仙台CTF2018 セキュリティ技術競技会(CTF)

# 問題解説 Forensic

# 平成30年11月10日 仙台CTF推進プロジェクト 五十嵐 良一

Copyright (C) 2018 Sendai CTF. All Rights Reserved. https://www.sendai-ctf.org/



# Forensic01

#### 問題1

検体を解析し、ダウンロード元URLを特定してください。

[検知したファイル]

- フォルダ名:
  - C:¥Users¥user01¥AppData¥Local¥Mozilla¥Firefox¥Profiles¥o5j56hgo.default ¥cache2¥entries
- ファイル名:
  - E0274DBC37EC05DA0813E93E7A1C3260C93BE6DE
- [フラグ]
  - - 検体「E0274DBC37EC05DA0813E93E7A1C3260C93BE6DE」のダウンロード
     元のURL(半角、小文字)
     例:http://www.sendai-ctf.org/abc.exe

#### 解説

 Firefoxは、一時ファイル(キャッシュ)としてダウンロードしたファイルの末尾に、HTTP リクエスト/レスポンスの情報を追記するため、バイナリエディタで問題ファイルを確認す ることで、ダウンロード元URLを特定することができます。





# Forensic02

#### 問題2

検知したファイルのダウンロード元URLは、有名なフリーソフト「PC-Cleaner」(注記:架 空のフリーソフト)の公式サイトのようです。「PC-Cleaner」の公式サイトを確認したところ、 不正アクセス被害に遭い、マルウェアが混入されたプログラム「PC-Cleaner.exe」が配布 されたというお詫び文書が掲載されていました。

社員(以下user01という)に確認したところ、ダウンロードした「PC-Cleaner.exe」を実行 したか記憶が定かではないが、もしも実行していたとしても、すぐに削除したはずだと証言 しています。あなたは、user01のパソコンはマルウェアに感染している可能性が高いと考 え、パソコンをネットワークから隔離したうえで、いくつかのファイルをエビデンスとして証拠 保全しました。

user01のパソコンから証拠保全したエビデンスを解析し、「PC-Cleaner.exe」が実行された日時を特定してください。

[フラグ]

フリーソフト「PC-Cleaner.exe」の実行日時(YYYY/MM/DD-hh:mm)(半角)
 例:2018/11/10-23:59

#### 解説(1)

- Windowsには、アプリケーションの起動を高速化するための「Prefetch」と呼ばれる 機能が搭載されており、アプリケーションが起動されると、「C:¥Windows¥Prefetch」 に、Prefetchファイル(拡張子「.pf」で、アプリケーション名を含むファイル名)が作成さ れます。
- Prefetchファイルには、アプリケーションのフルパス、最終起動日時などが記録されているため、調査用ツール「WinPrefetchView」などを利用し、「PC-Cleaner.exe」の最終起動日時を確認することができます。

