MEMO	Thème : Forensic
	Sujet : Méthode - Applications
	Rédacteur : Frédéric POUPET – Date : 16/08/2023

Logiciels

Administration	CCleaner DevToys KeePass mRemoteNG NirLauncher (MDP : nirsoft9876$) PowerToys PuTTY Sysinternals Suite WhyNotWin11 WinSCP

COTS	.NET Framework 4.X | .NET Framework 6.X SQL Server 2022 Express (Online installer) Visual C++

Edition	LibreOffice Notepad++ PDFsam Basic Visual Studio Code Zotero : Application/Connecteur | Zotero : Plugins

Fichiers	7-Zip HashMyFiles HxD ImHex SumatraPDF SyncBackFree TeraCopy Visio 2016 Viewer WinDirStat WinMerge

Forensic : Acquisition	dd DumpIt FTK Imager HDD Raw Copy ImageUSB Magnet Acquire (Enregistrement requis) Magnet Process Capture (Enregistrement requis) Magnet RAM Capture (Enregistrement requis) Magnet Web Page Saver (Enregistrement requis) MDD Memoryze NotMyFault StartBlueScreen

	Tableau Forensic Imager WinPmem

Forensic : Analyse	Autopsy Bento DFIR Portable Toolkit DMDE ExifTool FOCA LogParser Magnet AXIOM Wordlist Generator (Enregistrement requis) Magnet Encrypted Disk Detector (Enregistrement requis) Malwarebytes AdwCleaner OSForensics (Trial Edition) PhotoRec Recuva Redline Rifiuti2 (Analyse de la corbeille Windows) SleuthKit THOR Lite WinfrGUI Zimmerman's Tools

Internet	Firefox Free Download Manager

ISO	Balena Etcher Free ISO Creator OSFClone OSFMount Rufus Ventoy Win32DiskImager

Matériel	CPU-Z DiskCheckup GPU-Z HWiNFO USBDeview RAMMon Seagate - SeaTools Speccy SSD-Z WD - Dashboard WD - Data Lifeguard Diagnostic

Multimédia	Captvty ffmpeg imagemagick IrfanView K-Lite Codec Pack Paint.NET

	VLC XnView Classic

Réseau	Angry IP Scanner GNS3 GNS3 VM iPerf NetCrunch Admin Toolset NetworkMiner Nmap Wireshark

Systèmes d'exploitation	Avira Rescue System CAINE Debian Dr.Web CureIt! ESET SysRescue Hiren's BootCD PE Ikki Boot Kali Linux [Metapackages] [Tools] Kaspersky Rescue Disk Linux Mint Medicat Plop Boot Manager REMnux Rocky Linux Santoku Sergei Strelec WinPE SIFT Workstation SystemRescue TinyCore Trace Labs OSINT Trend Micro Rescue Disk Tsurugi Acquire Tsurugi Linux Ultimate Boot CD Windows 11 22H2 Xplico (user: ubuntu | password: reverse)

Virtualisation	Disk2vhd StarWind V2V Converter / P2V Migrator (Conversion de VM) VirtualBox VMware Workstation Player

Editeurs

-	AdRema ArsenalRecon Eric Zimmerman FireEye Magnet

	Netresec NirSoft PassMark SolarWinds StarWind Sysinternals

Ressources

-	CrackStation : Password Cracking Dictionary Daniel Miessler : SecLists Digital Corpora : Dumps Flare VM : Installation script OSForensics : Hash Sets OSForensics : Rainbow Tables Volatility : Memory samples | Volatility : Sample Memory Dumps Tools : Installation script Zythom : French Wikipedia word list