002227140	conhost.exe	2692	368	2	50	1	0	2019-12-11 14:34:54 UTC+0000	
0xfffffa80022bab30	mspaint.exe	2424	604	6	128	1	0	2019-12-11 14:35:14 UTC+0000	
0xfffffa8000eac770	svchost.exe	2660	484	6	100	0	0	2019-12-11 14:35:14 UTC+0000	
0xfffffa8001e68060	cssrss.exe	2760	2680	7	172	2	0	2019-12-11 14:37:05 UTC+0000	
0xfffffa80000ccb30	winlogon.exe	2808	2680	4	119	2	0	2019-12-11 14:37:05 UTC+0000	
0xfffffa8000f3aab0	taskhost.exe	2908	484	9	158	2	0	2019-12-11 14:37:13 UTC+0000	
0xfffffa8000f4db30	dwm.exe	3004	852	5	72	2	0	2019-12-11 14:37:14 UTC+0000	
0xfffffa8000f4c670	explorer.exe	2504	3000	34	825	2	0	2019-12-11 14:37:14 UTC+0000	
0xfffffa8000ff630	VBoxTray.exe	2304	2504	14	144	2	0	2019-12-11 14:37:14 UTC+0000	
0xfffffa80000ceca60	SearchProtocolHo	2524	480	7	226	2	0	2019-12-11 14:37:21 UTC+0000	
0xfffffa80000ceca60	SearchFilterHo	1720	480	5	90	0	0	2019-12-11 14:37:21 UTC+0000	
0xfffffa8001010b30	WinRAR.exe	1512	2504	6	207	2	0	2019-12-11 14:37:23 UTC+0000	
0xfffffa8001020b30	SearchProtocol	2868	480	8	279	0	0	2019-12-11 14:37:23 UTC+0000	
0xfffffa8001040860	DumpIt.exe	796	604	2	45	1	1	2019-12-11 14:37:54 UTC+0000	
0xfffffa800104a780	conhost.exe	2260	368	2	50	1	0	2019-12-11 14:37:54 UTC+0000	

\* pstree werkt hetzelfde als pslist, maar toont daarbovenop ook de parent/child relatie.

Name	Pid	PPid	Thds	Hnds	Time	lists
explorer.exe	2504	3000	34	825	2019-12-11 14:37:14	UTC+0000
VBoxTray.exe	2304	2504	14	144	2019-12-11 14:37:14	UTC+0000
WinRAR.exe	1512	2504	6	207	2019-12-11 14:37:23	UTC+0000
wininit.exe	424	3120	3	75	2019-12-11 13:41:34	UTC+0000
services.exe	484	4240	13	219	2019-12-11 13:41:35	UTC+0000
wmpnetwk.exe	1856	484	16	451	2019-12-11 14:16:08	UTC+0000
TCPSVCS.EXE	1416	484	4	97	2019-12-11 13:41:55	UTC+0000
svchost.exe	876	484	32	941	2019-12-11 13:41:43	UTC+0000
VBoxService.exe	652	484	13	137	2019-12-11 13:41:40	UTC+0000
svchost.exe	2660	484	6	100	2019-12-11 14:35:14	UTC+0000
svchost.exe	2368	484	9	365	2019-12-11 14:32:51	UTC+0000
svchost.exe	1044	484	14	366	2019-12-11 13:41:48	UTC+0000
svchost.exe	816	484	23	569	2019-12-11 13:41:42	UTC+0000
audiodg.exe	2064	816	6	131	2019-12-11 14:32:37	UTC+0000
svchost.exe	948	484	13	322	2019-12-11 14:16:07	UTC+0000
spoolsv.exe	1208	484	13	282	2019-12-11 13:41:51	UTC+0000
SearchIndexeranner	480	484	14	701	2019-12-11 14:16:09	UTC+0000
SearchProtocol	2524	480	7	226	2019-12-11 14:37:21	UTC+0000
SearchProtocol	2868	480	8	279	2019-12-11 14:37:23	UTC+0000
SearchFilterHornel	1720	480	5	90	2019-12-11 14:37:21	UTC+0000
taskhost.exe	2908	484	9	158	2019-12-11 14:37:13	UTC+0000
svchost.exe	588	484	11	358	2019-12-11 13:41:39	UTC+0000
svchost.exe	720	484	8	279	2019-12-11 13:41:41	UTC+0000
svchost.exe	852	484	28	542	2019-12-11 13:41:43	UTC+0000
dwm.exe	3004	852	5	72	2019-12-11 14:37:14	UTC+0000
dwm.exe	1988	852	5	72	2019-12-11 14:32:25	UTC+0000
svchost.exe	472	484	19	476	2019-12-11 13:41:47	UTC+0000
sppsvc.exe	1508	484	4	141	2019-12-11 14:16:06	UTC+0000
svchost.exe	1372	484	22	295	2019-12-11 13:41:54	UTC+0000
svchost.exe	1248	484	19	313	2019-12-11 13:41:52	UTC+0000
taskhost.exe	296	484	8	151	2019-12-11 14:32:24	UTC+0000
lsass.exe	492	424	9	764	2019-12-11 13:41:35	UTC+0000
lsm.exe	500	424	11	185	2019-12-11 13:41:35	UTC+0000
csrss.exe	320	312	9	457	2019-12-11 13:41:32	UTC+0000
System	4	800	80	570	2019-12-11 13:41:25	UTC+0000
sms.exe	248	3	37	2019-12-11 13:41:25	UTC+0000	
psxss.exe	376	248	18	786	2019-12-11 13:41:33	UTC+0000
winlogon.exe	516	360	4	118	2019-12-11 13:41:34	UTC+0000
csrss.exe	368	360	7	199	2019-12-11 13:41:33	UTC+0000
conhost.exe	2692	368	2	50	2019-12-11 14:34:54	UTC+0000
conhost.exe	2260	368	2	50	2019-12-11 14:37:54	UTC+0000
explorer.exe	604	2016	33	927	2019-12-11 14:32:25	UTC+0000
VBoxTray.exe	1844	604	11	140	2019-12-11 14:32:35	UTC+0000
cmd.exe	1984	604	1	21	2019-12-11 14:34:54	UTC+0000
mspaint.exe	2424	604	6	128	2019-12-11 14:35:14	UTC+0000
DumpIt.exe	796	604	2	45	2019-12-11 14:37:54	UTC+0000
csrss.exe	2760	2680	7	172	2019-12-11 14:37:05	UTC+0000
winlogon.exe	2808	2680	4	119	2019-12-11 14:37:05	UTC+0000

\* Bovenstaande commando's werken door het doorlopen van de dubbelgelinkte lijst waarnaar verwezen wordt in de psactive process head (en deze bevat een lijst met eprocess objecten voor processen). Sommige malware kan deze eprocess objecten weliswaar 'unlinken' waardoor pslist en pstree deze processen dus niet kunnen opsporen. Hiervoor bestaat gelukkig psscan, dat verborgen en niet-gelinkte processes kan vinden door een techniek die pool tag scanning wordt genoemd.

