151 – Carless Drug Dealer

Team Information

Team Name : LuckyVicky

Team Member : Eungchang Lee, Hyun Yi, Juho Heo, Dongkyu Lee

Email Address : dfc_luckyvicky@googlegroups.com

Instructions

Description The police have recently identified that Suspect A, who has entered the country, has been traveling around various cities in the world selling drugs. While drug transactions were noted in two cities, the exact locations have not been specified. It appears that a drug sales ledger file was created in the first city and additional sales were made in another city. The police arrested Suspect A upon his return and obtained his USB. To conduct an international joint investigation, countries responded that the local time information of the files is needed. Find out the timestamps of these files.

Target	Hash (MD5)
USB.zip	9e6463aa60b403697222b1442df54a68

Questions

1. Identify the drug trade ledger file and find the filename. (20 points)
2. Identify the timezone values for the creation time and modification time of the drug trade ledger file. (50 points)
3. Identify the creation and modification times of the drug trade ledger file in local time. Write the times in the format YYYY-MM-DD HH:MM (UTC+00:00). (80 points)

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

Tools used:

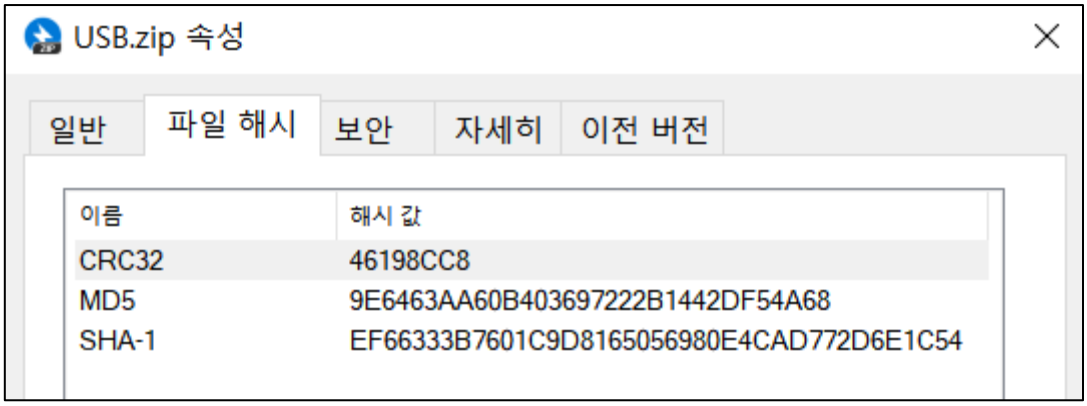
Name:	FTK Imager	Publisher:	AccessData® FTK® Imager
Version:	4.7.1.2		
URL:	https://go.exterro.com/l/43312/2023-05-03/fc4b78		

Name:	HxD	Publisher:	Maël Hörz
Version:	2.5.0.0		
URL:	https://www.mh-nexus.de		

Name:	HashTab	Publisher:	Implbits Software
Version:	6.0.0		
URL:	https://implbits.com		

Name:	Dcode	Publisher:	Digital Detective
Version:	5.5		
URL:	https://www.digital-detective.net/dcode/		

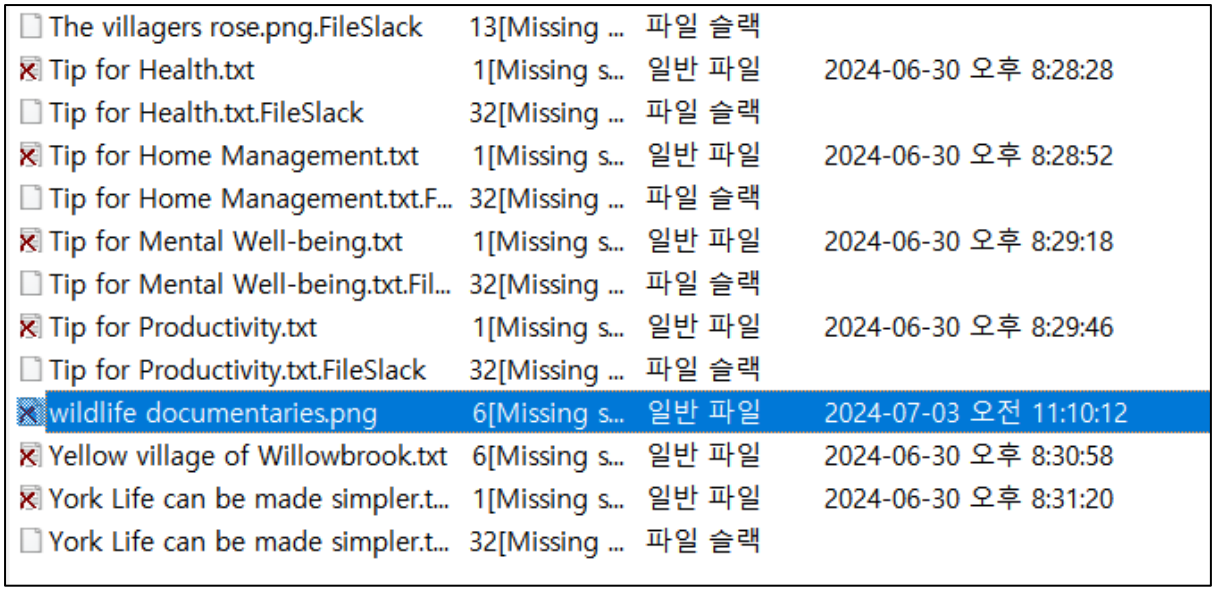
Step-by-step methodology:



[그림 1] USB.zip 파일 해시 값 확인

분석에 앞서, 주어진 target file인 USB.zip에 대한 md5 해시 값이 일치함을 확인하였습니다.

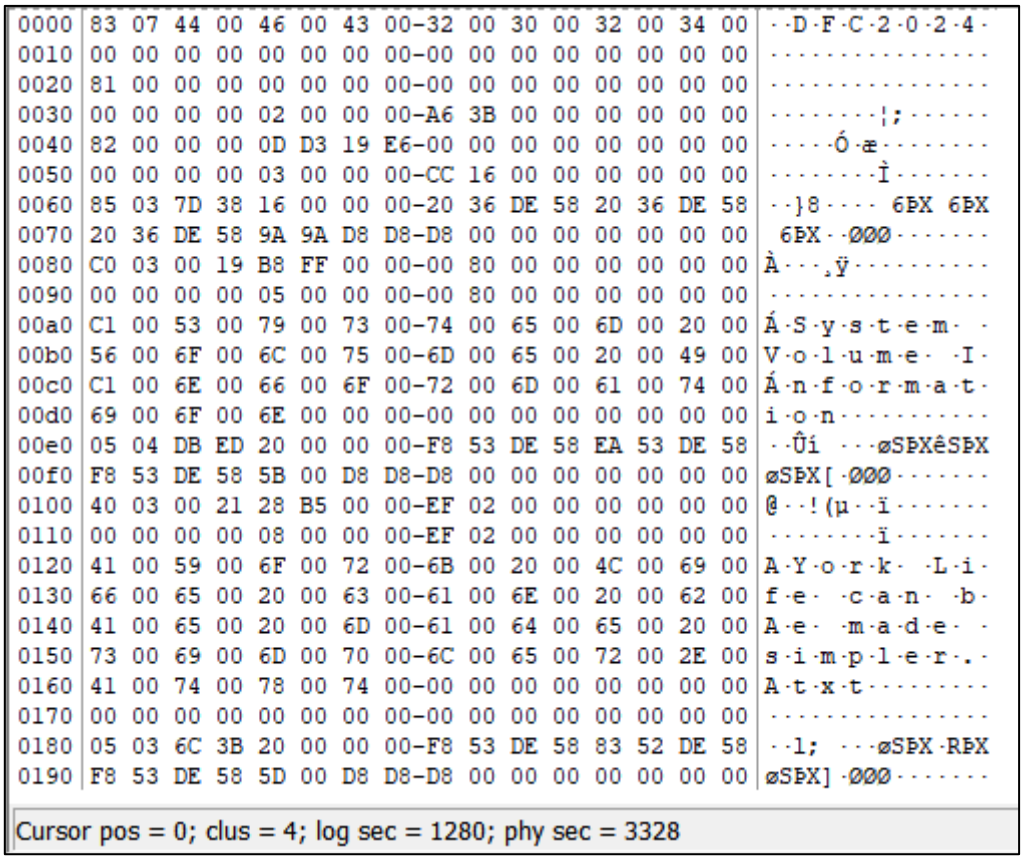
1. Identify the drug sales ledger file and find the filename. (20 points)



The villagers rose.png.FileSlack	13[Missing ...	파일 슬랙	
Tip for Health.txt	1[Missing s...	일반 파일	2024-06-30 오후 8:28:28
Tip for Health.txt.FileSlack	32[Missing ...	파일 슬랙	
Tip for Home Management.txt	1[Missing s...	일반 파일	2024-06-30 오후 8:28:52
Tip for Home Management.txt.F...	32[Missing ...	파일 슬랙	
Tip for Mental Well-being.txt	1[Missing s...	일반 파일	2024-06-30 오후 8:29:18
Tip for Mental Well-being.txt.Fil...	32[Missing ...	파일 슬랙	
Tip for Productivity.txt	1[Missing s...	일반 파일	2024-06-30 오후 8:29:46
Tip for Productivity.txt.FileSlack	32[Missing ...	파일 슬랙	
wildlife documentaries.png	6[Missing s...	일반 파일	2024-07-03 오전 11:10:12
Yellow village of Willowbrook.txt	6[Missing s...	일반 파일	2024-06-30 오후 8:30:58
York Life can be made simpler.t...	1[Missing s...	일반 파일	2024-06-30 오후 8:31:20
York Life can be made simpler.t...	32[Missing ...	파일 슬랙	

