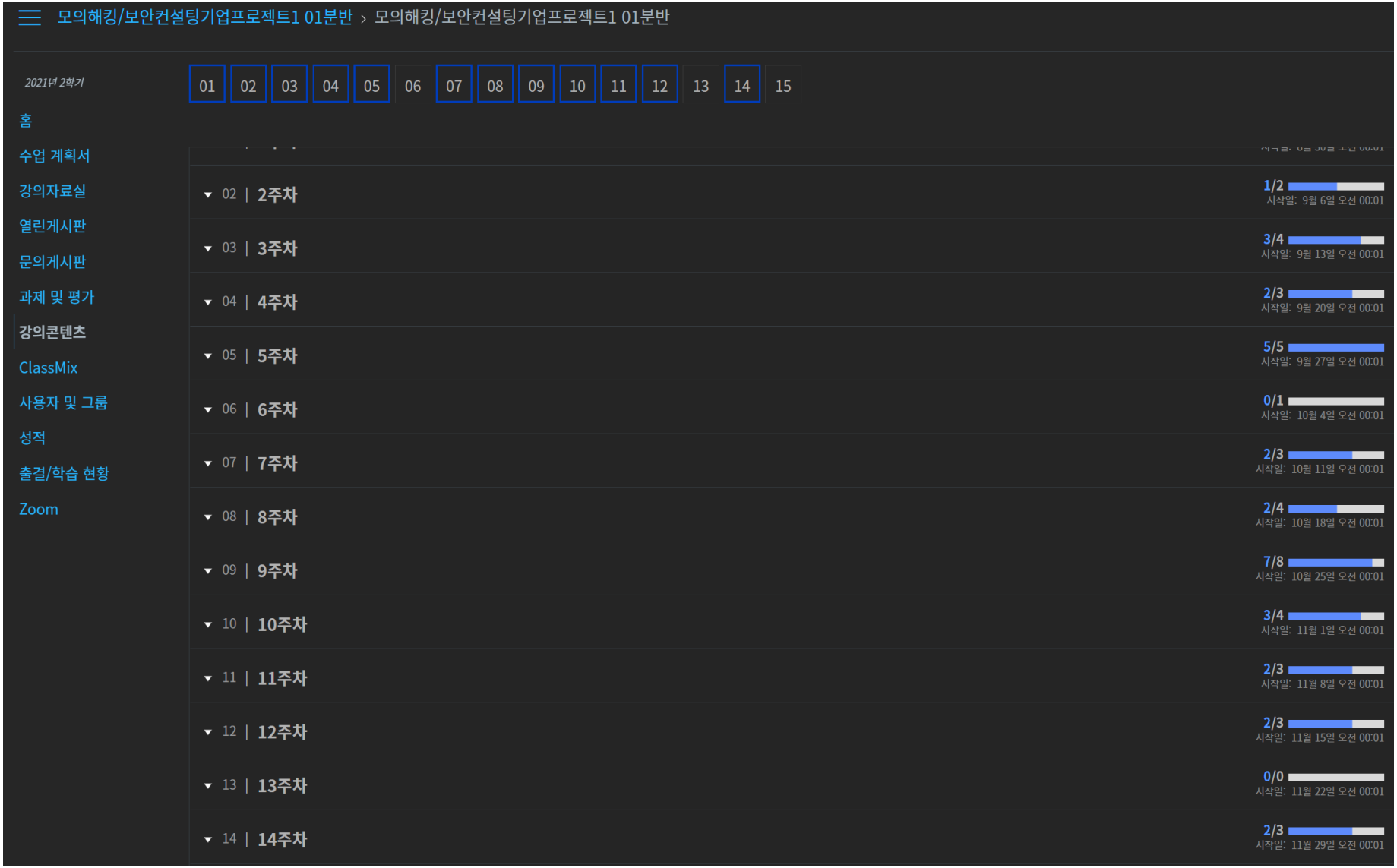
CTF-D 포렌식 문제풀이

91514701 김정식

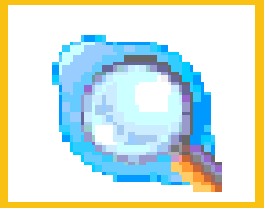
목 차

1. 주제 선정 이유

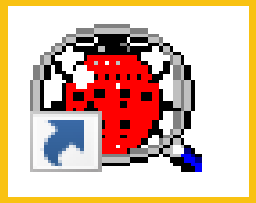

모의해킹/보안컨설팅기업프로젝트1 01분반 › 모의해킹/보안컨설팅기업프로젝트1 01분반
2021년 2학기
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
홈
수업 계획서
강의자료실
열린게시판
문의게시판
과제 및 평가
강의콘텐츠
ClassMix
사용자 및 그룹
성적
출결/학습 현황
Zoom
02 | 2주차 1/2 시작일: 9월 6일 오전 00:01
03 | 3주차 3/4 시작일: 9월 13일 오전 00:01
04 | 4주차 2/3 시작일: 9월 20일 오전 00:01
05 | 5주차 5/5 시작일: 9월 27일 오전 00:01
06 | 6주차 0/1 시작일: 10월 4일 오전 00:01
07 | 7주차 2/3 시작일: 10월 11일 오전 00:01
08 | 8주차 2/4 시작일: 10월 18일 오전 00:01
09 | 9주차 7/8 시작일: 10월 25일 오전 00:01
10 | 10주차 3/4 시작일: 11월 1일 오전 00:01
11 | 11주차 2/3 시작일: 11월 8일 오전 00:01
12 | 12주차 2/3 시작일: 11월 15일 오전 00:01
13 | 13주차 0/0 시작일: 11월 22일 오전 00:01
14 | 14주차 2/3 시작일: 11월 29일 오전 00:01

2. 사용 Tools

FTK IMAGER



SKYPE
LOG
VIEW



Thumbs.db
viewer

HXD

3. 문제풀이

Challenge | 25 Solves

거대한 마약 조직을 잡으려는...

320

거대한 마약 조직을 잡으려는 시도로 경찰은 습격을 하여 샬롯 윌 (Charlotte May)의 컴퓨터를 압수했다. 그녀는 다른 마약 거래를 돕는 혐의를 받고 있다. 이 컴퓨터에서 발견 된 의사소통은 다음 약물 거래가 있음을 증명했다. 분석관인 당신은 해당 시스템을 분석하여 다음 거래의 암호 코드를 찾아야한다.