L\$ sudo python vol.py -f ..\Alissas-PC.raw --profile=Win7SP1x64 psscan							
Offset(P)	Name	Patches	PID	PPID	PDB	Time created	Time exited
0x000000003e8199e0	svchost.exe	2368	484	0x000000002f8cf000	2019-12-11 14:32:51 UTC+0000		
0x000000003e822780	cmd.exe	1984	604	0x000000002457b000	2019-12-11 14:34:54 UTC+0000		
0x000000003e827140	conhost.exe	2692	368	0x0000000023e17000	2019-12-11 14:34:54 UTC+0000		
0x000000003e8bab30	mspaint.exe	2424	604	0x000000003a581000	2019-12-11 14:35:14 UTC+0000		
0x000000003ea46960	explorer.exe	604	2016	0x0000000035a79000	2019-12-11 14:32:25 UTC+0000		
0x000000003eb70630	wmpnetwk.exe	1856	484	0x00000000e83e0000	2019-12-11 14:16:08 UTC+0000		
0x000000003ebc75d0	VBoxTray.exe	1844	604	0x0000000034c66000	2019-12-11 14:32:35 UTC+0000		
0x000000003ebda060	audiogd.exe	2064	816	0x000000003218c000	2019-12-11 14:32:37 UTC+0000		
0x000000003ec1bb30	svchost.exe	472	484	0x000000001aa76000	2019-12-11 13:41:47 UTC+0000		
0x000000003ec5b030	svchost.exe	1044	484	0x000000001a6be000	2019-12-11 13:41:48 UTC+0000		
0x000000003ec68060	csrss.exe	2760	2680	0x000000001b94e000	2019-12-11 14:37:05 UTC+0000		
0x000000003ecb47f0	taskhost.exe	296	484	0x0000000036347000	2019-12-11 14:32:24 UTC+0000		
0x000000003ecba230	spoolsv.exe	1208	484	0x00000000177ce000	2019-12-11 13:41:51 UTC+0000		
0x000000003ecd0a60	svchost.exe	1248	484	0x000000001729c000	2019-12-11 13:41:52 UTC+0000		
0x000000003ed58890	svchost.exe	1372	484	0x0000000013f1b000	2019-12-11 13:41:54 UTC+0000		
0x000000003ed91b30	TCPVCS.EXE	1416	484	0x00000000098c0000	2019-12-11 13:41:55 UTC+0000		
0x000000003ee38580	svchost.exe	948	484	0x0000000000eab3000	2019-12-11 14:16:07 UTC+0000		
0x000000003ee45060	psxss.exe	376	248	0x00000000001f70a000	2019-12-11 13:41:33 UTC+0000		
0x000000003ee5f060	winlogon.exe	416	360	0x00000000001f20c000	2019-12-11 13:41:34 UTC+0000		
0x000000003ef630	wininit.exe	424	312	0x00000000001f079000	2019-12-11 13:41:34 UTC+0000		
0x000000003ee98530	services.exe	484	424	0x00000000001e531000	2019-12-11 13:41:35 UTC+0000		
0x000000003eea0580	lsass.exe	492	424	0x00000000001e3d2000	2019-12-11 13:41:35 UTC+0000		
0x000000003eea4b30	lsm.exe	500	424	0x00000000001e55a000	2019-12-11 13:41:35 UTC+0000		
0x000000003eecf4b30	svchost.exe	588	484	0x00000000001d4f4000	2019-12-11 13:41:39 UTC+0000		
0x000000003ef327c0	VBoxService.exe	652	484	0x00000000001d0dc000	2019-12-11 13:41:40 UTC+0000		
0x000000003ef376f0	SearchIndexer.exe	480	484	0x0000000000dc08000	2019-12-11 14:16:09 UTC+0000		
0x000000003ef9b30	svchost.exe	720	484	0x00000000001cdac000	2019-12-11 13:41:41 UTC+0000		
0x000000003ef8c420	svchost.exe	816	484	0x00000000001c795000	2019-12-11 13:41:42 UTC+0000		
0x000000003efa5b30	svchost.exe	852	484	0x00000000001bfde000	2019-12-11 13:41:43 UTC+0000		
0x000000003efa96c0	svchost.exe	876	484	0x00000000001c0e4000	2019-12-11 13:41:43 UTC+0000		
0x000000003effa910	dwm.exe	1988	852	0x0000000000350d7000	2019-12-11 14:32:25 UTC+0000		
0x000000003f68f040	smss.exe	248	424	0x0000000000261ec000	2019-12-11 13:41:25 UTC+0000		
0x000000003f74f740	csrss.exe	320	312	0x00000000001fc3000	2019-12-11 13:41:32 UTC+0000		
0x000000003fa10b30	WinRAR.exe	1512	2504	0x000000000019835000	2019-12-11 14:37:23 UTC+0000		
0x000000003fa20b30	SearchProtocol	2868	480	0x000000000017b1b000	2019-12-11 14:37:23 UTC+0000		
0x000000003fa48060	DumpIt.exe	796	604	0x0000000000143d6000	2019-12-11 14:37:54 UTC+0000		
0x000000003fa4a780	conhost.exe	2260	368	0x000000000012d9b000	2019-12-11 14:37:54 UTC+0000		
0x000000003fa95b30	WinRAR.exe	1512	2504	0x000000000019835000	2019-12-11 14:37:23 UTC+0000		
0x000000003faa5b30	SearchProtocol	2868	480	0x000000000017b1b000	2019-12-11 14:37:23 UTC+0000		
0x000000003facd060	DumpIt.exe	796	604	0x0000000000143d6000	2019-12-11 14:37:54 UTC+0000		
0x000000003facf780	conhost.exe	2260	368	0x000000000012d9b000	2019-12-11 14:37:54 UTC+0000		
0x000000003fb1ab30	WinRAR.exe	1512	2504	0x000000000019835000	2019-12-11 14:37:23 UTC+0000		
0x000000003fb2a30	SearchProtocol	2868	480	0x000000000017b1b000	2019-12-11 14:37:23 UTC+0000		
0x000000003fb52060	DumpIt.exe	796	604	0x0000000000143d6000	2019-12-11 14:37:54 UTC+0000		
0x000000003fb54780	conhost.exe	2260	368	0x000000000012d9b000	2019-12-11 14:37:54 UTC+0000		
0x000000003fcac770	svchost.exe	2660	484	0x000000000001d2e000	2019-12-11 14:35:14 UTC+0000		
0x000000003fccbb30	winlogon.exe	2808	2680	0x0000000000261d3000	2019-12-11 14:37:05 UTC+0000		
0x000000003fccea60	SearchFilterHo	1720	480	0x000000000019b05000	2019-12-11 14:37:21 UTC+0000		
0x000000003fd3aab0	taskhost.exe	2908	484	0x0000000000b291000	2019-12-11 14:37:13 UTC+0000		
0x000000003fd4c670	explorer.exe	2504	3000	0x00000000008771000	2019-12-11 14:37:14 UTC+0000		
0x000000003fd4db30	dwm.exe	3004	852	0x000000000016de7000	2019-12-11 14:37:14 UTC+0000		
0x000000003fd9a4e0	VBoxTray.exe	2304	2504	0x000000000007a54000	2019-12-11 14:37:14 UTC+0000		
0x000000003fdf630	SearchProtocol	2524	480	0x000000000037d69000	2019-12-11 14:37:21 UTC+0000		
0x000000003feb2400	sppsvc.exe	1508	484	0x0000000000f4ee000	2019-12-11 14:16:06 UTC+0000		
0x000000003ff5f040	System	4	0	0x000000000000187000	2019-12-11 13:41:25 UTC+0000		
0x000000003ff671e0	csrss.exe	368	360	0x00000000003bd46000	2019-12-11 13:41:33 UTC+0000		

Andere nuttige commands te gebruiken als toevoeging op de process listing commands:  
 dllist toont de ingeladen DLLs van een process. Aangezien dit een enorme lange lijst is, wordt deze meestal enkel gebruikt om de details van een bepaalde pid te vinden. Dit kan door parameter -p <PID> toe te voegen.

handles toont de open handles van een process en bevat dus zeer nuttige informatie over welke files, registry keys, threads en andere objecten bezig waren met een process.

## Analyse van de dump van het werkgeheugen

Met bovenstaande wetenschap gaan we aan de slag met het oplossen van de vragen:

### Opdracht 1: Recover het windows wachtwoord

1. Imageinfo leert ons profiel "Win7SP1x64" te gebruiken.

2. een belangrijk proces voor paswoordrecovery kan cmd.exe zijn aangezien hier de hele geschiedenis kan uitgelezen worden, inclusief command outputs. We kunnen hier commando "consoles" op los laten:

```
(kali㉿kali)-[~/Downloads/volatility]
└─$ sudo python vol.py -f ../Alissas-PC.raw --profile=Win7SP1x64 consoles
Volatility Foundation Volatility Framework 2.6.1
***** Processes by following the EPROCESS lists *****
ConsoleProcess: conhost.exe Pid: 2692
Console: 0x0000000000000000 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe - St4G3$1
AttachedProcess: cmd.exe Pid: 1984 Handle: 0x60
    — help           - List Windows services (ala Plugx)
    CommandHistory: 0x1fe9c0 Application: cmd.exe Flags: Allocated, ResetLogonSessions
    CommandCount: 1 LastAdded: 0 LastDisplayed: 0 info
    FirstCommand: 0 CommandCountMax: 50 the Application Compatibility Shim Cache registry key
    ProcessHandle: 0x60      - Print ShutdownTime of machine from registry
    Cmd #0 at 0x1de3c0: St4G3$1 - Print list of open sockets
    — scan           - Pool scanner for TCP socket objects
    Screen 0x1e0f70 X:80 Y:300 - Display SSDT entries
    Dump:             - Match physical offsets to virtual addresses (may take a while, VETOED)
    Microsoft Windows [Version 6.1.7601] - Windows services
    Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\SmartNet>St4G3$1 - Investigate _ETHREAD and _KTHREADS
ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0= - timeline from various artifacts in memory
Press any key to continue
***** Master Keys *****
ConsoleProcess: conhost.exe Pid: 2260
Console: 0x0000000000000000 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: C:\Users\SmartNet\Downloads\DumpIt\DumpIt.exe
Title: C:\Users\SmartNet\Downloads\DumpIt\DumpIt.exe
AttachedProcess: DumpIt.exe Pid: 796 Handle: 0x60
    — info           - Dump the VAD info
    CommandHistory: 0x38ea90 Application: DumpIt.exe Flags: Allocated, Format
    CommandCount: 0 LastAdded: -1 LastDisplayed: -1
    FirstCommand: 0 CommandCountMax: 50 VirtualBox information
    ProcessHandle: 0x60      - Prints out the version information from PE images
    — reinfo          - Dump VMware VMSS/VMSN information
    Screen 0x371050 X:80 Y:300 - Shell in the memory image
    Dump:             - Find the ObHeaderCookie value for Windows 10
        DumpIt - v1.3.2.20110401 - One click memory dump (details)
        Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
        Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>
    yaraScan           - Scan process or kernel memory with Yara signatures

    Address space size: loads/vc 1073676288 bytes ( 1023 Mb)
    Free space size:      24185389056 bytes ( 23064 Mb)

    * Destination = \??\C:\Users\SmartNet\Downloads\DumpIt\SMARTNET-PC-20191211-143755.raw

    → Are you sure you want to continue? [y/n] y
    + Processing ...
```

We zien dat conhost.exe een soort van commandline had, maar belangrijker:

C:\Users\SmartNet>St4G3\$1

ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=

⇒ dit is Base64 code. Decoden via website <https://www.base64decode.org/> geeft

**BASE64**

**Decode and Encode**

Do you have to deal with **Base64** format? Then this site is perfect for you! Use our super handy online tool to encode or decode Base64 strings.