[그림 2] 수정 날짜가 다른 하나의 파일 식별

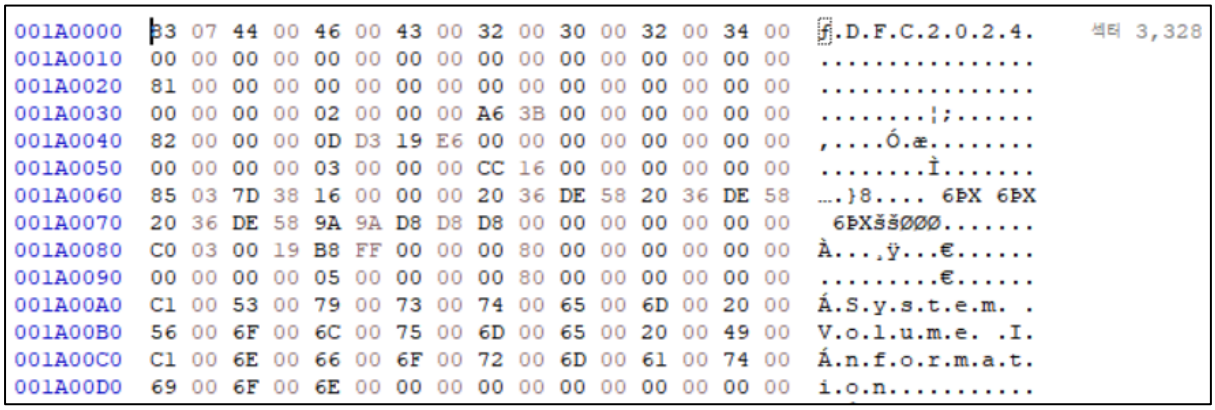
USB.zip 파일 압축 해제 후, USB.dd를 FTK imager로 로드하여 [root] 내 파일들을 확인하였습니다. 그 중, wildlife documentaries.png라는 파일이 유일하게 FTK 내에서 수정 날짜가 다른 파일로 인식되었고, 다른 png과 달리 그림에 대한 preview가 나타나지 않았습니다. Preview가 나타나지 않는 파일은 Aquatic ecosystem.png도 마찬가지였으며, 이러한 점들을 통해 HxD로 USB.dd를 디스크 이미지 열기로 열어 FTK 상에서 나타내는 클러스터로 이동하여 파일 내용을 확인해보는 것으로 분석을 수행하였습니다.



0000	83	07	44	00	46	00	43	00	32	00	30	00	32	00	34	00
0010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0020	81	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0030	00	00	00	00	02	00	00	00	A6	3B	00	00	00	00	00	00
0040	82	00	00	00	0D	D3	19	E6	00	00	00	00	00	00	00	00
0050	00	00	00	00	03	00	00	00	CC	16	00	00	00	00	00	00
0060	85	03	7D	38	16	00	00	00	20	36	DE	58	20	36	DE	58
0070	20	36	DE	58	9A	9A	D8	D8	D8	00	00	00	00	00	00	00
0080	C0	03	00	19	B8	FF	00	00	00	80	00	00	00	00	00	00
0090	00	00	00	00	05	00	00	00	00	80	00	00	00	00	00	00
00a0	C1	00	53	00	79	00	73	00	74	00	65	00	6D	00	20	00
00b0	56	00	6F	00	6C	00	75	00	6D	00	65	00	20	00	49	00
00c0	C1	00	6E	00	66	00	6F	00	72	00	6D	00	61	00	74	00
00d0	69	00	6F	00	6E	00	00	00	00	00	00	00	00	00	00	00
00e0	05	04	DB	ED	20	00	00	00	F8	53	DE	58	EA	53	DE	58
00f0	F8	53	DE	58	5B	00	D8	D8	D8	00	00	00	00	00	00	00
0100	40	03	00	21	28	B5	00	00	EF	02	00	00	00	00	00	00
0110	00	00	00	00	08	00	00	00	EF	02	00	00	00	00	00	00
0120	41	00	59	00	6F	00	72	00	6B	00	20	00	4C	00	69	00
0130	66	00	65	00	20	00	63	00	61	00	6E	00	20	00	62	00
0140	41	00	65	00	20	00	6D	00	61	00	64	00	65	00	20	00
0150	73	00	69	00	6D	00	70	00	6C	00	65	00	72	00	2E	00
0160	41	00	74	00	78	00	74	00	00	00	00	00	00	00	00	00
0170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0180	05	03	6C	3B	20	00	00	00	F8	53	DE	58	83	52	DE	58
0190	F8	53	DE	58	5D	00	D8	D8	D8	00	00	00	00	00	00	00

