

5월 TJC CTF 라이트업

2023111748 노희민

문제 1 **conversations** 미해결

문제 2 **pals** 해결

문제 3 **thatsmyjam** 미해결

1. 문제 conversations

The screenshot shows a challenge card for 'forensics/conversations'. At the top right, it says '113 solves / 125 points'. Below that is the handle 'bhkrayola'. The challenge title is 'baby shark, doo-doo, doo-doo, doo-doo'. There is a blue-bordered input field labeled 'Flag' and a 'SUBMIT' button. Below the input field, there is a 'Downloads' section with a link labeled 'capture.pcap'.

종목: 포렌식

문제 이름: conversations.

설명: '아기상어' 가사.

플래그 형식 : tjctf{...} (regex: tjctfW{[-z|~]+W}

2. 풀이과정

A screenshot of a file download confirmation dialog. It shows the file name 'capture', a checkmark icon, the date '2024-05-18 오후 1:06', the file type 'Wireshark capture...', and the size '667KB'.

다운로드 받은 파일. (확장자: pcap)

와이어샤크에 넣어봤다

No.	Time	Source	Destination	Protocol	Length	Info
28	0.020104	10.0.0.1	34.107.221.82	HTTP	355	GET /canonical.html HTTP/1.1
29	0.038679	127.0.0.1	127.0.0.53	DNS	99	Standard query 0xe671 A contile.services.mozilla.com OPT
30	0.039180	127.0.0.1	127.0.0.53	DNS	99	Standard query 0x4574 AAAA contile.services.mozilla.com OPT
31	0.039726	127.0.0.53	127.0.0.1	DNS	180	Standard query response 0x4574 AAAA contile.services.mozilla.com SOA ns-67
32	0.040385	127.0.0.53	127.0.0.1	DNS	115	Standard query response 0xe671 A contile.services.mozilla.com A 34.117.188
33	0.040888	127.0.0.1	127.0.0.53	DNS	82	Standard query 0x9ee8 A example.org OPT
34	0.041260	127.0.0.1	127.0.0.53	DNS	82	Standard query 0x8453 A example.org OPT
35	0.041789	127.0.0.1	127.0.0.53	DNS	82	Standard query 0xf75f AAAA example.org OPT
36	0.042246	127.0.0.1	127.0.0.53	DNS	84	Standard query 0x9fa8 A ipv4only.arpa OPT
37	0.042716	127.0.0.1	127.0.0.53	DNS	84	Standard query 0xbfac AAAA ipv4only.arpa OPT
38	0.043143	127.0.0.1	127.0.0.53	DNS	95	Standard query 0xea53 A detectportal.firefox.com OPT
39	0.043614	127.0.0.1	127.0.0.53	DNS	95	Standard query 0xda57 A detectportal.firefox.com OPT
40	0.043987	127.0.0.1	127.0.0.53	DNS	95	Standard query 0x610b A detectportal.firefox.com OPT
41	0.044497	127.0.0.53	127.0.0.1	DNS	234	Standard query response 0xea53 A detectportal.firefox.com CNAME detectport
42	0.045122	127.0.0.1	127.0.0.53	DNS	95	Standard query 0xd0d6 AAAA detectportal.firefox.com OPT
43	0.045705	127.0.0.53	127.0.0.1	DNS	234	Standard query response 0xda57 A detectportal.firefox.com CNAME detectport
44	0.046636	127.0.0.53	127.0.0.1	DNS	234	Standard query response 0x610b A detectportal.firefox.com CNAME detectport
45	0.047505	127.0.0.53	127.0.0.1	DNS	218	Standard query response 0xd0d6 AAAA detectportal.firefox.com CNAME detectp
46	0.048132	127.0.0.53	127.0.0.1	DNS	98	Standard query response 0x8453 A example.org A 93.184.215.14 OPT
47	0.048582	127.0.0.53	127.0.0.1	DNS	98	Standard query response 0x9ee8 A example.org A 93.184.215.14 OPT
48	0.049017	127.0.0.1	127.0.0.53	DNS	95	Standard query 0x2557 AAAA detectportal.firefox.com OPT
49	0.049557	127.0.0.53	127.0.0.1	DNS	218	Standard query response 0x2557 AAAA detectportal.firefox.com CNAME detectp
50	0.050262	127.0.0.1	127.0.0.53	DNS	95	Standard query 0x3ee9 A detectportal.firefox.com OPT
51	0.050809	127.0.0.1	127.0.0.53	DNS	95	Standard query 0x0bed AAAA detectportal.firefox.com OPT
52	0.051333	127.0.0.53	127.0.0.1	DNS	234	Standard query response 0x3ee9 A detectportal.firefox.com CNAME detectport
53	0.052140	127.0.0.53	127.0.0.1	DNS	218	Standard query response 0x0bed AAAA detectportal.firefox.com CNAME detectp
54	0.052737	127.0.0.53	127.0.0.1	DNS	116	Standard query response 0x9fa8 A ipv4only.arpa A 192.0.0.170 A 192.0.0.171

바로 엄청난 오류 메시지가 뜬다. 주로 쿼리 혹은 TCP CHECKSUM이 잘못되었다는 메시지다. TCP CHECKSUM이란 해시와 비슷한 무엇인데, 전송 측의 체크섬과 수신 측의 체크섬이 일치하면 데이터가 원본 그대로 전송되었음이 입증된다. 반면 이 체크섬이 일치하지 않을 경우 데이터 전송과정에서 무언가 훼손이 있었다는 이야기다. 즉 TCP CHECKSUM은 데이터의 무결성을 입증하는데 사용된다.

이번 케이스에서는 데이터가 전송 도중에 훼손된 것으로 보인다. 문제 이름이 conversations이었으니 일단 대화 내역을 찾아보자.

```
...1..GE T /canonical.htm 1 HTTP/1.1
.1..Host : detect
portal.firefox.com..User-Agent:
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/110.0..
Accept: */*..Accept-Language: en-US,en;q=0.5..Accept-Encoding: gzip, deflate..Cache-Control: no-cache..Pragma: n
```

TCP 필터로 검색한 결과 mozilla라는 유저가 우분투를 사용해 파일파스에 접속한 기록을 찾아냈다. uri [http://detectportal.firefox.com/canonical.html]는 검색 결과



Firefox

[다른 운영 체제 및 언어](#)

종속 포털 감지

종속 포털 검사

Firefox의 [종속 포털](#) 감지기는 네트워크 연결이 사용자의 로그인을 필요로하는지 여부를 테스트합니다. 이것은 때때로 공공 와이파이 핫스팟을 사용할 때 혹은 회사의 손님용 네트워크에 접속할 때 정책에 동의하는지 확인할 때 발생합니다. Firefox가 정기적으로 <http://detectportal.firefox.com/canonical.html>에 연결하여 이를 확인합니다. 또한 이 URL에 접속해 사용자의 현재 네트워크가 IPv6와 같은 특정 기술을 지원하는지 여부도 확인합니다.

