

삼성 스마트폰에서 생성된 통화녹음파일에 대한 위변조 검출을 위한 법과학적 분석 방법

박 남 인*, 이 지 우*, 김 진 환*, 임 재 성*, 나 기 현**, 전 옥 엽**
국립과학수사연구원 디지털과 (공업연구사)*, (공업연구관)**

Forensic Analysis Method for Forgery Detection of Call Recordings Generated by Samsung Smartphones

Nam In Park*, Ji Woo Lee*, Jin-Hwan Kim*, Jae Sung Lim*, Gi-Hyun Na**, Oc-Yeub Jeon**
Digital Analysis Section, National Forensic Service (Researcher)*, (Senior Researcher)**

요 약

스마트폰의 대중화로 인해 스마트폰을 이용한 범죄가 늘어나고 있다. 특히 안드로이드 계열의 스마트폰은 통화 녹음 기능을 내장하고 있기 때문에 통화녹음 파일에 대한 증거물 확보가 매우 중요하다. 이렇게 수집된 디지털 증거물은 법적 효력을 갖기 위해, 무결성이 보장되어야 한다. 본 논문에서는 삼성 스마트폰에 기본 내장된 통화기능에서 제공하는 통화녹음 파일에 대한 위변조 분석 방법에 대해 제안하였다. 제안한 위변조 분석 방법은 통화녹음 파일에 대한 분석과 통화녹음 파일이 기록된 스마트폰 내의 미디어로그 및 통화 내역 분석으로 구분된다. 먼저, 정상통화녹음 파일에 대한 오디오 대역폭, 음성 지연 구간, 파일 구조 및 통화녹음 파일을 기록한 스마트폰에 미디어로그 및 통화 내역 등을 분석하였다. 그 후, 스마트폰에서 제공하는 편집기능을 통해 통화녹음파일을 편집하였을 때, 음성 지연 구간, 파일 구조 및 스마트폰에 기록된 미디어로그와 통화 내역의 변화를 비교분석하였다. 그 결과, 통화녹음 파일에 대해 임의로 조작을 가했을 때, 음성 지연 구간, 파일 구조 및 스마트폰 내에 미디어로그의 시간 정보가 변경되는 것이 확인되었다. 이러한 방법으로 통화녹음 파일에서 추출한 시간 정보들과 해당 파일이 기록된 스마트폰의 미디어로그 및 통화 내역의 시간정보가 일치하는지와 파일 구조와 음향학적 특성을 이용해서, 제시된 통화녹음파일의 진본임을 확인하였다.

주제어 : 통화녹음, 음성 편집 여부, 스펙트로그램 분석, 파일 구조 분석, 통화 내역 분석

ABSTRACT

Due to the popularization of smartphones, crime using smartphones is increasing. In particular, since Android-based smartphones have a built-in call recording function, it is very important to secure evidence for the call recording file. For the digital evidence collected in this way to have legal effect, its integrity must be guaranteed. In this paper, we propose a forgery analysis method for call recordings generated by the built-in call function of Samsung smartphones. The proposed forgery analysis method is divided into the analysis of the call recordings itself and the media-log and call history analysis in the smartphone with the call recording. First, we analyzed the audio bandwidth of the normal call recording, the audio latency, the file structure, and the media-log, and call history in the smartphone that includes the call recordings. After that, we compared and analyzed the difference of the audio latency, the file structure, the media-log, and call history when the call recording was edited through the editing function provided by the smartphone. As a result, it was confirmed that time information of the audio latency time, file structure and media-log in the smartphone were changed when an arbitrary manipulation was applied to the call recording. In this way, we can classify the forensic authentication as comparing the time information extracted from the call recording and the media-log/call history in smartphone with the call recordings plus analyzing the file structure and acoustic characteristics.

