

152 – Reconnaissance

Team Information

Team Name : LuckyVicky

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

Email Address : dfc_luckyvicky@googlegroups.com

Instructions

Description A virtual disk was found on the suspect's PC, who is being investigated for evidence tampering. The given file is an image of the user data from the virtual disk.

Target	Hash (MD5)
Target.ad1	f5112719b720429525051d9a2830b8f9

Questions

1. What service(s) were used for pre-crime reconnaissance? (30 points)
2. Represent the service(s) usage history in a timeline (including usage times and details). (120 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:

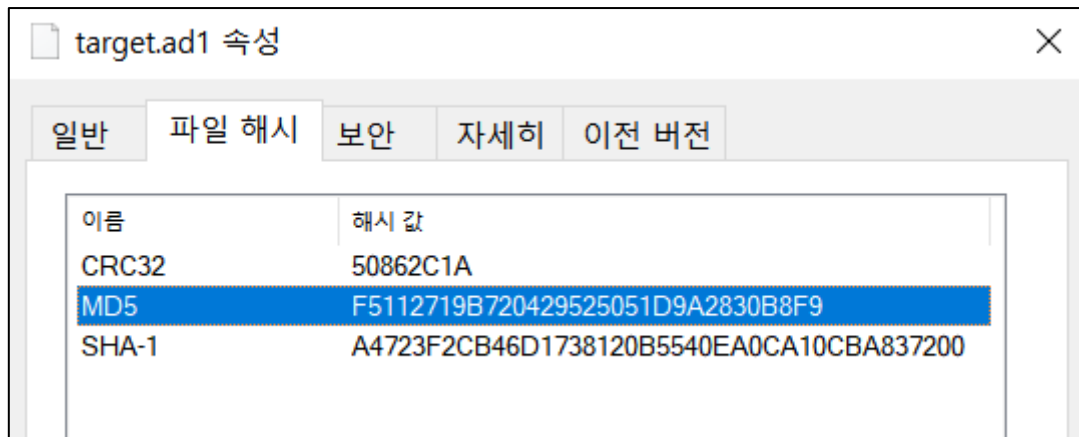
Name:	HashTab	Publisher:	Implbits Software
Version:	6.0.0		
URL:	https://implbits.com		

Name:	hindsight	Publisher:	obsidianforensics
Version:	v2023.03		
URL:	https://github.com/obsidianforensics/hindsight		

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

Name:	DCode	Publisher:	Digital Detective
Version:	5.6		
URL:	https://www.digital-detective.net/dcode/		

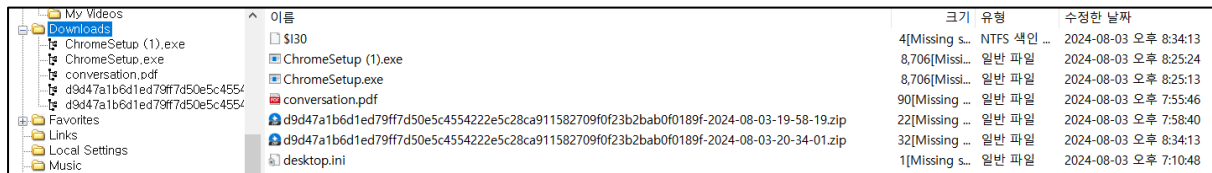
Step-by-step methodology:



[그림 1] target.ad1 파일 md5 해시 값 확인

주어진 파일에 대한 md5 해시 값이 일치함을 확인하였습니다.

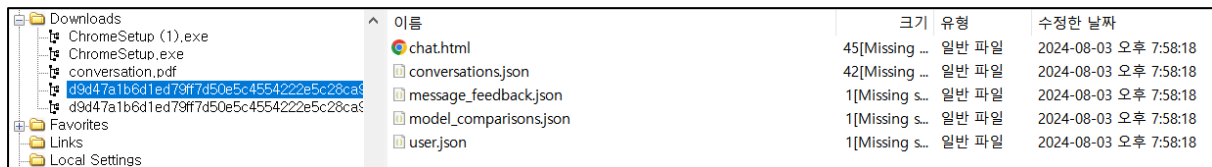
1. What service(s) were used for pre-crime reconnaissance? (30 points)



