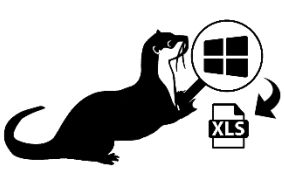


AIO FORENSICS

OTTER DOCUMENTATION

Last update on 20/10/2019

OTTER DESCRIPTION

1. What is Otter?

Otter is an **all-in-one Windows Forensic tool** that extracts data from the registry and other sources, analyzes it and generates an **investigative report** in xlsx format.

Otter can perform reconnaissance on Windows processes, DLL's, programs that run at startup and those that have been run by the user, wireless/wired network connections, user accounts and group membership, USB devices connected to system, user activities including documents recently opened, and more. It also comes with tips for Forensic Investigation and a scoring system for malware analysis which allows you to quickly write down the attack scenario.

2. What are the requirements?

Otter is able to run on **x64-bit and x86-bit** Windows systems including **virtualized machines.**

It doesn't require an internet connection and there is no need to install anything to use it.

After license expiry date, nothing should be uninstalled. Just delete it.

3. What are the key features?

All-In-One tool:
Otter performs live acquisition, analysis and reporting.

One Click tool:
Otter is user-friendly, you just need to launch otter.exe.

Customizable tool:
Otter can be customized to suit your needs : change default colors of the investigative report, incorporate your logo in it and remove or add new worksheets. For further details, contact the customer service.

4. Who can use Otter?

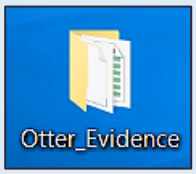
Digital Forensic examiners and investigators, Cybersecurity Analysts SOC, IT HELP Desk, and anyone who wants to perform Digital investigation and learns Digital Forensic tips.

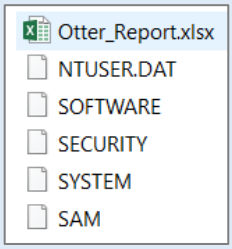
5. How do I use Otter?

Simply launch Otter.exe.

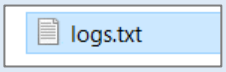
- Two folders will be created on the current user desktop:

- **Otter_Evidence:** contains the registry files SAM, SECURITY, SYSTEM, SOFTWARE, the NTUSER.dat file and the results report.





- **Otter_logs:** contains the log file that records actions performed on the machine



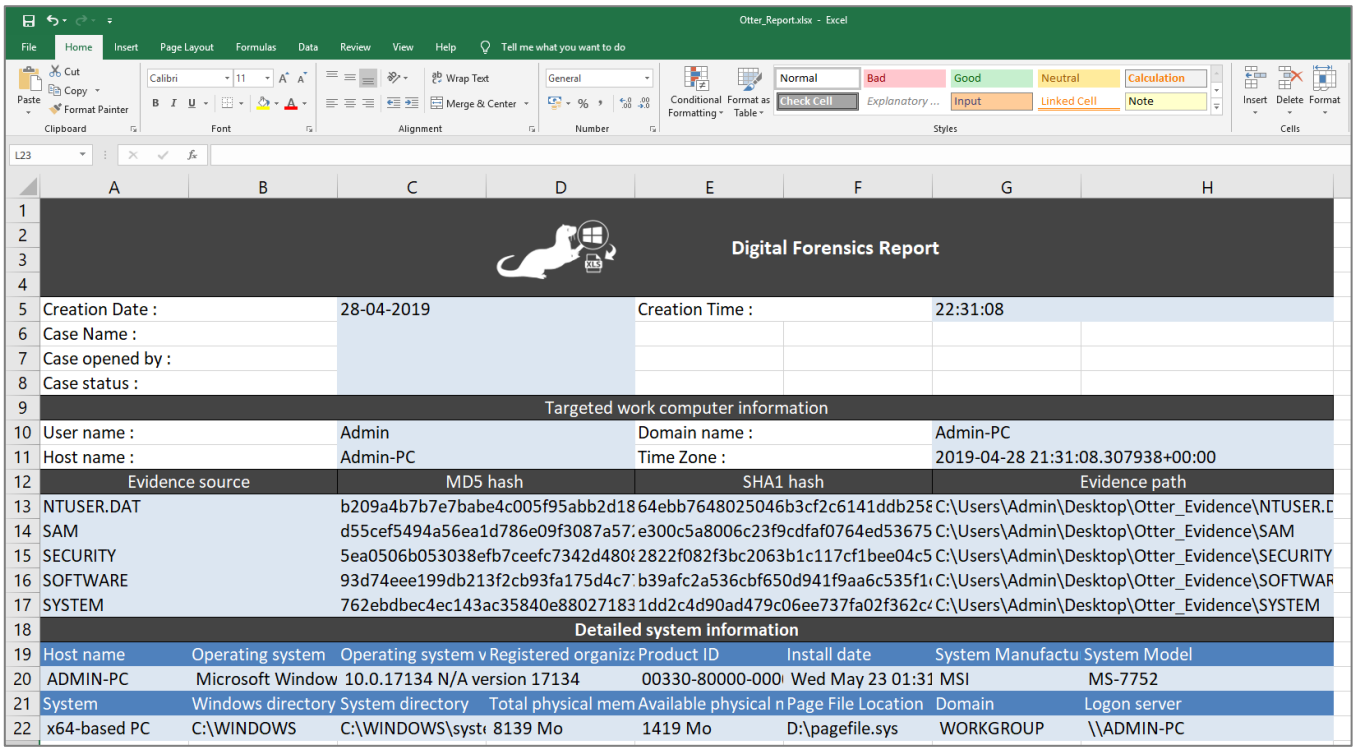
6. What does the results report in excel format contain?