Cursor pos = 0; clus = 4; log sec = 1280; phy sec = 3328

[그림 3] [root]의 File Directory Entry



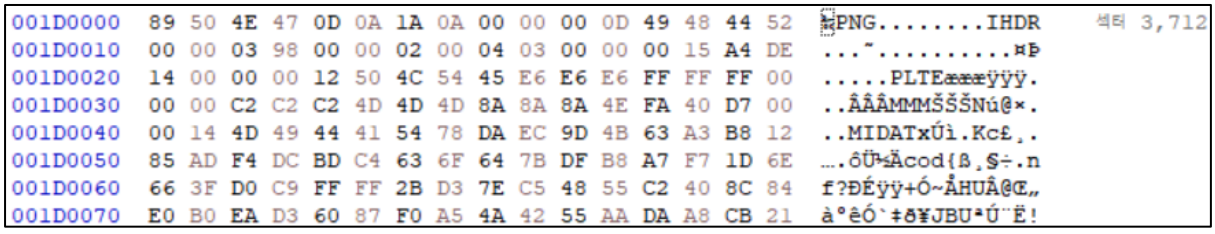
001A0000	83	07	44	00	46	00	43	00	32	00	30	00	32	00	34	00
001A0010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
001A0020	81	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
001A0030	00	00	00	00	02	00	00	00	A6	3B	00	00	00	00	00	00
001A0040	82	00	00	00	0D	D3	19	E6	00	00	00	00	00	00	00	00
001A0050	00	00	00	00	03	00	00	00	CC	16	00	00	00	00	00	00
001A0060	85	03	7D	38	16	00	00	00	20	36	DE	58	20	36	DE	58
001A0070	20	36	DE	58	9A	9A	D8	D8	D8	00	00	00	00	00	00	00
001A0080	C0	03	00	19	B8	FF	00	00	00	80	00	00	00	00	00	00
001A0090	00	00	00	00	05	00	00	00	00	80	00	00	00	00	00	00
001A00A0	C1	00	53	00	79	00	73	00	74	00	65	00	6D	00	20	00
001A00B0	56	00	6F	00	6C	00	75	00	6D	00	65	00	20	00	49	00
001A00C0	C1	00	6E	00	66	00	6F	00	72	00	6D	00	61	00	74	00
001A00D0	69	00	6F	00	6E	00	00	00	00	00	00	00	00	00	00	00

섹터 3,328

[그림 4] HxD에서 물리적 섹터 확인

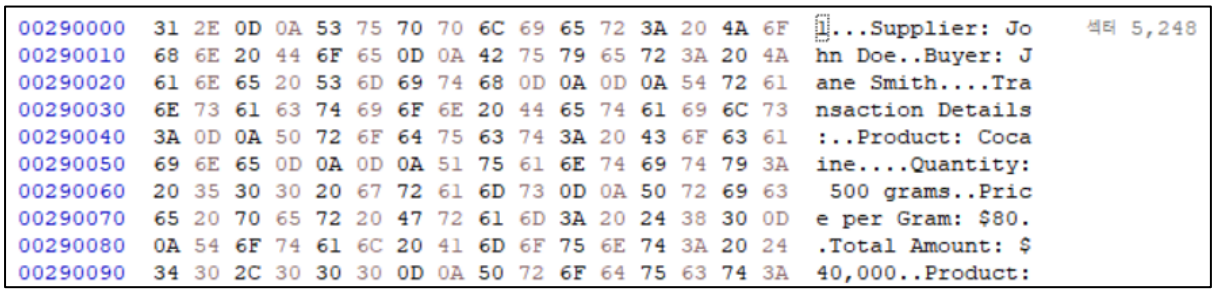
위 두 그림을 통해 [root] 폴더가 위치한 클러스터 4는 섹터 3328에 물리적으로 위치하고 있다는 것을 알 수 있습니다.

FTK imager에서 Aquatic ecosystems.png는 시작 클러스터가 10, wildlife documentaries.png는 시작 클러스터가 34임을 확인한 결과를 토대로 HxD에서 확인하였습니다.



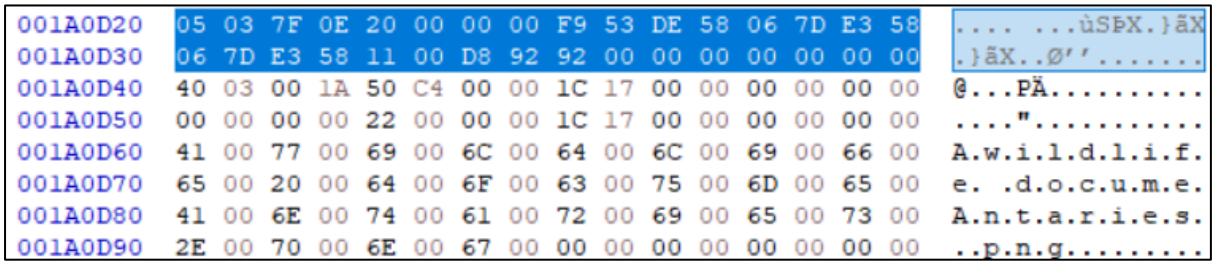
[그림 5] Aquatic ecosystems.png 파일이 위치한 섹터

시작 클러스터가 10이기 때문에 기존에 [root]가 위치했던 4에서 6 * 64를 계산하여 더하면 섹터 3712가 되고, 해당 섹터 3712에서 해당 파일 내용을 확인할 수 있었으나, hex값을 카빙한 뒤 살펴본 결과 일반적인 아이콘 이미지 파일이었습니다.