Hint :

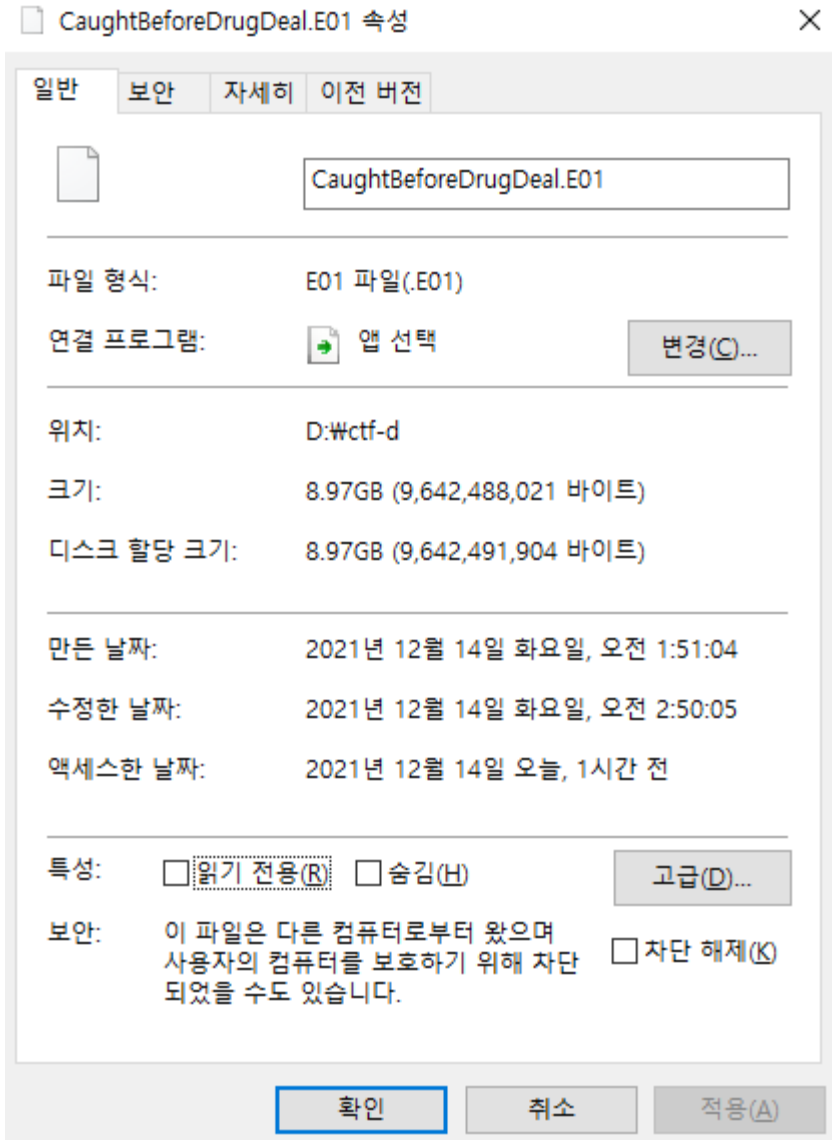
- 메일만이 유일한 통신 수단이 아니다.
- 파일이 삭제돼도 일부 아티팩트가 시스템에 계속 존재한다.

KEY Format : Text(Code)

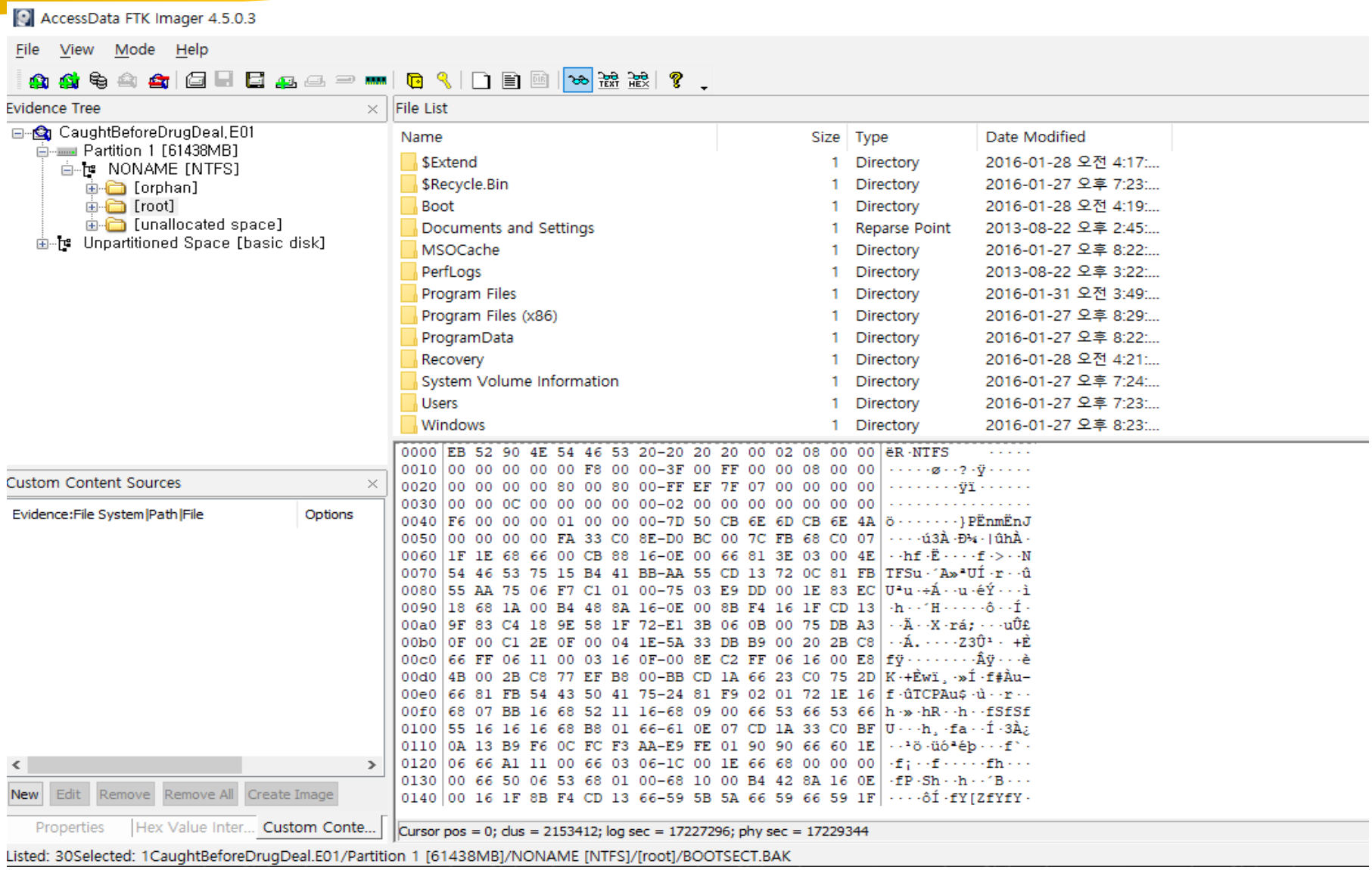
CaughtBefore...