**SAMSUNG Galaxy Watch3**

**Decode from Base64 format**

Simply enter your data then push the decode button.

```
ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

**< DECODE >** Decodes your data into the area below.

```
flag{th1s_1s_th3_1st_st4g3!!}
```

Voila! Het windows paswoord is gevonden! (flag{th1s\_1s\_th3\_1st\_st4g3!!})

Opdracht 2 : Vind 'important.rar' en toon de inhoud

1. Uit pslist zien we hier proces WinRAR.exe op de machine.

2. de cmdline module leert ons dat dit proces inderdaad Important.rar 'vast' heeft

```
*****  
WinRAR.exe pid: 1512 - Print 7-Order Desktop Windows Tree  
Command line : "C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\Alissa Simpson\Documents\Important.rar"  
*****
```

3. Een memdump kan meer licht op de file werpen

```
>sudo python vol.py -f ..\Alissas-PC.raw --profile=Win7SP1x64 memdump -p 1512 -D ./dump/
```

4. De offset kunnen wij uit onze psscan eerder in deze opdracht lezen om de file met “dumpfiles” te extracten.

```
(kali㉿kali)-[~/Downloads/volatility]
└─$ sudo python vol.py -f ../../Alissas-PC.raw --profile=Win7SP1x64 dumpfiles -D ./dump/ -Q 0x000000003fb48bc0 -n
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3fb48bc0 None \Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar

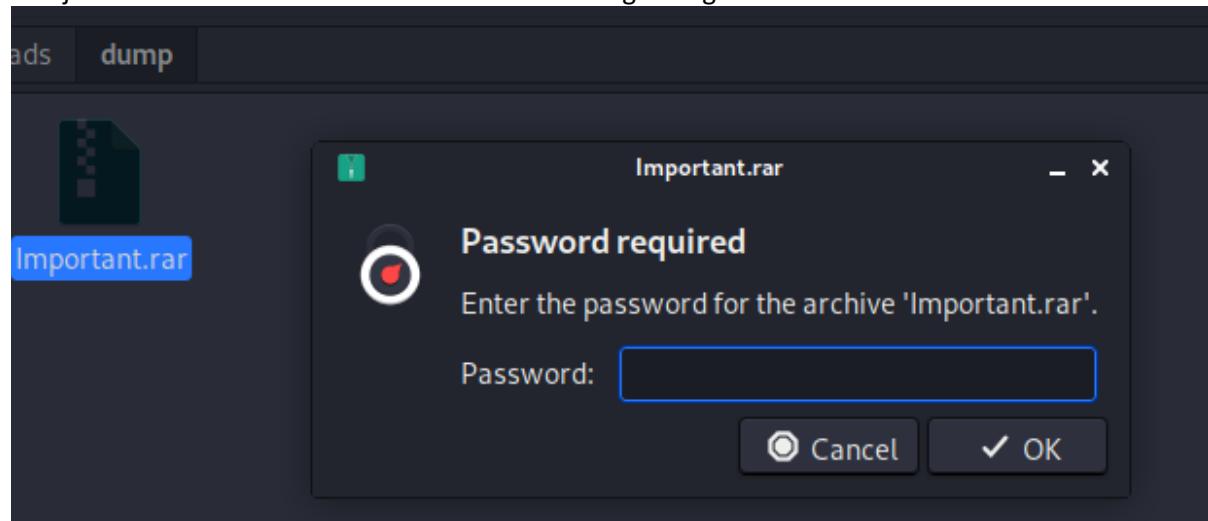
(kali㉿kali)-[~/Downloads/volatility]
└─$ cd ./dump

(kali㉿kali)-[~/Downloads/dump]
└─$ ls
1512.dmp  file.None.0xfffffa8001034450.dat

(kali㉿kali)-[~/Downloads/dump]
└─$ ls
1512.dmp  file.None.0xfffffa8001034450.dat

(kali㉿kali)-[~/Downloads/dump]
└─$ mv file.None.0xfffffa8001034450.dat Important.rar
```

5. Bij het extracten wordt er voor een wachtwoord gevraagd



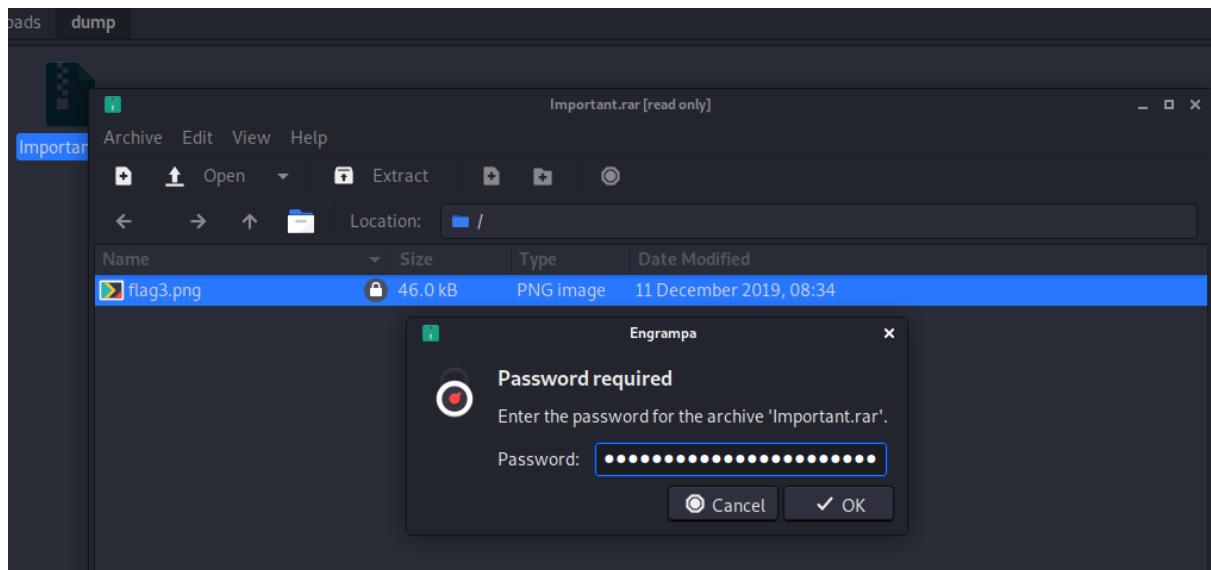
6. Met volatility strings op de dumpfile en een grep op string “pass” leert ons “Password is NTLM hash(in uppercase) of Alissa's account passwd.”

7. LM/NTLM hashes kunnen rechtstreeks uit het geheugen gehaald worden via een hashdump