Otter_Report.xlsx contains **12** worksheets:

1. Global summary, detailed system information, MD5 and SHA-1 hashes of registry files
2. Analysis tips for Forensic Investigation
3. User accounts and group membership list
4. Process list
5. Process legitimacy analysis
6. DLL's
7. Documents recently opened
8. USB devices connected to system
9. Programs run by the user
10. Programs running at startup
11. Wireless/wired network connections
12. Malware analysis with a scoring system

OTTER RESULTS REPORT

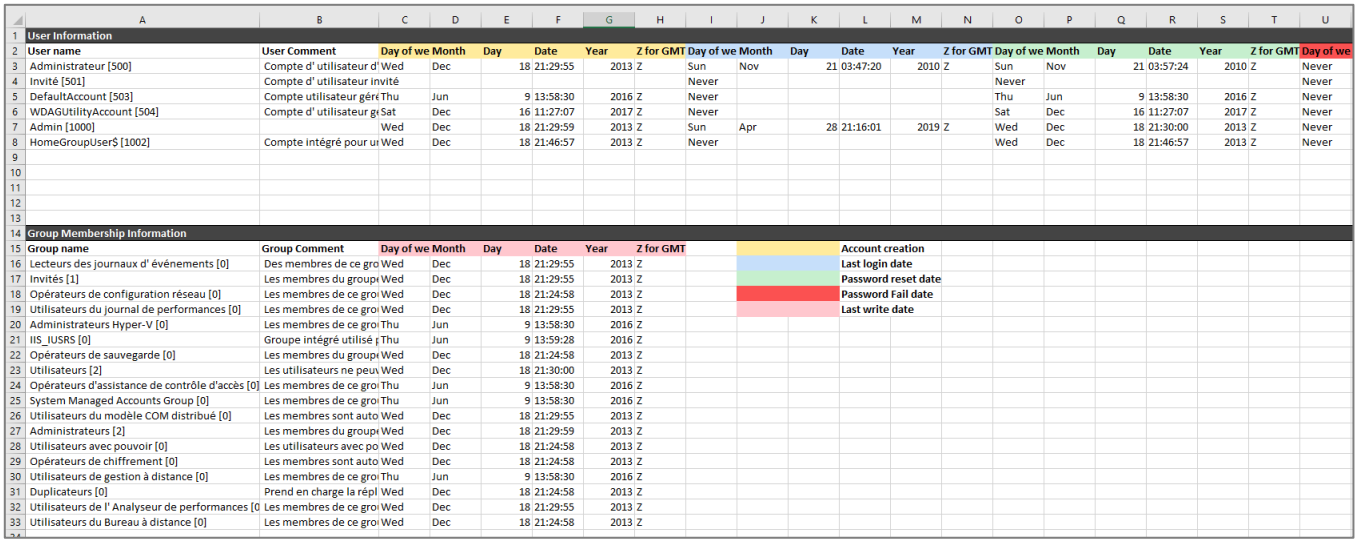
- **Summary**



Otter_Report.xlsx - Excel

			Digital Forensics Report				
Creation Date :	28-04-2019			Creation Time :		22:31:08	
Case Name :							
Case opened by :							
Case status :							
Targeted work computer information							
User name :	Admin			Domain name :		Admin-PC	
Host name :	Admin-PC			Time Zone :		2019-04-28 21:31:08.307938+00:00	
Evidence source	**MD5 hash**			**SHA1 hash**		**Evidence path**	
NTUSER.DAT	b209a4b7b7e7babe4c005f95abb2d18			64ebb7648025046b3cf2c6141ddb258		C:\Users\Admin\Desktop\Otter_Evidence\NTUSER.D	
SAM	d55cef5494a56ea1d786e09f3087a57			e300c5a8006c23f9cdfaf0764ed53675		C:\Users\Admin\Desktop\Otter_Evidence\SAM	
SECURITY	5ea0506b053038efb7ceefc7342d480			2822f082f3bc2063b1c117cf1bee04c5		C:\Users\Admin\Desktop\Otter_Evidence\SECURITY	
SOFTWARE	93d74eee199db213f2cb93fa175d4c7			b39afc2a536cbf650d941f9aa6c535f1		C:\Users\Admin\Desktop\Otter_Evidence\SOFTWAR	
SYSTEM	762ebdbec4ec143ac35840e880271831			dd2c4d90ad479c06ee737fa02f362c4		C:\Users\Admin\Desktop\Otter_Evidence\SYSTEM	
Detailed system information							
Host name	**Operating system**	**Operating system v**	**Registered organiza**	**Product ID**	**Install date**	**System Manufactu**	**System Model**
ADMIN-PC	Microsoft Window	10.0.17134 N/A version 17134		00330-80000-000	Wed May 23 01:31	MSI	MS-7752
System	**Windows directory**	**System directory**	**Total physical mem**	**Available physical n**	**Page File Location**	**Domain**	**Logon server**
x64-based PC	C:\WINDOWS	C:\WINDOWS\syst	8139 Mo	1419 Mo	D:\pagefile.sys	WORKGROUP	\\ADMIN-PC