#### 解説(2)

Pr WinPrefetchView								- 0	×
File Edit View Options Help									
× 🖬 🖗 🖻 📽 🔕 📲									
Filename /	Created Ti	Modified Ti	File Si	Process EXE	Process Path		Run	Last Run Time	^
INETSH.EXE-3DD790C5.pf	2018/10/07	2018/09/30	62,070	NETSH.EXE	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS	SYSTEM32¥NETSH.EXE	8	2018/08/25 8:43:11	
NOTEPAD.EXE-EB1B961A.pf	2018/10/07	2018/09/30	35,704	NOTEPAD.EXE	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS	SYSTEM32¥NOTEPAD.	1	2018/08/24 22:50:16	
INSD379.TMP-B4698A38.pf	2018/10/07	2018/09/30	10,686	NSD379.TMP	¥DEVICE¥HARDDISKVOLUME1¥USERS¥USE	R01¥APPDATA¥LOCAL	1	2018/09/30 22:44:28	
NTOSBOOT-B00DFAAD.pf	2018/10/07	2018/09/30	2,224,				0		
PC-CLEANER.EXE-0FC5C951.pf	2018/10/07	2018/09/30	45,458	PC-CLEANER.E	¥DEVICE¥HARDDISKVOLUME1¥USERS¥USE	R01¥DOWNLOADS¥PC	1	2018/09/30 22:56:12	
PDMSETUP:EXE-9BBEDFF7.pf	2018/10/07	2018/09/30	10,114	PDMSETUPEXE	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS	¥WINSXS¥X86_MICROS	1	2018/08/25 7:38:10	٦ ۱
PINGSENDER.EXE-CA8AA85B	2018/10/07	2018/09/30	42,414	PINGSENDER.E	¥DEVICE¥HARDDISKVOLUME1¥PROGRAM	FILES¥MOZILLA FIREFO	1	2018/09/30 23:04:12	
POQEXEC.EXE-7C336EAC.pf	2018/10/07	2018/09/30	131,686	POQEXEC.EXE	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS	SYSTEM32¥POQLXEC.	2	2018/08/25 8:41:33	
PRINTUI.EXE-E9F4354A.pf	2018/10/07	2018/09/30	47,766	PRINTUI.EXE	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS	SYSTEM32#PRINTULE	2	2018/08/24 22:44:19	
RDRMEMPTYLST.EXE-B3FF6C	2018/10/07	2018/09/30	5,310	RDRMEMPTYL	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS	SVSTEM32¥RDRMEMP	1	2018/08/25 8:43:15	
E REBUILDSEARCHINDEX.EXE	2018/10/07	2018/09/30	5,838		ſ		<u> </u>		<b>_</b>
<						FLAG			
Filename	Full Path			Device Path		2010/0	0/2	0 22.56	^
SORTDEFAULT.NLS				¥DEVICE¥HARDDI	SKVOLUME1¥WINDOWS¥GLOBALIZATION	2010/0	1913	0-22.30	
ADVAPI32.DLL				¥DEVICE¥HARDDI	SKVOLUME1¥WINDOWS¥SYSTEM32¥ADVAP	32.DLL			_
APISETSCHEMA.DLL				¥DEVICE¥HARDDI	SKVOLUME1¥WINDOWS¥SYSTEM32¥APISETS	SCHEMA.DLL			
GDI32.DLL				¥DEVICE¥HARDDI	SKVOLUME1¥WINDOWS¥SYSTEM32¥GDI32.	DLL			
IMJPPDMG.EXE				¥DEVICE¥HARDDI	SKVOLUME1¥WINDOWS¥SYSTEM32¥IME¥IM	EJP10¥IMJPPDMG.EXE			
IMJP10K.DLL				¥DEVICE¥HARDDI	SKVOLUME1¥WINDOWS¥SYSTEM32¥IMJP10	K.DLL			
IMM32.DLL				¥DEVICE¥HARDDI	SKVOLUME1¥WINDOWS¥SYSTEM32¥IMM32.	DLL			
KERNEL32.DLL				¥DEVICE¥HARDDI	SKVOLUME1¥WINDOWS¥SYSTEM32¥KERNEL	.32.DLL			
KERNELBASE.DLL				¥DEVICE¥HARDDI	SKVOLUME1¥WINDOWS¥SYSTEM32¥KERNEL	BASE.DLL			
IOCALE.NLS				¥DEVICE¥HARDDI	SKVOLUME1¥WINDOWS¥SYSTEM32¥LOCALE	.NLS			
E LPK.DLL				¥DEVICE¥HARDDI	SKVOLUME1¥WINDOWS¥SYSTEM32¥LPK.DLL				~
<									>
111 Files, 1 Selected	NirS	oft Freeware. http:	//www.nirs	oft.net					