```
(kali㉿kali)-[~/Downloads/volatility]
└─$ sudo python vol.py -f ../../Alissas-PC.raw --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
SmartNet:1001:aad3b435b51404eeaad3b435b51404ee:4943abb39473a6f32c11301f4987e7e0 :::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f0fc3d257814e08fea06e63c5762ebd5 :::
Alissa Simpson:1003:aad3b435b51404eeaad3b435b51404ee:f4ff64c8baac57d22f22edc681055ba6 :::
```

f4ff64c8baac57d22f22edc681055ba6 in allemaal hoofdletters moet volgens voorgaande tip dus het paswoord zijn.

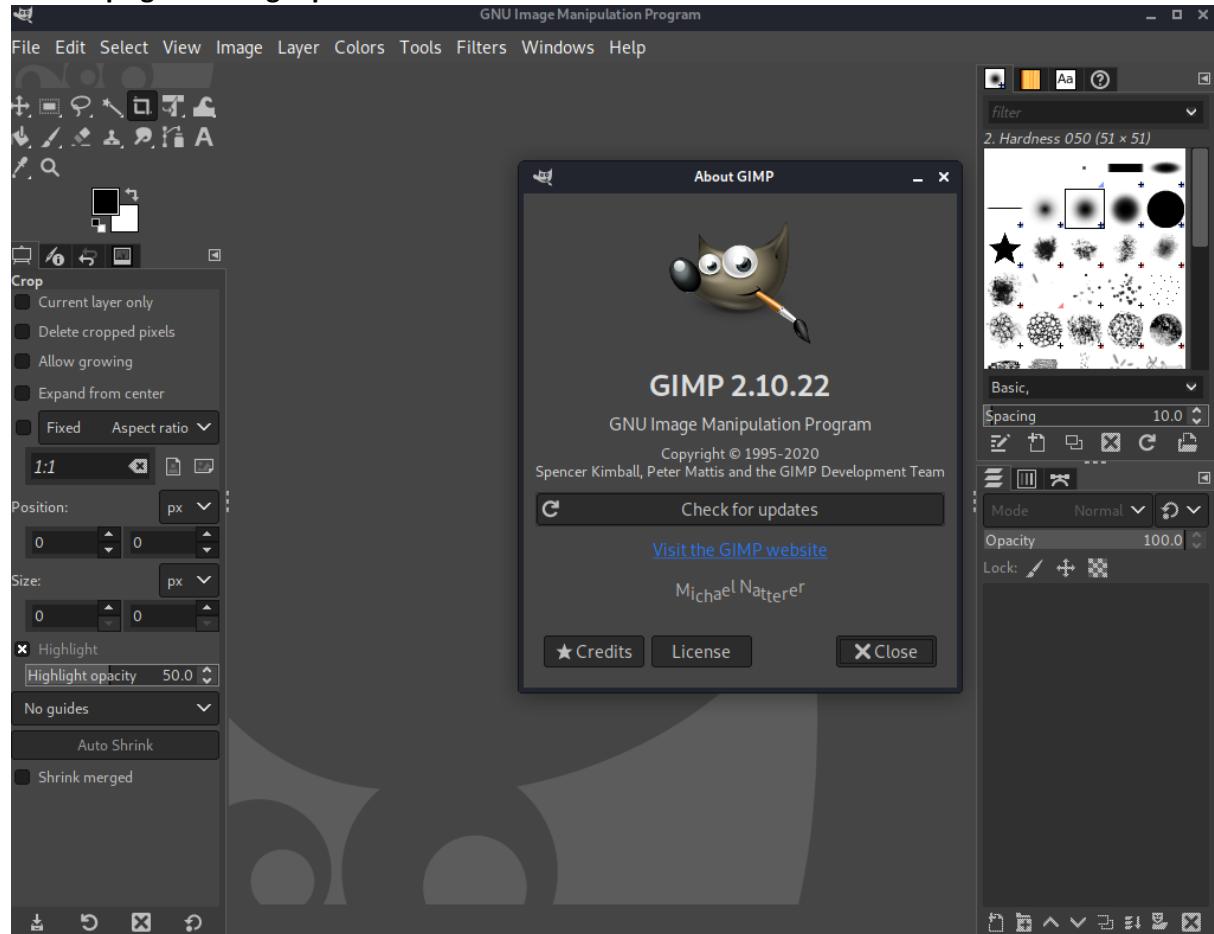
8. Succes! =>



### Opdracht 3: Terughalen tekening MSPaint

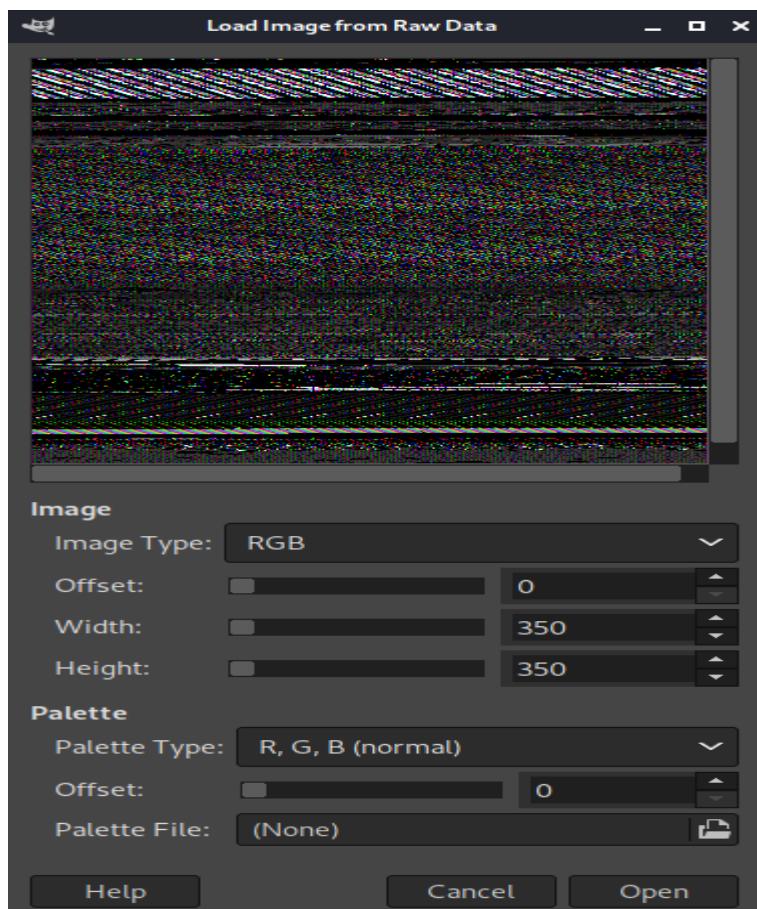
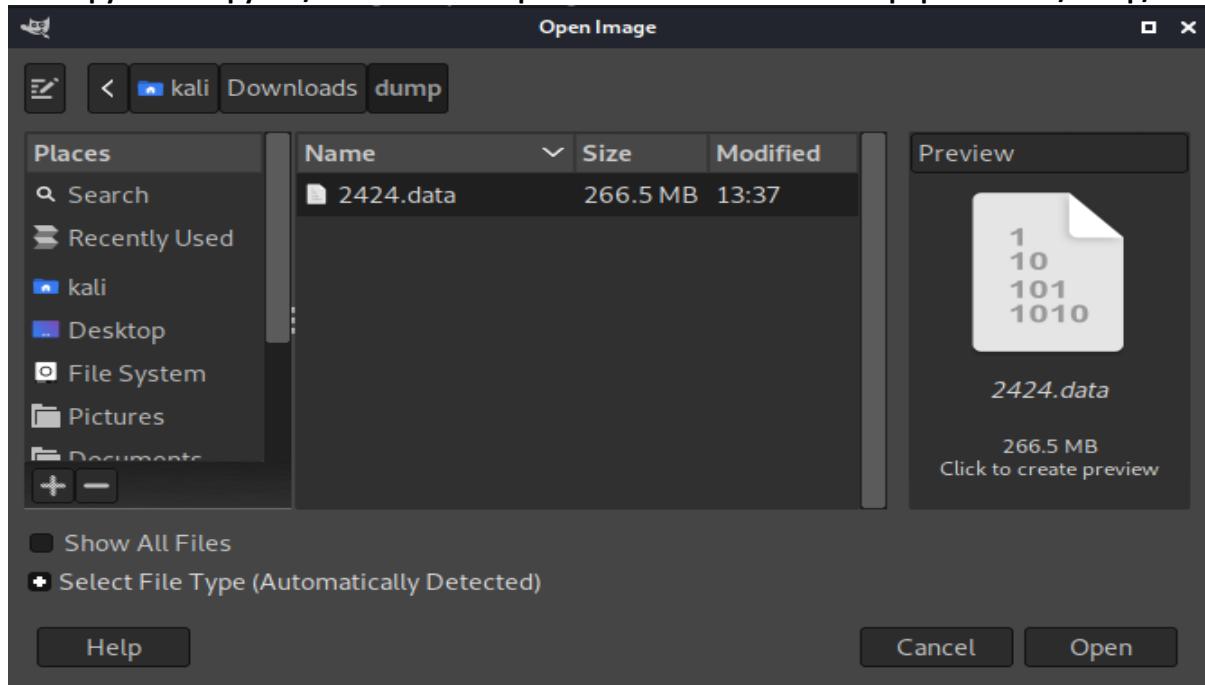
Gimp is een handig beeldverwerkingsprogramma geschreven in Python dat cross-platform werkt en ideaal is om MSPaint van Microsoft te vervangen in Linux. Méér nog! Gimp kan raw image data lezen!

**>sudo apt-get install gimp**

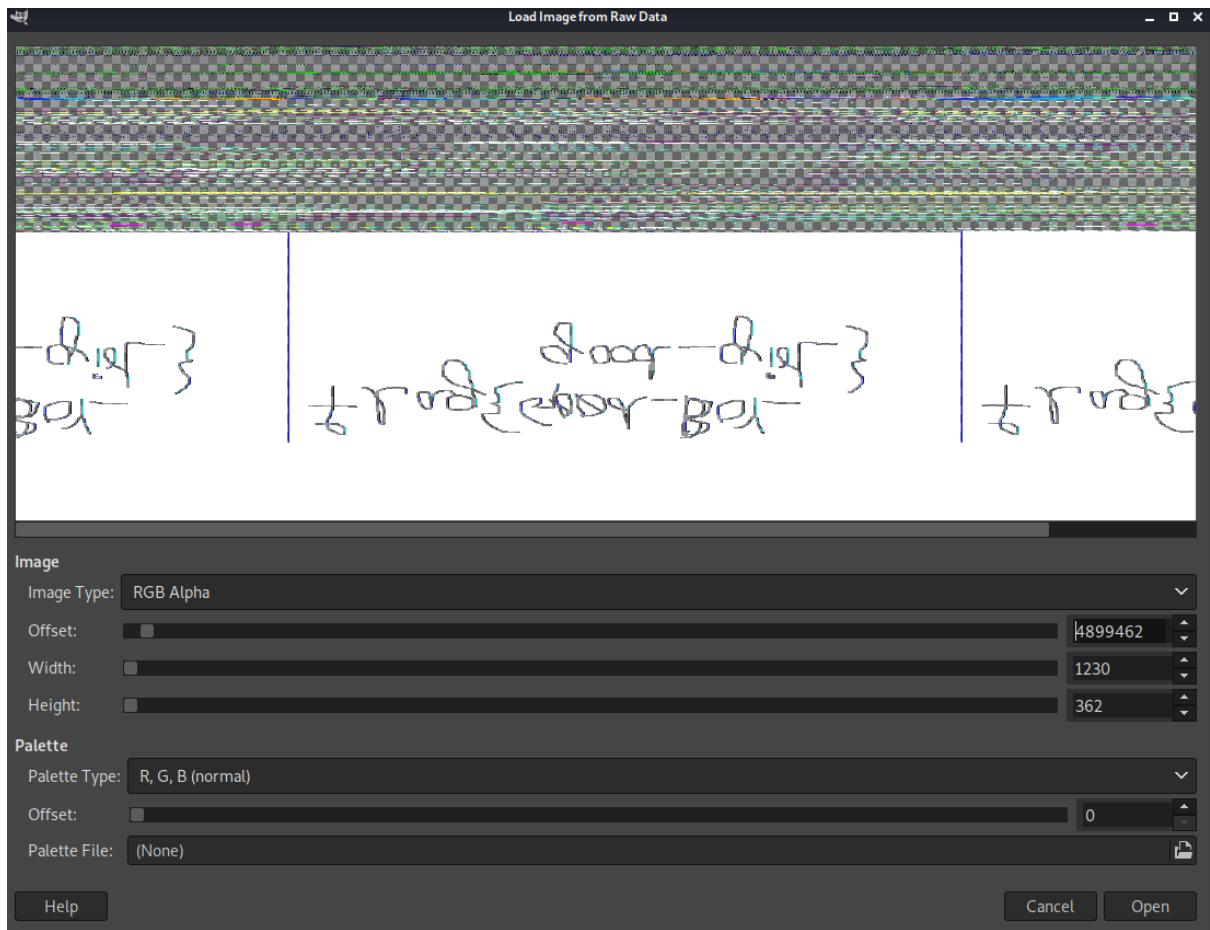


Na installatie nemen we een memdump van het mspaint.exe proces en renamen we het naar .data zodat Gimp deze herkent en kan openen.

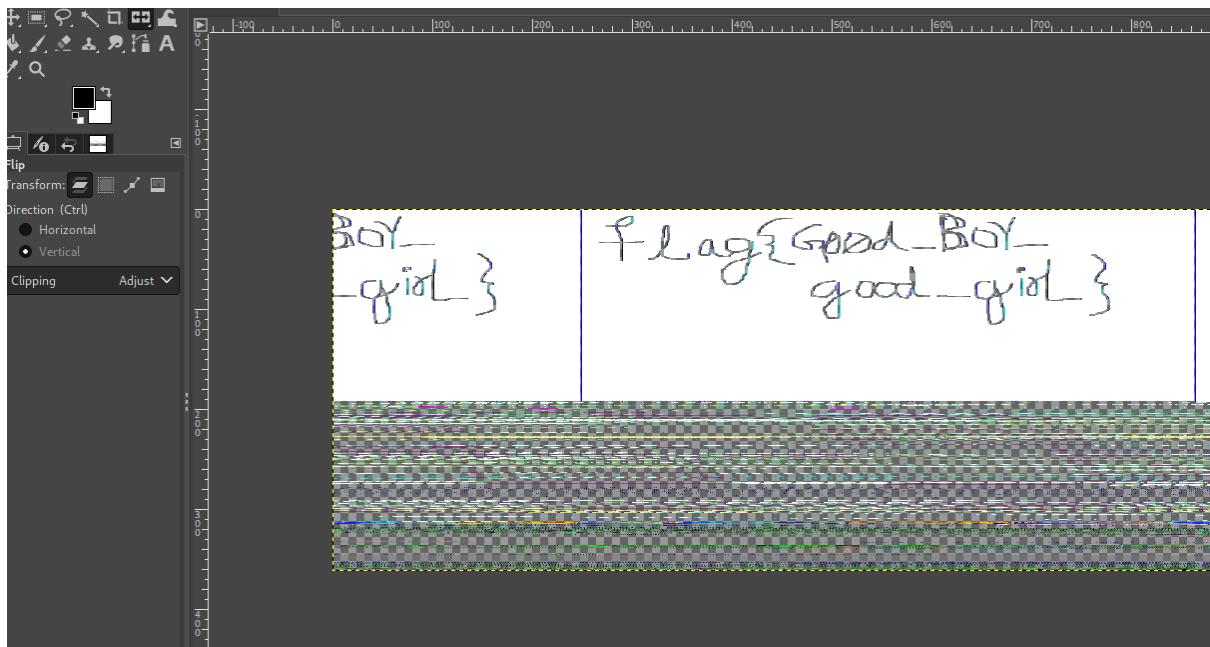
```
>sudo python vol.py -f ..\Alissas-PC.raw --profile=Win7SP1x64 memdump -p 2424 -D ..\dump\
```



Na wat spelen met de offset krijgen we onderstaande resultaat!



En als we de picture omdraaien, krijgen we de oplossing!  
=> flag{G00d\_BOY\_good\_girl\_}



Samenvatting:

Opdracht1 : Windows Wachtwoord = flag{th1s\_1s\_th3\_1st\_st4g3!!}

Opdracht2: Important.rar = flag{w311\_3rd\_stage\_was\_easy}

Opdracht3: MSPaint = flag{G00d\_BOY\_good\_girl\_}

## Level A(+) requirements

### Voorbereiding

#### Installeren Autopsy op Kali

Installatie was al gebeurd in de VM gedownload van Offensive Security => versie 2.24

Downloaden forensic image and memory dump of Steve Kowhai (Narcos-1) van

<https://digitalcorpora.org/corpora/scenarios/2019-narcos>

#### Start nieuwe Autopsy Case

\* Start autopsy in Kali Linux:

**>sudo autopsy**