- **User accounts and group membership list**



User Information																				
User name	**User Comment**	**Day of we**	**Month**	**Day**	**Date**	**Year**	**Z for GMT**	**Day of we**	**Month**	**Day**	**Date**	**Year**	**Z for GMT**	**Day of we**	**Month**	**Day**	**Date**	**Year**	**Z for GMT**	**Day of we**
Administrateur [500]	Compte d' utilisateur d'	Wed	Dec	18	21:29:55	2013	Z	Sun	Nov	21	03:47:20	2010	Z	Sun	Nov	21	03:57:24	2010	Z	Never
Invité [501]	Compte d' utilisateur invité							Never						Never						Never
DefaultAccount [503]	Compte utilisateur géré	Thu	Jun	9	13:58:30	2016	Z	Never						Thu	Jun	9	13:58:30	2016	Z	Never
WDAGUtilityAccount [504]	Compte d' utilisateur g	Sat	Dec	16	11:27:07	2017	Z	Never						Sat	Dec	16	11:27:07	2017	Z	Never
Admin [1000]		Wed	Dec	18	21:29:59	2013	Z	Sun	Apr	28	21:16:01	2019	Z	Wed	Dec	18	21:30:00	2013	Z	Never
HomeGroupUser$ [1002]	Compte intégré pour ut	Wed	Dec	18	21:46:57	2013	Z	Never						Wed	Dec	18	21:46:57	2013	Z	Never
Group Membership Information																				
Group name	**Group Comment**	**Day of we**	**Month**	**Day**	**Date**	**Year**	**Z for GMT**													
Lecteurs des journaux d' événements [0]	Des membres de ce gro	Wed	Dec	18	21:29:55	2013	Z													
Invités [1]	Les membres du groupe	Wed	Dec	18	21:29:55	2013	Z													
Opérateurs de configuration réseau [0]	Les membres de ce gro	Wed	Dec	18	21:24:58	2013	Z													
Utilisateurs du journal de performances [0]	Les membres de ce gro	Wed	Dec	18	21:29:55	2013	Z													
Administrateurs Hyper-V [0]	Les membres de ce gro	Thu	Jun	9	13:58:30	2016	Z													
IIS_IUSRS [0]	Groupe intégré utilisé p	Thu	Jun	9	13:59:28	2016	Z													
Opérateurs de sauvegarde [0]	Les membres du groupe	Wed	Dec	18	21:24:58	2013	Z													
Utilisateurs [2]	Les utilisateurs ne peu	Wed	Dec	18	21:30:00	2013	Z													
Opérateurs d'assistance de contrôle d'accès [0]	Les membres de ce gro	Thu	Jun	9	13:58:30	2016	Z													
System Managed Accounts Group [0]	Les membres de ce gro	Thu	Jun	9	13:58:30	2016	Z													
Utilisateurs du modèle COM distribué [0]	Les membres sont auto	Wed	Dec	18	21:29:55	2013	Z													
Administrateurs [2]	Les membres du groupe	Wed	Dec	18	21:29:59	2013	Z													
Utilisateurs avec pouvoir [0]	Les utilisateurs avec po	Wed	Dec	18	21:24:58	2013	Z													