이름	크기	유형	수정된 날짜
ChromeSetup (1).exe	4[Missing s...	NTFS 색인 ...	2024-08-03 오후 8:34:13
ChromeSetup.exe	8,706[Missi...	일반 파일	2024-08-03 오후 8:25:24
conversation.pdf	8,706[Missi...	일반 파일	2024-08-03 오후 8:25:13
d9d47a1b6d1ed79ff7d50e5c4554222e5c28ca911582709f0f23b2bab0f0189f-2024-08-03-19-58-19.zip	90[Missing ...	일반 파일	2024-08-03 오후 7:55:46
d9d47a1b6d1ed79ff7d50e5c4554222e5c28ca911582709f0f23b2bab0f0189f-2024-08-03-20-34-01.zip	22[Missing ...	일반 파일	2024-08-03 오후 7:58:40
desktop.ini	32[Missing ...	일반 파일	2024-08-03 오후 8:34:13
	1[Missing s...	일반 파일	2024-08-03 오후 7:10:48

[그림 2] Downloads 경로에서 발견된 파일

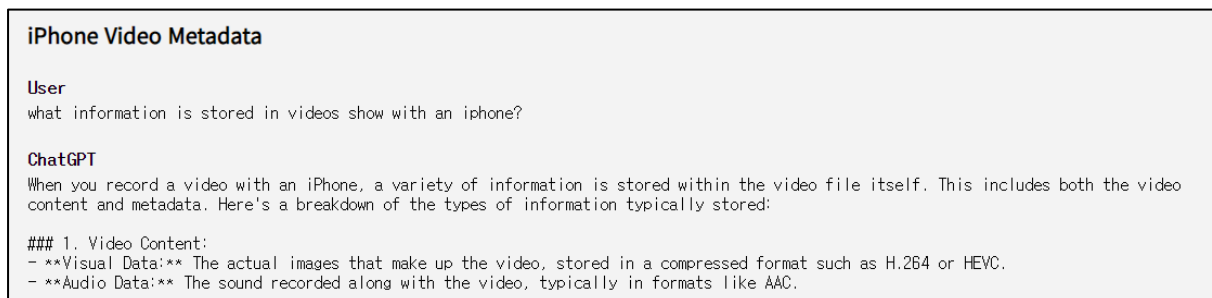
주어진 target.ad1 파일을 FTK imager로 로드해본 결과, Users 폴더를 확인할 수 있었고 그 중 하위에 있는 Downloads 폴더에서 conversation.pdf와 두 개의 zip파일을 확인할 수 있었습니다.



이름	크기	유형	수정된 날짜
chat.html	45[Missing ...	일반 파일	2024-08-03 오후 7:58:18
conversations.json	42[Missing ...	일반 파일	2024-08-03 오후 7:58:18
message_feedback.json	1[Missing s...	일반 파일	2024-08-03 오후 7:58:18
model_comparisons.json	1[Missing s...	일반 파일	2024-08-03 오후 7:58:18
user.json	1[Missing s...	일반 파일	2024-08-03 오후 7:58:18

[그림 3] zip 파일 내 확인 가능한 파일들

zip파일 내에는 chat.html과 conversation.json, user.json 등의 파일들이 존재했습니다.



iPhone Video Metadata
User what information is stored in videos show with an iphone?
ChatGPT When you record a video with an iPhone, a variety of information is stored within the video file itself. This includes both the video content and metadata. Here's a breakdown of the types of information typically stored: ### 1. Video Content: - **Visual Data:** The actual images that make up the video, stored in a compressed format such as H.264 or HEVC. - **Audio Data:** The sound recorded along with the video, typically in formats like AAC.

[그림 4] chat.html 파일

Chat.html 파일을 열어보면 다음과 같이 chatgpt와의 대화 내역이 저장된 파일임을 알 수 있습니다. 이를 통해 conversation.json도 대화 내역과 관련된 데이터임을 알 수 있었습니다.



ChatGPT ▾



dropdown menu.

- Click "Save".
- **Google Docs:**
 - Go to "File" > "Download" > "PDF Document (.pdf)".
 - The PDF will be downloaded to your default download location.
- **Other Word Processors:**
 - Look for a "Save As" or "Export" option and choose PDF as the format.