[그림 6] wildlife documentaries.png

이번에는 시작 클러스터가 34인 wildlife documentaries.png를 확인하기 위해 30 * 64를 더해 5248 섹터에서 위 그림과 같은 내용을 확인할 수 있었습니다.



[그림 7] wildlife documentaries.png에 대한 File Directory Entry

또한, 해당 png 파일의 File Directory Entry 를 살펴보면 0x1 offset 이 0x05 로 이는 파일이 삭제되었음을 의미합니다.

```
1.
Supplier: John Doe
Buyer: Jane Smith

Transaction Details:
Product: Cocaine

Quantity: 500 grams
Price per Gram: $80
Total Amount: $40,000
Product: MDMA

Quantity: 200 pills
Price per Pill: $20
Total Amount: $4,000
Payment Method: Cash

Delivery Method: Personal Hand-off

Notes:
Buyer requested delivery at 5th Avenue, NYC.
Supplier mentioned potential delay due to increased police patrols.
Buyer has requested an additional 300 grams of cocaine for the next deal.
Witness: Tom Wilson (driver)

Additional Comments:
Ensure to use burner phones for all communications.
Dispose of all packaging materials securely.
Keep track of surveillance cameras around the meeting point.

2.
Supplier: Michael Johnson
Buyer: Robert Brown

Transaction Details:
Product: Heroin

Quantity: 1 kilogram
Price per Kilogram: $120,000
Total Amount: $120,000
Product: Methamphetamine

Quantity: 300 grams
Price per Gram: $50
Total Amount: $15,000
Payment Method: Bank Transfer (offshore account)
```

```
Delivery Method: Drop-off at specified location

Notes:
Buyer instructed to pick up the package from a locker at the Central
Station.
Supplier used a disguised parcel to avoid suspicion.
Buyer interested in discussing bulk purchase discounts for future deals.
Witness: David Lee (logistics coordinator)

Additional Comments:
Double-check all bank transfer details to avoid traceable errors.
Utilize encrypted messaging apps for all communications.
Implement additional security measures during drop-offs to ensure no
surveillance or interception.

3.
Supplier: Alice Morgan
Buyer: Brian White

Transaction Details:
Product: LSD

Quantity: 150 tabs
Price per Tab: $10
Total Amount: $1,500
Product: Ecstasy

Quantity: 500 pills
Price per Pill: $15
Total Amount: $7,500
Payment Method: Bitcoin

Delivery Method: Mail (disguised package)

Notes:
Buyer requested expedited shipping.
Supplier used a decoy return address to avoid tracing.
Buyer requested additional 200 Ecstasy pills for the next deal.
Witness: Sarah Green (packager)

Additional Comments:
Ensure secure packaging to prevent detection by mail scanners.
Use VPN for all online communications.
Monitor cryptocurrency wallet for payment confirmation.

=====
```

```
4.
Supplier: Kevin Brown
Buyer: Laura Davis

Transaction Details:
Product: Marijuana

Quantity: 2 kilograms
Price per Kilogram: $3,000
Total Amount: $6,000
Product: Hashish

Quantity: 500 grams
Price per Gram: $20
Total Amount: $10,000
Payment Method: Cash and Bank Transfer

Delivery Method: In-person meeting

Notes:
Buyer prefers weekend delivery at the agreed location.
Supplier mentioned an increase in police activity in the area.
Buyer inquired about bulk discount for future large orders.
Witness: James Carter (security)

Additional Comments:
Confirm bank transfer details before proceeding with delivery.
Arrange for a discreet meeting point to avoid detection.
Maintain a low profile during transactions.

5.
Supplier: Jessica Thompson
Buyer: Mark Williams

Transaction Details:
Product: Cocaine

Quantity: 300 grams
Price per Gram: $90
Total Amount: $27,000
Product: Heroin

Quantity: 150 grams
Price per Gram: $100
Total Amount: $15,000
Payment Method: Cryptocurrency
```

```
Delivery Method: Dead drop location

Notes:
Delivery location: Abandoned warehouse at 4th Street.
Supplier used a coded message to convey the location to the buyer.
Buyer interested in purchasing synthetic opioids for the next deal.
Witness: Rachel Adams (assistant)

Additional Comments:
Use encrypted communication channels to maintain anonymity.
Regularly change drop locations to avoid detection.
Verify cryptocurrency transaction through multiple confirmations.

6.
Supplier: Daniel Harris
Buyer: Emily Johnson

Transaction Details:
Product: Methamphetamine

Quantity: 400 grams
Price per Gram: $50
Total Amount: $20,000
Product: LSD

Quantity: 200 tabs
Price per Tab: $12
Total Amount: $2,400
Payment Method: Wire transfer

Delivery Method: Courier service

Notes:
Supplier utilized a trusted courier service with secure packaging.
Buyer requested expedited processing for future orders.
Witness: Michael Stevens (courier)

Additional Comments:
Maintain discreet communication with the courier service.
Ensure all packages are tamper-proof.
Document all transactions for future reference.

7.
Supplier: Sarah Martinez
Buyer: David Lee

Transaction Details:
```

```
Product: MDMA

Quantity: 600 pills
Price per Pill: $25
Total Amount: $15,000
Product: Ketamine

Quantity: 200 grams
Price per Gram: $45
Total Amount: $9,000
Payment Method: Cash on delivery

Delivery Method: Personal delivery

Notes:
Delivery to be made at a private parking lot.
Supplier to confirm presence before hand-off.
Buyer requested a larger quantity of MDMA for the next deal.
Witness: Chris Turner (bodyguard)

Additional Comments:
Ensure thorough surveillance of the meeting point before arrival.
Use unmarked vehicles to avoid suspicion.
Carry emergency communication devices in case of issues.

8.
Supplier: William Johnson
Buyer: Olivia Brown

Transaction Details:
Product: Cocaine

Quantity: 1 kilogram
Price per Kilogram: $85,000
Total Amount: $85,000
Product: Methamphetamine

Quantity: 500 grams
Price per Gram: $55
Total Amount: $27,500
Payment Method: Bank transfer (domestic account)

Delivery Method: Secure courier

Notes:
Delivery made to buyer's safe house.
Supplier ensured double packaging to avoid detection.
```

```
Buyer interested in exploring new product lines.
Witness: Karen White (logistics manager)

Additional Comments:
Confirm bank transfer clearance before dispatch.
Use trusted and reliable couriers for all high-value deliveries.
Maintain updated records of all transactions and communications.
```