Key Words : call recording, speech forgery detection, spectrogram analysis, file structure analysis, call history analysis

※ 이 논문은 행정안전부 주관 국립과학수사연구원 중장기과학수사감정기법연구개발(R&D)사업의 지원을 받아 수행한 연구임 (NFS2022DTB03).
• 제1저자(First Author) : Nam In Park (Email : namin.park@gmail.com)
• 교신저자(Corresponding Author) : Oc-Yeub Jeon (Email : yeubjeon@korea.kr)

I. 서 론

최근 스마트폰을 이용한 금융사기 범죄가 증가하면서 스마트폰의 통화녹음파일은 증거물로서 활용도가 높아지고 있다. 통화녹음은 스마트폰의 음성메모 및 음성녹음과는 달리 송수화자 통화 중에만 수행되는 특징이 있다. 이렇게 녹음된 통화녹음파일은 스마트폰에서 기본 제공하는 편집 기능을 통해 추가적인 어플리케이션을 사용하지 않아도 일반 사용자에게 의해 위·변조가 쉽게 가능하여 수사에 어려움을 초래한다 [1]. 따라서, 통화녹음파일이 최초 생성된 후, 수사기관에 디지털 증거물로서 제출되기 전까지 해당 증거물은 소유자에 의해 악의적으로 편집될 수 있기 때문에, 증거물 관리의 연속성 측면에서, 제시된 디지털 증거물이 위·변조되지 않은 진본임을 확인하는 과정이 매우 중요하다 [2]. 아이폰의 경우, 개인 사생활 보호 등의 이유로 통화 녹음을 지원하지 않지만, 안드로이드 계열인 삼성 스마트폰에서는 통화녹음 기능을 기본적으로 지원한다. 또한, 국내 스마트폰 시장점유율도 아이폰에 비해 월등히 많기 때문에, 수사기관에서 증거물로서 제시된 통화녹음파일의 위·변조 분석에 대한 연구가 필요하다 [3].

최근에는 디지털 오디오 파일에 대한 무결성 입증 방법으로 데이터의 저작권 정보에 대해 암호화 코드를 삽입하는 디지털워터마킹 기술들이 연구되었으나, 문서 보안 음원 저작권 관련 사업 등에 한정되어 있다 [4]. 또한, 딥러닝의 급속한 발전으로 인해, 디지털 오디오의 위변조 여부를 학습에 의한 방법으로 접근하는 연구가 활발히 이루어지고 있다 [5]. 그러나, 대부분의 연구는 디지털 오디오에서 인위적으로 음성 신호가 혹은 배경잡음 등이 삽입된 경우에 검출하는 방법을 제시하였으며, 실제로 디지털 오디오 파일에서 특정 구간을 정교히 삭제하였을 경우, 일반적인 오디오 편집 특성으로 볼수 있는 스펙트로그램 상의 불연속성이 확인되지 않는다 [5-7]. 디지털 증거물의 법과학적 위·변조 분석을 위해, 전통적인 방법으로 파일 구조 분석 및 스펙트로그램 분석에 의한 검출 방법이 연구되었다 [1,7,8]. 특히, 김경화[7]는 삼성 스마트폰에서 녹음된 일반녹음 파일의 파일 구조 측면에서 일반 녹음파일이 위·변조되었을 때의 파일 구조를 분석하였고, 박남인 등[8]은 오디오 파일의 위·변조 검출을 위해 모바일 포렌식을 추가로 도입한 최초의 연구이지만, 분석 대상이 아이폰의 음성메모 앱으로 녹음된 음성 파일에 한정되었다.

본 논문에서는 삼성 스마트폰으로 녹음된 통화녹음파일에 대한 편집 여부 검출 방법을 제안한다. 제안한 방법은 통화녹음파일에 대한 파일 구조, 음향 신호 및 모바일 포렌식기반의 미디어로그 분석으로 구성된다. 먼저 정상적으로 녹음된 통화녹음파일에 대한 특성을 알아보고, 삼성 스마트폰의 기본 제공하는 음성녹음 앱 등에서 위변조를 수행하여, 파일 구조, 음향 신호 및 미디어로그의 변화를 관찰하였다. 그 결과, 편집된 파일은 파일 구조에서 정상적인 통화녹음파일과 차이가 존재하였으며, 특히, 음성 지연 시간을 측정하면, 오디오 파일의 앞부분을 삭제하였는지 여부에 대해 확인이 가능하였다. 최종적으로 통화 내역 및 미디어로그를 확인함으로써, 통화녹음파일의 진위성을 강화할 수 있었다. 최종적으로 이러한 과정을 구조화하여 삼성 스마트폰으로 생성된 통화녹음 파일에 대한 편집 여부 분석 절차에 대해 정의하였다.