Using Browser Print to PDF Feature

1. **Highlight the Conversation:**
 - Highlight the entire conversation from your browser or chat window.
2. **Print the Conversation:**
 - Right-click and select "Print" or press `Ctrl+P` (Windows) or `Command+P` (Mac).
3. **Print to PDF:**
 - In the print dialog, choose "Save as PDF" or "Microsoft Print to PDF" as the printer.
 - Click "Save" or "Print".
4. **Save the PDF:**
 - Choose a location on your computer to save the PDF file.
 - Enter a name for the file and click "Save".

By following these steps, you can save the conversation for offline viewing as either a text file or a PDF document.



i want to save all conversations at once



Message ChatGPT



ChatGPT can make mistakes. Check important info.

<https://chatgpt.com/c/6f32df8b-3199-4c64-aae6-63c983f72a6a>

1/1

[그림 5] conversation.pdf

이전 페이지의 그림 5처럼 conversation.pdf 파일도 대화내역의 일부를 이행하여 pdf로 저장된 파일로 보입니다. 이처럼 chatgpt 활용 흔적에 따라, 추가 흔적이 있는지 hindsight로 웹 브라우저 기록과 ad1파일에 남아있는 Chrome과 Edge 아티팩트를 살펴보았습니다.

Type	Timestamp (UTC)	URL	Title / Name / Status	Data / Value / Path
cookie (accessed)	2024-08-03 20:33:34.441	.claude.ai/	intercom-session-lupk8zyo	<encrypted>
cookie (accessed)	2024-08-03 20:33:34.441	.claude.ai/	lastActiveOrg	<encrypted>
cookie (accessed)	2024-08-03 20:33:34.441	.claude.ai/	user-sidebar-pinned	<encrypted>
cookie (accessed)	2024-08-03 20:33:34.441	.claude.ai/	cf_clearance	<encrypted>
url	2024-08-03 20:33:34.707	https://claude.ai/chat/76d307c5-1d9d-494c-ba1a-3aa1dd8f9943	Ethical Video Metadata Management - Claude	
url	2024-08-03 20:33:34.937	https://claude.ai/chat/76d307c5-1d9d-494c-ba1a-3aa1dd8f9943	Ethical Video Metadata Management - Claude	

[그림 6] Claude 사용 기록 확인 - hindsight tool

https://claude.ai/chat/9a9ffc14-4ac9-4f3c-97fd-eee631bd13ea	Saving ChatGPT Conversations - Claude	3	0.13367190861547496
https://claude.ai/chat/76d307c5-1d9d-494c-ba1a-3aa1dd8f9943	Ethical Video Metadata Management - Claude	2	0.13367190814937361
https://chatgpt.com/c/35bba9c2-f482-416d-a3e8-77920c3209f0#settings	ChatGPT	1	0.13367190835857267
https://chatgpt.com/c/35bba9c2-f482-416d-a3e8-77920c3209f0#settings/...	ChatGPT	1	0.13367190837047195

[그림 7] Chrome History 아티팩트 확인

위 그림 6과 그림 7을 통해 용의자의 디스크에서 Claude 사용 기록도 확인할 수 있습니다.

```
{"id": "user-F1Kdn3ymIFBaMWNpjuq3v5ZA", "email": "newnewdfc@gmail.com", "chatgpt_plus_user": false, "birth_year": 2000}
```

[그림 8] chatgpt user.json에서 확인한 용의자의 email주소

```
C:\> Users > ehfeh > AppData > Local > Temp > ccvCC2D.tmp > 94557da5-e603-4d06-942f-16389003a735.json
1 {
2   "uuid": "94557da5-e603-4d06-942f-16389003a735",
3   "name": "newnewdfc@gmail.com's Organization",
4   "settings":
5     {
6       "claude_console_privacy": "default_private",
7       "allowed_invite_domains": null
8     },
9   "capabilities": ["chat"],
10  "rate_limit_tier": "default_claude_ai",
11  "billing_type": null,
12  "free_credits_status": null,
13  "data_retention": "default",
14  "api_disabled_reason": null,
15  "api_disabled_until": null,
16  "billable_usage_paused_until": null,
17  "raven_type": null,
18  "created_at": "2024-08-03T19:38:46.520893Z",
19  "updated_at": "2024-08-03T19:38:46.520893Z",
20  "active_flags": []
21 }
```

[그림 9] chromecacheview에서 확인한 claude.ai 관련 캐시 데이터

또한, 그림 8과 그림 9를 통해 용의자는 PC 내 프로필 이름인 newnew임을 감안할 때, newnewdfc@gmail.com 이메일을 사용함으로써 두 서비스를 이용했다고 추정해볼 수 있습니다.