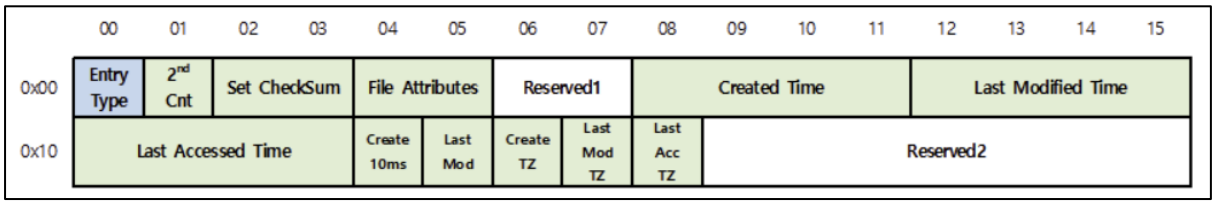
[표 1] drug ledger file로 식별되는 파일의 내용

앞서 그림 6에서 살펴본 HxD 데이터를 가져와서 보면, 위 Supplier, Buyer 등과 Product 명이 Cocaine, Heroin이며, 수량과 전달방식 등이 적혀 있는 것을 토대로 해당 파일에 마약 거래 내용이 포함되어 있기 때문에 drug ledger file임을 판단하였습니다. 따라서, drug ledger file의 이름은 wildlife documentaries.png로 확인됩니다.

답 : wildlife documentaries.png

2. Identify the timezone values for the creation time and modification time of the drug trade ledger file. (50 points)

Ledger file의 생성 시간과 수정 시간에 대한 timezone을 판단하기 위해서 파일이나 디렉토리의 메타데이터를 저장하는 영역인 exFAT의 File Directory Entry를 참고하였습니다.