Key

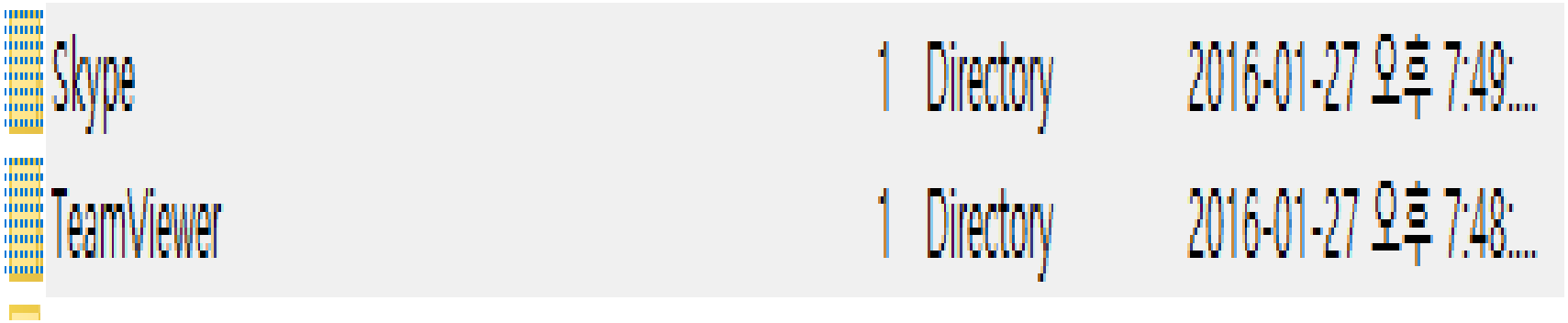
SUBMIT



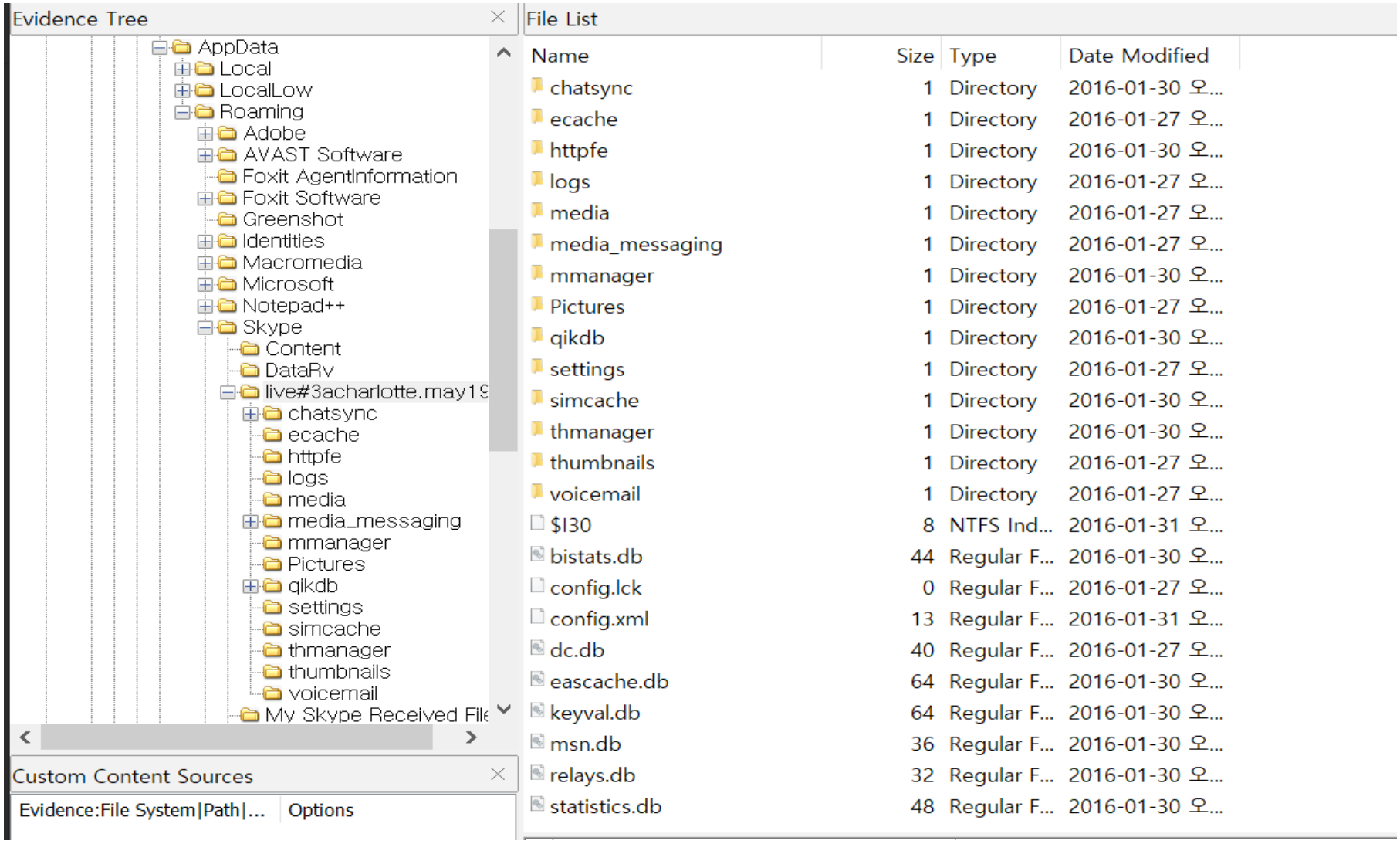
3. 문제풀이


AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
CaughtBeforeDrugDeal.E01
Partition 1 [61438MB]
NONAME [NTFS]
[orphan]
[root]
[unallocated space]
Unpartitioned Space [basic disk]
File List
Name Size Type Date Modified
$Extend 1 Directory 2016-01-28 오전 4:17:...
$Recycle.Bin 1 Directory 2016-01-27 오후 7:23:...
Boot 1 Directory 2016-01-28 오전 4:19:...
Documents and Settings 1 Reparse Point 2013-08-22 오후 2:45:...
MSOCache 1 Directory 2016-01-27 오후 8:22:...
PerfLogs 1 Directory 2013-08-22 오후 3:22:...
Program Files 1 Directory 2016-01-31 오전 3:49:...
Program Files (x86) 1 Directory 2016-01-27 오후 8:29:...
ProgramData 1 Directory 2016-01-27 오후 8:22:...
Recovery 1 Directory 2016-01-28 오전 4:21:...
System Volume Information 1 Directory 2016-01-27 오후 7:24:...
Users 1 Directory 2016-01-27 오후 7:23:...
Windows 1 Directory 2016-01-27 오후 8:23:...
0000 EB 52 90 4E 54 46 53 20-20 20 20 00 02 08 00 00
0010 00 00 00 00 00 F8 00 00-3F 00 FF 00 00 08 00 00
0020 00 00 00 00 80 00 80 00-FF EF 7F 07 00 00 00 00
0030 00 00 0C 00 00 00 00 00-02 00 00 00 00 00 00 00
0040 F6 00 00 00 01 00 00 00-7D 50 CB 6E 6D CB 6E 4A