User

i need to correct the time and location

ChatGPT

If you need to correct or modify the time and location metadata of a file (such as an image or video), you can use several tools to do this accurately. Here's a step-by-step guide using common tools for adjusting metadata:

[그림 10] 2024-08-03 20:34:01 export 데이터 중 chat.html 내 일부 대화 내용 - 1

User

without any traces

ChatGPT

If your goal is to correct the time and location metadata of a file without leaving any traces of modifications, you'll need to be cautious and precise in how you handle the metadata. Here's how to do it effectively:

[그림 11] 2024-08-03 20:34:01 export 데이터 중 chat.html 내 일부 대화 내용 - 2

```
{
  "uuid": "f381253d-e3e3-40f9-8d4b-486574499320",
  "text": "i want to change the video attribute info to protect privacy. and there must be no traces of modifications left. is there any way?",
  "sender": "human",
  "index": 4,
  "created_at": "2024-08-03T20:01:06.785155+00:00",
  "updated_at": "2024-08-03T20:01:06.785155+00:00",
  "truncated": false,
  "attachments": [],
  "files": [],
  "parent_message_uuid": "db741e2e-fa78-4b7a-a826-76dbbf447546"
},
{
  "uuid": "166631d4-7559-49ee-9f4c-9a08e3612dbf",
  "text": " I understand you're looking for ways to modify video attribute information for privacy reasons, while leaving no traces of the modifications.",
  "sender": "assistant",
  "index": 5,
  "created_at": "2024-08-03T20:01:06.785155+00:00",
  "updated_at": "2024-08-03T20:01:06.785155+00:00",
  "truncated": false,
  "attachments": [],
  "files": [],
  "parent_message_uuid": "f381253d-e3e3-40f9-8d4b-486574499320"
}
```

[그림 12] chromecacheview에서 export한 claude 대화 내역 일부

차후 2번 문제에서 상세히 기술하겠지만, 요약하자면 용의자는 chatgpt 서비스에서 메타데이터 제거와 관해 질의를 하면서 위 그림 10과 그림 11을 통해 시간과 위치 정보를 어떠한 흔적 없이 수정할 수 있는 방법을 질의하였습니다. 그리고 Claude 서비스에서도 그림 12와 같이 어떠한 변조 흔적을 남기지 않고 개인정보 보호라는 명목을 붙여서 비디오 속성 정보를 수정하고자 질의를 수행한 것을 알 수 있습니다.

따라서, 앞선 분석 정보를 토대로 용의자는 사전 범죄(비디오 조작)를 위한 정찰(사전 정보 획득)의 일환으로 ChatGPT와 Claude라는 AI chat 서비스를 활용하였습니다.

2. Represent the service(s) usage history in a timeline (including usage times and details). (120 points)

위 1번 문제에서 활용한 hindsight로 추출한 웹 브라우저 사용 기록, Chrome과 Edge의 각 History 내 방문 기록, 그리고 Chrome과 Edge에 저장된 Cache Data 내 확인 가능한 서비스 사용 기록을 종합하여 용의자의 타임라인을 구성하여 제출합니다. 특히 사항은 전체 사용 기록 중 대화 내역이 길어 용의자의 증거 조작을 위한 정찰 활동과 관련될만한 중요 대화 내역 위주로 첨부하였습니다.