# Forensic03

調査により、社員(以下、user01という)のパソコンは、マルウェアが混入したフリーソフト を実行していたことが確認されました。

フリーソフト「PC-Cleaner」(注記:架空のフリーソフト)に混入したマルウェアについて、 セキュリティ研究者のブログなどで情報収集したところ、ダウンローダーという種類のマル ウェアであり、他のマルウェア(以下、マルウェアBという)をダウンロードする機能を有して いるようです。

マルウェアBは、実行されると、パソコンのあるフォルダに自身をコピーするとともに、パ ソコンのログオン時に自動的に実行されるようレジストリを改変するようです。

あなたは、user01のパソコンに潜伏しているマルウェアBの検体をウイルス対策ソフトの 開発元に送付し、パターンファイルの作成を依頼する必要があると考えました。

user01のパソコンから証拠保全したエビデンスを解析し、マルウェアBのフルパスを特定してください。

[フラグ]

マルウェアBのフルパス(半角)例:C:¥Windows¥abc.exe

#### 解説(1)

 \$MFTを「MFTECmd」および「mactime」でタイムライン解析し、フリーソフト 「PC-Cleaner」が実行された日時で2018/09/30-22:56」の直後に、不審なファイルが 作成されていないか確認します。

```
C:¥work>mftecmd -f $MFT --body . --bdl C

MFTECmd version 0.3.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)

https://github.com/EricZimmerman/MFTECmd

Command line: -f $MFT --body . --bdl C

Warning: Administrator privileges not found!

Processed '$MFT' in 3.9603 seconds

Bodyfile output will be saved to '.¥20181007233902_MFTECmd_Output.body'

C:¥work>mactime -z Japan -b 20181007233902_MFTECmd_Output.body -m -d > timeline_mft.txt

C:¥work>
```

https://github.com/EricZimmerman/MFTECmd/releases https://www.sleuthkit.org/ (The Sleuth Kitに同梱)

# 解説(2)

Line	 Timestamp	macb	Meta	File Name	File Size
-	-	#OC	s 🛛 c	ADC .	=
640191	2018-09-30 22:55:33	macb	46208-128-1	c:/Users/user01/AppData/Local/Mozilla/Firefox/Profiles/o5j56hgo.default/cache2/entries/18CE467B00ED7B507CC72681EDCE.	. 101
640192	2018-09-30 22:55:33	macb	46208-48-2	c:/Users/user01/AppData/Local/Mozilla/Firefox/Profiles/o5j56hgo.default/cache2/entries/18CE467B00ED7B507CC72681EDCE.	. 101
640193	2018-09-30 22:55:40	m.,,	1719-128-4	c:/Windows/Prefetch/SEARCHPROTOCOLHOST.EXE-AFAD3EF9.pf	11960
640194	2018-09-30 22:55:41	m	1757-128-4	c:/Windows/Prefetch/SEARCHFILTERHOST.EXE-AA7A1FDD.pf	18804
640195	2018-09-30 22:56:09	m	11727-128-4	c:/Windows/Prefetch/DLLHOST.EXE-71214090.pf	64754