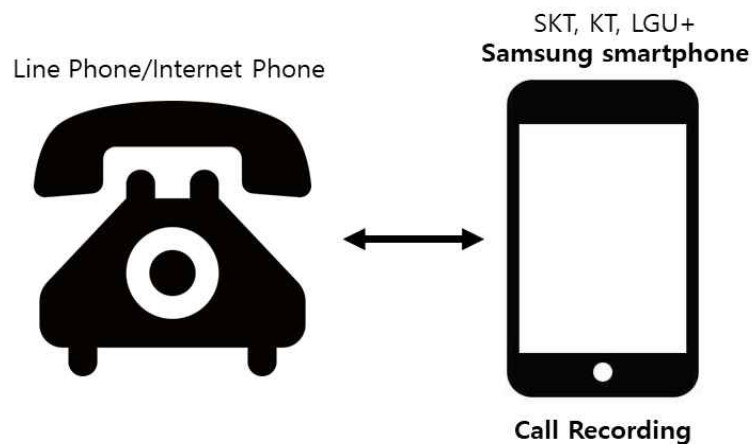
논문은 다음과 같은 형식으로 구성되어 있다. 2장에서는 삼성 스마트폰에서의 통화 녹음 방법 및 통화녹음파일의 특성에 대해서 소개하고, 3장과 4장에서 통화 녹음파일이 편집되었을 때의 파일 구조, 음향 신호 및 스마트폰 내의 미디어로그의 특징 변화 및 제안한 통화녹음파일의 위변조 검출 분석 절차에 대해 기술하면서 5장에서 결론을 맺는다.

II. 삼성 스마트폰에서 생성된 통화녹음 파일 데이터 수집

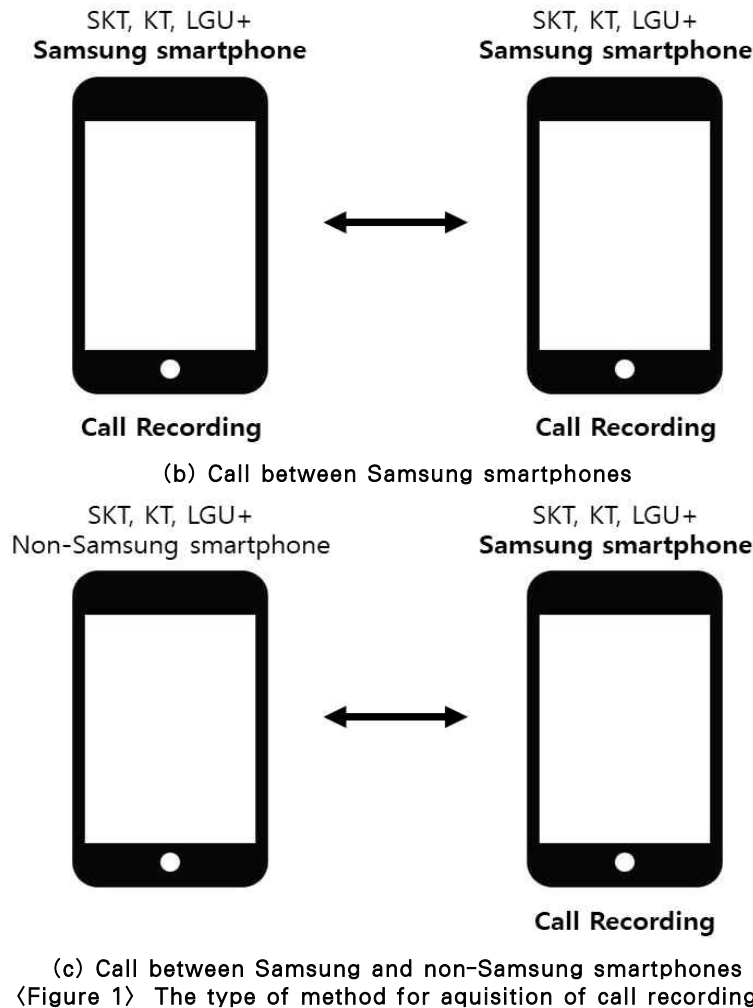
[표1]은 통화녹음 파일 수집을 위해 디바이스 정보를 나타낸다. 11대의 안드로이드 계열의 삼성 스마트폰을 사용하였으며, 일부 LG (1대) 및 애플사의 아이폰(3대), 그리고 유선전화를 비교 분석을 위해 실험에 추가하였다. 안드로이드계열의 스마트폰을 통화 녹음 기능이 있지만, iOS 계열의 스마트폰 및 실험에 사용된 유선전화([표1]의 16)는 녹음 기능을 제공하고 있지 않기 때문에, 통신 연결 용도로만 사용하였다. [그림1]은 실험데이터를 얻기 위한 방법에 대해 도식화한 것이다. [그림1]의 (a)와 같이 우선 유선전화와 3개의 통신사(SKTEL, KT, LGU+)에 등록된 삼성 스마트폰 간의 통화 녹음 파일을 획득하였고, [그림1]의 (b)에서 보는 바와 같이 3개의 통신사(SKTEL, KT, LGU+)에 등록된 삼성 스마트폰 간에 통화 녹음 및 [그림1]의 (c)와 같이 3개의 통신사(SKTEL, KT, LGU+)에 등록된 삼성 스마트폰 및 그 외 스마트폰(LG 스마트폰 및 아이폰) 간에 통화 녹음 파일을 30초 분량으로 각각 2개씩 총 330개의 통화 녹음 파일을 획득하였다.

