Forensic Report and Documentation
Course 10 Project

Case 001 - The Case of the Stolen Szechuan Sauce from DRIF Madness
https://dfirmadness.com/the-stolen-szechuan-sauce/

Investigators and Report by Evelyn Wolfe and Amber Phoenix

September 23 2024 Flex Cohort

Table of Contents

Overview/Summary

This investigation aims to analyze the DC01/Desktop disk image for evidence related to the security breach in *The Stolen Szechuan Sauce* case. The effort was a collaboration between Amber and Evelyn, with Amber reviewing the DC01 Evidence Files and Evelyn examining the Desktop Evidence Files. The analysis includes identifying the operating system, determining the occurrence of a breach, detecting malware presence, and uncovering any attacker activity.

Artifact Responsibility Split

DC01 Artifacts: **Amber Phoenix**
Desktop Artifacts: **Evelyn Wolfe**

Tools used:

Reviewing the forensic image provided by DFIR Madness onto the Windows 11 Virtual Machine Desktops, the following tools were used to review, and investigate the case.

- FTK Imager
- Autopsy Forensic
- Plaso (log2timeline)
- Volatility
- Wireshark
- Event Log Explorer
- SigCheck & YARA Rules

Artifact Overview

Artifact	File Size	Assigned Investigator
DC01 Disk Image (E01)	4.7 GB	Amber Phoenix
DC01 Memory & Pagefile	550 MB	Amber Phoenix
DC01 Autoruns		Amber Phoenix
DC01 Protected Files (opt)		Amber Phoenix
Desktop Disk Image (E01)	6.4 GB	Evelyn Wolfe
Desktop Memory + Pagefile	1.6Gb memdump.mem | 1.0GB - pagefile.sys	Evelyn Wolfe
Desktop Autoruns	20KB - desktop-autoruns.csv	Evelyn Wolfe
Desktop Protected Files (opt)		Evelyn Wolfe
Case001 PCAP		Evelyn and Amber

What is the Operating System of The Server?

Provided by Amber Phoenix

The server is running Windows Server 2012 R2 Standard, version 6.3.9600.

Evidence from memory analysis and the server (DC01) confirms:
- NtProductType: NtProductLanManNt (Windows Server)
- NtMajorVersion / MinorVersion: 6 / 3 → Version 6.3
- ● SystemTime: 2020-09-19 04:39:59
- PE TimeDateStamp: Sat Feb 22 08:08:18 2014 (kernel build timestamp)

This OS build corresponds to Windows Server 2012 R2, validated against Microsoft's versioning documentation.

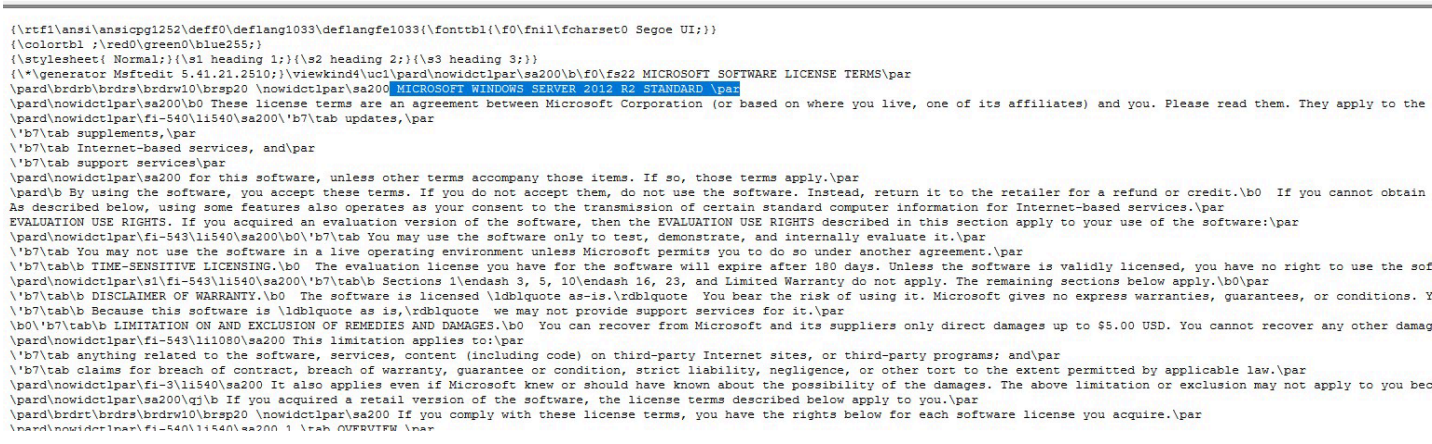
This was confirmed by reviewing the system license file located in C:\Windows\System32\license.rtf using FTK Imager. The license explicitly references "MICROSOFT WINDOWS SERVER 2012 R2 STANDARD" within the first few lines, which verifies the installed OS version.

PROCESS & TOOLS USED:

- FTK Imager: Used to mount and explore the DC01 disk image.
- Volatility 3: Plugin: windows.info
- Registry Explorer: Opened the file in FTK Imager's built-in viewer to verify OS information.

ARTIFACTS REFERENCED:

DC01 Disk Image (E01)
DC01 Memory



```
{\rtf1\ansi\ansicpg1252\deff0\deflang1033\deflangfe1033{\fonttbl{\f0\fnil\fcharset0 Segoe UI;}}
{\colortbl ;\red0\green0\blue255;}
{\stylesheet{ Normal;}{\s1 heading 1;}{\s2 heading 2;}{\s3 heading 3;}}
{\*\generator Msftedit 5.41.21.2510;}\viewkind4\uc1\pard\nowidctlpar\sa200\b\f0\fs22 MICROSOFT SOFTWARE LICENSE TERMS\par
\pard\brdrb\brdrs\brdrw10\brsp20 \nowidctlpar\sa200 MICROSOFT WINDOWS SERVER 2012 R2 STANDARD \par
\pard\nowidctlpar\sa200\b0 These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the
\pard\nowidctlpar\fi-540\li1540\sa200\'b7\tab updates,\par
\'b7\tab supplements,\par
\'b7\tab Internet-based services, and\par
\'b7\tab support services\par
\pard\nowidctlpar\sa200 for this software, unless other terms accompany those items. If so, those terms apply.\par
\pard\b By using the software, you accept these terms. If you do not accept them, do not use the software. Instead, return it to the retailer for a refund or credit.\b0  If you cannot obtain
As described below, using some features also operates as your consent to the transmission of certain standard computer information for Internet-based services.\par
EVALUATION USE RIGHTS. If you acquired an evaluation version of the software, then the EVALUATION USE RIGHTS described in this section apply to your use of the software:\par
\pard\nowidctlpar\fi-543\li1540\sa200\b0\'b7\tab You may use the software only to test, demonstrate, and internally evaluate it.\par
\'b7\tab You may not use the software in a live operating environment unless Microsoft permits you to do so under another agreement.\par
\'b7\tab\b TIME-SENSITIVE LICENSING.\b0  The evaluation license you have for the software will expire after 180 days. Unless the software is validly licensed, you have no right to use the sof
\pard\nowidctlpar\s1\fi-543\li540\sa200\'b7\tab\b Sections 1\endash 3, 5, 10\endash 16, 23, and Limited Warranty do not apply. The remaining sections below apply.\b0\par
\'b7\tab\b DISCLAIMER OF WARRANTY.\b0  The software is licensed \ldblquote as-is.\rdblquote  You bear the risk of using it. Microsoft gives no express warranties, guarantees, or conditions. Y
\'b7\tab\b Because this software is \ldblquote as is,\rdblquote  we may not provide support services for it.\par
\b0\'b7\tab\b LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES.\b0  You can recover from Microsoft and its suppliers only direct damages up to $5.00 USD. You cannot recover any other damag
\pard\nowidctlpar\fi-543\li1080\sa200 This limitation applies to:\par
\'b7\tab anything related to the software, services, content (including code) on third-party Internet sites, or third-party programs; and\par
\'b7\tab claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.\par
\pard\nowidctlpar\fi-3\li1540\sa200 It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you bec
\pard\nowidctlpar\sa200\qj\b If you acquired a retail version of the software, the license terms described below apply to you.\par
\pard\brdrt\brdrs\brdrw10\brsp20 \nowidctlpar\sa200 If you comply with these license terms, you have the rights below for each software license you acquire.\par
\pard\nowidctlpar\fi-540\li1540\sa200 1 \tab OVERVIEW \par
```

The screenshot contains evidence supporting the OS identification.

This would include:
- Memory analysis output from Volatility showing NtProductType: NtProductLanManNt and NtMajorVersion / MinorVersion: 6 / 3, which confirms it is a Windows Server OS.
- SystemTime from memory (2020-09-19 04:39:59), verifying the OS's active state at the time of capture.
- License file evidence from FTK Imager, showing MICROSOFT WINDOWS SERVER 2012 R2
  - STANDARD extracted from C:\Windows\System32\license.rtf.

What is the Operating System of the Desktop?

Provided by Evelyn Wolfe

The Operating System of the Desktop **Desktop-SDN1RPT** is Windows 10, Version 10.0.19041 Build 19041 (64-bit). This was confirmed in multiple locations, within Event Viewer under System, as well as Volatility windows.info plug in, which did extract the OS Version details from the memory dump. With multiple methods of retrieving the data, this was located under both the SOFTWARE registry, as well as the System Event Reviewer Logs review. This was exported as a file from FTK Imager resources OS as Windows 10 Enterprise Evaluation, Version 6.3, Build 19041, providing further evidence.

LOCAL TIME EVIDENCE (TIMESTAMP CONTEXT):
Event Log - System - Event ID 6009 Time Stamp: 2020-09-19 01:24:09 UTC
This aligns with system uptime and process creation timestamps, confirming the Desktop OS state at the time of memory capture.

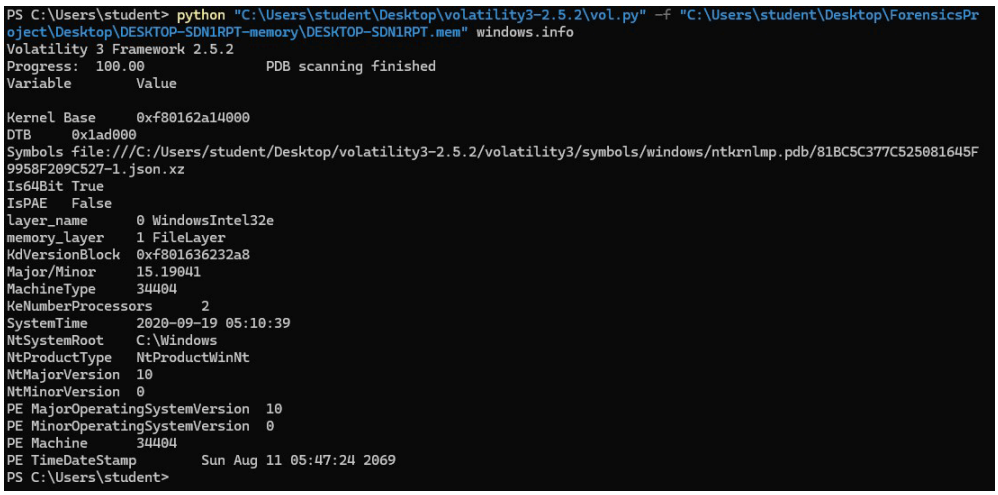
PROCESS & TOOLS USED:

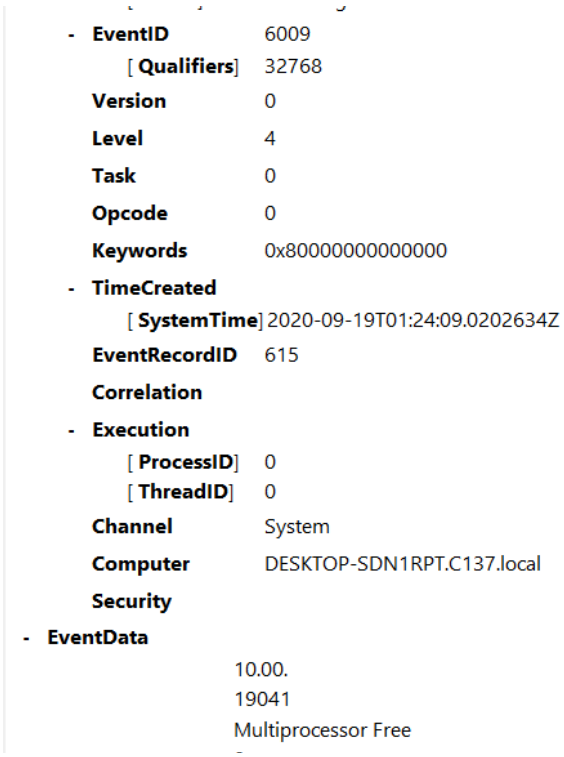
- Volatility 3:
  - Plugin Used: windows.info
  - Purpose: Identified OS version, build number, and system architecture from memory.
- Event Viewer via FTK Imager
  - Exported the file from C:\Windows\System32\winevt\Logs\System.evtx
  - Imported System.evtx into Event Viewer
  - Located 6009 for the details regarding Event Data for Windows Version
  - Validated OS-related processes indicative of Windows 10.

ARTIFACTS REFERENCED:

- DESKTOP-SDN1RPT.mem – Desktop system memory dump
- Volatility plugin outputs (info, pslist)
- DESKTOP-E01
- FTK Imager
- Event Viewer
- Registry Explorer

CompositionEditionID	RegSz	EnterpriseEval	00-00-00-00-00-00
CurrentBuild	RegSz	19041	
CurrentBuildNumber	RegSz	19041	
CurrentMajorVersionNumber	RegDword	10	
CurrentMinorVersionNumber	RegDword	0	
CurrentType	RegSz	Multiprocessor Free	65-00-64-00-00-00-00-00-00-00
CurrentVersion	RegSz	6.3	00-00-00-00
EditionID	RegSz	EnterpriseEval	00-00-00-00-00-00
EditionSubManufacturer	RegSz		
EditionSubstring	RegSz		
EditionSubVersion	RegSz		
InstallationType	RegSz	Client	00-00-00-00-00-00
InstallDate	RegDword	1600408023	
ProductName	RegSz	Windows 10 Enterprise Evaluation	00-00
ReleaseId	RegSz	2004	00-00
SoftwareType	RegSz	System	00-00-00-00-00-00





These screenshots contain evidence confirming the desktop OS version.

This evidence includes:

- Memory analysis output from Volatility:
  - windows.info plugin showing OS Version: 10.0.19041 (Windows 10 Pro, 64-bit).
  - windows.pslist showing active processes that confirm a Windows 10 environment.
- Registry verification using FTK Imager:
  - Extraction of the SOFTWARE registry hive from the desktop disk image (E01).
  - Opening Windows NT\CurrentVersion in Registry Explorer, revealing Windows 10 Enterprise Evaluation, Version 6.3, Build 19041.
- Local Time Evidence for Context:
  - Memory Capture Time (Volatility System Time): 2020-09-19 05:08:43 UTC.
  - This aligns with system uptime and process creation timestamps.
- Event Viewer also shows the Event ID of 6009 corresponds with Windows Product. The Event data reflect the “Make” of 10.00. Which is Windows 10, and version is 19041.

What was the Local Time of the Server?

Provided by Amber Phoenix
The server's local time zone is Pacific Standard Time (PST), with a Bias of 480 minutes (UTC-8).

Local Time Evidence:

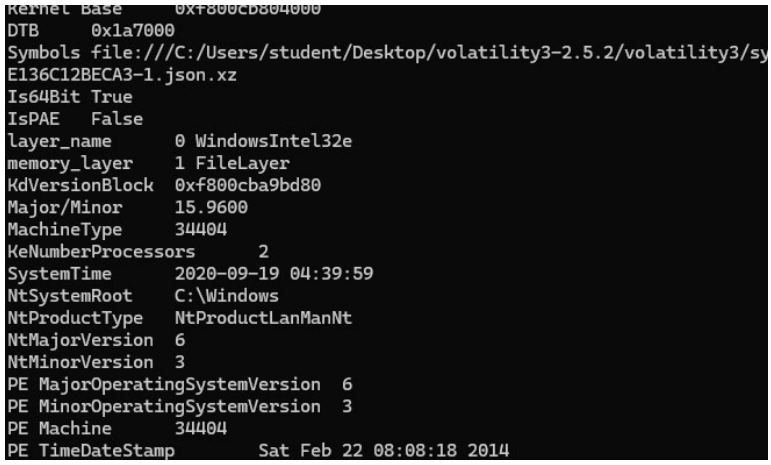
- Memory capture time (SystemTime): 2020-09-19 04:39:59 (UTC)
- Registry data (FTK Imager):
    - TimeZoneKeyName: Pacific Standard Time
    - Bias: 480
    - ActiveTimeBias: 420
- This confirms that the local system's time was UTC - 8 hours, aligning with PST.

PROCESS & TOOLS USED:

- FTK Imager: Used to mount and navigate the disk image of DC01.
- Registry Explorer: Loaded the SYSTEM hive to analyze TimeZoneInformation.
- Volatility 3: Plugin: windows.info

ARTIFACTS REFERENCED:

- DC01.E01 (Disk Image)
- DC01-memory



Value Name	Value Type	Data	Value Slack	Is Deleted
DaylightBias	RegDword	4294967236		
DaylightName	RegSz	@tzres.dll,-211	00-00-00-00	
StandardStart	RegBinary	00-00-0B-00-01-00-02-00-00-00-00-00-00-00...	00-00-00-00	
StandardBias	RegDword	0		
StandardName	RegSz	@tzres.dll,-212	00-00-00-00	
Bias	RegDword	480		
DaylightStart	RegBinary	00-00-03-00-02-00-02-00-00-00-00-00-00-00...	F0-62-42-00	
TimeZoneKeyName	RegSz	Pacific Standard Time		
DynamicDaylightTimeDisabled	RegDword	0		
ActiveTimeBias	RegDword	420		