0050 00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB 68 C0 07
0060 1F 1E 68 66 00 CB 88 16-0E 00 66 81 3E 03 00 4E
0070 54 46 53 75 15 B4 41 BB-AA 55 CD 13 72 0C 81 FB
0080 55 AA 75 06 F7 C1 01 00-75 03 E9 DD 00 1E 83 EC
0090 18 68 1A 00 B4 48 8A 16-0E 00 8B F4 16 1F CD 13
00a0 9F 83 C4 18 9E 58 1F 72-E1 3B 06 0B 00 75 DB A3
00b0 0F 00 C1 2E 0F 00 04 1E-5A 33 DB B9 00 20 2B C8
00c0 66 FF 06 11 00 03 16 0F-00 8E C2 FF 06 16 00 E8
00d0 4B 00 2B C8 77 EF B8 00-BB CD 1A 66 23 C0 75 2D
00e0 66 81 FB 54 43 50 41 75-24 81 F9 02 01 72 1E 16
00f0 68 07 BB 16 68 52 11 16-68 09 00 66 53 66 53 66
0100 55 16 16 16 68 B8 01 66-61 0E 07 CD 1A 33 C0 BF
0110 0A 13 B9 F6 0C FC F3 AA-E9 FE 01 90 90 66 60 1E
0120 06 66 A1 11 00 66 03 06-1C 00 1E 66 68 00 00 00
0130 00 66 50 06 53 68 01 00-68 10 00 B4 42 8A 16 0E
0140 00 16 1F 8B F4 CD 13 66-59 5B 5A 66 59 66 59 1F
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Cursor pos = 0; clus = 2153412; log sec = 17227296; phy sec = 17229344
Listed: 30Selected: 1CaughtBeforeDrugDeal.E01/Partition 1 [61438MB]/NONAME [NTFS]/[root]/BOOTSECT.BAK

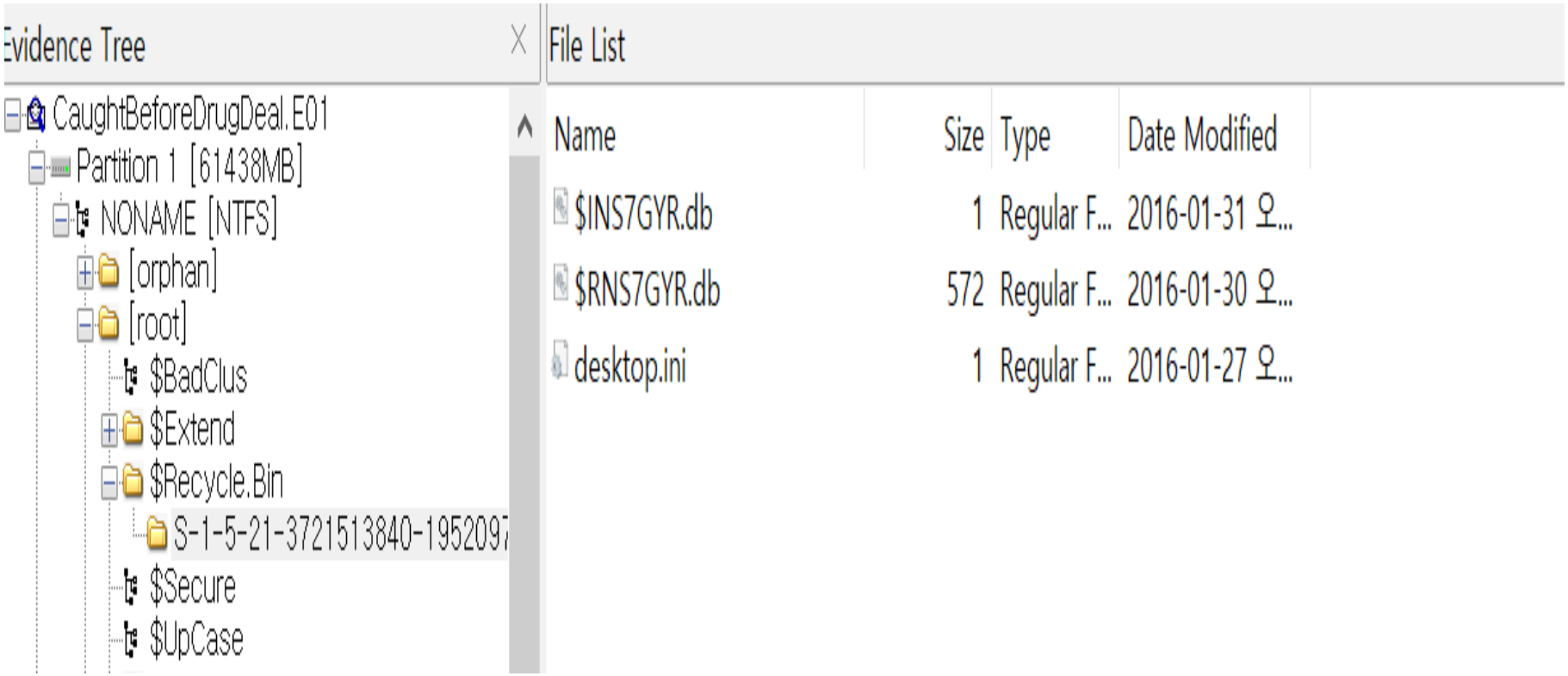
3. 문제풀이


Skype 1 Directory 2016-01-27 오후 7:49:...
TeamViewer 1 Directory 2016-01-27 오후 7:48:...