Opérateurs de chiffrement [0]	Les membres sont auto	Wed	Dec	18	21:24:58	2013	Z													
Utilisateurs de gestion à distance [0]	Les membres de ce gro	Thu	Jun	9	13:58:30	2016	Z													
Duplicateurs [0]	Prend en charge la répl	Wed	Dec	18	21:24:58	2013	Z													
Utilisateurs de l' Analyseur de performances [0	Les membres de ce gro	Wed	Dec	18	21:29:55	2013	Z													
Utilisateurs du Bureau à distance [0]	Les membres de ce gro	Wed	Dec	18	21:24:58	2013	Z													

	Account creation
	Last login date
	Password reset date
	Password Fail date
	Last write date

- **Process list**

Name	PID	Session name	Session numb	Memory usag	State	User name	Process time	Windows name
System Idle Process	0	Services	0	8 Ko	Unknown	AUTORITE NT\Systme	319:52:09	N/A
System	4	Services	0	1156 Ko	Unknown	N/A	4:31:54	N/A
Registry	96	Services	0	136196 Ko	Unknown	AUTORITE NT\Systme	0:00:17	N/A
smss.exe	376	Services	0	408 Ko	Unknown	AUTORITE NT\Systme	0:00:00	N/A
csrss.exe	564	Services	0	1780 Ko	Unknown	AUTORITE NT\Systme	0:00:08	N/A
wininit.exe	656	Services	0	2676 Ko	Unknown	AUTORITE NT\Systme	0:00:00	N/A
services.exe	732	Services	0	5492 Ko	Unknown	AUTORITE NT\Systme	0:01:17	N/A

- **Process legitimacy**

[svchost.exe] Parent is services.exe. Check all svchost instances.			
Command Line	Executable Path	Parent PID	PID
c:\windows\system32\svchos	c:\windows\system32\svchos	732	932
C:\WINDOWS\system32\svch	C:\WINDOWS\system32\svch	732	960
c:\windows\system32\svchos	c:\windows\system32\svchos	732	512
c:\windows\system32\svchos	c:\windows\system32\svchos	732	820
c:\windows\system32\svchos	c:\windows\system32\svchos	732	1156
c:\windows\system32\svchos	c:\windows\system32\svchos	732	1164
c:\windows\system32\svchos	c:\windows\system32\svchos	732	1232
c:\windows\system32\svchos	c:\windows\system32\svchos	732	1304
C:\WINDOWS\system32\svch	C:\WINDOWS\system32\svch	732	1372
c:\windows\system32\svchos	c:\windows\system32\svchos	732	1436
c:\windows\system32\svchos	c:\windows\system32\svchos	732	1460
c:\windows\system32\svchos	c:\windows\system32\svchos	732	1552
c:\windows\system32\svchos	c:\windows\system32\svchos	732	1560
c:\windows\system32\svchos	c:\windows\system32\svchos	732	1568
c:\windows\system32\svchos	c:\windows\system32\svchos	732	1580