Value Name	Value Data	Value Data Raw
DaylightBias	-60	4294967236
DaylightName	@tzres.dll,-211	@tzres.dll,-211
StandardStart	Month 11, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-0B-00-01-00-02-00-00-00-00-00-00-00-00-00
StandardBias	0	0
StandardName	@tzres.dll,-212	@tzres.dll,-212
Bias	480	480
DaylightStart	Month 3, week of month 2, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-03-00-02-00-02-00-00-00-00-00-00-00-00-00
TimeZoneKeyName	Pacific Standard Time	Pacific Standard Time
ActiveTimeBias	420	420

Screenshot Information:

- Top image is a reflection of a capture of Volatility 3 Memory analysis output.
    - The SystemTime field displays 2020-09-19 04:39:59 which is in Coordinated Universal Time (UTC.)
    - The NrProductType: NtProductLanManNt confirms this is a Windows Server
    - The Major and Minor OS Version (6.3) align with Windows Server 2012 R2
- The next set of screenshots is a Windows Registry Values extracted from SYSTEM hive
    - TimeZoneInformation registry Key
        - TimeZoneKeyName is set to Pacific Standard Time. Confirming with the Server is set to PST (UTC-8)
    - Bias Value is 480, meaning local time is UTC -8 hours.
    - ActiveTimeBias is 420 accounting for DayLight Savings Time adjustment

Was there a Breach?

Provided by Amber Phoenix and Evelyn Wolfe

Yes, there was a breach. evidence confirms that malicious activity occurred on both the desktop system and server (dc01). A malicious executable named coreupdater.exe was installed and executed on both systems, along with powershell-based payloads indicating remote code execution and post-exploitation activity. the presence of code injection, malware persistence via registry, and suspicious ip connections further confirm the breach.

LOCAL TIME EVIDENCE:

- Desktop Memory Capture Time: 2020-09-19 05:08:43 UTC
- Server Memory Capture Time: 2020-09-19 04:39:59 UTC
- Local Time Zone (DC01): Pacific Standard Time (PST, UTC -8)
    - (From Registry Hive analysis)

EVIDENCE SUMMARY:

- Malware Detected: coreupdater.exe
- Persistence Mechanism: Registry Run Key under
  HKLM\System\CurrentControlSet\Services
- Malfind Analysis: Detected code injection in powershell.exe and MsMpEng.exe processes
- PowerShell Payloads: Observed executing suspicious commands via encoded payloads
- Suspicious Network Activity: Presence of malicious IP addresses observed in network logs and memory artifacts
- Autoruns Data: Confirmed malware persistence and execution path for coreupdater.exe

PROCESS & TOOLS USED:

- Volatility 3:
    - Plugins: windows.malfind, windows.pslist, windows.cmdline, windows.info, windows.netscan
    - Used for identifying malicious processes, memory injection, and PowerShell payloads
- FTK Imager: Mounted disk images for both Desktop and DC01 to review registry hives and file structures.
- Autoruns (Sysinternals): Analyzed persistence mechanisms for coreupdater.exe in registry.
- Strings (strings64.exe): Extracted and searched through pagefile.sys for payload references and IP data.
- Registry Explorer: Loaded SYSTEM and SOFTWARE hives to confirm timezone and persistence data.

ARTIFACTS REFERENCED:

- DESKTOP-SDN1RPT.mem (Desktop memory dump)
- citadeldc01.mem (DC01 memory dump)
- pagefile.sys (DC01 and Desktop)
- Autoruns.csv (Desktop and DC01 autoruns export)
- Registry Hives (SYSTEM, SOFTWARE from DC01)
- Volatility malfind output (Desktop & DC01):

Screenshot Information

- Volatility Malfind Output (Desktop & DC01)

- Injected memory regions in powershell.exe and MsMpEng.exe

```
3316    powershell.exe  0x10c6c070000   0x10c6c093fff   VadS    PAGE_EXECUTE_READWRITE  36      1       Disabled
4d 5a 90 00 03 00 00 00 MZ......
04 00 00 00 ff ff 00 00 ........
b8 00 00 00 00 00 00 00 ........
40 00 00 00 00 00 00 00 @.......
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 e0 00 00 00 ........
0x10c6c070000:  pop     r10
0x10c6c070002:  nop
0x10c6c070003:  add     byte ptr [rbx], al
0x10c6c070005:  add     byte ptr [rax], al
0x10c6c070007:  add     byte ptr [rax + rax], al
0x10c6c07000a:  add     byte ptr [rax], al
3316    powershell.exe  0x7df4f5a90000  0x7df4f5b2ffff  VadS    PAGE_EXECUTE_READWRITE  2       1       Disabled
20 72 46 53 fd 7f 00 00  rFS....
```

  - Screenshot Information:
    - Displays injected memory regions in powershell.exe and MsMpEng.exe.
    - Indicates Malware Injection, meaning the attacker used these processes to execute malicious code in legitimate system files, avoiding detection

- Volatility pslist
  - coreupdater.exe and powershell.exe processes with PIDs and timestamps

```
860     764     MicrosoftEdge.  0xbe8e790c2080  0       -       3       False   2020-09-19 03:36:40.000000      2020-09-19 03:44:52.000000      Disabled
8324    4008    coreupdater.ex  0xbe8e7a447080  0       -       3       False   2020-09-19 03:40:49.000000      2020-09-19 03:43:10.000000      Disabled
3232    448     sihost.exe      0xbe8e7767d080  20      -       2       False   2020-09-19 05:08:15.000000      N/A     Disabled
```

  - Screenshot Information:
    - List of active processes, confirming coreupdater.exe and powershell is running. Shows the PID and Timestamps.
    - This aligns with timeline of attack
    - Validates that the malicious process was active post-infection

- Autoruns Analysis
  - Registry persistence for coreupdater.exe under HKLM\System\CurrentControlSet\Services.

```
PS C:\Users\student\Desktop\ForensicsProject\Desktop\Desktop-SDN1RPT-pagefile> Select-String -Path "pagefile_strings.txt
" -Pattern "Meterpreter"
```

  - Screenshot Information:
    - Displays the registry persistence for coreupdater.exe under
    - Confirms that malware was configured to run at startup, maintaining its foothold on the system after.