640196	2018-09-30 22:56:12	mac.	18339-144-0	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/RYYA134L	0
640197	2018-09-30 22:56:12	ma.b	18467-128-4	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/RYYA134L/lupin[1].jpg	37888
640198	2018-09-30 22:56:12	macb	18467-48-2	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/RYYA134L/lupin[1].jpg (\$FILE_NAME)	37888
640199	2018-09-30 22:56:12	macb	46113-128-3	c:/Users/user01/AppData/Local/Temp/a.exe	37888
640200	2018-09-30 22:56:12	macb	46113-48-2	c:/Users/user01/AppData/Local/Temp/a.exe (\$FILE_NAME)	37888
640201	2018-09-30 22:56:12	m.c.	46222-128-1	c:/Users/user01/AppData/Roaming/svchost.exe	37888
640202	2018-09-30 22:56:19	m	11787-128-4	c:/Windows/Prefetch/RUNDLL32.EXE-AFD98684.pf	18692
640203	2018-09-30 22:56:22	ma.b	18482-128-4	c:/Windows/Prefetch/PC-CLEANER.EXE-0FC5C951.pf	45458
640204	2018-09-30 22:56:22	macb	18482-48-2	c:/Window/Prefetch/PC-CLEANER.EXE-0FC5C951.pf (\$FILE_NAME)	45458
640205	2018-09-30 22:56:22	ma.b	46183-128-4	c:/Windows/Prefetch/A.EXE-E042BB59.pf	28550
640206	2018-09-30 22:56:22	macb	46183-48-2	c:/Windows/Prefetch/A.EXE-E042BB59.of (\$FILE NAME)	28550
640207	2018-09-30 22:		_		0
640208	2018-09-30 22: 2	7	の不宠	ファイルを発見	1086
640209	2018-09-30 22:				1086
640210	2018-09-30 22:	:•/U	lsers/i	iser01/AppData/Local/Temp/a exe	0
640211	2018-09-30 22:				25944
640212	2018-09-30 22:	:=/U	sers/u	Iser01/AppData/Roaming/sychost.exe	19362
640213	2018-09-30 22:			tions-ms	19362
640214	2018-09-30 22:			==.ico	2989
640215	2018-09-30 22:56:24	macb	46209-48-2	c:/Users/user01/AppData/Local/Mozilla/Firefox/Profiles/o5j56hgo.default/jumpListCache/MW3sU0k0_hvs1i7XbP1NKQ==.ico (\$FI	2989
640216	2018-09-30 22:56:29	m	44475-128-4	c:/Windows/Prefetch/AUDIODG.EXE-D0D776AC.pf	30650
640217	2018-09-30 22:56:45	m.c.	45891-128-4	c:/Users/user01/AppData/Local/Mozilla/Firefox/Profiles/o5i56hgo.default/cache2/entries/8C8ED651EE3EA7170F1F56FA86C40	51953