〈Table 1〉 Device specification and its telecommunication company used for experiments.

No	Model	OS type and version	Mobile carrier	Remark
1	Samsung galaxy S10+	Android 11.0.0	KT	Provision of call recording function
2	삼실 갤럭시 Note10+	Android 10.0.0	SKT	
3	Samsung galaxy S9	Android 11.0.0	SKT	
4	Samsung galaxy S21	Android 12.0.0	LGU+	
5	Samsung galaxy S10+	Android 11.0.0	LGU+	
6	Samsung galaxy Note20	Android 11.0.0	LGU+	
7	Samsung galaxy S10 LTE	Android 11.0.0	KT	
9	Samsung galaxy S10+ 5G	Android 11.0.0	KT	
10	Samsung galaxy S7 Edge	Android 8.0.0	SKT	
11	Samsung galaxy Note10 5G	Android 11.0.0	SKT	
12	LG V50	Android 11.0.0	KT	
13	iPone 8	iOS 14.4.2	SKT	No call recording function
14	iPone 11	iOS 14.4.2	KT	
15	iPone 11	iOS 15.1	KT	
16	Other (Internet Phone)	-	-	



(a) Call between line phone and Samsung smartphone

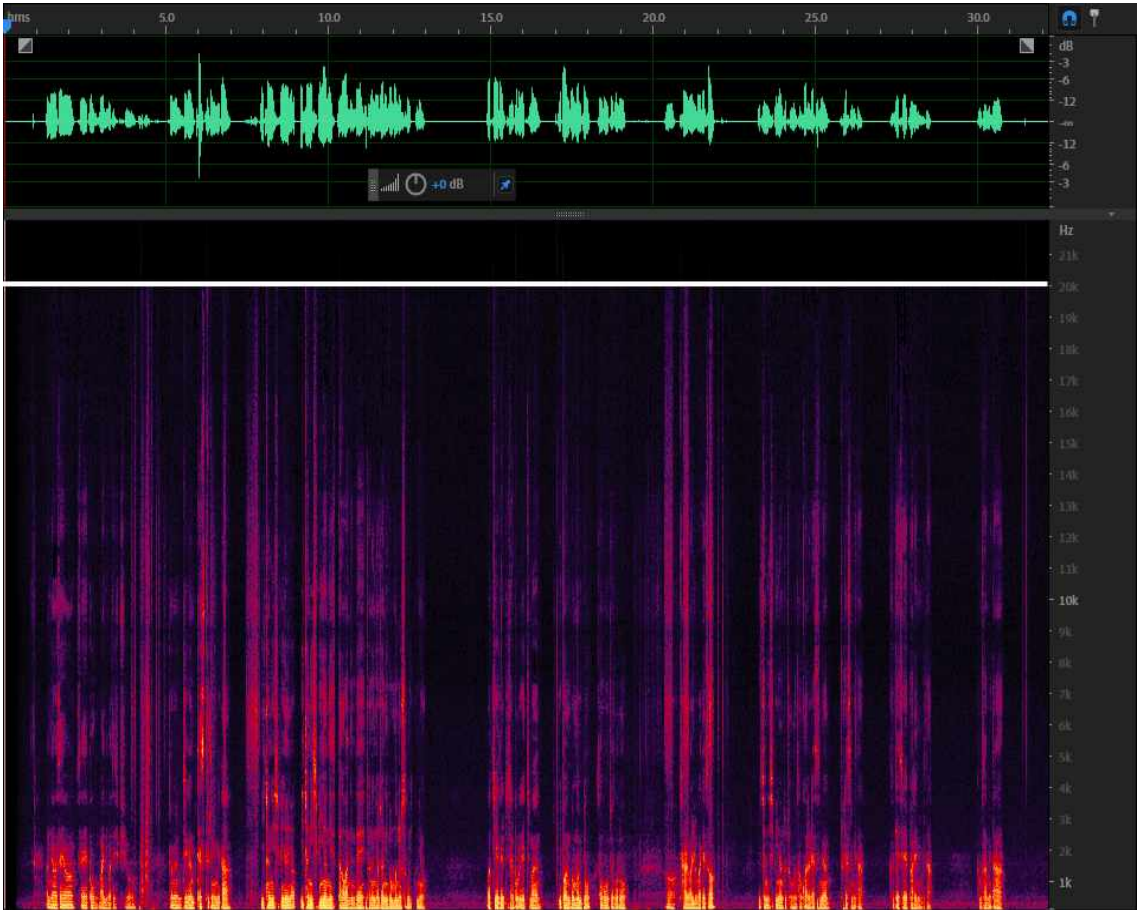


III. 삼성 스마트폰에서 생성된 통화녹음 파일 데이터 수집

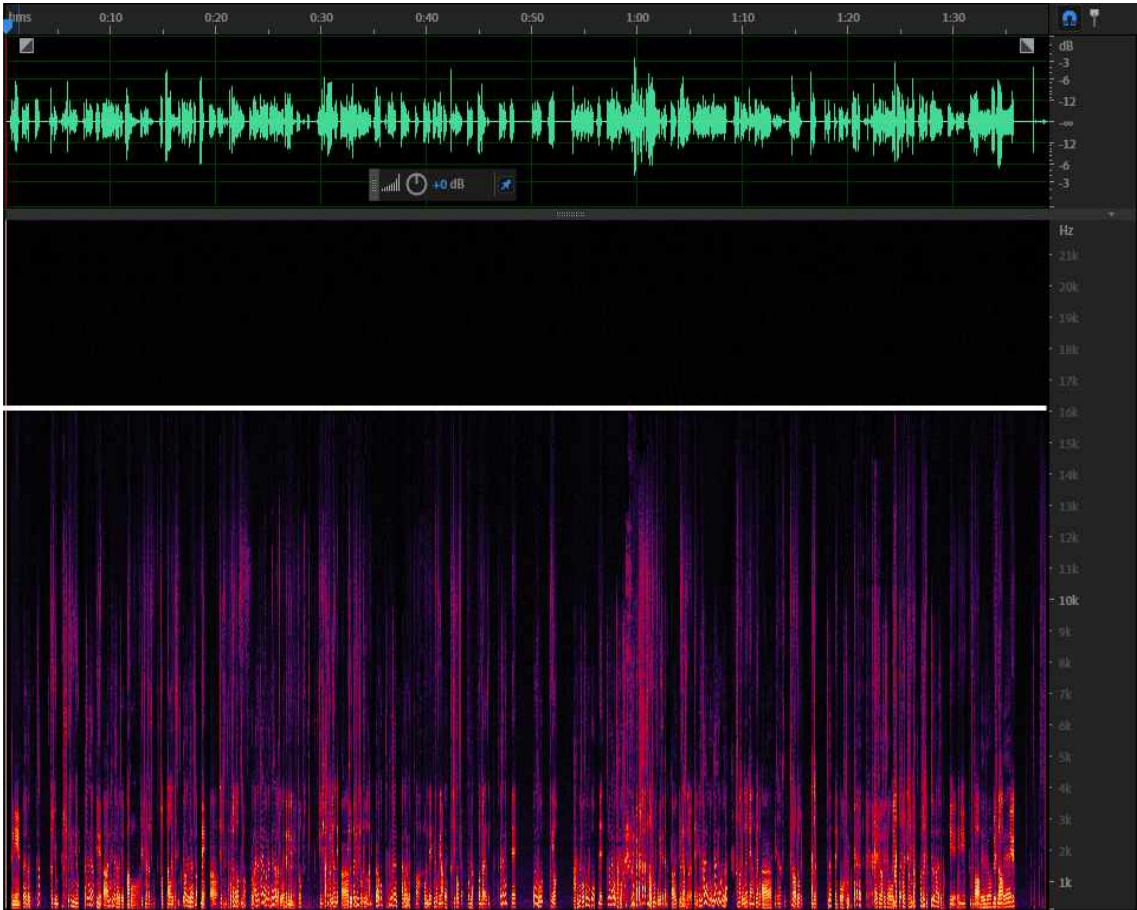
본 장에서는 삼성 스마트폰에 기본 탑재된 전화 어플리케이션의 통화녹음 기능을 통해 녹음한 음성 파일에 대한 오디오 대역폭, 파일 구조의 특징 및 스마트폰 내의 미디어로그 및 통화내역 특징에 대해 살펴본다.