- Strings search from pagefile.sys
  - coreupdater.exe and PowerShell payloads in the extracted strings.

```
PS C:\Users\student\Desktop\ForensicsProject\Desktop\Desktop-SDN1RPT-pagefile> Select-String -Path "pagefile_strings.txt
" -Pattern "payload"

pagefile_strings.txt:4827:sendingpayload
pagefile_strings.txt:131796:RemovePayloadF
pagefile_strings.txt:134086:/Payload.cl
pagefile_strings.txt:580140:microsoft_payload_1 = tmp_dir + "\" & rand_name & ".exe.1"a.writeline ("@start /min powe"
& chr(114) & "sh" & chr(101) & "ll.exe "
pagefile_strings.txt:784133:EventPayload
```

  - Screenshot Information:
    - Shows extracted strings from pagefile.sys using a search for “Meterpreter” and “Payload”
    - Confirms that coreupdater.exe is presence
    - Meterpreter, is a well-know remote access tool, was found indicating that the attacker maintained Command and Control Communication (C2)

What was the initial entry vector (how did they get in?)

Provided by Amber Phoenix

The attacker gained access to the Desktop system through a **malicious USB device (SanDisk Cruzer Glide 3.0)** which was inserted a**t 2020/09/18 22:08:58**, as confirmed by the **SetupAPI.dev.log**. Shortly after insertion, **coreupdater.exe** was installed and registered as a system service, providing persistence. The executable's install date was **falsely time-stamped** to 4/14/2010, indicating time stomping for evasion.

Memory analysis confirmed **coreupdater.exe** (PID 8324) was running, aligning with the USB insertion time**. VirusTotal flagged the file as malicious** (66/76 vendors) and identified C2 traffic to 203.78.103.109, confirming it was used to establish a remote connection. This evidence confirms the USB was the initial entry vector, used to introduce and execute malware on the Desktop.

PROCESS & TOOLS USED:

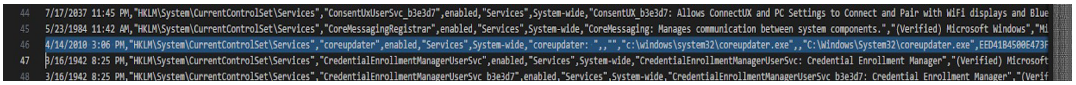
- SetupAPI.dev.log: Tracked USB insertion time
- Volatility 3: Used pslist to identify coreupdater.exe running in memory
- Excel: Analyzed autoruns CSV for coreupdater.exe service entry and timestamp
- VirusTotal: Verified malware behavior, network connections, and reputation
- Wireshark: Correlated C2 communication to 203.78.103.109 post-infection

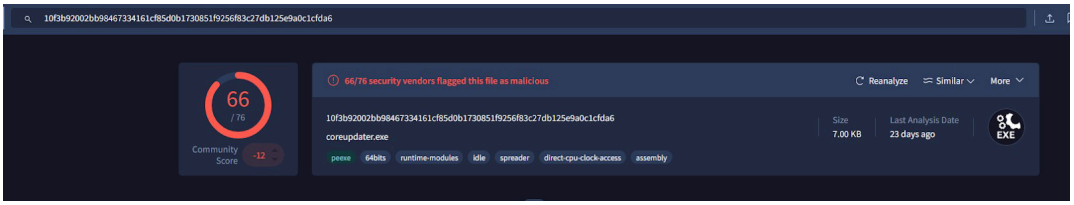
ARTIFACTS REFERENCED:

- DESKTOP-SDN1RPT.E01
- autoruns-desktop-sdn1rpt.csv
- DESKTOP-SDN1RPT.mem

Screenshot Information:

- 

    - PID 8324 - Confirms execution timestamp (2020-09-19 03:40:49 UTC) and the alignment of a USB Insertion
- 

    - Evidence of coreupdater.exe registered as a system service in HKLM\System\CurrentControlSet\Services\coreupdater
- 

    - This is a capture from **VirusTotal** indicating the malicious flag of 66 out of 76.
    - Confirms remote access capabilities, data exfiltration, and C2 activities

- This is a capture of insertion of a USB “SanDisk Cruzer Glide 3.0”
- Confirms the exact time: 2020-09-18 22:08:58
- Indicates USB device enumeration, and the malware introduction

Was Malware Used? If so, what was it?

Provided by Amber Phoenix

Malicious Process: Yes, **coreupdater.exe** was used. It is not a legitimate Windows process and was confirmed as **malicious** by **66/76 vendors** on VirusTotal. It was executed shortly after USB insertion and provided remote access capabilities.

Payload Delivery IP Address: **194.61.24.102** — Attempted to deliver the payload via RDP brute-force and potentially seeded the USB.

C2 (Command & Control) IP Address: 203.78.103.109 — Used by coreupdater.exe for outbound encrypted communications (TLS port 443). This IP is linked to **Metasploit Meterpreter** as per VirusTotal decoded output.

Disk Location:
C:\Windows\System32\coreupdater.exe
Confirmed via **autoruns-desktop-sdn1rpt.csv** and **VirusTotal** file hash.

First Appearance: 4/14/2010 (time-stamped) False timestamp indicating **time stomping**.
Actual install time corresponds to **USB insertion on 2020/09/18 22:08:58** (SetupAPI.dev.log).

Was it Moved: No evidence indicates relocation post-installation. It was directly executed and persisted in **System32.**

Malware Capabilities:
- Remote access via Meterpreter
- Data manipulation (XOR encoding)
- System discovery
- Encrypted C2 via HTTPS
- Process injection (WMIADAP.EXE)
- Persistence through Windows services

Is it Easily Obtained: Yes, VirusTotal metadata shows it is associated with **Metasploit-generated payloads**, indicating easy public access for attackers.

Persistence Installed? When / Where:
Yes, persistence was installed at:
- Location: Registry entry in HKLM\SYSTEM\CurrentControlSet\Services\coreupdater
- When: Immediately after USB insertion on 2020/09/18 22:08:58
- Tool: Identified in autoruns CSV

ANSWER: coreupdater.exe is confirmed malware, installed via USB, persisting as a Windows service, and communicating with 203.78.103.109 for remote control.
VirusTotal, Volatility, and Wireshark confirmed its malicious behavior, persistence, and C2 communication.