# 解説(3)

sury nives (1)   Available bookmarks	(18/0	)			Values				
ey name		# s	Last write timestamp		NUL-9111 #13500	×~~8~た	(-k=R) ==		
]c	=6	1	12		570 510020 540	NUX ACC	121.302.04.99		
🔺 💳 CurrentVersion	0	22	2018-08-24 22:39:13		Value Name	Value T	. Data		Value
Action Center	1	2	2018-08-24 22:27:52		9 8 <b>0</b> 0	REC	RBC		R B C
Applets	0	1	2018-08-24 13:42:58		<ul> <li>fakeMalware</li> </ul>	RegSz	C:¥Users¥user01¥AppData¥Roar	ming¥svchost.exe	
Controls Folder	2	0	2018-08-24 22:39:13			1			1
Explorer	3	31	2018-09-30 14:04:16						
▷ 🧰 Ext	0	1	2018-08-24 15:09:19						
Group Policy	0	2	2018-09-30 14:00:39						
	_					-			
▷ 🔁 HomeGroup	1	1	2018-09-30 14:00:48						
▷ HomeGroup▷ ime	1	1 1	2018-09-30 14:00:48 2018-08-24 13:42:41						
▷ HomeGroup▷ ime▷ Internet Settings	1 0 23	1 1 10	2018-09-30 14:00:48 2018-08-24 13:42:41						
▷ HomeGroup ▷ ime ▷ Internet Settings ▷ MCT	1 0 23 0	1 1 10 1	2018-09-30 14:00:48 2018-08-24 13:42:41				を 2つの不来つ	マイルタコ	でよう
<ul> <li>▷ HomeGroup</li> <li>▷ ime</li> <li>▷ Internet Settings</li> <li>▷ MCT</li> <li>○ NetCache</li> </ul>	1 0 23 0 1	1 10 1 0	2018-09-30 14:00:48 2018-08-24 13:42:41 レジストリ	NT	USERT.I		を、2つの不審フ	アイル名で	で検索
<ul> <li>HomeGroup</li> <li>ime</li> <li>Internet Settings</li> <li>MCT</li> <li>NetCache</li> <li>Policies</li> </ul>	1 0 23 0 1	1 10 1 0 0	2018-09-30 14:00:48 2018-08-24 13:42:41 レジストリ「 すると、「sy	NT /ch	USERT.I	/ DAT」 」が自	を、2つの不審フ 動実行設定され	マイル名で ていること	で検索
<ul> <li>HomeGroup</li> <li>ime</li> <li>Internet Settings</li> <li>MCT</li> <li>NetCache</li> <li>Policies</li> <li>RADAR</li> </ul>	1 0 23 0 1 0 2	1 10 1 0 0 0	2018-09-30 14:00:48 2018-08-24 13:42:41 レジストリ「 すると、「s、	NT /ch	USERT.I	´ DAT」 」が自	を、2つの不審フ 動実行設定され	アイル名で ていること	で検索 -を確
HomeGroup     HomeGroup     Internet Settings     MCT     NetCache     Policies     RADAR     Run	1 0 23 0 1 0 2 1	1 10 1 0 0 0 0	2018-09-30 14:00:48 2018-08-24 13:42:41 レジストリ「 すると、「s、	NT /ch	USERT.I	/ DAT」 」が自	を、2つの不審フ 動実行設定され	アイル名で ていること	で検 え を確
HomeGroup     HomeGroup     Internet Settings     MCT     NetCache     Policies     RADAR     Run     RunOnce	1 0 23 0 1 0 2 1 0	1 10 1 0 0 0 0 0	2018-09-30 14:00:48 2018-08-24 13:42:41 レジストリ「 すると、「s、	NT /ch	USERT.I	DAT」 」が自	を、2つの不審フ 動実行設定され	アイル名で ていること	で検す -を確
HomeGroup     HomeGroup     ime     Internet Settings     MCT     NetCache     Policies     RADAR     Run     RunOnce     Screensavers	1 0 23 0 1 0 2 1 0 0 0	1 10 1 0 0 0 0 0 4	2018-09-30 14:00:48 2018-08-24 13:42:41 レジストリ「 すると、「sv FLAG	NT /ch	USERT.I	´ DAT」 」が自	を、2つの不審フ 動実行設定され	マイル名で ていること	で検 ま を確
<ul> <li>HomeGroup</li> <li>HomeGroup</li> <li>ime</li> <li>Internet Settings</li> <li>MCT</li> <li>NetCache</li> <li>Policies</li> <li>RADAR</li> <li>Run</li> <li>RunOnce</li> <li>Screensavers</li> <li>Shell Extensions</li> </ul>	1 0 23 0 1 0 2 1 0 0 0 0 0	1 10 1 0 0 0 0 0 4 1	2018-09-30 14:00:48 2018-08-24 13:42:41 レジストリ「 すると、「sv FLAG C:¥IIse	NT /ch	USERT.I	/ DAT」 」が自	を、2つの不審フ 動実行設定され Data¥Roaming	アイル名つ ていること	で検索 こを確