3. 문제풀이


Evidence Tree
AppData
Local
LocalLow
Roaming
Adobe
AVAST Software
Foxit AgentInformation
Foxit Software
Greenshot
Identities
Macromedia
Microsoft
Notepad++
Skype
Content
DataRv
live#3acharlotte.may19
chatsync
ecache
httpfe
logs
media
media_messaging
mmanager
Pictures
qikdb
settings
simcache
thmanager
thumbnails
voicemail
My Skype Received File
Custom Content Sources
Evidence:File System|Path|...
Options
File List
Name
Size
Type
Date Modified
chatsync 1 Directory 2016-01-30 오...
ecache 1 Directory 2016-01-27 오...
httpfe 1 Directory 2016-01-30 오...
logs 1 Directory 2016-01-27 오...
media 1 Directory 2016-01-27 오...
media_messaging 1 Directory 2016-01-27 오...
mmanager 1 Directory 2016-01-30 오...
Pictures 1 Directory 2016-01-27 오...
qikdb 1 Directory 2016-01-30 오...
settings 1 Directory 2016-01-27 오...
simcache 1 Directory 2016-01-30 오...
thmanager 1 Directory 2016-01-30 오...
thumbnails 1 Directory 2016-01-27 오...
voicemail 1 Directory 2016-01-27 오...
$I30 8 NTFS Ind... 2016-01-31 오...
bistats.db 44 Regular F... 2016-01-30 오...
config.lck 0 Regular F... 2016-01-27 오...
config.xml 13 Regular F... 2016-01-31 오...
dc.db 40 Regular F... 2016-01-27 오...
eascache.db 64 Regular F... 2016-01-30 오...
keyval.db 64 Regular F... 2016-01-30 오...
msn.db 36 Regular F... 2016-01-30 오...
relays.db 32 Regular F... 2016-01-30 오...
statistics.db 48 Regular F... 2016-01-30 오...

3. 문제풀이


Evidence Tree
CaughtBeforeDrugDeal.E01
Partition 1 [61438MB]
NONAME [NTFS]
[orphan]
[root]
$BadClus
$Extend
$Recycle.Bin
S-1-5-21-3721513840-1952097
$Secure
$UpCase
File List
Name
Size
Type
Date Modified
$INS7GYR.db
1
Regular F...
2016-01-31 오...
$RNS7GYR.db
572
Regular F...
2016-01-30 오...
desktop.ini
1
Regular F...
2016-01-27 오...

3. 문제풀이

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text	
00000000	01	00	00	00	00	00	00	00	00	F0	08	00	00	00	00	00	.........ð.....	섹터 0
00000010	90	15	B9	BA	61	5C	D1	01	43	00	3A	00	5C	00	55	00	..¹ºa\Ñ.C.:.\.U.	
00000020	73	00	65	00	72	00	73	00	5C	00	43	00	68	00	61	00	s.e.r.s.\.C.h.a.	
00000030	72	00	6C	00	6F	00	74	00	74	00	65	00	5C	00	41	00	r.l.o.t.t.e.\.A.	
00000040	70	00	70	00	44	00	61	00	74	00	61	00	5C	00	52	00	p.p.D.a.t.a.\.R.	
00000050	6F	00	61	00	6D	00	69	00	6E	00	67	00	5C	00	53	00	o.a.m.i.n.g.\.S.	
00000060	6B	00	79	00	70	00	65	00	5C	00	6C	00	69	00	76	00	k.y.p.e.\.l.i.v.	
00000070	65	00	23	00	33	00	61	00	63	00	68	00	61	00	72	00	e.#.3.a.c.h.a.r.	
00000080	6C	00	6F	00	74	00	74	00	65	00	2E	00	6D	00	61	00	l.o.t.t.e...m.a.	
00000090	79	00	31	00	39	00	38	00	39	00	5C	00	6D	00	61	00	y.1.9.8.9.\.m.a.	
000000A0	69	00	6E	00	2E	00	64	00	62	00	00	00	00	00	00	00	i.n...d.b.....	
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
00000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
000001B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
000001C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
00000200	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	섹터 1
00000210	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	