[lsass.exe] Parent is wininit.exe			
Command Line	Executable Path	Parent PID	PID
C:\WINDOWS\system32\lsass	C:\WINDOWS\system32\lsass	656	748

[v Parent is smss.exe, but	
Command Line	Exe
C:\WINDOWS\System32\Win	C:\

- **DLL's loaded into processes**

Process	PID	DLLs																	
System Idle Process	0	N/A																	
System	4	N/A																	
Registry	96	N/A																	
smss.exe	376	N/A																	
csrss.exe	564	N/A																	
wininit.exe	656	N/A																	
services.exe	732	N/A																	
lsass.exe	748	ntdll.dll	KERNEL32	KERNELBA	RPCRT4.dl	lsasrv.dll	msvcrt.dll	WS2_32.d	SspiCli.dll	sechost.dl	WLDAP32.	ucrtbase.(	MSASN1.c	samsrv.dll	CRYPT32.c	bcrypt.dll	ncrypt.dll	NTASN1.d	Wldp.dll	combase.(
svchost.exe	932	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	umpnpmg	msvcrt.dll	WLDP.DLL	combase.(	bcryptPrir	CRYPT32.c	MSASN1.c	WINTRUS	advapi32.				
svchost.exe	960	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	umpo.dll	WLDP.DLL	msvcrt.dll	combase.(	bcryptPrir	CRYPT32.c	MSASN1.c	WINTRUS	advapi32.(	slc.dll	sppc.dll	umpoext.	cfgmgr32.
fontdrvhost.exe	980	ntdll.dll	KERNEL32	KERNELBA	ucrtbase.(	GDI32.dll	gdi32full.(	msvcp_wi	USER32.dl	win32u.dll										
svchost.exe	512	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	rpcepmap	WLDP.DLL	msvcrt.dll	combase.(	bcryptPrir	CRYPT32.c	MSASN1.c	WINTRUS	advapi32.(	sspicli.dll	RpcRtRem	rpcss.dll	WS2_32.d
svchost.exe	820	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	lsm.dll	msvcrt.dll	combase.(	bcryptPrir	USER32.dl	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	advapi32.(	tdh.dll	mintdh.dl	OLEAUT32
svchost.exe	1156	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	ncbservic	WS2_32.d	OLEAUT32	NSI.dll
svchost.exe	1164	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	timebroke	powrprof.	BrokerLib.	WLDP.DLL
svchost.exe	1232	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	hidserv.dl	HID.DLL	WLDP.DLL	CRYPT32.c
svchost.exe	1304	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	wevtsvc.d	shcore.dll	WS2_32.d	USERENV.
svchost.exe	1372	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	semgrsvc.	OLEAUT32	cfgmgr32.	shcore.dll
NVDisplay.Container.e	1380	ntdll.dll	KERNEL32	KERNELBA	SHLWAPI.	msvcrt.dll	combase.(	ucrtbase.(	RPCRT4.dl	bcryptPrir	GDI32.dll	gdi32full.(	msvcp_wi	USER32.dl	win32u.dl	PSAPI.DLL	SHELL32.d	VERSION.(	cfgmgr32.	shcore.dll
svchost.exe	1436	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	nsisvc.dll	WLDP.DLL	CRYPT32.c	MSASN1.c
svchost.exe	1460	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	dhcpcore.	WS2_32.d	powrprof.	DNSAPI.dl
svchost.exe	1552	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	profsvc.dl	OLEAUT32	advapi32.	profapi.dl
svchost.exe	1560	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	themeser	WLDP.DLL	CRYPT32.c	MSASN1.c
svchost.exe	1568	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	cscsvc.dll	OLEAUT32	USERENV.	profapi.dl
svchost.exe	1580	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	sysmain.d	cfgmgr32.	POWRPRC	WLDP.DLL
svchost.exe	1588	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	es.dll	WLDP.DLL	CRYPT32.c	MSASN1.c
svchost.exe	1708	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	nlasvc.dll	cfgmgr32.	IPHLPAPI.	dhcpcsvc.(
svchost.exe	1772	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	schedsvc.(	OLEAUT32	UBPM.dll	EventAggr
Memory Compression	1788	N/A																		
svchost.exe	1884	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	sens.dll	SYSNTFY.c	WLDP.DLL	CRYPT32.c
svchost.exe	1964	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	netprofm	NSI.dll	nlaapi.dll	WLDP.DLL
igfxCUIService.exe	1996	ntdll.dll	KERNEL32	KERNELBA	USER32.dl	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	ucrtbase.(	ADVAPI32	msvcrt.dll	sechost.dl	RPCRT4.dl	ole32.dll	combase.(	bcryptPrir	OLEAUT32	SHLWAPI.	SETUPAPI.
svchost.exe	1312	ntdll.dll	KERNEL32	KERNELBA	sechost.dl	RPCRT4.dl	ucrtbase.(	combase.(	bcryptPrir	kernel.ap	msvcrt.dll	user32.dll	win32u.dl	GDI32.dll	gdi32full.(	msvcp_wi	audioend	OLEAUT32	cfgmgr32.	shcore.dll