<https://support.mozilla.org/ko/kb/captive-portal>로 연결되었다. "네트워크 연결이 사용자의 로그인을 필요로하는지 여부를 테스트" 스타벅스 같은 곳에서 공공 와이파이를 사용하려고 할 때 또는 로그인 페이지 같은 것인가 보다.

```
+ 66 0.060337 34.107.221.82 10.0.0.1      HTTP      352 HTTP/1.1 200 OK (text/html)
| 67 0.060733 10.0.0.1       34.107.221.82  TCP      54 48150 → 80 [ACK] Seq=302 Ack=299 Win=63942 [TCP

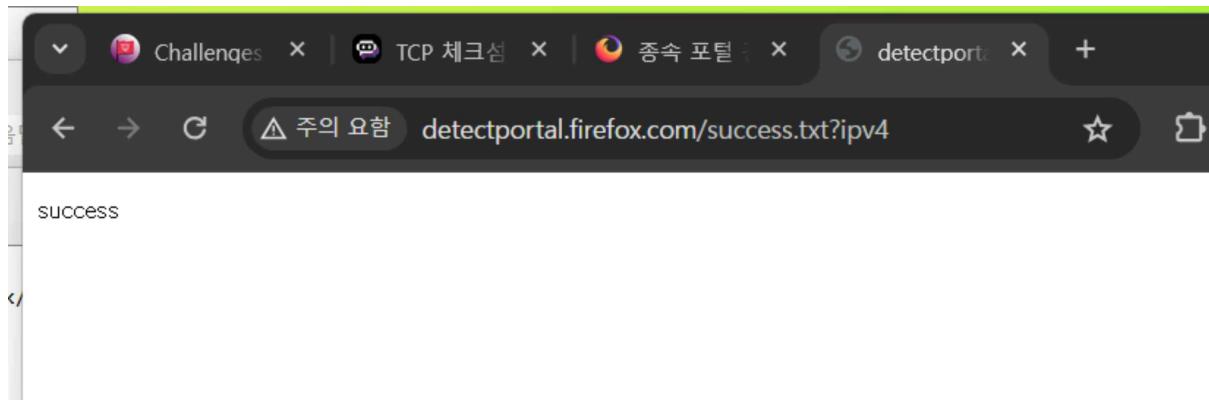
```

이후 그 서버와 무언가 텍스트를 교류?한 모습. 로그인을 한 건가?

```
→ 83 0.068997 10.0.0.1       34.107.221.82  TCP      54 48160 → 80 [ACK] Seq=1 Ack=1 Win=64240 [TCP CHECKSUM ] IN
| 84 0.069608 10.0.0.1       34.107.221.82  HTTP     357 GET /success.txt?ipv4 HTTP/1.1
| 85 0.070361 34.107.221.82 10.0.0.1      TCP      60 80 → 48160 [ACK] Seq=1 Ack=304 Win=64240 [TCP CHECKSUM ]
| 86 0.070767 34.107.221.82 10.0.0.1      HTTP     270 HTTP/1.1 200 OK (text/plain)
| 87 0.071242 10.0.0.1       34.107.221.82  TCP      54 48160 → 80 [ACK] Seq=304 Ack=217 Win=64024 [TCP CHECKSUM ] IN

```

"success"를 받고 "ok"를 전송.



success 화면.

```
▼ [Conversation completeness: Incomplete, DATA (15)]
  ..0. .... = RST: Absent
  ...0 .... = FIN: Absent
```

또한 데이터 전송이 미결이란다.

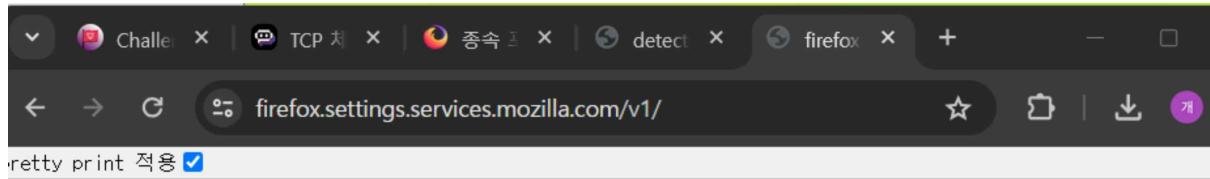
```

104 0.079205 10.0.0.1      34.117.188.166  TCP      54 34928 → 443 [ACK] Seq=1 Ack=1 Win=64240 [TCP CHECKSUM]
105 0.079824 10.0.0.1      34.117.188.166  TLSv1.3   571 Client Hello (SNI=contile.services.mozilla.com)
106 0.080340 34.117.188.166 10.0.0.1      TCP      60 443 → 34928 [ACK] Seq=1 Ack=518 Win=64240 [TCP CHECKSUM]

firefox.settings.services.mozilla.com
d_master_secret (len=0)

```

이 단계에서 전송이 끝났다. 구글에 해당 uri를 입력하자 다음과 같은 화면이 출력됐다.



```

"project_name": "Remote Settings PROD",
"project_version": "18.1.0",
"http_api_version": "1.22",
"project_docs": "https://remote-settings.readthedocs.io",
"url": "https://firefox.settings.services.mozilla.com/v1/",
"settings": {
    "batch_max_requests": 25,
    "explicit_permissions": false,
    "readonly": true
},
"capabilities": {
    "changes": {
        "description": "Track modifications of records in Kinto and store the collection timestamps into a specific bucket and collection.",
        "url": "http://kinto.readthedocs.io/en/latest/tutorials/synchronisation.html#polling-for-remote-changes",
        "version": "31.2.0",
        "collections": [
            "/buckets/blocklists",
            "/buckets/blocklists-preview",
            "/buckets/main",
            "/buckets/main-preview",
            "/buckets/security-state",
            "/buckets/security-state-preview"
        ],
        "attachments": {
            "description": "Add file attachments to records",
            "url": "https://github.com/Kinto/kinto-attachment/",
            "version": "6.4.0",
            "base_url": "https://firefox-settings-attachments.cdn.mozilla.net/"
        }
    }
}

```

'Track modifications of records in Kinto and store the collection timestamps into a specific bucket and collection.'

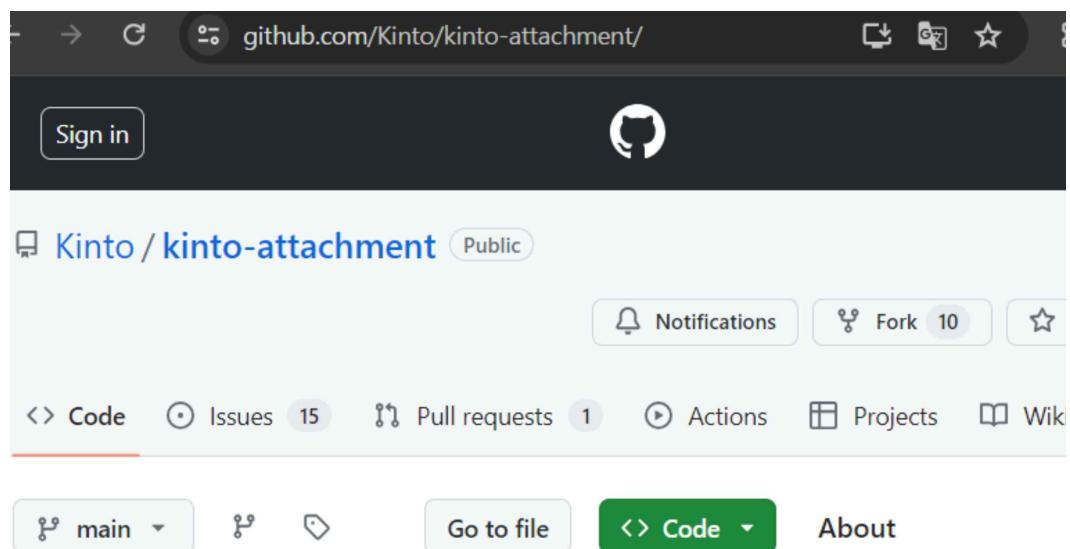
킨토에 있는 기록들을 교정하고 특정한 버켓과 컬렉션에 타임스탬프 컬렉션을 저장해라. (?)

```

"url": "http://kinto.readthedocs.io/en/latest/tutorials/synchronisation.html#polling-for-remote-changes",
"version": "31.2.0",