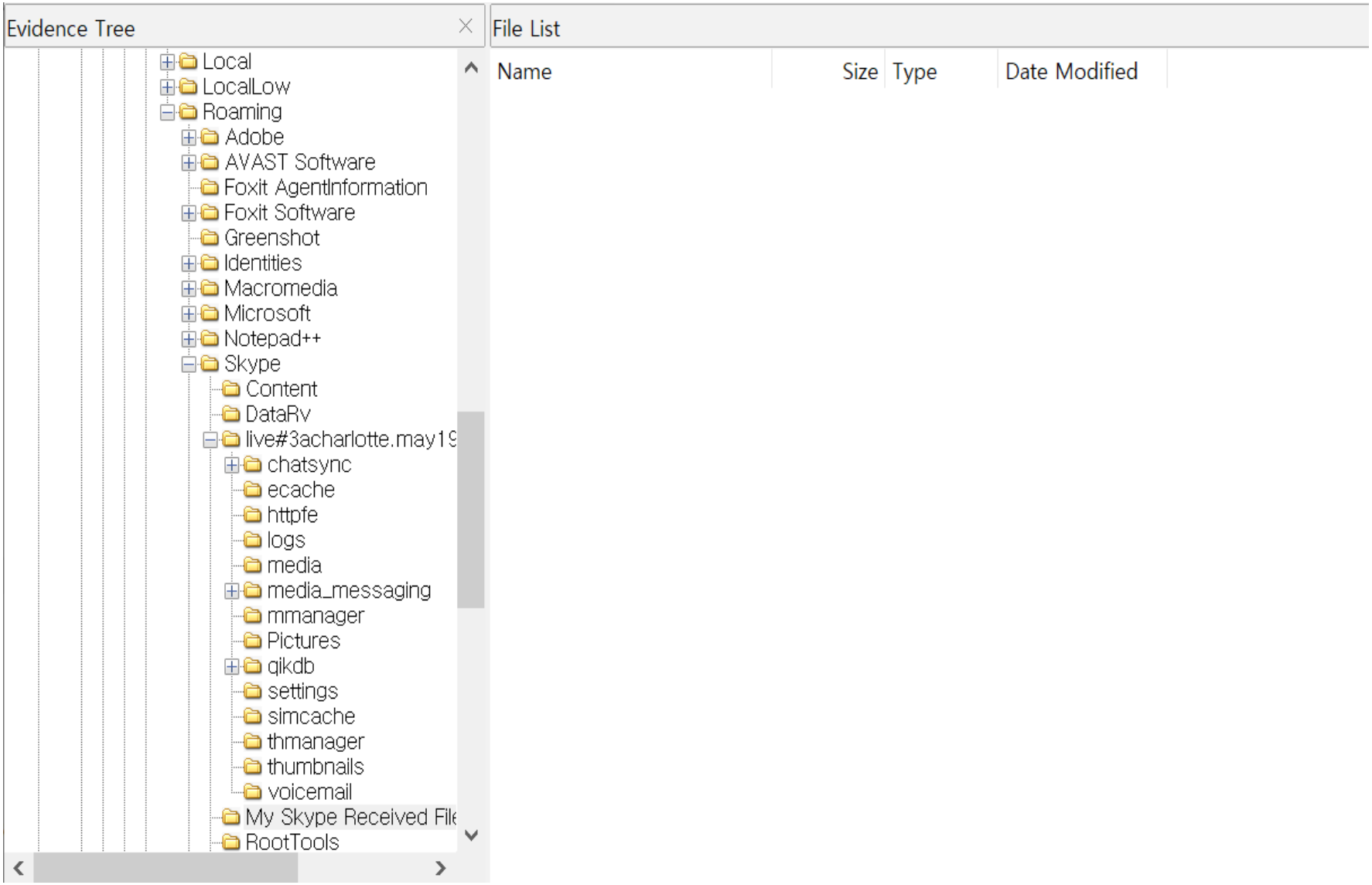
3. 문제풀이

SkypeLogView: D:₩

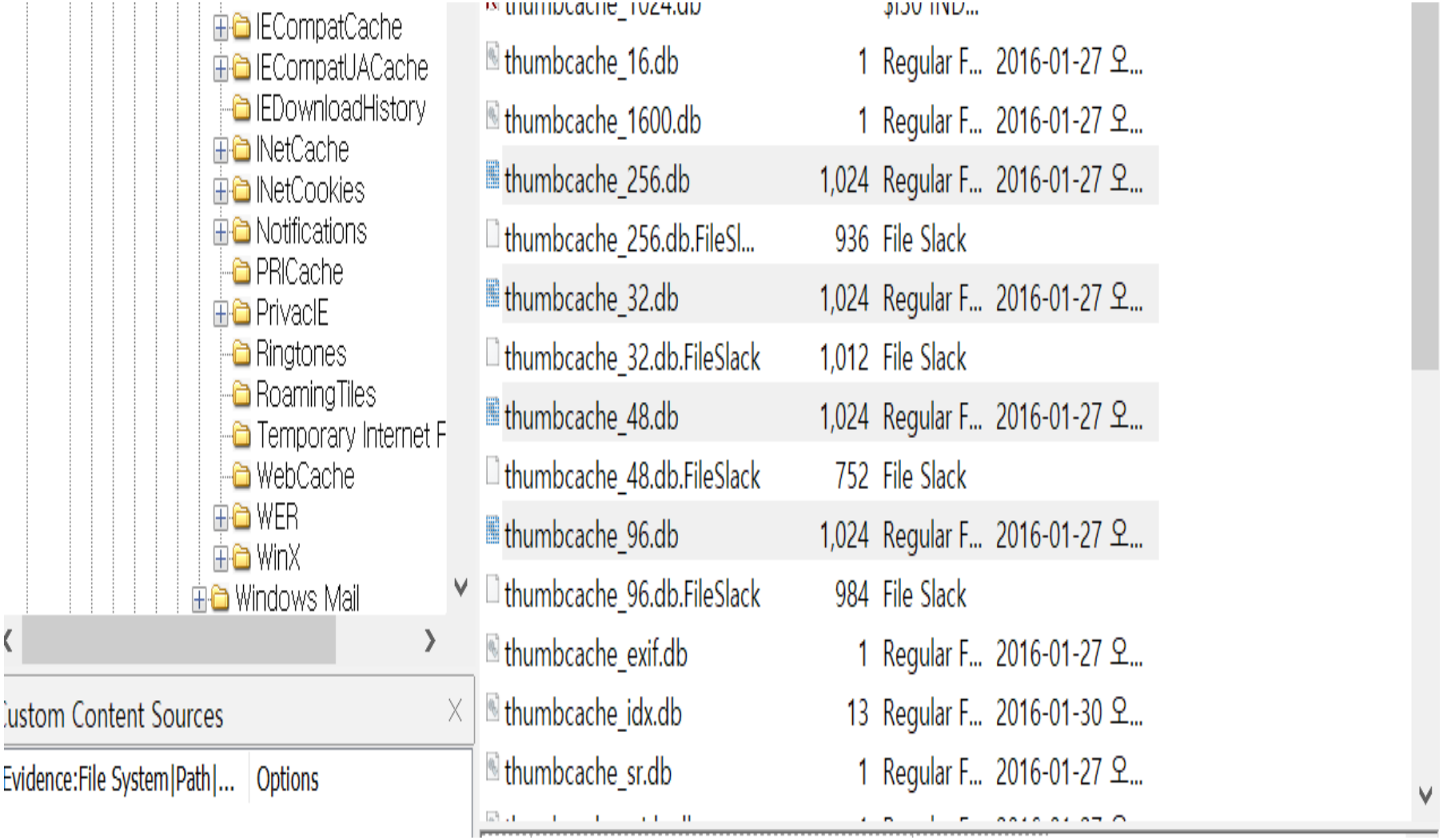
File Edit View Options Help

Action Type	Action Time	E..	User Name	Display Name	[	Chat Message	ChatID	Filename
Chat	2016-01-28 오전 ...		live:charlotte.may1989 l...					
Outgoing Call			live:john_smith.1992	john smith				
Chat Message	2016-01-30 오후 ...		live:john_smith.1992	live:john_smith.1992		Hey	live:jo...	
Chat	2016-01-30 오후 ...		live:charlotte.may1989 l...					
Chat	2016-01-30 오후 ...		live:charlotte.may1989 l...					
Chat Message	2016-01-30 오후 ...		live:john_smith.1992	john smith		is it safe?	#live:j...	
Chat Message	2016-01-30 오후 ...		live:charlotte.may1989	Charlotte May		Hi	#live:j...	
Chat Message	2016-01-30 오후 ...		live:charlotte.may1989	Charlotte May		Yes. I've reconfigured my pc. Wiped everything and did a clean in...	#live:j...	
Chat Message	2016-01-30 오후 ...		live:john_smith.1992	john smith		alright great	#live:j...	
Chat Message	2016-01-30 오후 ...		live:charlotte.may1989	Charlotte May		any news from the boss?	#live:j...	
Chat Message	2016-01-30 오후 ...		live:john_smith.1992	john smith		yeah, could you help us out again?	#live:j...	
Chat Message	2016-01-30 오후 ...		live:charlotte.may1989	Charlotte May		what do you need?	#live:j...	
Chat Message	2016-01-30 오후 ...		live:john_smith.1992	john smith		hold on, I'll send you the list	#live:j...	
Chat Message	2016-01-30 오후 ...		live:charlotte.may1989	Charlotte May		okay	#live:j...	
Receive File	2016-01-30 오후 ...		live:john_smith.1992	john smith				C:₩Users₩Charlotte₩AppData₩Roaming₩Skype₩My Skype Received Files₩Details.docx
Chat Message	2016-01-30 오후 ...		live:charlotte.may1989	Charlotte May		Let me see if it is possible to do	#live:j...	
Chat Message	2016-01-30 오후 ...		live:john_smith.1992	john smith		let me know asap	#live:j...	
Chat Message	2016-01-30 오후 ...		live:john_smith.1992	john smith		how many days do you need?	#live:j...	
Chat Message	2016-01-30 오후 ...		live:charlotte.may1989	Charlotte May		okay.. still a lot to prepare	#live:j...	
Chat Message	2016-01-31 오전 ...		live:charlotte.may1989	Charlotte May		Beginning of February will be hard, but if I pull some strings and make s...	#live:j...	
Chat Message	2016-01-31 오전 ...		live:john_smith.1992	john smith		the boss will highly appreciate it	live:jo...	