```
(kali㉿kali)-[~] kali 1572864000 Feb 17 2019 Narcos-1.003
$ sudo autopsy
[sudo] password for kali:
[kali] 1572864000 Feb 17 2019 Narcos-1.004
[kali] 1572864000 Feb 17 2019 Narcos-1.005
[kali] 1572864000 Feb 17 2019 Narcos-1.006
[kali] 1572864000 Feb 17 2019 Narcos-1.007
[kali] 1572864000 Feb 17 2019 Narcos-1.008
[kali] 1572864000 Feb 17 2019 Narcos-1.009
Autopsy Forensic Browser
[kali] http://www.sleuthkit.org/autopsy/
[kali] ver 2.24
[kali] 1572864000 Feb 17 2019 Narcos-1.011
[kali] 1572864000 Feb 17 2019 Narcos-1.012
[kali] 1572864000 Feb 17 2019 Narcos-1.013
Evidence Locker: /var/lib/autopsy
Start Time: Sun May 30 05:55:36 2021
Remote Host: localhost
Local Port: 9999
Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy
Keep this process running and use <ctrl-c> to exit
(kali㉿kali)-[~/Downloads/Narcos-1/Image]
```

\* Ga naar <http://localhost:9999/autopsy> in de browser.

\* Kies "New Case"

① localhost:9999/autopsy

Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

WARNING: Your browser currently has Java Script enabled.

You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

Autopsy Forensic Browser 2.24

<http://www.sleuthkit.org/autopsy/>

OPEN CASE NEW CASE HELP

\* Kies weer "New Case" na het invullen van enkele gegevens

**CREATE A NEW CASE**

**1. Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

BlueTeamNarcos2019

**2. Description:** An optional, one line description of this case.

Opdracht 2TIW Security Advanced

**3. Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. JanVinkenroye	b. VinceWouters
c. WardLenaerts	d.
e.	f.
g.	h.
i.	j.

**NEW CASE**      **CANCEL**      **HELP**

\* Klik "Add Host"

**Creating Case: BlueTeamNarcos**

Case directory (/var/lib/autopsy/BlueTeamNarcos/) created  
Configuration file (/var/lib/autopsy/BlueTeamNarcos/case.aut) created

We must now create a host for this case.

Please select your name from the list: WardLenaerts ▾

**ADD HOST**

\* Klik weer “Add Host” na het invullen van enkele velden

**ADD A NEW HOST**

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

host1

2. **Description:** An optional one-line description or note about this computer.

Opdracht 3 Blue team

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

GMT

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

0

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

**ADD HOST**    **CANCEL**    **HELP**

\* Klik "Add Image"

## Adding host: host1 to case BlueTeamNarcos

Host Directory (/var/lib/autopsy/BlueTeamNarcos/host1/) created

Configuration file (/var/lib/autopsy/BlueTeamNarcos/host1/host.aut) created

We must now import an image file for this host

**ADD IMAGE**

\* Klik "Add Image File"

Case: BlueTeamNarcos  
Host: host1

No images have been added to this host yet

Select the Add Image File button below to add one

**ADD IMAGE FILE**

**CLOSE HOST**

**HELP**

**FILE ACTIVITY TIME LINES**

**IMAGE INTEGRITY**

**HASH DATABASES**

**VIEW NOTES**

**EVENT SEQUENCER**

\* Klik "Next" na het invullen van de nodige velden

Case: BlueTeamNarcos  
Host: host1

**ADD A NEW IMAGE**

### 1. Location

Enter the full path (starting with /) to the image file.  
If the image is split (either raw or EnCase), then enter '\*' for the extension.

/home/kali/Downloads/Narcos-1/Image/Narcos-1.\*

### 2. Type

Please select if this image file is for a disk or a single partition.

Disk

Partition

### 3. Import Method

To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

Symlink

Copy

Move

**NEXT**

**CANCEL**

**HELP**

\* Klik weer "Next"

## Split Image Confirmation

The following images will be added to the case.

If this is not the correct order, then you should change the naming convention.

Press the Next button at the bottom of the page if this is correct.

- 0 /home/kali/Downloads/Narcos-1/Image/Narcos-1.001
- 1 /home/kali/Downloads/Narcos-1/Image/Narcos-1.002
- 2 /home/kali/Downloads/Narcos-1/Image/Narcos-1.003
- 3 /home/kali/Downloads/Narcos-1/Image/Narcos-1.004
- 4 /home/kali/Downloads/Narcos-1/Image/Narcos-1.005
- 5 /home/kali/Downloads/Narcos-1/Image/Narcos-1.006
- 6 /home/kali/Downloads/Narcos-1/Image/Narcos-1.007
- 7 /home/kali/Downloads/Narcos-1/Image/Narcos-1.008
- 8 /home/kali/Downloads/Narcos-1/Image/Narcos-1.009
- 9 /home/kali/Downloads/Narcos-1/Image/Narcos-1.010
- 10 /home/kali/Downloads/Narcos-1/Image/Narcos-1.011
- 11 /home/kali/Downloads/Narcos-1/Image/Narcos-1.012
- 12 /home/kali/Downloads/Narcos-1/Image/Narcos-1.013
- 13 /home/kali/Downloads/Narcos-1/Image/Narcos-1.014
- 14 /home/kali/Downloads/Narcos-1/Image/Narcos-1.015
- 15 /home/kali/Downloads/Narcos-1/Image/Narcos-1.016
- 16 /home/kali/Downloads/Narcos-1/Image/Narcos-1.017
- 17 /home/kali/Downloads/Narcos-1/Image/Narcos-1.018
- 18 /home/kali/Downloads/Narcos-1/Image/Narcos-1.019
- 19 /home/kali/Downloads/Narcos-1/Image/Narcos-1.020
- 20 /home/kali/Downloads/Narcos-1/Image/Narcos-1.021

NEXT

CANCEL

\* Vul de meegeleverde hash in om de integriteit te controleren . Klik "Add"

## Image File Details

**Local Name:** "/home/kali/Downloads/Narcos-1/Image/Narcos-1.001"  
"/home/kali/Downloads/Narcos-1/Image/Narcos-1.002" "/home  
/kali/Downloads/Narcos-1/Image/Narcos-1.003" "/home/kali/Downloads  
/Narcos-1/Image/Narcos-1.004" "/home/kali/Downloads/Narcos-1/Image  
/Narcos-1.005" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.006"  
"/home/kali/Downloads/Narcos-1/Image/Narcos-1.007" "/home  
/kali/Downloads/Narcos-1/Image/Narcos-1.008" "/home/kali/Downloads  
/Narcos-1/Image/Narcos-1.009" "/home/kali/Downloads/Narcos-1/Image  
/Narcos-1.010" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.011"  
"/home/kali/Downloads/Narcos-1/Image/Narcos-1.012" "/home  
/kali/Downloads/Narcos-1/Image/Narcos-1.013" "/home/kali/Downloads  
/Narcos-1/Image/Narcos-1.014" "/home/kali/Downloads/Narcos-1/Image  
/Narcos-1.015" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.016"  
"/home/kali/Downloads/Narcos-1/Image/Narcos-1.017" "/home  
/kali/Downloads/Narcos-1/Image/Narcos-1.018" "/home/kali/Downloads  
/Narcos-1/Image/Narcos-1.019" "/home/kali/Downloads/Narcos-1/Image  
/Narcos-1.020" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.021"

**Data Integrity:** An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

- Ignore the hash value for this image.
- Calculate the hash value for this image.
- Add the following MD5 hash value for this image:

c63a3d19e9c9495b573f45be544e50f9

Verify hash after importing?

**File System Details**

Analysis of the image file shows the following partitions:

**Partition 1** (Type: Basic data partition)  
 Add to case?  
 Sector Range: 2048 to 1023999  
 Mount Point: C: File System Type: ntfs

**Partition 2** (Type: EFI system partition)  
 Add to case?  
 Sector Range: 1024000 to 1226751  
 Mount Point: D: File System Type: fat32

**Partition 3** (Type: Microsoft reserved partition)  
 Add to case?  
 Sector Range: 1226752 to 1259519  
 Mount Point: /3/ File System Type: raw

**Partition 4** (Type: Basic data partition)  
 Add to case?  
 Sector Range: 1259520 to 62912511  
 Mount Point: E: File System Type: ntfs

**ADD**    **CANCEL**    **HELP**

For your reference, the `mmls` output was the following:

```
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors

Slot Start End Length Description
004: 000 0000002048 0001023999 0001021952 Basic data partition
005: 001 0001024000 0001226751 00000202752 EFI system partition
006: 002 0001226752 0001259519 00000032768 Microsoft reserved partition
007: 003 0001259520 0062912511 0061652992 Basic data partition
```

**Calculating MD5 (this could take a while)**

\* \*

\* Klik "OK"

```
Calculating MD5 (this could take a while)
Current MD5: c63A3D19E9C9495B573F45BE544E50F9
Integrity Check Passed
Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1

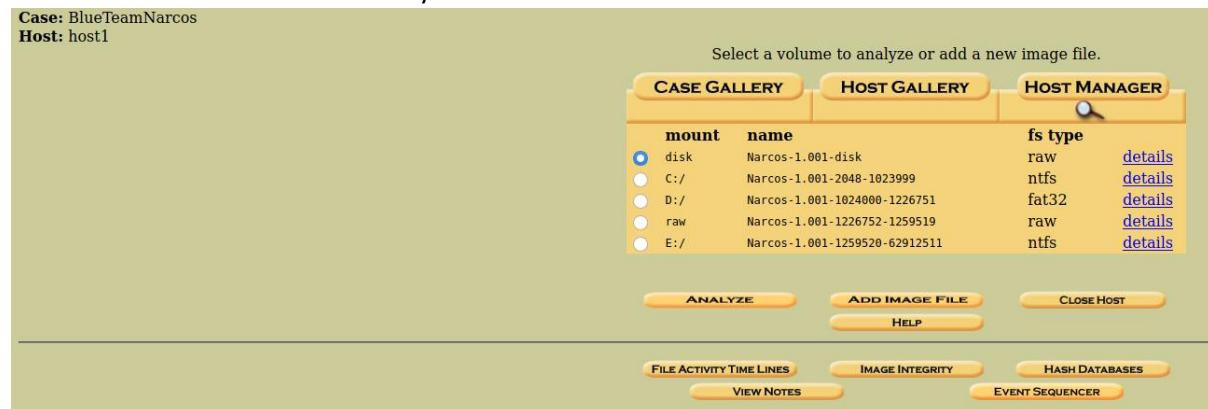
Disk image (type gpt) added with ID vol1
Volume image (2048 to 1023999 - ntfs - C:) added with ID vol2
Volume image (1024000 to 1226751 - fat32 - D:) added with ID vol3
Volume image (1226752 to 1259519 - raw - /3/) added with ID vol4
Volume image (1259520 to 62912511 - ntfs - E:) added with ID vol5
```

OK

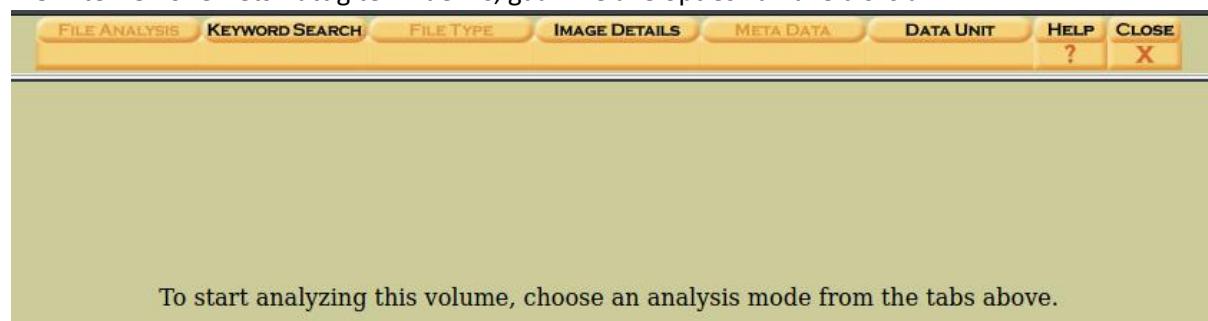
ADD IMAGE

## Analyse

\* Selecteer een disk een klik “Analyze”



\* Om te zien of er iets nuttig te vinden is, gaan we alle opties van alle disks af



\* We onderzoeken enkel “nuttige” informatie gebaseerd op de info die we ontvangen hebben:

1. *“Their chat contains information on where they are going and what he wants John Fredricksen to deliver. Furthermore, Steve shares some documents via (email, cloud, etc) that will assist with his job.”*
2. *“Steve has provided John with information about New Zealand and points on how best to smuggle the product into Wellington without raising any alarms at customs. Steve knows a thing or two about digital forensics and decided to use steganography to hide the document within a picture.”*

De enige nuttige partitie lijkt de E-partitie. Hier vinden we sporen van Discord en verschillende mogelijk nuttige files en pictures terug.

\* In E:/ProgramData/Microsoft/Diagnosis/osver.txt lezen we alvast dat er een windows 10 october 2018 update draait

Contents Of File: E:/ProgramData/Microsoft/Diagnosis/osver.txt

10.0.17763

[Article](#) [Talk](#)

[Read](#) [Edit](#) [View history](#) [Search](#)

## Windows 10 version history (version 1809)

From Wikipedia, the free encyclopedia

**Windows 10 October 2018 Update**<sup>[1]</sup> (also known as **version 1809**<sup>[2]</sup> and codenamed "**Redstone 5**") is the sixth major update to Windows 10 and the fifth in a series of updates under the Redstone codenames. It carries the build number **10.0.17763**.

### Version history [\[edit\]](#)

En een programma "Image Stenography"!

**Current Directory:** [E:/ /Users/ /Steve/ /AppData/ /Roaming/ /Image\\_Steganography/ /Image\\_Steganography/ /1.5.2.0/](#)

[ADD NOTE](#) [GENERATE MD5 LIST OF FILES](#)

Deze versie kan gedownload worden van

<https://www.softpedia.com/get/Multimedia/Graphic/Graphic-Editors/Image-Steganography.shtml>

### Onderzoeken van Discord

(source: <https://abrigonni.blogspot.com/2018/03/finding-discord-app-chats-in-windows.html> )

We trekken een volledige lijst van files aanwezig op deze drive.

The screenshot shows the Autopsy Forensic Browser interface. The top navigation bar includes links for Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, NetHunter, Offensive Security, MSFU, Exploit-DB, GHDB, FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE (which is selected), IMAGE DETAILS, META DATA, DATA UNIT, HELP, and CLOSE. A message in the center states: "File Type Sorting" and "Autopsy does not currently support viewing the sorted files. After sorting, you can view the results by opening the following file: /var/lib/autopsy/BlueTeamNarcos/host1/output/sorter-vol5/index.html". On the left, there are links for "Sort Files by Type" and "View Sorted Files".

Volledige lijst wordt door autopsy opgeslagen in  
file:///var/lib/autopsy/BlueTeamNarcos/host1/output/sorter-vol5/data.html

## Enkele mogelijk belangrijke files hier:

file:///var/lib/autopsy/BlueTeamNarcos/host1/output/sorter-vol5/images.html							
Kali Linux  Kali Tools  Kali Docs  Offensive Security  Exploit-DB MS Windows icon resource - 3 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel Image: /var/lib/autopsy/BlueTeamNarcos/host1/images/Narcos-1.001 Inode: 96198-128-3							
E:/Users/Steve/AppData/Roaming/Discord/badge-8.ico		MS Windows icon resource - 3 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel					
Image: /var/lib/autopsy/BlueTeamNarcos/host1/images/Narcos-1.001 Inode: 96199-128-3							
E:/Users/Steve/AppData/Roaming/Discord/badge-9.ico		MS Windows icon resource - 3 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel					
Image: /var/lib/autopsy/BlueTeamNarcos/host1/images/Narcos-1.001 Inode: 96200-128-3							
E:/Users/Steve/AppData/Roaming/Discord/Cache/f_00000d		JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1920x1080, components 3					
Image: /var/lib/autopsy/BlueTeamNarcos/host1/images/Narcos-1.001 Inode: 96235-128-3							
E:/Users/Steve/AppData/Roaming/Discord/Cache/f_00000e		PNG image data, 1058 x 1113, 8-bit colormap, non-interlaced					
Image: /var/lib/autopsy/BlueTeamNarcos/host1/images/Narcos-1.001 Inode: 96236-128-3							
E:/Users/Steve/AppData/Roaming/Discord/Cache/f_000016		PNG image data, 1890 x 776, 8-bit/color RGB, non-interlaced					
Image: /var/lib/autopsy/BlueTeamNarcos/host1/images/Narcos-1.001 Inode: 96432-128-3							
E:/Users/Steve/AppData/Roaming/Discord/Cache/f_00001d		PNG image data, 484 x 220, 8-bit/color RGBA, non-interlaced					
Image: /var/lib/autopsy/BlueTeamNarcos/host1/images/Narcos-1.001 Inode: 96464-128-3							
E:/Users/Steve/AppData/Roaming/Discord/Cache/f_000029		PNG image data, 1024 x 576, 8-bit/color RGBA, non-interlaced					
Image: /var/lib/autopsy/BlueTeamNarcos/host1/images/Narcos-1.001 Inode: 100158-128-3							
E:/Users/Steve/AppData/Roaming/Discord/Cache/f_00003b		PNG image data, 1280 x 720, 8-bit colormap, non-interlaced					
Image: /var/lib/autopsy/BlueTeamNarcos/host1/images/Narcos-1.001 Inode: 88392-128-3							
E:/Users/Steve/AppData/Roaming/Discord/Cache/f_000041		PNG image data, 1024 x 576, 8-bit/color RGB, non-interlaced					