```

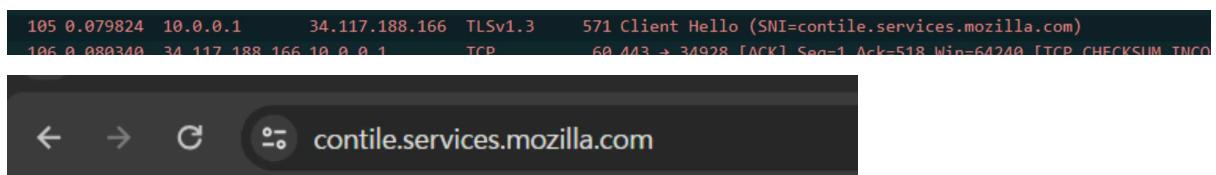
```
"collections": [  
    "/buckets/blocklists",  
    "/buckets/blocklists-preview",  
    "/buckets/main",  
    "/buckets/main-preview",  
    "/buckets/security-state",  
    "/buckets/security-state-preview"  
  
    "attachments": {  
  
        "description": "Add file attachments to records",  
        "url": "https://github.com/Kinto/kinto-attachment/",  
        "version": "6.4.0",  
  
        "base_url": "https://firefox-settings-attachments.cdn.mozilla.net/"  
  
    }  
}  
}
```



실제로 깃허브 페이지가 나왔다. base url은 무슨 뜻이지?



검색해 보자 이런 이미지가 나왔다. 설명은 이해할 수 없었기에 일단 이미지만 참고했다.



12 0.007289	127.0.0.1	127.0.0.1	UDP	96 45431 → 12345 Len=54
13 0.008978	127.0.0.1	127.0.0.53	DNS	95 Standard query 0xcc33 A detectportal.firefox.com OPT
14 0.009408	127.0.0.1	127.0.0.53	DNS	95 Standard query 0x6238 AAAA detectportal.firefox.com OPT
15 0.009833	10.0.0.1	10.0.0.2	DNS	84 Standard query 0xb82c A detectportal.firefox.com
16 0.010303	10.0.0.1	10.0.0.2	DNS	84 Standard query 0x1934 AAAA detectportal.firefox.com
17 0.010766	127.0.0.53	127.0.0.1	DNS	206 Standard query response 0xcc33 A detectportal.firefox.com CNAME detectportal.prod.mozilla.org
18 0.011968	127.0.0.53	127.0.0.1	DNS	218 Standard query response 0x6238 AAAA detectportal.firefox.com CNAME detectportal.prod.mozilla.org
19 0.013251	10.0.0.2	10.0.0.1	DNS	195 Standard query response 0xb82c A detectportal.firefox.com CNAME detectportal.prod.mozilla.org

<https://detectportal.firefox.com/>에 접속했더니 웹 파일이 다운로드 받아졌다.

The screenshot shows a browser window with a download dialog. The dialog title is '다운로드' (Download) and the URL is 'https://detectportal.firefox.com/'. Below the dialog, a file viewer window is open, showing the contents of the downloaded file. The window has a menu bar in Korean: 파일(F), 편집(E), 찾기(S), 보기(V), 분석(A), 도구(T), 창 설정(W), 도움말(H). The file viewer displays hex and ASCII data. The ASCII dump shows the text 'success.'.

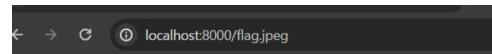
Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
00000000	73 75 63 63 65 73 73 0A	success.

헥사디로 디코딩한 메시지: "success."

```
Answers
detectportal.firefox.com: type CNAME, class IN, cname detectportal.prod.mozaws.net
Name: detectportal.firefox.com
Type: CNAME (5) (Canonical NAME for an alias)
Class: IN (0x0001)
Time to live: 5 (5 seconds)
Data length: 30
```

.

>	1182	1.063673	127.0.0.1	127.0.0.1	HTTP	609 GET /flag.jpeg HTTP/1.1
-	1198	1.352168	127.0.0.1	127.0.0.1	HTTP	8540 HTTP/1.0 200 OK (JPEG JFIF image)



사이트에 연결할 수 없음

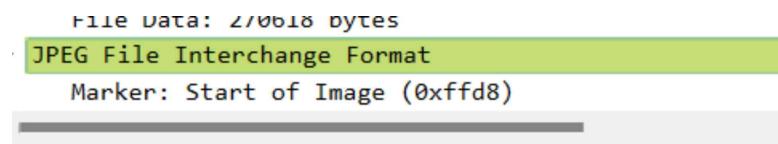
localhost에서 연결을 거부했습니다.

다음 방법을 시도해 보세요.

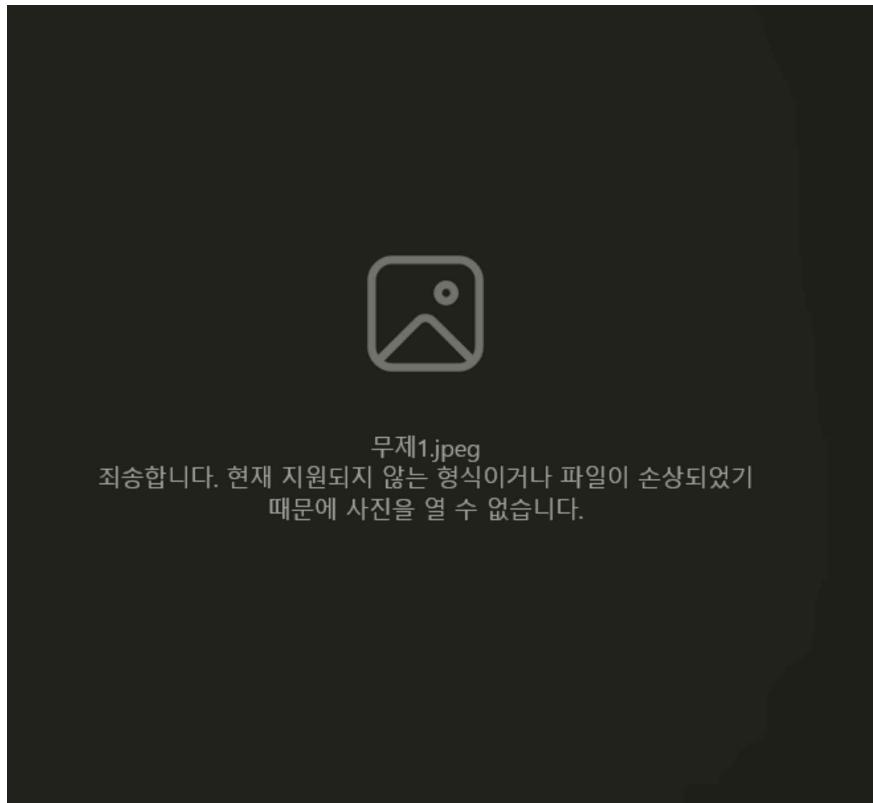
- 연결 확인
- 프록시 및 방화벽 확인

ERR_CONNECTION_REFUSED

새로고침



밑의 jpeg 이미지의 헥사 덤프를 복사해 헥사디에 입력했다.



무제1.jpeg

죄송합니다. 현재 지원되지 않는 형식이거나 파일이 손상되었기 때문에 사진을 열 수 없습니다.