- **Documents recently opened**

	Document	File extension	Day of week	Month	Day	Time	Year	Timezone
1	1 Téléchargements		Fri	Apr	26	19:59:20	2019	(UTC)
2	2 Documents							
3	16 africatwin.pdf							
4	149 Brochure_Accord.pdf							
5	139 Monuments Paris.xlsx							
6	118 Cycle Drenaï							
7	3 24.S05E01.FRENCH.720p.WEB-DL.DD5.1.H264-AUTHORiTY-Zone-Telechargement.Ws.mkv							
8	148 org_ammc_fr_new_2.pdf							
9	128 [EgyBest].Game.Of.Thrones.S08E02.DVDScr.480p.x264.mp4							
10								
11								
12	1 SCP-DS-Driver-Package-1.2.0.160.7z	.7z	Wed	May	23	01:26:45	2018	(UTC)
13	3 [opensource] IDM trial reset.rar.7z							
14	2 SCP-DS-Driver-Package-1.2.2.175-Update.7z							
15								
16	1 Enregistrement automatique deQuestions entretien AMMC (Enregistré automatiquement).asd	.asd	Wed	May	23	01:26:45	2018	(UTC)
17	0 Enregistrement automatique deQuestions entretien AMMC.asd							
18	It).7z							
19								
20	1 Telechargement-Histo-Valeur (1).aspx	.aspx	Sat	Feb	23	13:24:28	2019	(UTC)
21	0 Telechargement-Histo-Valeur.aspx							
22								
23								
24	2 finalll.ass	.ass	Wed	May	23	01:26:45	2018	(UTC)
25	1 ok.ass							
26	0 Black.Sails.S03E07.WEBRip.RMTeam.en.ass							
27								
28								
29	3 FanBea2-Annuaire-Telechargement.Com.avi	.avi	Wed	Feb	27	22:03:52	2019	(UTC)
30	10 Deutschland.83.S02E01.FRENCH.WEB-DL.XviD-ZT.WwW.Annuaire-Telechargement.CoM.avi							
31	19 TC.JR.107.VOSTFR.WwW.Zone-Telechargement1.ORG.avi							
32	8 TC.JR.106.VOSTFR.WwW.Zone-Telechargement1.ORG.avi							
33	1 TC.JR.101.VOSTFR.WwW.Zone-Telechargement1.ORG.avi							
34	9 Bodyguard.S01E02.FASTSUB.VOSTFR.HDTV.XviD-ZT.WwW.Zone-Telechargement1.ORG.avi							