Image: /var/lib/autopsy/BlueTeamNarcos/host1/images/Narcos-1.001 Inode: 87802-128-3							

## En

E:/Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Cache/f\_000361  
JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=19, height=3648, bps=242, PhotometricIntepretation=RGB, description=AUCKLAND, NEW ZEALAND - DECEMBER 13: Kendra Cocksedge holds the Kelvin R Tremain Memorial Player of the Year Award during the 2, manufacturer=Canon, model=Canon EOS-1D X Mark II, orientation=upper-left, width=5472], baseline, precision 8, 502x268, components 3  
Image: /var/lib/autopsy/BlueTeamNarcos/host1/images/Narcos-1.001 Inode: 88304

E:/Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Cache/f\_000361

JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=19, height=3648, bps=242, PhotometricIntepretation=RGB, description=AUCKLAND, NEW ZEALAND - DECEMBER 13: Kendra Cocksedge holds the Kelvin R Tremain Memorial Player of the Year Award during the 2, manufacturer=Canon, model=Canon EOS-1D X Mark II, orientation=upper-left, width=5472], baseline, precision 8, 502x268, components 3  
Image: /var/lib/autopsy/BlueTeamNarcos/host1/images/Narcos-1.001 Inode: 88304

## Onderzoek van deleted files in the Recycle bin levert ons de volgende files op:

Current Directory: E:/ /Recycle.Bin/										
ADD NOTE GENERATE MD5 LIST OF FILES										
DEL	Type	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
r / r	dir	<a href="#">\$35WIK39.jpg</a>	2019-02-01 02:48:41 (GMT)	2019-02-01 02:38:06 (GMT)	2019-02-01 02:48:41 (GMT)	2019-02-01 02:48:41 (GMT)	128	0	0	<a href="#">828-128-1</a>
r / r	dir	<a href="#">\$3A3TE5E.jpg</a>	2019-02-01 02:48:41 (GMT)	2019-02-01 02:48:41 (GMT)	2019-02-01 02:48:41 (GMT)	2019-02-01 02:48:41 (GMT)	120	0	0	<a href="#">808-128-1</a>
r / r	dir	<a href="#">\$3T1K1AS.jpg</a>	2019-02-01 02:48:41 (GMT)	2019-02-01 02:48:41 (GMT)	2019-02-01 02:48:41 (GMT)	2019-02-01 02:48:41 (GMT)	100	0	0	<a href="#">810-128-1</a>
r / r	dir	<a href="#">\$R5WIK39.jpg</a>	2019-01-31 02:59:38 (GMT)	2019-02-01 02:42:46 (GMT)	2019-02-01 02:48:41 (GMT)	2019-01-31 02:59:38 (GMT)	86240	0	0	<a href="#">90267-128-4</a>
r / r	dir	<a href="#">\$R5WIK39.jpg_Zone.Identifier</a>	2019-01-31 02:59:38 (GMT)	2019-02-01 02:42:46 (GMT)	2019-02-01 02:48:41 (GMT)	2019-01-31 02:59:38 (GMT)	159	0	0	<a href="#">90267-128-9</a>
r / r	dir	<a href="#">\$R3A3TE5E.jpg</a>	2019-01-31 02:58:22 (GMT)	2019-02-01 03:04:13 (GMT)	2019-02-01 02:48:41 (GMT)	2019-01-31 02:58:22 (GMT)	118136	0	0	<a href="#">23371-128-4</a>
r / r	dir	<a href="#">\$R3A3TE5E.jpg_Zone.Identifier</a>	2019-01-31 02:58:22 (GMT)	2019-02-01 03:04:13 (GMT)	2019-02-01 02:48:41 (GMT)	2019-01-31 02:58:22 (GMT)	163	0	0	<a href="#">23371-128-9</a>
r / r	dir	<a href="#">\$R1T1K1AS.jpg</a>	2019-01-31 02:57:06 (GMT)	2019-01-31 03:04:13 (GMT)	2019-02-01 02:48:41 (GMT)	2019-01-31 02:57:06 (GMT)	19342	0	0	<a href="#">21221-128-4</a>
r / r	dir	<a href="#">\$R1T1K1AS.jpg_Zone.Identifier</a>	2019-01-31 02:57:06 (GMT)	2019-02-01 03:04:13 (GMT)	2019-02-01 02:48:41 (GMT)	2019-01-31 02:57:06 (GMT)	360	0	0	<a href="#">21221-128-8</a>
d / d	dir	<a href="#">..</a>	2019-01-29 20:58:41 (GMT)	2019-02-01 02:48:41 (GMT)	2019-01-29 20:58:41 (GMT)	2018-09-15 07:33:50 (GMT)	712	0	0	<a href="#">64-144-1</a>

We merken dat de eerste file eindigt op jpg, maar in feite geen picture, maar een datafile is! Dit is verdacht!

**Pointed to by file:**

E:/\$Recycle.Bin/S-1-5-21-1474204758-2504895174-1356074821-1001/\$I5WIK39.jpg

**File Type:**

data

We vinden hier via Hex een path naar een picture

Hex Contents Of File: E:/vol5-meta-828-128-1

00000000:	0200 0000 0000 0000 E050 0100 0000 0000	.....P.....
00000010:	4000 1CA4 D8B9 D401 3200 0000 4300 3A00	@.....2...C..:
00000020:	5C00 5500 7300 6500 7200 7300 5C00 5300	\.U.s.e.r.s.\.S.
00000030:	7400 6500 7600 6500 5C00 5000 6900 6300	t.e.v.e.\.P.i.c.
00000040:	7400 7500 7200 6500 7300 5C00 6500 6900	t.u.r.e.s.\.e.i.
00000050:	6700 6800 7400 5F00 6300 6F00 6C00 5F00	g.h.t._.c.o.l._.
00000060:	7000 6100 7400 6300 6800 6500 7300 5F00	p.a.t.c.h.e.s._.
00000070:	6300 7200 7000 2E00 6A00 7000 6700 0000	c.r.p...j.p.g...

Voluit staat hier [....P...@2.c/Users/Steve/Pictures/eight\\_cols\\_patches\\_crp.jpg](#).

Iets soortgelijk vinden we voor de tweede file

Hex Contents Of File: E:/\$Recycle.Bin/S-1-5-21-1474204758-2504895174-1356074821-1001/\$IA3IE5E.jpg

00000000:	0200 0000 0000 0000 78CD 0100 0000 0000	.....x.....
00000010:	802B 1AA4 D8B9 D401 2E00 0000 4300 3A00	.+.....C..:
00000020:	5C00 5500 7300 6500 7200 7300 5C00 5300	\.U.s.e.r.s.\.S.
00000030:	7400 6500 7600 6500 5C00 5000 6900 6300	t.e.v.e.\.P.i.c.
00000040:	7400 7500 7200 6500 7300 5C00 7000 7200	t.u.r.e.s.\.p.r.
00000050:	6900 6300 6500 2D00 6D00 6500 7400 6800	i.c.e.-.m.e.t.h.
00000060:	2D00 6200 7500 7300 7400 2D00 3400 2E00	-b.u.s.t.-.4...
00000070:	6A00 7000 6700 0000	j.p.g...

En voor de derde file

Hex Contents Of File: E:/\$Recycle.Bin/S-1-5-21-1474204758-2504895174-1356074821-1001/\$IIIK1AS.jpg

00000000:	0200 0000 0000 0000 8E4B 0000 0000 0000	.....K.....
00000010:	20B2 1BA4 D8B9 D401 2400 0000 4300 3A00	.....\$...C..:
00000020:	5C00 5500 7300 6500 7200 7300 5C00 5300	\.U.s.e.r.s.\.S.
00000030:	7400 6500 7600 6500 5C00 5000 6900 6300	t.e.v.e.\.P.i.c.
00000040:	7400 7500 7200 6500 7300 5C00 3600 3200	t.u.r.e.s.\.6.2.
00000050:	3000 7800 3300 3400 3900 2E00 6A00 7000	0.x.3.4.9...j.p.
00000060:	6700 0000	g...

Onderzoek naar “cloud”-toepassingen

We vinden dan snel Onedrive

Current Directory: E:/ /Users/ /Steve/ /OneDrive/ /Documents/				
		GENERATE MD5 LIST OF FILES		
DEL	Type <u>dir</u> / <u>in</u>	NAME 	WRITTEN	ACCESSED
	d / d	<u>..</u>	2019-02-02 02:38:49 (GMT)	2019-02-02 02:38:51 (GMT)
	d / d	<u>..</u>	2019-02-01 02:40:55 (GMT)	2019-02-02 02:38:51 (GMT)
	r / r	<u>Steve's Notebook.url</u>	2019-02-01 00:25:39 (GMT)	2019-02-01 02:41:35 (GMT)

ASCII ([display](#) - [report](#)) \* Hex ([display](#) - [report](#))  
File Type: MS Windows 95 Internet shortcut text (URL=)

Contents Of File: E:/Users/Steve/OneDrive/Documents/Steve's Notebook.url