3.1. 통화녹음파일의 오디오 대역폭

삼성 스마트폰으로 녹음된 통화녹음파일의 주파수 대역폭은 기본적으로 크게 3가지 형태로 나타난다. 삼성 스마트폰의 일반 녹음파일과 비교하였을 때와 가장 큰 차이점은 파일의 포맷은 m4a형태로 서로 동일하나, 기록 가능한 오디오 대역폭이 다르다는 것이다. [그림2]는 [표1]의 11로 녹음한 일반 녹음 파일을 오디오 대역폭을 보여준다 [9]. [그림2]의 흰색선으로 나타낸 바와 같이 일반녹음의 경우, 샘플링 레이트 44.1 kHz로 구성되어 있으며, 녹음 가능한 오디오 대역폭은 약 20 kHz로 확인된다. [그림3]은 [표1]의 11에 기본 탑재된 전화 어플리케이션의 통화녹음 기능을 통해 획득된 통화녹음파일의 스펙트로그램을 보여준다. 그림에서 보는 바와 같이, 샘플링 레이트는 44.1 kHz로 일반 녹음 파일의 샘플링 레이트는 동일하지만, [그림3]의 흰색선으로 나타낸 바와 같이 통화 채널에 따라 기록가능한 오디오 대역폭이 약 4 kHz, 약 8 kHz 및 약 16 kHz 이 내로 분포하는 형태를 보여주고 있다. 통화 채널이 LTE(Long-Term Evolution)로 연결되어 있을 경우, [그림3](a)와 (b)에서 보는 바와 같이, 통화녹음이 고품질 광대역 음성[10]으로 녹음되지만, 유선전화 및 스마트폰이 LTE(Long-Term Evolution)이 아닌 3G로 통화가 연결될 경우, 통화 품질이 4 kHz 이하로 매우 떨어지는 것이 확인할 수 있었다. 여기서, 송수화자 중 어느 한쪽이 3G 혹은 유 선 전화로 연결되었을 경우, 통화 품질 역시 기록가능한 오디오 대역폭이 4 kHz 이하로 음질 열화가 발생한다.