- **USB devices connected to system**

	USB Device	day of week	month	day	time	year
1	Imation ImationFlashDriv USB Devi	Sun	Mar	3	22:22:55	2019
2	JetFlash Transcend 64GB USB Devic	Wed	May	23	02:03:40	2018
3	Kingston DataTraveler 2.0 USB Devi	Sun	Feb	10	21:39:29	2019
4	Kingston DataTraveler 3.0 USB Devi	Thu	Feb	28	19:46:54	2019
5	TOSHIBA External USB 3.0 USB Devi	Wed	May	23	01:32:05	2018
6	TOSHIBA External USB 3.0 USB Devi	Fri	Jun	15	11:12:20	2018
7	TOSHIBA MK1059GSM USB Device	Wed	Jun	6	00:12:40	2018

- **Programs running at startup**

	Name	Command line	Location	User
1	OneDriveSetup	C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup	HKU\S-1-5-19\SOFTWARE\Microsoft\Windows\CurrentVersion\R	AUTORITE NT\SERVICE LOCAL
2	OneDriveSetup	C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup	HKU\S-1-5-20\SOFTWARE\Microsoft\Windows\CurrentVersion\R	AUTORITE NT\SERVICE R\x90SEAU
3	Sidebar225	Sidebar225.lnk	Startup	Admin-PC\Admin
4	IDM trial reset	"C:\Users\Admin\Documents\[opensource] IDM trial reset\idm_	HKU\S-1-5-21-3882095817-914125327-1005476804-1000\SOFTWAR	Admin-PC\Admin
5	uTorrent	"C:\Program Files (x86)\uTorrent\uTorrent.exe"	HKU\S-1-5-21-3882095817-914125327-1005476804-1000\SOFTWAR	Admin-PC\Admin
6	Sidebar	C:\Program Files\Windows Sidebar\sidebar.exe /autoRun	HKU\S-1-5-21-3882095817-914125327-1005476804-1000\SOFTWAR	Admin-PC\Admin
7	OneDrive	"C:\Users\Admin\AppData\Local\Microsoft\OneDrive\OneDrive.	HKU\S-1-5-21-3882095817-914125327-1005476804-1000\SOFTWAR	Admin-PC\Admin
8	Skype	"C:\Program Files (x86)\Skype\Phone\Skype.exe" /minimized /r	HKU\S-1-5-21-3882095817-914125327-1005476804-1000\SOFTWAR	Admin-PC\Admin
9	DAEMON Tools Lite Automa	"C:\Program Files\DAEMON Tools Lite\DTAgent.exe" -autorun	HKU\S-1-5-21-3882095817-914125327-1005476804-1000\SOFTWAR	Admin-PC\Admin
10	IDMan	C:\Program Files (x86)\Internet Download Manager\IDMan.exe /	HKU\S-1-5-21-3882095817-914125327-1005476804-1000\SOFTWAR	Admin-PC\Admin
11	GoogleChromeAutoLaunch	"C:\Program Files (x86)\Google\Chrome\Application\chrome.ex	HKU\S-1-5-21-3882095817-914125327-1005476804-1000\SOFTWAR	Admin-PC\Admin
12	NordVPN	C:\Program Files (x86)\NordVPN\NordVPN.exe	HKU\S-1-5-21-3882095817-914125327-1005476804-1000\SOFTWAR	Admin-PC\Admin
13	Install LastPass FF RunOnce	C:\PROGRA~2\COMMON~1\LPUNIN~1.EXE -q -name	Common Startup	Public
14	iSCTsysTray	C:\PROGRA~1\Intel\INTEL(~2\ISCTSY~1.EXE	Common Startup	Public
15	SecurityHealth	%ProgramFiles%\Windows Defender\MSASCuiL.exe	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Public