```
[InternetShortcut]
URL=https://onedrive.live.com/redir.aspx?cid=2418c0082017486a&resid=2418C0082017486A!105&type=3
```

Zelfreflectie na het doorlopen van de opdrachten:

NOTE van (lichte) frustratie: Ik heb Wine geinstalleerd op mijn Kali Linux om de 2 windows programma's te kunnen runnen in mijn VM, maar ik krijg ze niet aan de praat ... :-(  
 ChromeCacheView v1.77 om de discord files uit te lezen  
 image steganography 1.5.2.0 om de images die gecodeerd werden door Suspect Steve te kunnen "decoden"

Als "leek" in het security-gebeuren had ik verwacht dat alles zich voornamelijk in de linux-wereld zou afspelen, maar voor de laatste opdracht valt het vinden van alternatieve tools mij hard tegen.  
 Ik lees over Hindsight, Steghide, Stegosuite,... en heb deze ook geprobeerd, maar ik blijf botsen tegen problemen waardoor ik niet helemaal tot aan de oplossing van 3 geraakt ben.  
 Ik heb het gevoel dat ik er heel kort bij zit, maar dat mijn persoonlijke hardware mij de das om doet. Mijn CPU heeft vaak tegen 100% gedraaid en ik heb mijn harde schijf van 500GB grondig moeten opkuisen om zelfs al maar te kunnen beginnen aan de opdracht.  
 Ik vond het wel heel leuke opdrachten en heb er ook enorm veel van opgestoken. Het niveau is voor mij persoonlijk erg hoog, maar dat maakt de uitdaging zoveel leuker.

MVG,

Ward Lenaerts