Chat Message	2016-01-31 오전 ...		live:john_smith.1992	john smith		so, the first week of february, same time, same place?	live:jo...	
Chat Message	2016-01-31 오전 ...		live:charlotte.may1989	Charlotte May		Agreed.	#live:j...	
Chat Message	2016-01-31 오전 ...		live:charlotte.may1989	Charlotte May		Still reachable on the same number of have you changed it again?	#live:j...	
Chat Message	2016-01-31 오전 ...		live:john_smith.1992	john smith		same number, I'll change it again after our meeting	live:jo...	
Chat Message	2016-01-31 오전 ...		live:charlotte.may1989	Charlotte May		Okay. Let's get to work. See you there and then.	#live:j...	
Chat Message	2016-01-31 오전 ...		live:john_smith.1992	john smith		don't forget to the destroy the doc	#live:j...	
Chat Message	2016-01-31 오전 ...		live:charlotte.may1989	Charlotte May		Consider it done	#live:j...	
Chat Message	2016-01-31 오전 ...		live:john_smith.1992	john smith		good, bye	#live:j...	
Chat Message	2016-01-31 오전 ...		live:charlotte.may1989	Charlotte May		bye	#live:j...	

3. 문제풀이


Evidence Tree
File List
Name
Size
Type
Date Modified
Local
LocalLow
Roaming
Adobe
AVAST Software
Foxit AgentInformation
Foxit Software
Greenshot
Identities
Macromedia
Microsoft
Notepad++
Skype
Content
DataRv
live#3acharlotte.may19
chatsync
ecache
httpfe
logs
media
media_messaging
mmanager
Pictures
qikdb
settings
simcache
thmanager
thumbnails
voicemail
My Skype Received File
RootTools

3. 문제풀이

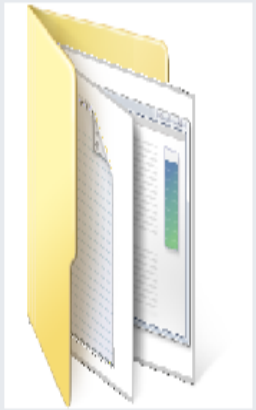

IECompatCache
IECompatUACache
IEDownloadHistory
INetCache
INetCookies
Notifications
PRICache
PrivacIE
Ringtones
RoamingTiles
Temporary Internet F
WebCache
WER
WinX
Windows Mail
ustom Content Sources
Evidence:File System|Path|...
Options
thumbcache_16.db 1 Regular F... 2016-01-27 오...
thumbcache_1600.db 1 Regular F... 2016-01-27 오...
thumbcache_256.db 1,024 Regular F... 2016-01-27 오...
thumbcache_256.db.FileSl... 936 File Slack
thumbcache_32.db 1,024 Regular F... 2016-01-27 오...
thumbcache_32.db.FileSlack 1,012 File Slack
thumbcache_48.db 1,024 Regular F... 2016-01-27 오...
thumbcache_48.db.FileSlack 752 File Slack
thumbcache_96.db 1,024 Regular F... 2016-01-27 오...
thumbcache_96.db.FileSlack 984 File Slack
thumbcache_exif.db 1 Regular F... 2016-01-27 오...
thumbcache_idx.db 13 Regular F... 2016-01-30 오...
thumbcache_sr.db 1 Regular F... 2016-01-27 오...