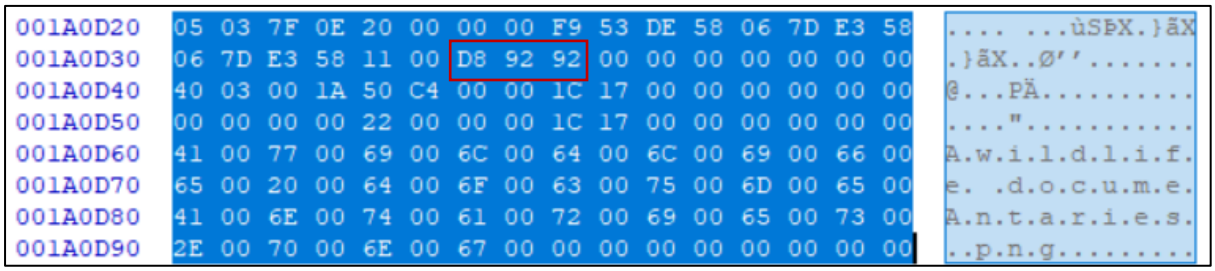
[그림 8] File Directory Entry Layout

Address Range	Size	Field Name	Description
0x00~0x00	1	Entry Type	파일 존재 : 0x85, 파일 삭제됨 : 0x05, 0xE5
0x01~0x01	1	Secondary Count	
0x02~0x03	2	Set CheckSum	체크섬
0x04~0x05	2	File Attribute	파일의 속성
0x06~0x07	2	Reserved 1	예약된 영역
0x08~0x0B	4	Created Time	DOS TimeStamp 형식
0x0C~0x0F	4	Last Modified Time	DOS TimeStamp 형식
0x10~0x13	4	Last Accessed Time	DOS TimeStamp 형식
0x14~0x14	1	Created 10ms	생성 시간 10ms 증가값
0x15~0x15	1	Last Modified 10ms	마지막 수정 시간 10ms 증가값
0x16~0x16	1	Created TZ Offset	생성시간 Timezone 위치
0x17~0x17	1	Last Modified TZ Offset	마지막 수정시간 Timezone 위치
0x18~0x18	1	Last Accessed TZ Offset	마지막 접근시간 Timezone 위치
0x19~0x1F	7	Reserved 2	예약된 영역

[그림 9] File Directory Entry Data[1]

위 두 그림을 보면 0x16과 0x17에 해당하는 값이 파일의 생성시간에 대한 timezone 위치, 마지막 수정시간 timezone 위치임을 알 수 있습니다.

[1] https://blog.forensicresearch.kr/5



001A0D20	05	03	7F	0E	20	00	00	00	F9	53	DE	58	06	7D	E3	58
001A0D30	06	7D	E3	58	11	00	D8	92	92	00	00	00	00	00	00	00
001A0D40	40	03	00	1A	50	C4	00	00	1C	17	00	00	00	00	00	00
001A0D50	00	00	00	00	22	00	00	00	1C	17	00	00	00	00	00	00
001A0D60	41	00	77	00	69	00	6C	00	64	00	6C	00	69	00	66	00
001A0D70	65	00	20	00	64	00	6F	00	63	00	75	00	6D	00	65	00
001A0D80	41	00	6E	00	74	00	61	00	72	00	69	00	65	00	73	00
001A0D90	2E	00	70	00	6E	00	67	00	00	00	00	00	00	00	00	00

[그림 10] wildlife documentaries.png 파일에 대한 메타데이터

위 그림은 wildlife documentaries.png 파일에 대한 File Directory Entry와 Stream Extension Entry, File Name Extension Entry 영역에 대한 값입니다.

File Directory Entry영역에서 Created Timezone offset인 0x16 offset에 해당하는 값이 0xD8 이고, Last Modified Timezone offset인 0x17 offset에 해당하는 값이 0x92 입니다.

144 (0x90)	UTC+04:00	Arabian Standard Time
148 (0x94)	UTC+05:00	West Asia Standard Time
152 (0x98)	UTC+06:00	Central Asia Standard Time
156 (0x9C)	UTC+07:00	North Asia Standard Time
160 (0xA0)	UTC+08:00	North Asia East Standard Time
164 (0xA4)	UTC+09:00	Tokyo Standard Time
168 (0xA8)	UTC+10:00	West Pacific Standard Time
172 (0xAC)	UTC+11:00	Central Pacific Standard Time
176 (0xB0)	UTC+12:00	New Zealand Standard Time
180 (0xB4)	UTC+13:00	Tonga Standard Time
208 (0xD0)	UTC-12:00	Dateline Standard Time
212 (0xD4)	UTC-11:00	Samoa Standard Time
216 (0xD8)	UTC-10:00	Hawaii Standard Time

[그림 7] exFAT Timestamp Format

Timezone Format은 위 그림과 같습니다. 따라서, drug trade ledger file의 Creation time에 대한 timezone value는 0xD8로 UTC-10:00인 Hawaii Standard Time임을 알 수 있습니다.

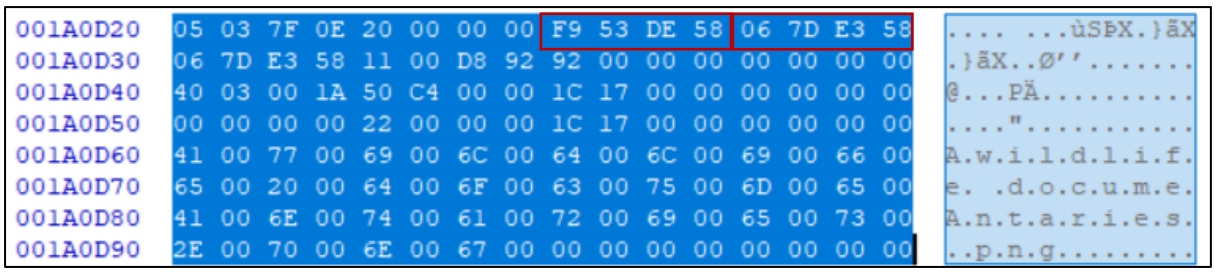
또한, Modification time에 대한 timezone value는 0x92로 0x90와 0x94 사이로 timestamp format 테이블에서는 확인할 수 없습니다. 다만, 0x04 값 증가에 따라 저 구간에서는 +1시간이 증가되는 것에 따라 0x02 값에 따라서 30분 증가될 것으로 파악됩니다. 따라서, modification time은 UTC+04:30로 이는 Afghanistan Standard Time로 볼 수 있습니다.