파일 시그니처를 jpeg 파일에 맞춰 수정한 뒤 파일을 열자 열리지 않았다.

```
File Data: 270010 bytes
JPEG File Interchange Format
Marker: Start of Image (0xffd8)
Marker segment: Reserved for application segments - 1 (0xFFE1)
    Marker: Reserved for application segments - 1 (0xffe1)
    Length: 148
    Identifier: Exif
        [Expert Info (Warning/Protocol): Initial App0 segment with "JFIF" Identifier not found]
            [Initial App0 segment with "JFIF" Identifier not found]
            [Severity level: Warning]
            [Group: Protocol]
    Endianess: big endian
```

와이어샤크를 다시 체크해보자 아이덴티파이어 : exif 라고 표기되어있다. APP0의 데이터(세그먼트)에 "JFIF" 식별자가 존재하지 않는다는 오류 메시지.

Decoded text
FF D8 FF E0 00 94 45 78 69 66 00 00 4D 4D 00 2A ýØÿà."Exif..MM.*
00 10 00 00 08 00 03 01 28 00 03 00 00 00 01(.....
00 02 00 20 00 00 02 13 00 03 00 00 00 01 00 01
00 00 87 69 00 30 00 04 00 00 00 01 00 00 00 32 ..#i.0.....2
00 00 00 00 04 00 40 90 00 00 07 00 00 00 04@.....
30 32 33 32 91 01 00 07 00 50 00 00 00 04 01 02 0232`....P.....

헥사디로 디코딩한 맨 처음 부분에는 EXif라는 표시가 남아있다. EXif: 디지털 카메라 등에서 사용

되는 이미지 파일 메타데이터.

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
FF D8 FF E0 00 00 00 4A 46 49 46 00 4D 4D 00 2A	ÿØÿà...JFIF.MM.*
00 10 00 00 00 08 00 03 01 28 00 03 00 00 00 01(.....
00 02 00 20 00 00 02 13 00 03 00 00 00 01 00 01
00 00 87 69 00 30 00 04 00 00 00 01 00 00 00 32	..#i.0.....2

파일 시그니처를 jfif로 수정했으나 여전히 열리지 않았다.

비트 수준
압축
해상도 단위
색 대표
픽셀당 압축 비트
카메라
카메라 제조업체
카메라 모델
F-스톱
노출 시간
ISO 감도
노출 바이어스
초점 거리
조리개 최대 개방
측광 모드
피사체 거리
플래시 모드
플래시 에너지
25mm 초점 거리

파일 속성을 보니 확실히 exif 파일이다.

```
et(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D (00000  FF D8 FF E8 00 94 45 78 69 66 00 00 4D 4D (00100  00 10 00 00 00 08 00 03 01 28 00 03 00 00 (
```

헥사 덤프를 다시 붙여넣기 해 어긋난 파일 시그니처를 고쳤다.

파일
를 무제2.exif
형 EXIF 파일
일 위치 C:\사용자\ronnf\OneDrive\바탕 화면\
기 303KB
든 날짜 2024-05-18 오후 2:44
정한 날짜 2024-05-18 오후 2:46
성 AL
용성 상태 이 장치에서 사용 가능

? 오히려 메타데이터가 표시되지 않는다.

수식 애상노
비트 수준
압축
해상도 단위
색 대표
픽셀당 압축 비트
[카메라](#)
카메라 제조업체
카메라 모델
F-스톱
노출 시간
ISO 감도
노출 바이어스
조점 거리
조리개 최대 개방
측광 모드
...

파일 확장자를 jpeg로 바꾸니 같은 화면이 나오는 걸 확인했다. 그냥 jpeg 확장자 파일에 공통적으로 표시되는 속성인가 보다.

아까 깃허브 페이지와 코드로 돌아가 대체 뭘 하려고 했던건지부터 알아보자.

깃허브 페이지 소개글:

킨토 어태치먼트

 Run CI checks passing

 pypi v6.4.0

[Kinto 레코드](#)에 파일을 첨부합니다.

설치하다

kinto-record에 파일을 업로드해주는 프로그램.



Kinto는 동기화 및 공유 기능을 갖춘 미니멀리스트 JSON 스토리지 서비스입니다.

[왜 Kinto를 사용하나요?](#)

[Kinto 설치](#)

소개페이지:

킨토는 동기화 및 공유 기능을 갖춘 json 스토리지 서비스이다.

메모:

Mozilla에서 *Kinto*는 차단 목록, 실험, A/B 테스트, 검색 엔진 목록과 같이 자주 변경되는 설정의 전역 동기화 또는 글꼴이나 하이픈 사전과 같은 추가 자산 제공을 위해 *Firefox*에서 사용됩니다.

Mozilla와 firefox에서 사용된다.

Mozilla: firefox의 제조사.

그러니까 모질라에서 데이터베이스 및 파일박스를 관리하기 위해 킨토를 사용한다는 이야기인 것 같다. 킨토=쿼리와 유사한 동기형 데이터베이스 관리 프로그램.

Firefox의 Kinto 통합

Kinto는 Firefox에 통합되어 현재 RemoteSettings에 사용되는 간단한 JSON 스토리지 서비스입니다.

대충 비슷한 듯?

Preview [Code](#) | [Blame](#)

Kinto at Mozilla

lang

모질라(및 파이어폭스)에서의 킨토 사용 설명글

Firefox 원격 설정

원본!

Firefox 엔지니어는 Kinto 관리 UI를 통해 차단 목록이나 인증서 취소 목록과 같은 원격 설정을 편집합니다. 아래 나열된 각 설정 범주에 대한 여러 버킷이 있습니다.

수억 개의 Firefox 브라우저는 kinto-changes 엔드포인트를 사용하여 정기적으로 변경 사항을 폴링 합니다. 두 개의 인스턴스가 동일한 데이터베이스로 배포됩니다. 하나는 CDN 뒤의 읽기 전용 공용 인스턴스이고 다른 하나는 보안 VPN을 통해서만 액세스할 수 있는 프라이빗 인스턴스입니다.

원격 설정이 중요하고 CDN을 통해 제공되므로 진위성과 무결성을 보장하기 위해 kinto-signer를 사용하여 데이터에 서명합니다. 또한 검토 및 승인 기능은 물론 QA 팀을 위한 변경 사항 미리보기 기능도 제공합니다. 기록 플러그인을 사용하면 시간 경과에 따른 변경 사항을 추적할 수 있습니다.

클라이언트는 kinto.js로 구현된 Firefox 코드베이스에 있습니다. 설정이 적합한지 확인하기 위해 콘텐츠 서명을 확인하고, IndexedDB 대신 SQLite에 로컬 데이터를 저장하는 특정 어댑터가 있습니다. 일부 원격 측정 데이터는 전역적으로 활용을 추적하기 위해 원격 설정이 로컬로 동기화될 때 전송됩니다.

버킷과 컬렉션은 물론 그룹과 관련 권한을 관리하기 위해 Github 개인 저장소에서 YAML 파일을 읽고 누락된 객체를 생성하거나 업데이트하는 kinto-wizard를 사용합니다

사례 링크: <https://firefox.settings.services.mozilla.com>

```

pretty print 적용 ✓

{
  "project_name": "Remote Settings PROD",
  "project_version": "18.1.0",
  "http_api_version": "1.22",
  "project_docs": "https://remote-settings.readthedocs.io",
  "url": "https://firefox.settings.services.mozilla.com/v1/",
  "settings": {
    "readonly": true,
    "batch_max_requests": 25,
    "explicit_permissions": false
  },
  "capabilities": {
    "changes": {
      "description": "Track modifications of records in Kinto and store the collection and collection.",
      "url": "http://kinto.readthedocs.io/en/latest/tutorials/synchronisation.html#pol",
      "version": "31.2.0",
      "collections": [
        "/buckets/blocklists",
        "/buckets/blocklists-preview",
        "/buckets/main",
        "/buckets/main-preview",
        "/buckets/security-state",
        "/buckets/security-state-preview"
      ]
    },
    "attachments": {
      "description": "Add file attachments to records",
      "url": "https://github.com/Kinto/kinto-attachment/",
      "version": "6.4.0",
      "base_url": "https://firefox-settings-attachments.cdn.mozilla.net/"
    }
  }
}

```

! 아까 본 그 페이지다.