PROCESS & TOOLS USED:

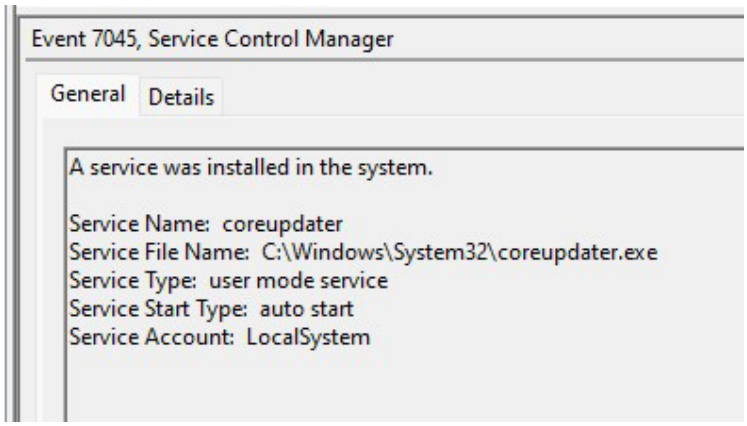
- Volatility 3: pslist to find coreupdater.exe in memory
- Excel: Analyzed autoruns for registry service persistence
- VirusTotal: Malware behavior, IPs, capabilities
- Wireshark: Tracked outbound connections to 203.78.103.109
- SetupAPI.dev.log: Determined install timing linked to USB insertion

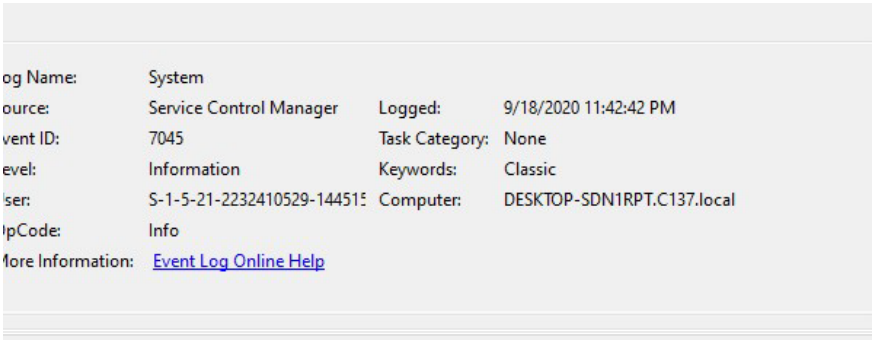
ARTIFACTS REFERENCED:

- Autoruns-desktop-sdn1rpt.csv
- DESKTOP-SDN1RPT.mem
- SetupAPI.dev.log

Screenshots of the Coreupdater on the infected desktop:

Provided by Evelyn regarding the desktop.

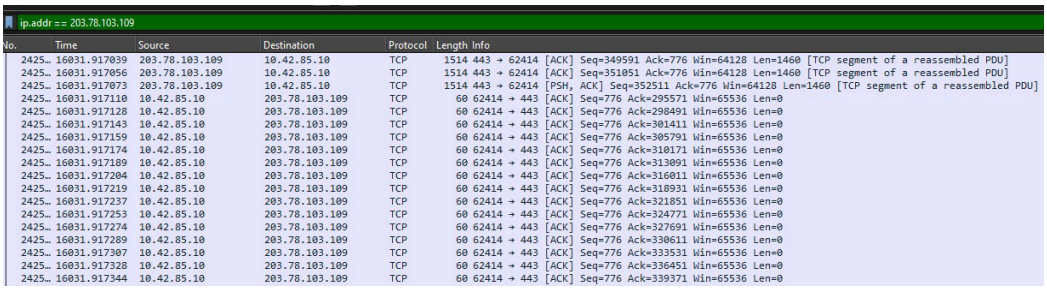
- Event ID 7045 - Installation of a New Service
  - 

  - 

    - Indication of a service being installed was coreupdater.exe which is the malware infection.
    - This shows additional support of the malware being operated as a service under an auto start execution

WHAT MALICIOUS IP ADDRESSES WERE INVOLVED?

- **IP Address That Delivered the Payload: 194.61.24.102**
    - **Activity**: Initiated repeated RDP connection attempts to 10.42.85.10 (likely DC01).
    - **Purpose**: Gained initial access, possibly delivered Meterpreter payload (including coreupdater.exe).
    - **Evidence**: Multiple SYN packets, Client Hello (TLS) sessions, followed by RST, ACK — indicative of brute-force or unauthorized access attempts.
- **IP Address Used for Command & Control (C2): 203.78.103.109**
    - **Activity**: Established TLS traffic with 10.42.85.115 (compromised Desktop) post malware execution.
    - **Purpose**: C2 server communicating with the coreupdater.exe malware
    - **Evidence**: TLS sessions seen after malware executed



ip.addr == 203.78.103.109

No.	Time	Source	Destination	Protocol	Length	Info
2425…	16031.917039	203.78.103.109	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=349591 Ack=776 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
2425…	16031.917056	203.78.103.109	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=351051 Ack=776 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
2425…	16031.917073	203.78.103.109	10.42.85.10	TCP	1514	443 → 62414 [PSH, ACK] Seq=352511 Ack=776 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
2425…	16031.917110	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=776 Ack=295571 Win=65536 Len=0
2425…	16031.917128	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=776 Ack=298491 Win=65536 Len=0
2425…	16031.917143	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=776 Ack=301411 Win=65536 Len=0
2425…	16031.917159	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=776 Ack=305791 Win=65536 Len=0
2425…	16031.917174	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=776 Ack=310171 Win=65536 Len=0
2425…	16031.917189	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=776 Ack=313091 Win=65536 Len=0
2425…	16031.917204	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=776 Ack=316011 Win=65536 Len=0
2425…	16031.917219	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=776 Ack=318931 Win=65536 Len=0
2425…	16031.917237	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=776 Ack=321851 Win=65536 Len=0
2425…	16031.917253	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=776 Ack=324771 Win=65536 Len=0
2425…	16031.917274	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=776 Ack=327691 Win=65536 Len=0
2425…	16031.917289	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=776 Ack=330611 Win=65536 Len=0
2425…	16031.917307	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=776 Ack=333531 Win=65536 Len=0
2425…	16031.917328	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=776 Ack=336451 Win=65536 Len=0
2425…	16031.917344	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=776 Ack=339371 Win=65536 Len=0