Time(UTC+0)	Artifact	Behavior
2024-08-03 19:42:35	Edge History	ChatGPT 접속(https://chatgpt.com/)
2024-08-03 19:42:38	Edge History	ChatGPT 로그인
2024-08-03 19:42:47 ~ 2024-08-03 19:43:03	Edge History	Oauth를 통해 Newnewdfc@gmail.com 계정 사용하여 로그인
2024-08-03 19:43:30 ~ 2024-08-03 19:43:50	Conversation.json	User: what information is stored in videos show with an iphone?을 통해 iphone에 동영상에 저장되는 정보는 무엇인지에 대한 질문 수행 후 답변을 받음. 대화 이후, 대화 관련 url 링크 자동 생성 https://chatgpt.com/c/6f32df8b-3199-4c64-aae6-63c983f72a6a
2024-08-03 19:45:39 ~ 2024-08-03 19:45:58	Conversation.json	User: what can i do to protect my privacy in the video? 라는 질의를 통해 동영상 내 개인정보를 보호하는 방법에 대한 답변을 받음. (일부생략) 2. **Edit Metadata:** Remove or edit metadata before sharing your videos. - Use apps or software tools like ExifTool, Adobe Premiere, or other metadata editors to strip out or modify sensitive metadata.
2024-08-03 19:47:24 ~ 2024-08-03 19:47:50	Conversation.json	User: tell me more about 2. 앞선 대화에서 Metadata 수정에 대한 답변을 추가 질의를 수행하고 답변을 받음.
2024-08-03 19:49:49 ~ 2024-08-03 19:50:12	conversation.json	User: free program that beginners can use easily 라는 질의를 통해 metadata 수정에 초보자도 쉽게 사용할 수 있는 프로그램을 답변 받음.

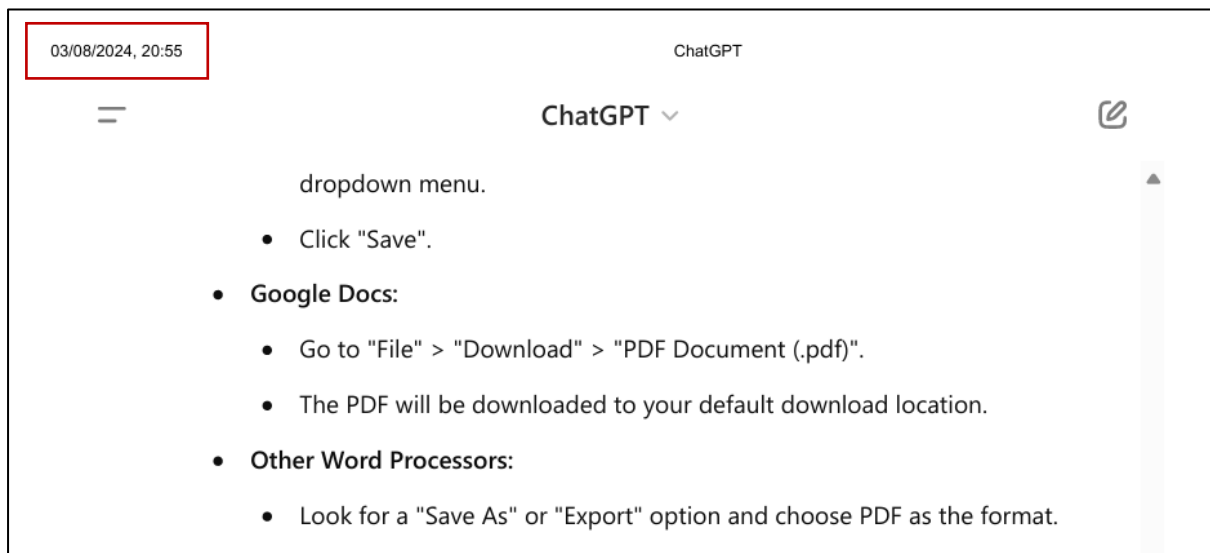
2024-08-03 19:51:02 ~ 2024-08-03 19:51:25	conversation.json	User: you can change location info? 라는 질의를 통해 위치 정보도 수정할 수 있는 지 질의를 하였으며, Exiftool 또는 GeoSetter를 통해 위치 정보 수정 방법을 답변 받음.
2024-08-03 19:52:35 ~ 2024-08-03 19:52:56	conversation.json	User: if i edit info using exiftool , there be any trace of the modification left? 라는 질의를 통해 exiftool을 사용하면 어떠한 변조의 흔적도 남기지 않을 수 있는지에 대해 물어봄으로써 증거 변조와 관련하여 정보 습득의 의도로 보임. Exiftool을 통해 변조 시 흔적 최소화에 관한 방법을 답변 받음.
2024-08-03 19:53:35 ~ 2024-08-03 19:53:55	conversation.json	User: ok. how do i view this conversation offline? 라는 질의를 통해 대화 내용을 오프라인으로 확인하기 위한 방법을 답변 받음.
2024-08-03 19:54:36 ~ 2024-08-03 19:54:56	conversation.json	User: i want to save all conversations at once 라는 추가 질의를 통해 모든 대화를 한번에 저장하는 방법을 답변 받음.
2024-08-03 19:55:45 ~ 2024-08-03 19:55:48	Edge History conversation.pdf	conversation.pdf라는 파일을 다운로드 받은 후에 file:///C:/Users/newnew/Downloads/conversation.pdf를 통해 해당 pdf파일을 열었음. pdf파일은 위에서 생성되었다고 기록했던 https://chatgpt.com/c/6f32df8b-3199-4c64-aae6-63c983f72a6a정보를 포함하고 있으며, 상단 부에 03/08/2024, 20:55로 시간 정보가 포함되어 있음. 그리고, 위 i want to save all conversations at once 라는 질문을 하기 전 시점의 캡처로 확인됨.
2024-08-03 19:56:29 ~ 2024-08-03 19:56:45	conversation.json	User: is there any save function by chatgpt? 라는 질의를 통해 chatgpt내에서 저장하는 기능에 대해 질의함.
2024-08-03 19:57:04 ~ 2024-08-03 19:57:15	Edge History	Claude 접속 후 oauth(newnewdfc@gmail.com)로 로그인