아무튼 정리하자면 파이어폭스는 킨토를 데이터베이스로 사용한다. kinto - attachment는 킨토에 파일을 업로드해주는 프로그램이다.

▼ Queries

- ▼ detectportal.firefox.com: type A, class IN
 - Name: detectportal.firefox.com
 - [Name Length: 24]
 - [Label Count: 3]
 - Type: A (1) (Host Address)
 - Class: IN (0x0001)
- ▼ Additional records

그럼 이건 무슨 뜻이지? 쿼리와 파이어폭스를 연결했다는 건가?

detectportal을 검색하면 바로 파이어폭스의 종속 포털 감지 페이지로 연결된다. 알겠는데 이게 쿼리랑 무슨 연관인지를 알고 싶다.

12	0.0.0.1	127.0.0.1	127.0.0.1	DNS	95 Standard query 0xcc33 A detectportal.firefox.com OPT
13	0.008978	127.0.0.1	127.0.0.53	DNS	95 Standard query 0x6238 AAAA detectportal.firefox.com OPT
14	0.009408	127.0.0.1	127.0.0.53	DNS	84 Standard query 0xb82c A detectportal.firefox.com
15	0.009833	10.0.0.1	10.0.0.2	DNS	84 Standard query 0x1934 AAAA detectportal.firefox.com
16	0.010303	10.0.0.1	10.0.0.2	DNS	

아무튼 쿼리/파이어폭스 포탈 감지간 교류가 총 4번 이루어졌는데, 타입 A는 호스트 주소고 타입 AAAA는 IP6 주소라고 한다.

```
84 Standard query 0x1934 AAAA detectportal.firefox.com
206 Standard query response 0xcc33 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.dete...
218 Standard query response 0x6238 AAAA detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.d...
195 Standard query response 0xb82c A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.dete...
    ↳ 195. 114. 188.111
    ↳ Answers
        ↳ detectportal.firefox.com: type CNAME, class IN, cname detectportal.prod.mozaws.net
            Name: detectportal.firefox.com
            Type: CNAME (5) (Canonical NAME for an alias)
            Class: IN (0x0001)
            Time to live: 5 (5 seconds)
            Data length: 30
            CNAME: detectportal.prod.mozaws.net
        ↳ detectportal.prod.mozaws.net: type CNAME, class IN, cname prod.detectportal.prod.cloudops.mo
```

이후 쿼리의 응답 내용.

위키백과, 우리 모두의 백과사전.

캐노니컬 네임 레코드(Canonical Name record), 줄여서 **CNAME 레코드**(CNAME record)는 하나의 도메인 네임(에일리어스)을 다른 이름(**표준 형식**의 이름)으로 매핑시키는 **도메인 네임 시스템**(DNS)의 **리소스 레코드**의 일종이다.^[1]

하나의 IP 주소로부터 여러 개의 서비스를 실행할 때(예: 각기 다른 포트로 각각 구동되는 **FTP 서버**와 **웹 서버** 등) 편리함을 입증할 수 있다. 이를테면 *ftp.example.com*과 *www.example.com*를 (IP 주소를 가리키는) **A 레코드**를 보유한 *example.com*의 DNS 엔트리를 가리킬 수 있다. 그러면 IP 주소가 변경이 될 경우 네트워크 안의 한 지점에서 변경사항을 기록하기만 하면 된다.

CNAME 레코드는 무조건 다른 도메인 네임을 가리켜야 하며 직접 IP 주소를 가리켜서는 안 된다.

일단 그렇다고 한다. 파일어폭스 포털 감지 링크 : cname 태입으로 쿼리에 저장으로 일단 알아들었다.

검색 결과 쿼리가 내가 아는 MySQL이 아니라 DNS의 쿼리를 뜻함을 알게 되었다.

쿼리: 사용자가 도메인 이름(url 등)을 입력하고 ip 주소를 얻기 위해 dns 서버에 보내는 요청.

```

184 Standard query response 0x7223 A r3.o.lencr.org CNAME o.lencr.edgesuite.n
208 Standard query response 0x1221 AAAA r3.o.lencr.org CNAME o.lencr.edgesuit
106 Standard query 0xf380 A content-signature-2.cdn.mozilla.net OPT
106 Standard query 0x9e85 AAAA content-signature-2.cdn.mozilla.net OPT
85 Standard query 0x3313 A r3.o.lencr.org OPT
85 Standard query 0xdb17 AAAA r3.o.lencr.org OPT
240 Standard query response 0x3313 A r3.o.lencr.org CNAME o.lencr.edgesuite.n
208 Standard query response 0xdb17 AAAA r3.o.lencr.org CNAME o.lencr.edgesuit
85 Standard query 0x00ab A r3.o.lencr.org OPT
240 Standard query response 0x00ab A r3.o.lencr.org CNAME o.lencr.edgesuite.n
85 Standard query 0x0ea4 AAAA r3.o.lencr.org OPT
208 Standard query response 0x0ea4 AAAA r3.o.lencr.org CNAME o.lencr.edgesuit
85 Standard query 0xf2f3 A r3.o.lencr.org OPT
240 Standard query response 0xf2f3 A r3.o.lencr.org CNAME o.lencr.edgesuite.n
272 Standard query response 0x9e85 AAAA content-signature-2.cdn.mozilla.net C

```

쿼리 요청/응답.

```

/* Protected Payload (KPO), DCID=10904050000e2290
54 34928 → 443 [ACK] Seq=783 Ack=3732 Win=62780 [TCP CHECKSUM INCORRECT] Len=0
69 Protected Payload (KPO), DCID=b51168
74 Standard query 0x11d3 A www.google.com
85 Standard query 0xb29d A www.google.com OPT
81 Standard query 0x7c4e A google.com OPT
84 Standard query 0x4927 A m.youtube.com OPT
94 Standard query 0xf94f A youtubei.googleapis.com OPT
86 Standard query 0x225c A www.youtube.com OPT
97 Standard query 0xa21f A forcesafesearch.google.com OPT
93 Standard query 0x77f7 A youtube.googleapis.com OPT
95 Standard query 0x216a A www.youtube-nocookie.com OPT
70 Standard query 0x241b A google.com
73 Standard query 0x1a3c A m.youtube.com
181 Standard query response 0xb29d A www.google.com A 142.251.16.99 A 142.251.16.147 A 142.251.16.103 A 142.2
83 Standard query 0xb113 A youtubei.googleapis.com
75 Standard query 0x199b A www.youtube.com
86 Standard query 0x7042 A forcesafesearch.google.com
82 Standard query 0x7176 A youtube.googleapis.com
84 Standard query 0x6416 A www.youtube-nocookie.com
170 Standard query response 0x11d3 A www.google.com A 142.251.16.99 A 142.251.16.147 A 142.251.16.103 A 142.2
374 Standard query response 0x6416 A www.youtube-nocookie.com CNAME youtube-ui.l.google.com A 142.251.163.93
227 Standard query response 0xb113 A youtubei.googleapis.com A 172.253.62.95 A 172.253.115.95 A 172.253.122.9
365 Standard query response 0x199b A www.youtube.com CNAME youtube-ui.l.google.com A 172.253.63.93 A 142.250.