3. 문제풀이

D:₩ctf-d₩thum₩thumbcache_256.db

페이지: 1/1. 썸네일: 5

e3ebb0f98a107405



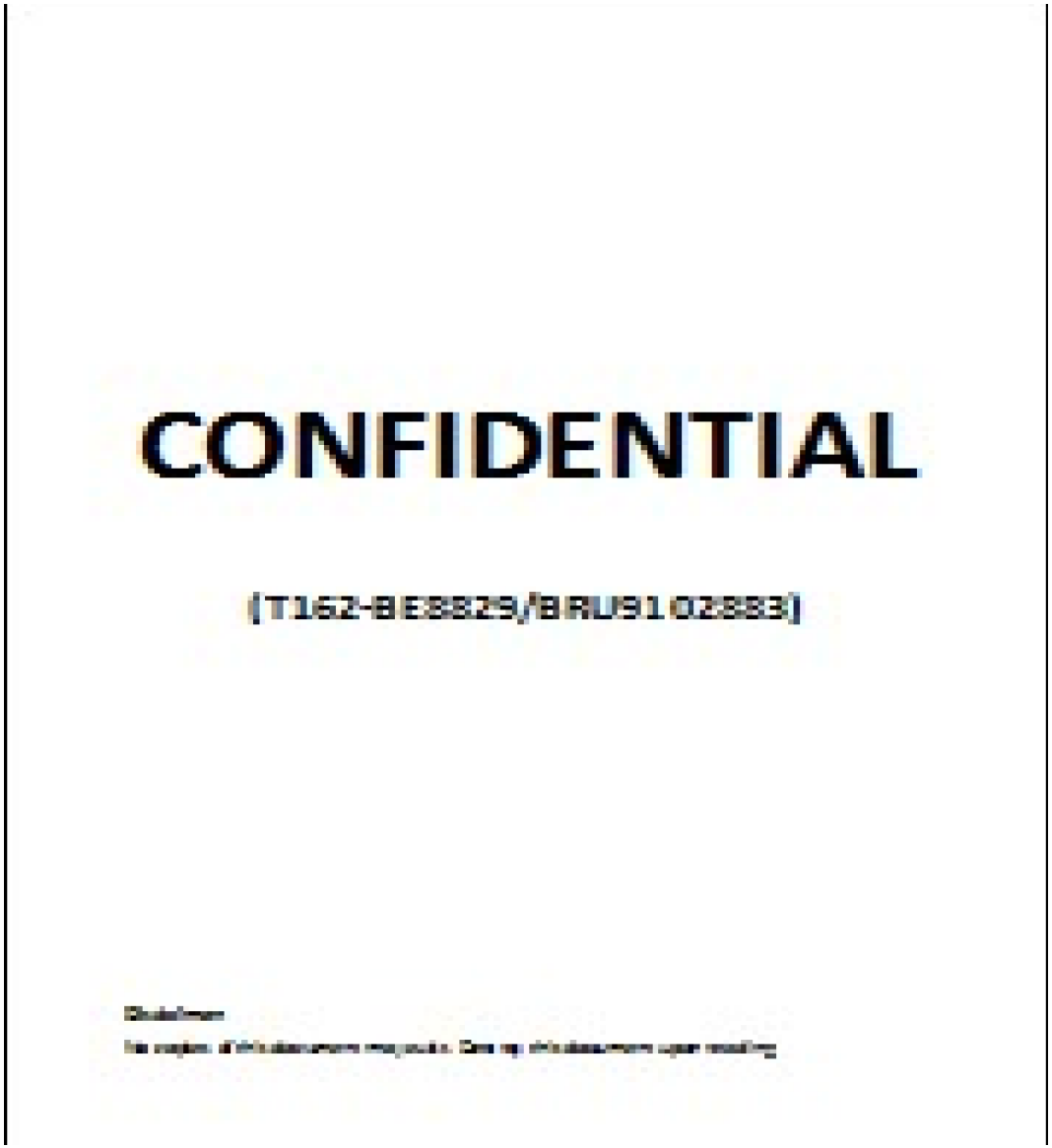
10c482279f068f4a

d3590cc931655cc6

714ec1eca24b83ff

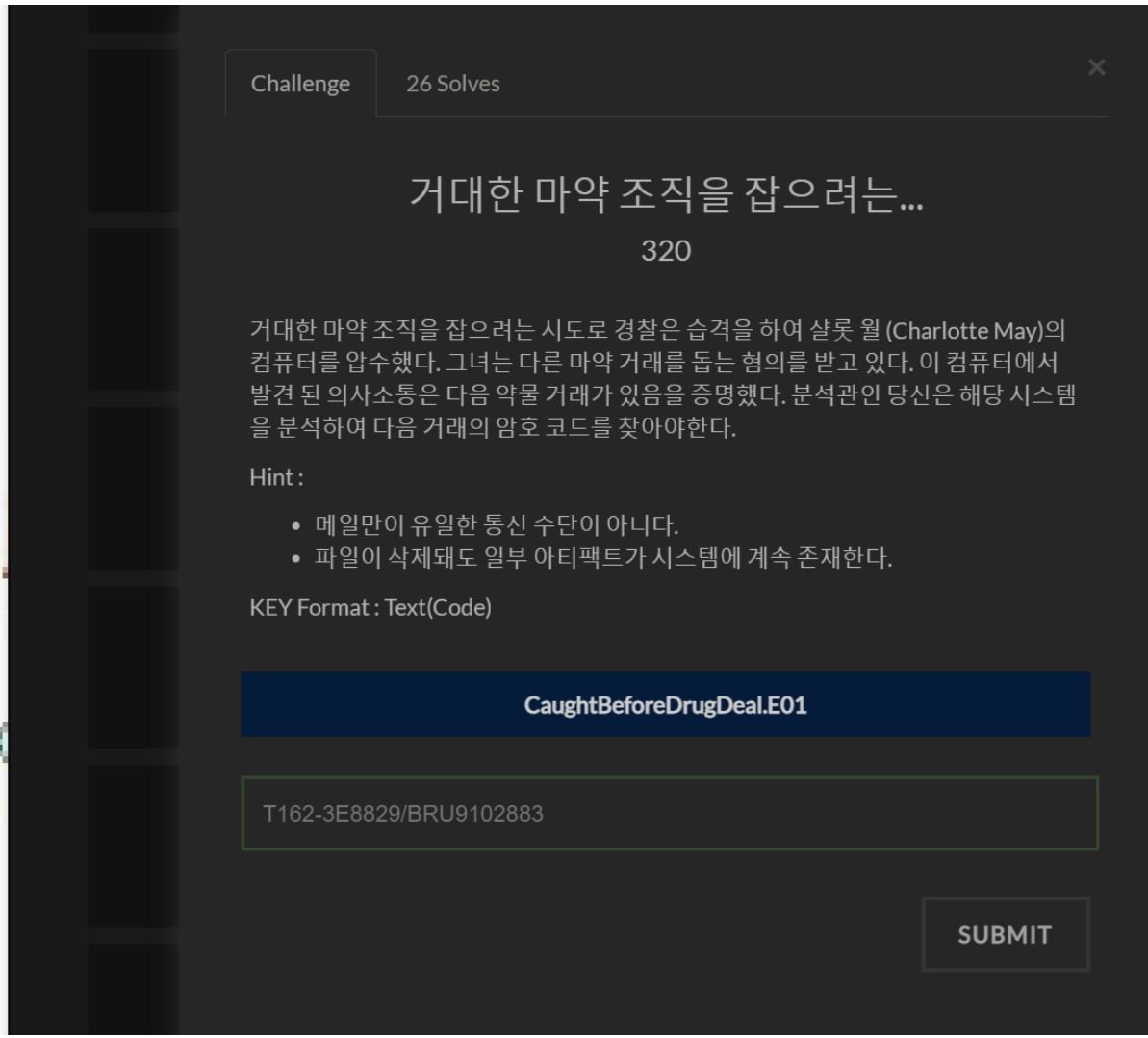
c4041073461dea06

3. 문제풀이



3. 문제풀이


CONFIDENTI
{T162-3E8829/BRU9102883}


Challenge
26 Solves
거대한 마약 조직을 잡으려는...
320
거대한 마약 조직을 잡으려는 시도로 경찰은 습격을 하여 샬롯 웰 (Charlotte May)의 컴퓨터를 압수했다. 그녀는 다른 마약 거래를 돕는 혐의를 받고 있다. 이 컴퓨터에서 발견 된 의사소통은 다음 약물 거래가 있음을 증명했다. 분석관인 당신은 해당 시스템을 분석하여 다음 거래의 암호 코드를 찾아야한다.
Hint :
메일만이 유일한 통신 수단이 아니다.
파일이 삭제돼도 일부 아티팩트가 시스템에 계속 존재한다.
KEY Format : Text(Code)
CaughtBeforeDrugDeal.E01
T162-3E8829/BRU9102883
SUBMIT

4. 마치며

감사합니다.