2024-08-03 19:57:38	Chrome Cache Data	<p>Human: i want to save all conversation in chatgpt Claude에 질의 수행 (일부 생략)</p> <p>2. Use the built-in export feature: ChatGPT has an option to export your conversation history. Look for an export or download button in the interface</p>
2024-08-03 19:58:03	Chrome Cache Data	<p>Human: good. tell me more about num2 라는 질의 수행을 통해 위 built-in export feature에 대한 추가 설명을 답변 받음.</p>
2024-08-03 20:01:06	Chrome Cache Data	<p>Human: i want to change the video attribute info to protect privacy. and there must be no traces of modifications left. is there any way? 변조 흔적이 반드시 남지 않는 방법으로 개인정보 보호 목적으로 비디오 속성 정보를 변경할 수 있는 방법을 질의함.</p>
2024-08-03 20:02:05	Chrome Cache Data	<p>Human: what is digital forensic tool. recommend it to me 라는 질문을 통해 디지털 포렌식 도구를 추천 받음.</p>
2024-08-03 20:03:37	Chrome Cache Data	<p>Human: so does that mean that traces of manipulation can be completely hidden if the traces cannot be detected by digital forensic tool? 라는 질문을 통해 디지털 포렌식 도구로 흔적을 감지할 수 없는 경우 조작 흔적을 완전히 숨길 수 있는지 질의함. 하지만, assistant 답변은 illegal 혹은 비윤리적 활동으로 간주하여 윤리적 접근 방식을 답변함.</p>
2024-08-03 20:04:18	Chrome Cache Data	<p>Human: this is not for illegal purposes but for privacy 라며 우회적인 질문을 수행하지만, Claude는 잠재적인 오용 가능성을 두고 투명하고 합법적인 방법에 대한 다른 답변을 수행함.</p>
2024-08-03 19:58:09 ~ 2024-08-03 19:58:11	Edge History	<p>https://chatgpt.com/c/6f32df8b-3199-4c64-aae6-63c983f72a6a#settings https://chatgpt.com/c/6f32df8b-3199-4c64-aae6-63c983f72a6a#settings/Speech https://chatgpt.com/c/6f32df8b-3199-4c64-aae6-63c983f72a6a#settings/DataControls 순차적인 URL 접근을 통해 ChatGPT 내 설정 -> 데이터 제어 -> 데이터 내보내기로 이동함.</p>