```

이후 인터넷 접속 기록.

- ✓ **Queries**
 - ✓ **forcesafesearch.google.com:** type A, class IN
 - Name: forcesafesearch.google.com

Google 도메인을 forcesafesearch.google.com에 매팅

이 방법은 세이프서치 VIP를 활용해 HTTPS를 통한 보안 연결을 허용하면서도 네트워크상의 모든 사용자가 Google 검색에서 세이프서치를 사용하도록 강제합니다. 세이프서치 VIP에서 VIP란 가상 IP를 의미하며 가상 VIP는 여러 Google 서버에 내부적으로 라우팅할 수 있는 IP 주소입니다. Google은 이 VIP에서 수신하는 모든 요청에 대해 다음을 포함한 세이프서치 결과를 제공합니다.

- Google 검색
- 이미지 검색
- 동영상 검색

이 방법은 기기의 모든 브라우저에서 작동하며 기기 관리자는 이 변경사항을 실행취소 할 수 있습니다. 다음 단계를 따르세요.

세이프서치 강제.

youtube-nocookie : 유튜브 광고없이 시청.

IMG-GETPOCKET.CDN.MOZILLA.NET - 도메인 정보

탐지 정보

다음 페이지에서는 img-getpocket.cdn.mozilla.net 도메인과 연결된 애플리케이션을 제공합니다. Netify Data Feed API를 통해 전체 데이터 세트에 액세스할 수 있습니다.



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

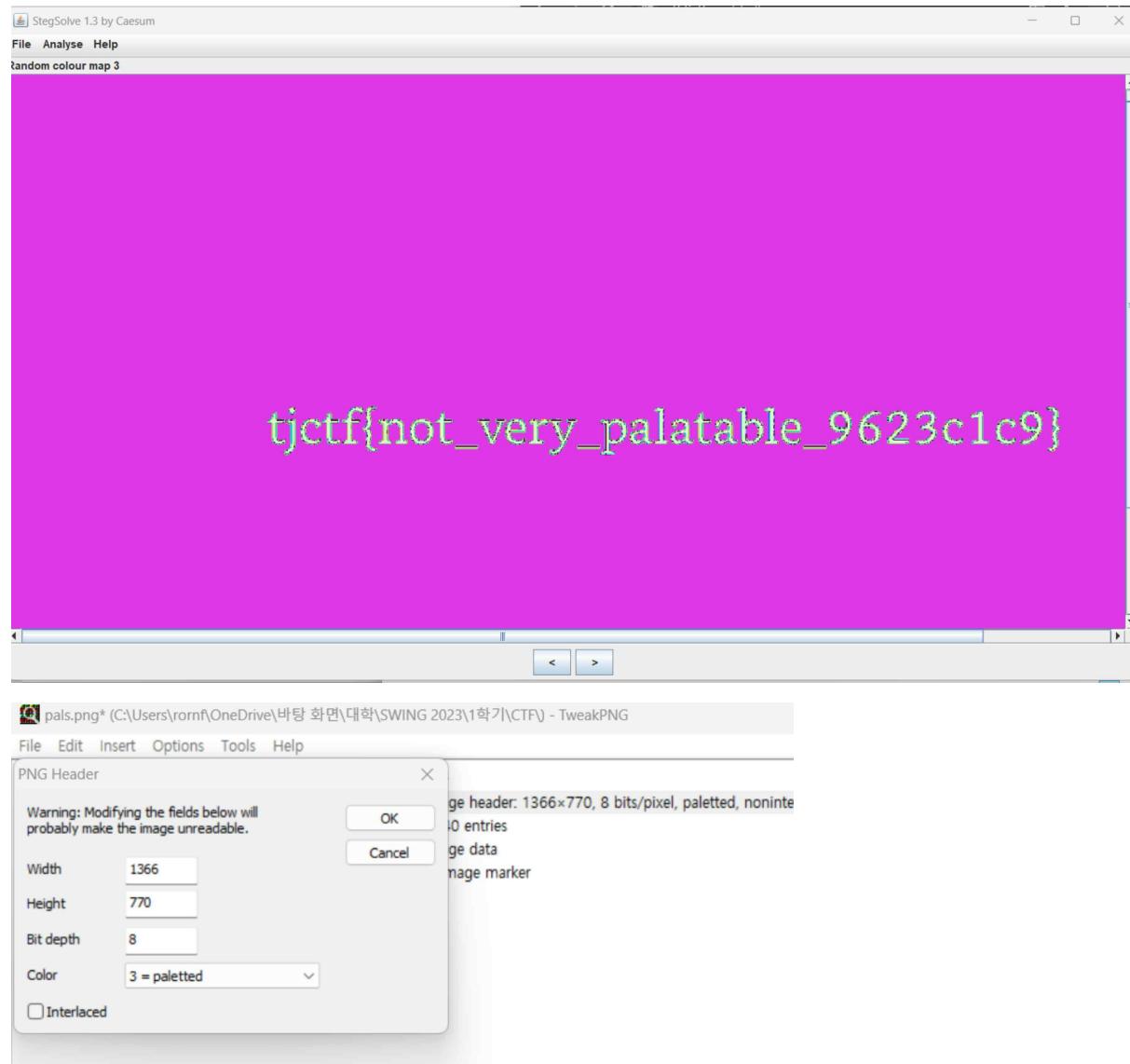
For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com.

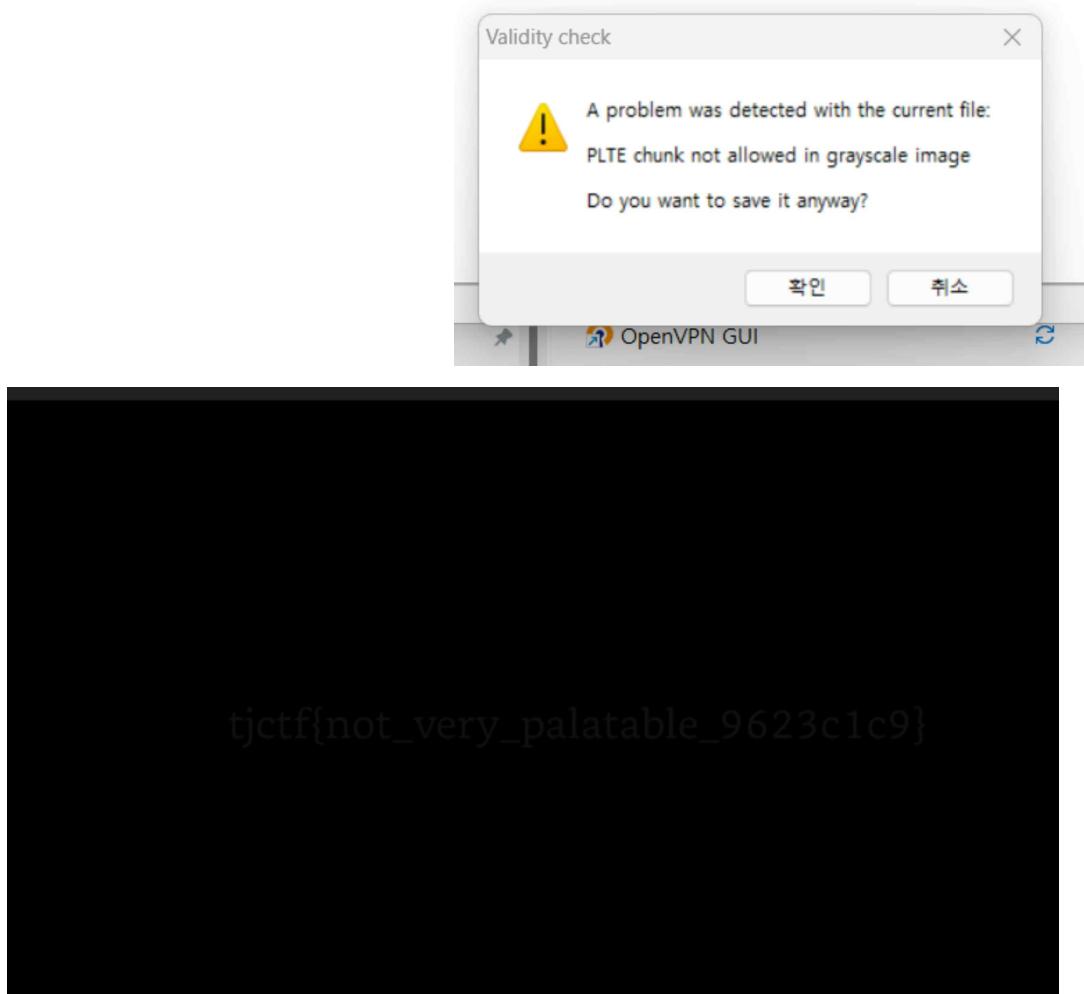
Thank you for using nginx.