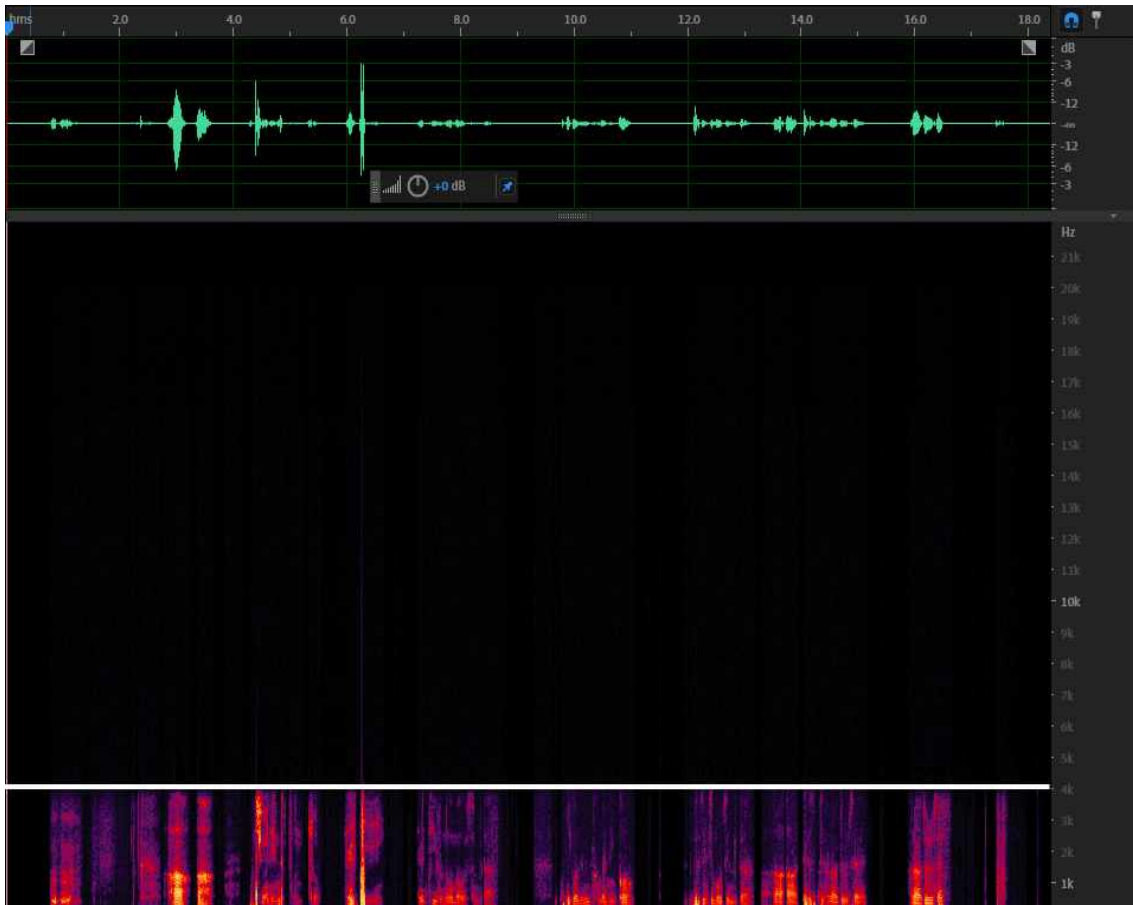
〈Figure 2〉 Spectrogram of audio recording obtained from Samsung smartphone(Samsung Galaxy Note10 5G).