<ul> <li>HomeGroup</li> <li>ime</li> <li>Internet Settings</li> <li>MCT</li> <li>NetCache</li> <li>Policies</li> <li>RADAR</li> <li>Run</li> <li>RunOnce</li> <li>Screensavers</li> <li>Shell Extensions</li> <li>Sidebar</li> </ul>	1 0 23 0 1 0 2 1 0 0 0 0 0 0	1 10 1 0 0 0 0 0 4 1 1	2018-09-30 14:00:48 2018-08-24 13:42:41 レジストリ「 すると、「sv FLAG C:¥Use	NT /ch rs¥	USERT.I	/ DAT」 」が自 Appl	を、2つの不審フ 動実行設定され Data¥Roaming	アイル名で ていること J¥svchos	で検す こを確 st.exe
<ul> <li>HomeGroup</li> <li>ime</li> <li>Internet Settings</li> <li>MCT</li> <li>NetCache</li> <li>Policies</li> <li>RADAR</li> <li>RunOnce</li> <li>Screensavers</li> <li>Shell Extensions</li> <li>Sidebar</li> <li>Telephony</li> </ul>	1 0 23 0 1 0 2 1 0 0 0 0 0 0 0	1 10 1 0 0 0 0 0 4 1 1 1	2018-09-30 14:00:48 2018-08-24 13:42:41 レジストリ「 すると、「sv FLAG C:¥Use	NT /ch rs¥	USERT.I	クAT」 」が自 Appl	を、2つの不審フ 動実行設定され Data¥Roaming	アイル名つ ていること J¥svchos	で検す こを確 st.exe
<ul> <li>HomeGroup</li> <li>ime</li> <li>Internet Settings</li> <li>MCT</li> <li>NetCache</li> <li>Policies</li> <li>RADAR</li> <li>RunOnce</li> <li>Screensavers</li> <li>Screensavers</li> <li>Sidebar</li> <li>Telephony</li> <li>ThemeManager</li> </ul>	1 0 23 0 1 0 2 1 0 0 0 0 0 0 8	1 10 1 0 0 0 0 0 4 1 1 1 0	2018-09-30 14:00:48 2018-08-24 13:42:41 レジストリ「 すると、「sv FLAG C:¥Use 2018-08-24 13:49:23	NT /ch rs¥	USERT.I	DAT」 」が自 Appl	を、2つの不審フ 動実行設定され Data¥Roaming	アイル名で ていること J¥svchos	で検索 生を確 st.exe
<ul> <li>HomeGroup</li> <li>ime</li> <li>Internet Settings</li> <li>MCT</li> <li>NetCache</li> <li>Policies</li> <li>RADAR</li> <li>RunOnce</li> <li>Screensavers</li> <li>Shell Extensions</li> <li>Sidebar</li> <li>Telephony</li> <li>ThemeManager</li> <li>Themes</li> </ul>	1 0 23 0 1 0 2 1 0 0 0 0 0 0 0 0 8 9	1 10 1 0 0 0 0 0 4 1 1 1 0 3	2018-09-30 14:00:48 2018-08-24 13:42:41 レジストリ「 すると、「sv FLAG C:¥Use 2018-08-24 13:49:23 2018-09-30 13:42:55	NT /ch rs¥	USERT.I	DAT」 」が自 Appl 75-00-73- 70-00-44	を、2つの不審フ 動実行設定され Data¥Roaming	アイル名で ていること J¥svchos	で検索 た確 t.exe
<ul> <li>P → HomeGroup</li> <li>P → ime</li> <li>P → Internet Settings</li> <li>MCT</li> <li>NetCache</li> <li>Policies</li> <li>RADAR</li> <li>RunOnce</li> <li>P → Screensavers</li> <li>&gt; Shell Extensions</li> <li>&gt; Sidebar</li> <li>&gt; Telephony</li> <li>→ ThemeS</li> <li>&gt; WinTrust</li> </ul>	1 0 23 0 1 0 2 1 0 0 0 0 0 0 0 0 8 9 0	1 10 1 0 0 0 0 0 0 4 1 1 1 1 0 3 1	2018-09-30 14:00:48 2018-08-24 13:42:41 レジストリ「 すると、「sv FLAG C:¥Use 2018-08-24 13:49:23 2018-09-30 13:42:55 2018-08-24 13:42:41	NT /ch rs¥	USERT.I	DAT」 」が自 Appl 75-00-73- 70-00-44	を、2つの不審フ 動実行設定され Data¥Roaming	アイル名で ていること J¥svchos	で検す さを確 st.exe