2024-08-03 19:58:38	Edge History	https://mail.google.com/mail/u/0/#inbox/FMfcgzQV xtnpQWrHGgkphSqpKCZnrgKn 접근을 통해 ChatGPT에서 export한 대화 내역을 다운로드 하기위한 메일 확인
2024-08-03 19:58:39	Edge History	d9d47a1b6d1ed79ff7d50e5c4554222e5c28ca91158 2709f0f23b2bab0f0189f-2024-08-03-19-58-19.zip ChatGPT 대화내역 파일 다운로드 수행
2024-08-03 20:04:48	Edge History	file:///C:/Users/newnew/AppData/Local/Temp/b37c e889-a9f5-4bf9-a1d3- 40cd2f1d6493_d9d47a1b6d1ed79ff7d50e5c455422 2e5c28ca911582709f0f23b2bab0f0189f-2024-08- 03-19-58-19.zip.493/chat.html 를 통해 export한 파일에서 대화 내역이 포함된 chat.html를 확인
2024-08-03 20:26:53	Chrome History	로그인 후 ChatGPT 재 접속
2024-08-03 20:28:17 ~ 2024-08-03 20:28:36	conversation.json	User: tell me digital forensic tool that can check if iphone video has been manipulated 라는 질의를 통해 iphone 영상이 조작된 경우 확인할 수 있는 디지털 포렌식 도구를 답변 받음.
2024-08-03 20:29:18 ~ 2024-08-03 20:29:25	conversation.json	User: how to prevent metadata modifications from leaving traces to protect privacy? 라는 질의를 통해 Claude에서 질문했던 것과 비슷한 질의를 수행하고 답변 받음.
2024-08-03 20:31:24 ~ 2024-08-03 20:31:34	conversation.json	User: i need to correct the time and location 라는 질의를 통해 용의자는 시간과 위치 정보를 수정하기 위한 정보를 습득하려 함.
2024-08-03 20:31:41 ~ 2024-08-03 20:31:50	conversation.json	User: without any traces 라는 질의를 통해 흔적 없이 수정하는 방법을 추가로 질의하였고, ChatGPT는 여러 방법을 제안함.
2024-08-03 20:31:50 ~ 2024-08-03 20:33:34	Chrome History	Claude에 다시 로그인하여 접속한 뒤, Saving ChatGPT Conversations – Claude Ethical Video Metadata Management – Claude 채팅 내역을 한번씩 접근하여 살펴봄.

2024-08-03 20:33:55 ~ 2024-08-03 20:33:57	Chrome History	https://chatgpt.com/c/35bba9c2-f482-416d-a3e8-77920c3209f0#settings https://chatgpt.com/c/35bba9c2-f482-416d-a3e8-77920c3209f0#settings/DataControls 기록을 통해 데이터 내보내기 수행했음을 파악
2024-08-03 20:34:12	Chrome History	메일에 다시 접속하여 d9d47a1b6d1ed79ff7d50e5c4554222e5c28ca91158 2709f0f23b2bab0f0189f-2024-08-03-20-34-01.zip Chatgpt data export 파일 다운로드
2024-08-03 20:34:21	Chrome History	https://claude.ai/chat/9a9ffc14-4ac9-4f3c-97fd-eee631bd13ea 마지막으로 claude 접속

[표 1] 용의자의 사전 범죄를 위한 정보 습득(정찰) 활동 타임라인



[그림 13] conversation.pdf 내 이상한 시간 데이터

추가 특이사항으로는 2024-08-03 19:55:45(UTC+0) 경에 conversation.pdf파일을 다운로드 받은 후 연 기록이 있으나, 조사 과정에서 export하여 해당 파일을 열었을 때는 20:55로 확인됩니다. 또한, 해당 pdf파일은 메타데이터 변조 흔적도 없습니다. 따라서, 해당 용의자의 PC는 선별 압수로 local time을 레지스트리 등을 통해 정확하게 파악할 수는 없으나 UTC+01:00으로 의심됩니다.

결론적으로, 타임라인을 통해 용의자가 ChatGPT와 Claude 서비스를 사용하여 사전 범죄를 위해 정찰(정보 습득)을 수행했음을 파악할 수 있습니다.