    - **Screenshot Information:**
        - The screenshot displays network traffic logs from Wireshark, filtered to show packets involving 203.78.103.109 (C2 server)
        - Source: 203.78.103.109
        - Destination: 10.42.85.10 - Victims System
        - Protocol: TCP over 443 - TLS Encryption - Confirms secure C2 communication
        - Packet Details:
            - Several ACK Packets - Confirms that a 2-way communication was established
            - High Frequency, encrypted data exchanges, indicating a remote command session or data exfiltration
            - The traffic pattern suggests a persistent connection, meaning the malware was actively communicating with the attacker
- Were any IP addresses from known adversary infrastructure?
    - Yes: 203.78.103.109 is confirmed adversary infrastructure, linked to Metasploit C2 activity.
    - 194.61.24.102 is blacklisted for RDP brute-force attacks and malware delivery, confirming its role in multiple intrusions.
- Are these adversary infrastructure IPs involved in other attacks around the time of this incident?
    - Yes: Both IPs are documented in threat intelligence feeds (AbuseIPDB, Netresec, CleanTalk) for ongoing attacks during the same timeframe
    - Their involvement in Meterpreter payload campaigns makes them repeat offenders.

TOOLS/COMMANDS USED:

- Wireshark: Analyzed PCAP traffic to identify RDP attempts and TLS C2 connections.
- Volatility 3 (windows.netscan): Validated active connections and IP address associations in memory.
- Netresec IOC Reports: Correlated IP addresses with known adversary infrastructure.

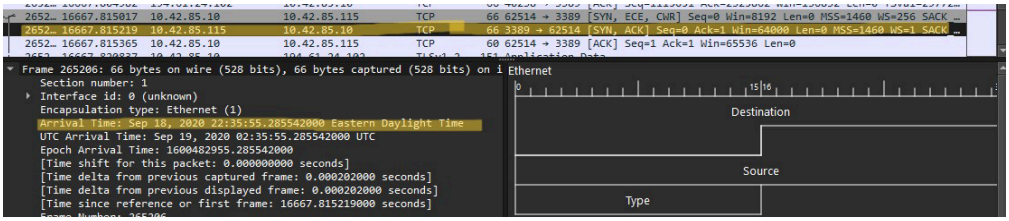
ARTIFACTS ANALYZED:

- Wireshark PCAP
- Desktop.mem
- Network Log Analysis

DID THE ATTACKER ACCESS ANY OTHER SYSTEMS?

Provided by Amber Phoenix

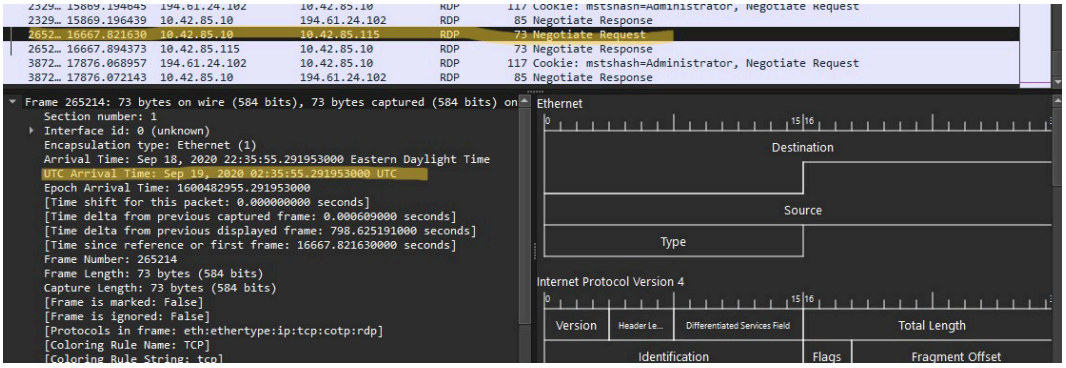
- Yes. The attacker accessed the domain controller DC01 from the compromised Desktop system.
- How: The attacker used a reverse TCP Meterpreter session to control the Desktop system, then initiated RDP (Remote Desktop Protocol) connections to DC01. This is confirmed through
- SYN/ACK and RDP traffic between the two systems in the network capture.
- When: THIS ACTIVITY OCCURRED ON SEPTEMBER 19, 2020 AT 02:35:55 UTC.
- BOTH THE RDP NEGOTIATE REQUEST AND SYN/ACK PACKETS FROM DESKTOP TO DC01 AND TO 194.61.24.102 (ATTACKER) SHOW THIS TIMESTAMP.



- Screenshot Information:
  - Packet Capture - **Wireshark** showing exfiltrated Data
    - Displays TCP connection between DC01 - 10.42.85.10 and the Attackers System.
    - Files Exfiltration Time Stamps Indicate secret.zip (02:31 UTC) and loot.zip (02:48 UTC)
    - Confirms successful data theft

Did the Attacker Steal or Access Any Data?

- Yes, the attacker accessed files and attempted lateral movement using RDP.
  - secret.zip was exfiltrated from the DC at 02:31 UTC
  - loot.zip was exfiltrated from the Desktop Machine at 02:48 UTC
- When: Access to DC01 occurred immediately after malware execution, around 02:35:55 UTC on September 19, 2020.



- Screenshot Information:
  - RDP Negotiation Traffic: Shows RDP Negotiation request and response
  - Confirms an RDP session was initiated from the Desktop (10.42.85.115) to DC01 (10.42.85.10)
  - Indicates lateral movement as part of the attack

PROCESS & TOOLS USED:

- Wireshark – Analyze PCAP for RDP and SYN/ACK packets.
- Volatility – Verified process activity and network behavior.

Artifacts Referenced:

- Wireshark PCAP,
- Desktop E01,
- Desktop.mem

WHAT WAS THE NETWORK LAYOUT OF THE VICTIM NETWORK?