感染していたマルウェアの挙動について情報収集したところ、以下のようなキーロガー機能を有していることが判明しました。

[キーロガー機能の動作]

- (1) 利用者が入力した、オンラインバンキング等のユーザーIDとパスワードを「C:¥Users¥【ユー ザー名】¥AppData¥keylogger.txt」に記録する。
- (2) 「keylogger.txt」の内容を、C2サーバに送信する。
- (3)「keylogger.txt」の内容を、Oバイトの文字列で上書き保存することにより消去する。

感染したパソコンを確認したところ「keylogger.txt」が発見されたため、何らかのユー ザーIDとパスワードが情報流出した可能性があると考えられます。

あなたは、感染したパソコンディスクイメージを解析し、消去されたデータ(=情報流出したデータ)の復元を試みることにしました。

感染したパソコンの模擬ディスクイメージを解析し、情報流出した「パスワード」を特定してください。

[フラグ]

「keylogger.txt」に記録されていたパスワードと思われる文字列(半角)
 例:1qaz2wsx3edc

#### 解説(1)

- 問題ファイルのディスクイメージのファイルシステムは、NTFSです。
- NTFSは、ファイル名やタイムスタンプなどの属性情報「\$MFT」のFILEレコード記録し ます。また、ファイルに記録されるデータのサイズが小さい場合、FILEレコードにデータ が保存されます。
- また、FILEレコードに保存されたデータは、元データよりも小さなデータで上書き保存された場合、FILEレコードに古いデータの残骸が残るという特性があります。
- 従って、ディスクイメージをバイナリエディタなどで開き、ファイルシステムを目視確認することで、「keylogger.txt」の古いデータの残骸を確認することができます。

#### 解説(2)

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	1	<b>CN</b>		II v
17653760	46	49	4C	45	30	00	03	00	2D	4B	20	00	00	00	00	00	FILE	0	-K	
17653776	01	00	01	00	38	00	01	00	30	01	00	00	00	04	00	00		8	0	
17653792	00	00	00	00	00	00	00	00	03	00	00	00	BO	00	00	00				۰
17653808	03	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00				*
17653824	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00			Н	
17653840	EA	F5	55	1E	92	5B	D4	01	03	99	6A	26	92	5B	D4	01	êõU	'[Ô	™j	۵] <b>'</b> ه
17653856	03	99	6A	26	92	5B	D4	01	EA	F5	55	1E	92	5B	D4	01	™js	' [Ô	êõU	'[Ô
17653872	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
17653888	00	00	00	00	08	01	00	00	00	00	00	00	00	00	00	00				
17653904	00	00	00	00	00	00	00	00	30	00	0.0	0.0	78	0.0	0.0	0.0			0	x
17653920	00	00	00	00	00	00	02	00	5C	00	00	00	18	00	01	00			1	
17653936	28	00	00	00	00	00	01	00	EA	F5	55	1E	92	5B	D4	01	(		êõU	'[Ĉ
17653952	EA	F5	55	1E	92	51											êõU	'[Ô	êõU	′[Ĉ
17653968	EA	F5	55	1E	92	51	FL	AG									êõU	'[Ô		
17653984	00	00	00	00	00	00			1r (	) t c	lefi	'r0-	sØ	D						
17654000	OD	00	6B	00	65	00			1. 6								k	е у	1 0	gg
17654016	65	00	72	00	2E	00	74	00	78	00	74	00	00	00	00	00	e r	. t	x t	
17654032	80	00	00	00	18	00	00	00	00	00	18	00	00	00	01	00	€			
17654048	00	00	00	00	18	00	00	00	FF	FF	FF	FF	82	79	47	11			999	₽,yG
17654064	73	65	72	30	31	OD	0A	5D	72	40	74	64	65	66	5B	72	ser	1	]r@t	def[r
17654080	30	2D	73	40	0D	OA	0D	AO	OD	0A	00	00	00	00	00	00	0-30	1		0.00000000000000000000
17654096	FF	FF	FF	FF	82	79	47	11	00	00	00	00	00	00	00	00	<u>8888</u>	,yG		
17654112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
Sector 34,480	) of	102	,400	)							Off	set:					10	1	7,653	8,760