문제2. pals

문제를 다운로드 받아 stegosolve로 분석하자 다음과 같은 글귀가 나왔다.

글귀를 그대로 입력하자 문제가 해결됐다. not very palatable이라는 것을 보아 아까 트윅png로 분석했을 때 색깔 항목을 모노톤으로 선택했으면 해결되었을 것 같다.





결과

플래그: tjctf{not_very_palatable_9623c1c9}

문제3. *thatsmyjam*

설명:

Please dont judge my Spotify Wrapped...

Submit your flag in lowercase and remember to wrap with {}.

내 스포티파이 wrapped를 판단하지 말아줘요

플래그를 소문자로 쓰고 {}로 감싸라.

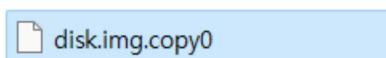
종목 : 포레식



암축을 해제하면 비어있는 풀더가 나온다.

Name	Size	Type	Date Modified
disk.img	194,560	Regular File	2024-05-16 오전 5...

ftk imager로 확인한 결과 비어있는 파일의 사이즈가 아니다. 파일을 추출했다.

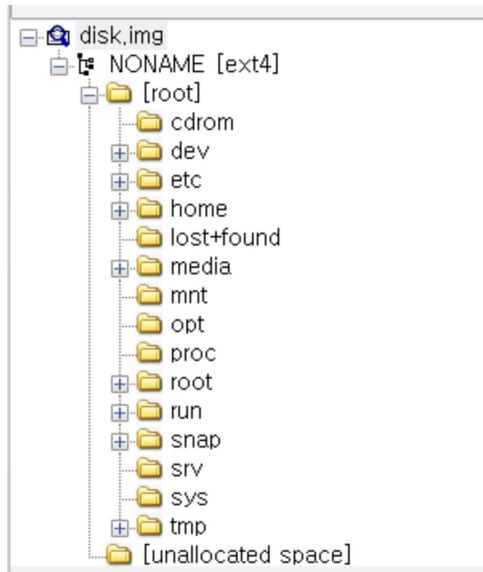


추출한 파일.

0 00
D 2D 2D 2D 2D 42 45 47 49 4E 20 43 45 52 54 49 -----BEGIN CERTI
FICATE-----MIIG
6 49 43 41 54 45 2D 2D 2D 2D 2D 0A 4D 49 49 47
6 6A 43 43 42 4E 4B 67 41 77 49 42 41 67 49 51
E 39 75 61 4F 41 62 58 43 73 63 2B 4F 4E 48 66
6jCCBNKgAwIBAgIQ
N9uaOAbXCsc+ONHf

헥사디로 본 파일 첫머리.





ftk imager 분석 결과

문제; Please dont judge my Spotify Wrapped..

Spotify Wrapped가 뭔가 했더니 스포티파이 연말정산이란다. 우선 스포티파이 관련 파일 폴더를 찾으면 될 것 같다.

저번처럼 레지스트리 파일을 추출해서 레지스트리를 확인하는 건가 싶었는데, 이번에는 아래 이미지에 있는 경로들이 보이지 않았다.

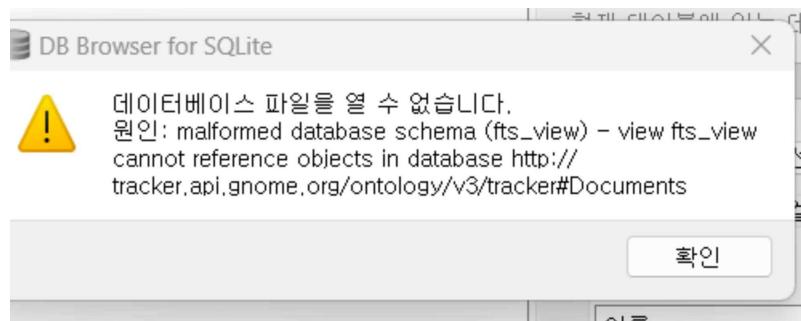
레지스트리 경로	하이브 파일 경로
HKEY_LOCAL_MACHINE\BCD00000000	{Boot Partition}\Boot\BCD
HKEY_LOCAL_MACHINE\COMPONENTS	%SystemRoot%\System32\Config\COMPONENTS
HKEY_LOCAL_MACHINE\SYSTEM	%SystemRoot%\System32\Config\SYSTEM
HKEY_LOCAL_MACHINE\SAM	%SystemRoot%\System32\Config\SAM
HKEY_LOCAL_MACHINE\SECURITY	%SystemRoot%\System32\Config\SECURITY
HKEY_LOCAL_MACHINE\SOFTWARE	%SystemRoot%\System32\Config\SOFTWARE
HKEY_LOCAL_MACHINE\HARDWARE	Volatile
HKEY_USERS\<SID of local service account>	%SystemRoot%\ServiceProfiles\LocalService\NTUSER.DAT
HKEY_USERS\<SID of network service account>	%SystemRoot%\ServiceProfiles\NetworkService\NTUSER.DAT
HKEY_USERS\<SID of username>	%UserProfile%\NTUSER.DAT
HKEY_USERS\<SID of username>_Classes	%UserProfile%\AppData\Local\Microsoft\Windows\Usrclass.dat
HKEY_USERS\DEFAULT	%SystemRoot%\System32\Config\DEFAULT

(그림) 참고로 REGA에서는 위 내용에 나와 있는 하이브 파일을 수집합니다.

그래서 디스크에서 어플리케이션 데이터를 모아두는 폴더가 어디인지 검색했다.

도움이 되는 정보를 찾을 수 없었기에 일단 직감적으로 끌리는 폴더들을 추출해 파일을 분석해보기로 했다.

그중 데이터베이스 파일 폴더를 추출해 DB viwer로 확인해보고자 했으나 다음과 같은 에러가 발생했다.



Why is database disk image malformed?

Sometimes a Storage Node Operator may encounter the "database disk image is malformed" error in their log. This could happen during unplanned shutdown or reboot. The error indicates that [one or more of the sqlite3 databases may have become corrupted](#).