답:

	Timezone Value	Timezone
Creation Time	**0xD8**	UTC-10:00 Hawaii Standard Time
Modification Time	**0x92**	UTC+04:30 Afghanistan Standard Time

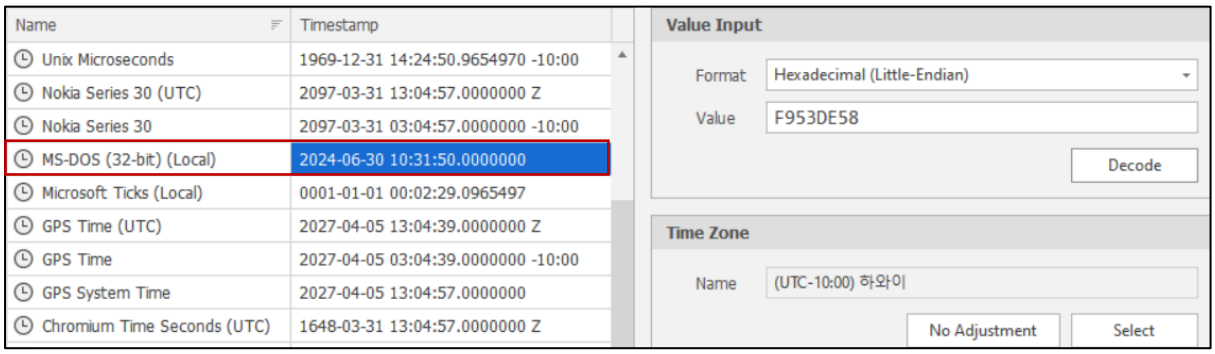
[표 2] drug ledger file의 Creation Time과 Modification Time에 대한 Timezone Value 식별

3. Identify the creation and modification times of the drug trade ledger file in local time. Write the times in the format YYYY-MM-DD HH:MM (UTC+00:00). (80 points)



[그림 12] ledger file에 대한 메타데이터

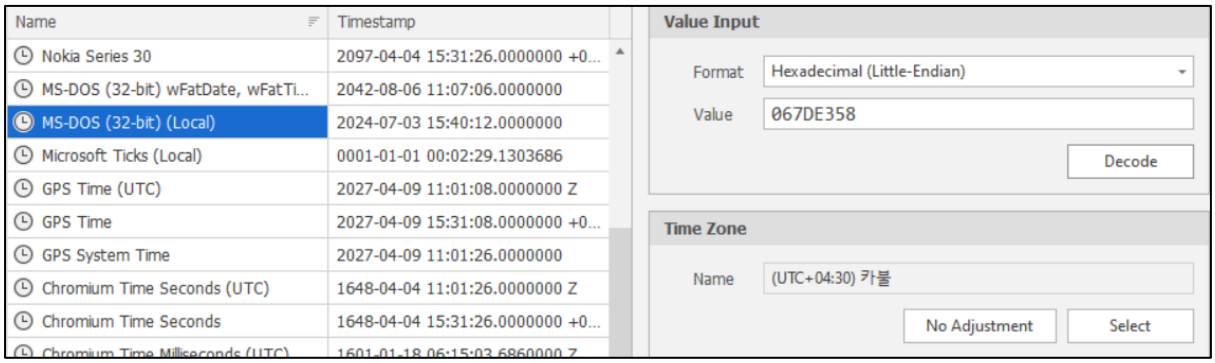
앞서 확인한 drug ledger file의 File Directory entry에서 Creation Time과 Modification Time을 확인하였습니다.



[그림 13] Creation Time 변환

exFAT에서 Creation Time과 Modification Time은 DOS Timestamp 형식을 사용해서, DCode 상에서 timezone을 변경해봤자 Local Time기준이기 때문에 시간 값이 동일한 것을 알 수 있습니다.

따라서, 0x08~0x0B offset에 위치한 Creation Time인 0xF953DE58(little-endian) 값은 문제에서 요구하는 형식에 따라 **2024-06-30 10:31(UTC-10:00)**임을 알 수 있습니다.



[그림 14] Modification Time 변환

0x0C~0x0F에 위치한 Last Modified Time인 0x067DE358(little-endian) 값은 문제에서 요구하는 형식에 따라 **2024-07-03 15:40(UTC+04:30)** 임을 알 수 있습니다.

답:

	Local Time
Creation Time	**2024-06-30 10:31(UTC-10:00)**
Modification Time	**2024-07-03 15:40(UTC+04:30)**

[표 3] drug ledger file에 대한 local time에서의 Creation Time과 Modification Time 식별