- **Programs run by the user**

	A	B	C
1	Name	Running count	Last time run
2	Apple.iTunes	0	30/10/2018 00:45:17
3	C:\Fraps\fraps.exe	0	23/08/2018 13:52:46
4	C:\Users\Admin\AppData\Roaming\NordVPN\NordVPN\prerequisites\NordVPNTapSetup.exe	0	
5	C:\Users\Admin\Desktop\Build\init.bat	0	07/04/2019 20:41:14
6	C:\Users\Admin\Desktop\Bureau\iTunes.lnk	0	30/10/2018 00:45:17
7	C:\Users\Admin\Desktop\Bureau\Live Update 5.lnk	0	22/09/2018 15:58:17
8	C:\Users\Admin\Desktop\Bureau\Mozilla Firefox.lnk	50	21/04/2019 21:03:53
9	C:\Users\Admin\Desktop\Core Temp.lnk	0	03/10/2018 20:33:11
10	C:\Users\Admin\Desktop\Fraps.lnk	0	23/08/2018 13:52:46
11	C:\Users\Admin\Desktop\Hollow Knight The Grimm Troupe GOG\setup_hollow_knight_1.2.1.0_(15953).exe	0	21/08/2018 23:55:04
12	C:\Users\Admin\Desktop\skse_loader.exe - Raccourci.lnk	0	13/05/2018 10:50:40
13	C:\Users\Admin\Downloads\7z1900-x64.exe	0	
14	C:\Users\Admin\Downloads\adwcleaner_5.201.exe	0	03/03/2019 22:24:32
15	C:\Users\Public\Desktop\Hollow Knight.lnk	0	22/08/2018 21:14:16
16	C:\Users\Public\Desktop\Origin.lnk	0	07/03/2018 01:54:53
17	C:\Users\Public\Desktop\PCSX2 1.4.0.lnk	0	10/02/2018 00:02:47
18	C:\Users\Public\Desktop\STAR WARS Battlefront II.lnk	0	02/12/2017 12:13:28
19	C:\Users\Public\Desktop\Steam.lnk	0	22/08/2018 23:40:05
20	Chrome	3	28/04/2019 22:16:10
21	D:\Hollow Knight\hollow_knight.exe	0	22/08/2018 21:14:16
22	E7CF176E110C211B	0	21/04/2019 21:03:53
23	E:\setup.exe	0	14/08/2018 14:42:24
24	G:\setup.exe	0	14/08/2018 14:23:44
25	Malwarebytes.Antimalware	0	

- **Network connections**

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1	Network Name	Month	Day of	Day	Time	Year	Z for GI	Month	Day of	Day	Time	Year	Month	Day of	Day	Time	Year	Default Gateway MA	Connection Type			LastWrite date	
2	Home	Tue	May	22	23:32:19	2018	Z	Sat	Dec	21	22:22:56	2013	Fri	Dec	20	17:09:51	2013	00-22-57-21-7A-AD	wired			Last connection date	
3	PTACC	Tue	May	22	23:32:19	2018	Z	Tue	Dec	31	23:47:50	2013	Sun	Dec	22	23:28:40	2013	90-F6-52-37-D1-FF	wired			Creation date	
4	Network 4	Tue	May	22	23:32:19	2018	Z	Sat	Jun	17	13:38:09	2017	Tue	Jan	14	20:48:26	2014	C8-D7-19-BA-EC-9E	wired				
5	Network 5	Sun	Apr	28	21:16:09	2019	Z	Sun	Apr	28	22:16:09	2019	Sun	Jun	18	14:01:46	2017	28-FF-3E-55-19-38	wired				
6	Network	Tue	May	22	23:32:19	2018	Z	Wed	Dec	18	16:33:36	2013	Wed	Dec	18	22:46:19	2013	00-78-9E-E3-DD-66	wired				

- **Malware analysis with a scoring system**

A	B	C
Information	Score	Comments
exe	[Good : process not found]	Detecting artifacts of running malware
	[Good : process not found]	
	[Good : process not found]	
xe	[Good : process not found]	
xe	[Good : process not found]	
	[Good : process not found]	
2.exe	[Good : process not found]	
	[Good : process not found]	
EXE	[Good : process not found]	
	[Good : process not found]	
	[Good : process not found]	
xe	[Good : process not found]	
	[Good : process not found]	
	[Good : process not found]	
	[Good : process not found]	
exe	[Good : process not found]	
exe	[Good : process not found]	
.exe	[Good : process not found]	
d.exe	[Good : process not found]	
exe	[Good : process not found]	
		Detecting Rogue Svchost Processes
e instance name	[Good]	Trojan programs are commonly injected into the svchost.exe process
	[Good]	RDP port legitimacy