2023. 10. 2.

찾아보니 급작스러운 셧다운이나 재시작으로 데이터베이스가 손상될 수도 있다고 한다.

/%2Fv3%2Ftracker%23Audio

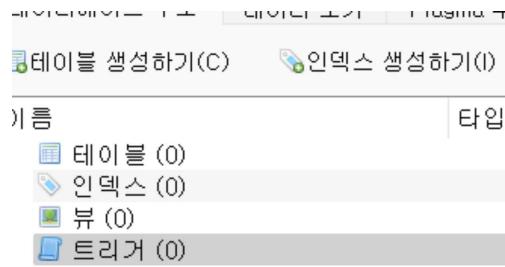
/%2Fv3%2Ftracker%23Audio.db-shm

/%2Fv3%2Ftracker%23Audio.db-wal

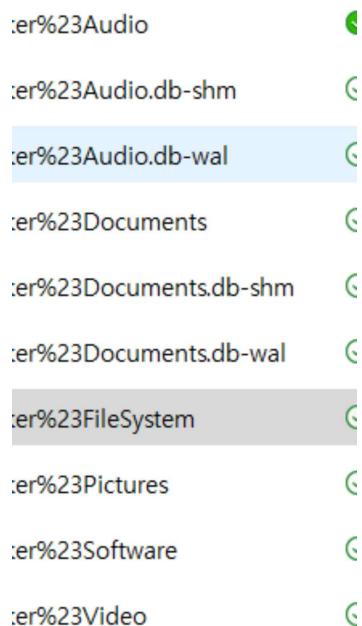
그래서 파일 목록을 다시 보았더니 -shm, -wal 파일도 같이 있는 것이 보였다. 이것들은 또 뭔가 했더니 -wal 파일은 트랜잭션이 실패했을 때 SQLite가 변경 사항을 롤백할 수 있도록 하는 최종 변경사항 적용 이전의 백업 파일이라고 한다. 그리고 -shm은 임시 데이터를 포함하는 공유 메모리 파일이다.

Ftracker%23Audio (2)

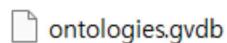
wal 파일의 확장자를 db로 바꾸고 db 뷰어에 넣어봤다.



마찬가지로 데이터는 나오지 않는다. wal과 shm을 사용해서 db 파일을 복원할 방법은 없을까?



이 데이터베이스들의 데이터를 읽는다면 컴퓨터에 대해 좀 알 수 있지 않을까?



gvdb 파일을 검색하자 바로 깃허브 링크가 나왔다. 설명글을 읽어보니 이 또한 데이터베이스 파일의 일종이라는 것 같다.

G GVDB

Star

1

More actions

Project information

A simple database file format that stores a mapping from strings to GVariant values in a way that is extremely efficient for lookups.

파일 뷰어로 추정되는 깃허브 페이지.

gvdb/gvdb-builder.c

비주얼 스튜디오에 코드를 붙여넣기 해 release해보자.

gvdb

Add getter for GVDB table contents

COPYING

Add COPYING file to indicate the licen...

README.md

docs: Add README

gvdb.doap

doap: Update maintainers list to sync...

meson.build

build: Add very basic meson build sys...

```

부여.c  새로운 기능
부여  (전역 범위)

1  /*
2   * Copyright © 2010 Codethink Limited
3   *
4   * This library is free software; you can redistribute it and/or
5   * modify it under the terms of the GNU Lesser General Public
6   * License as published by the Free Software Foundation; either
7   * version 2.1 of the License, or (at your option) any later version.
8   *
9   * This library is distributed in the hope that it will be useful,
10  * but WITHOUT ANY WARRANTY; without even the implied warranty of
11  * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
12  * Lesser General Public License for more details.
13  *
14  * You should have received a copy of the GNU Lesser General Public
15  * License along with this library; if not, see <http://www.gnu.org/licenses/>.
16  *
17  * Author: Ryan Lortie <desrt@desrt.ca>
18  */
19
20 #include "gvdb-reader.h"
21 #include "gvdb-format.h"
22
23 #include <string.h>

```

21 % 99+ ▲ 0 ↑ ↓ 🔍

오류 목록

전체 슬루션 197 오류 0 경고 0 메시지 빌드 + IntelliSense

코드	설명
C1083	포함 파일을 열 수 없습니다. 'gvdb-reader.h': No such file or directory
E1696	파일 소스를(를) 열 수 없습니다. "gvdb-reader.h"
E1696	파일 소스를(를) 열 수 없습니다. "gvdb-format.h"
E0029	식이 필요합니다.
E0029	식이 필요합니다.

오류 목록 출력

해당 코드들을 전부 비쥬얼 스튜디오로 release해 보았으나 오류가 발생하며 실행되지 않았다. 코드를 release하기 이전에 다운로드 받아야 할 실행 파일/라이브러리가 있는 것 같은데 깃허브 페이지에는 그러한 파일이 보이지 않는다.

Evidence Tree

File List

Name	Size	Type	Date Modified
[unallocated space]	0	Unallocate...	
bad blocks	0	Filesystem ...	2024-05-16 오전 5:...
block bitmap	8	Filesystem ...	
boot record	1	Filesystem ...	
group descriptor table	8	Filesystem ...	
inode bitmap	8	Filesystem ...	
inode table	12,160	Filesystem ...	
journal	16,384	Regular File	2024-05-16 오전 5:...
superblock	8	Filesystem ...	

다시 ftk imager에 들어가봤다가 수상하게 용량이 큰 파일이 있기에 복구해봤다.

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
1C 0B 00 00 18 00 0E 01 78 2D 66 6F 6E 74 2D 74 .....x-font-t  
65 78 2E 78 6D 6C 00 00 3D 0A 00 00 14 00 0C 01 ex.xml..=.....  
• 6A 72 64 2B 6A 73 6F 6E 2E 78 6D 6C 3B 0A 00 00 jrd+json.xml;...  
18 00 0F 01 69 6C 6C 75 73 74 72 61 74 6F 72 2E ....illustrator.  
78 6D 6C 00 B4 0A 00 00 48 00 3E 01 76 6E 64 2E xml.'...H.>.vnd.  
6F 70 65 6E 78 6D 6C 66 6F 72 6D 61 74 73 2D 6F openxmlformats-o  
66 66 69 63 65 64 6F 63 75 6D 65 6E 74 2E 70 72 fficedocument.pr  
65 73 65 6E 74 61 74 69 6F 6E 6D 6C 2E 73 6C 69 esentationml.sli  
64 65 73 68 6F 77 2E 78 6D 6C 00 00 97 0A 00 00 deshow.xml..=...  
64 65 73 68 6F 77 2E 78 6D 6C 00 00 97 0A 00 00
```

journal 파일 내의 디코딩 텍스트. 파일 시그니처는 어떤 것과도 일치하지 않는다.

```
) ¶„Cf.....  
3 ...../lib/sys  
4 temd/system/syst  
5 emd-timesyncd.se  
) rvice.....  
-
```

이런 걸 보면 뜯어보면 뭔가 있을 것도 같은데!

 out.qoi

qoi 파일.

```
qoif.....þ  
PNþG..þ...þ...þI  
HDþR..þ.þ.þ...þ.  
..þ..Óþ.±·þ...þ.  
IDþATxþøiþþC-(þ€  
..þÀþþþ·þþÛþmþþ  
w.þþ.þþ.þ.þ.þ.þ  
..þ...þ...þ.þ.þ.þ  
.þþþþþþþþþþþþþþ
```

이거 png파일 구조 아닌가?