Provided by Evelyn Wolfe with assistance from Amber Phoenix

The victim network consisted of at least two core systems in a flat local network environment

- Two hosts on 10.42.85.0/24. DC 10.42.85.10 (domain controller)
- User workstation 10.42.85.115 (Hostname: DESKTOP-SDN1RPT)
- The following details were assigned to the accounts from details from Event Viewer:
    - ADMIN: Security ID:
        - S-1-5-21-41211245-796119838-3940169921-1001
    - ricksanchez: Security ID:
        - S-1-5-21-2232410529-1445159330-2725690660-1106
    - mortysmith: Security ID:
        - S-1-5-21-2232410529-1445159330-2725690660-1108
    - Administrator: Security ID:
        - S-1-5-21-2232410529-1445159330-2725690660-500

A consideration with events:

- New Account “Admin” Desktop: Desktop-SDN1RPT was created 9/18/2020 at 1:47:07AM
- After this time frame the account was added to Administrators Group, which was created by the Administrator brute force take over prior to the malware injection. This appears to be a backdoor type of account to allow access. As this account was created prior to malware.

Observed Communication Paths:

- External Attacker (194.61.24.102) → Desktop (10.42.85.115) via RDP & Malware Delivery
- Desktop (10.42.85.115) ↔ C2 Server (203.78.103.109) via Meterpreter reverse TCP
- Desktop (10.42.85.115) → DC01 (10.42.85.10) via RDP for lateral movement

PROCESS & TOOLS USED:

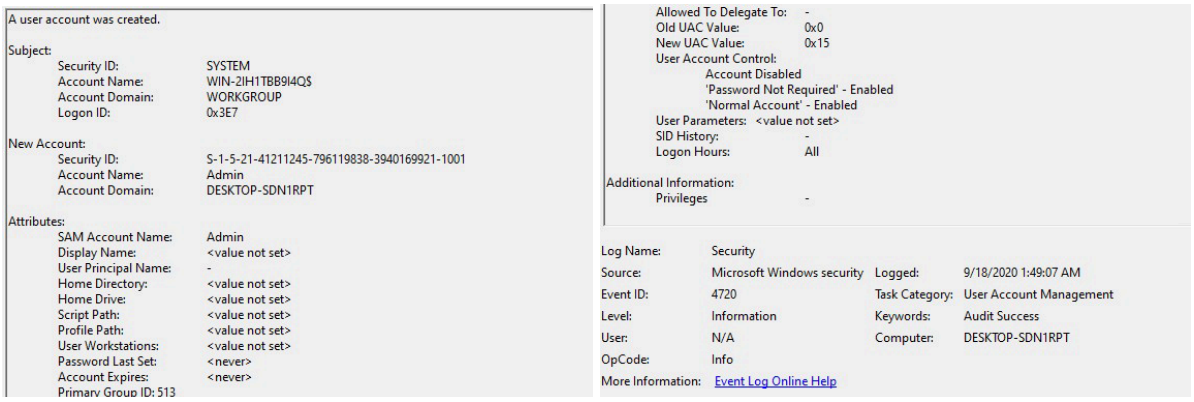
- Wireshark – Identified IP communications and RDP/TCP sessions.
- Volatility (netscan) – Revealed active network connections from memory.
- FTK Imager – Validated IP references and hostnames from disk artifacts.

ARTIFACTS REFERENCED:

- Wireshark PCAP: Showed SYN/ACK handshakes, RDP, and C2 communications.
- Volatility Output: Confirmed Desktop and DC01 IPs and their network activity.
- Registry/Prefetch: Confirmed system roles and user activity across the network.

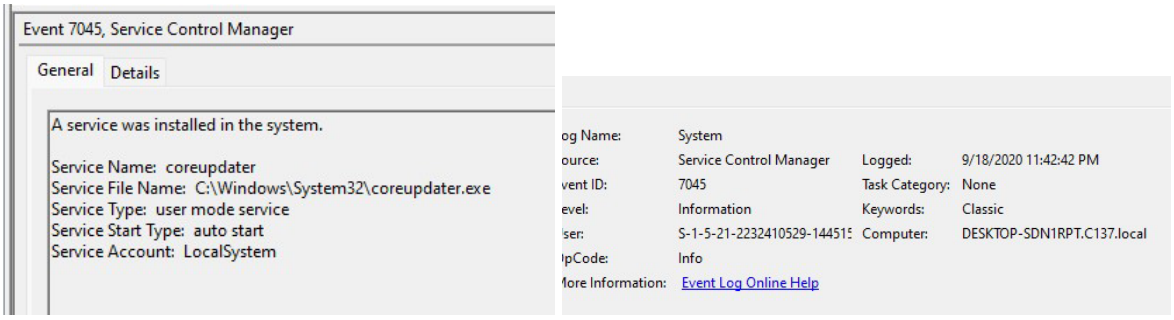
Evidence / Screenshots

- New account Creation - Event ID 4720



  - Indicates a Brute Force with Lateral Movement from this backdoor account
- Group Modification - Event ID 4732

  - Confirms Unauthorized “Admin” account was added to the Administrator Group
  - System Process indicating privilege escalation
  - Providing the attack with full administrative control over the system
- Malware Installation as a Service - Event ID 7045



  - Confirms that coreupdater.exe was installed as a persistent windows service
  - Location: C:\Windows\System32\coreupdater.exe
  - Service Start Type: Auto Start
    - Ensures execution after every reboot
  - Service Account: LocalSystem
  - Time Stamp: 09/18/2020 11:42:42pm - This aligns with the attack and execution of the malware injection

Citations/References

Wikipedia contributors. (2024, December 30). *Windows 10 version history*. Wikipedia. https://en.wikipedia.org/wiki/Windows_10_version_history

How to extract windows event logs from a hard disk forensic image? (n.d.). Information Security Stack Exchange. https://security.stackexchange.com/questions/118621/how-to-extract-windows-event-logs-from-a-hard-disk-forensic-image

DFIRScience. (2022, February 8). *Starting a new digital forensic investigation case in autopsy 4.19+* [Video]. YouTube. https://www.youtube.com/watch?v=fEqx0MeCCHg

Real-time, web based Active Directory Change Auditing and Reporting Solution by ManageEngine ADAudit Plus. (n.d.). ManageEngine ADAudit Plus. https://www.manageengine.com/products/active-directory-audit/kb/system-events/event-id-7045.html