(a) Recordable speech bandwidth: below around 16 kHz



(b) Recordable speech bandwidth: below around 8 kHz

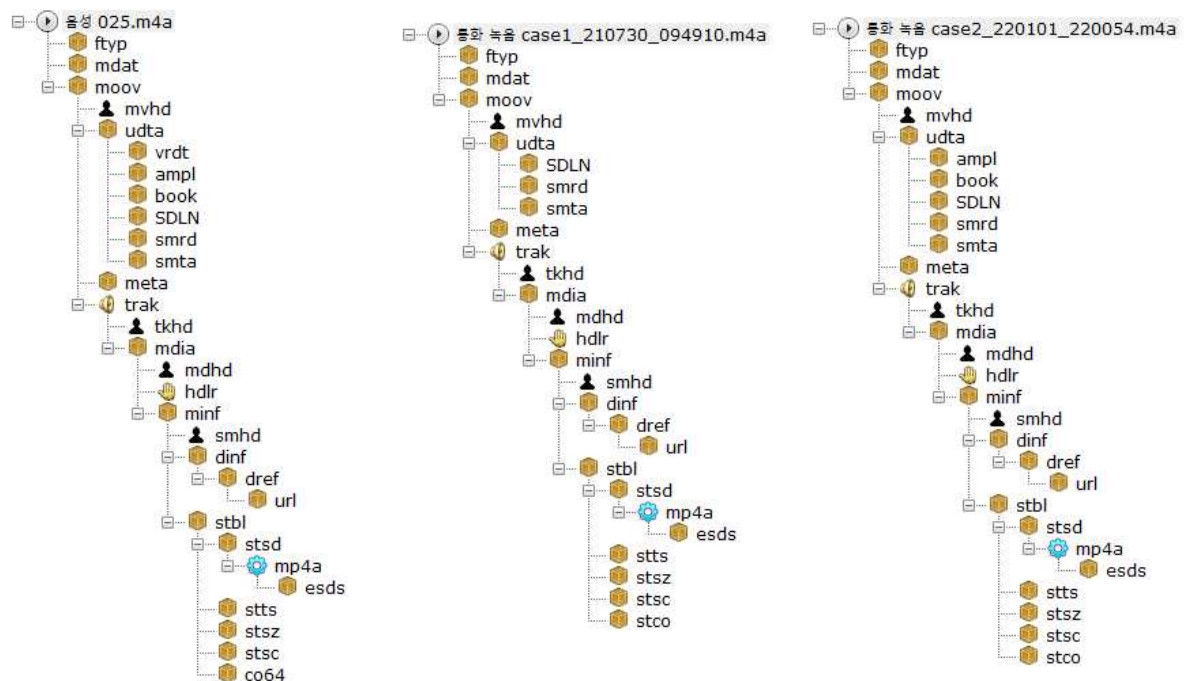


(c) Recordable speech bandwidth: below around 4 kHz

〈Figure 3〉 Spectrogram type of audio recording obtained from Samsung smartphone(Samsung Galaxy Note10 5G).

3.2. 통화녹음파일의 파일 구조 특징

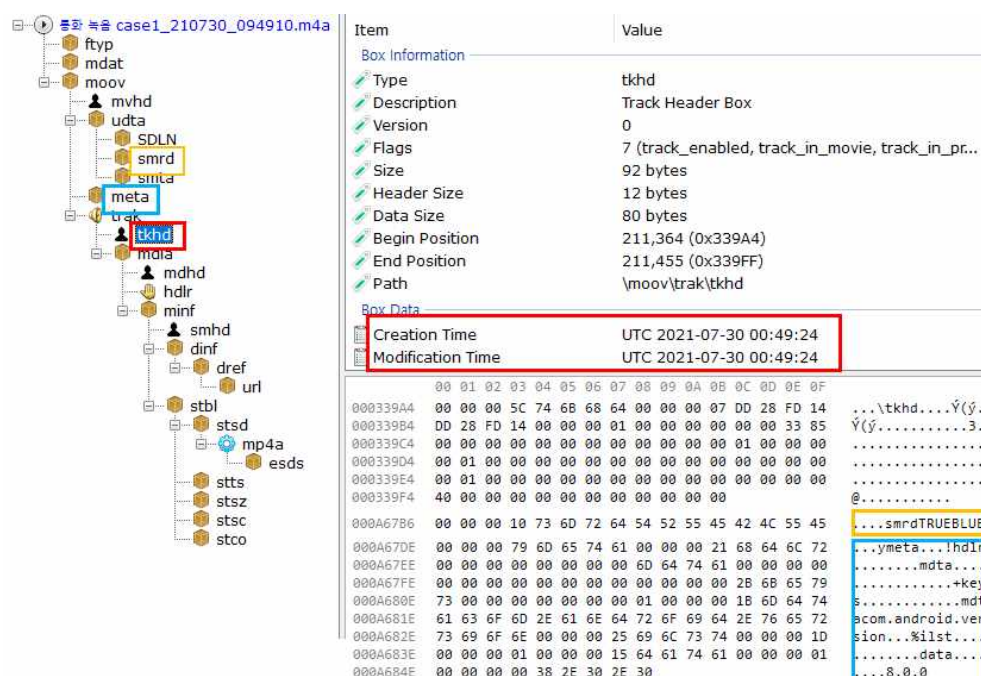
일반 녹음파일과 통화녹음파일의 파일 구조는 MP4 Inspector[11]를 통해 [그림4]이 확인할 수 있다. 일반적인 m4a형태와 동일하게 파일의 호환성을 확인하는 정보가 담긴 "\ftyp", 실제 미디어를 저장하는 "\mdat", 미디어의 모든 메타 데이터를 저장하는 "\moov" atom으로 구성된다 [12]. 그림에서와 같이 파일 구조상의 모든 atom은 동일하나, "\moov\udta\"의 하위 atom 구조가 일반 녹음파일과 통화녹음파일이 차이가 발생하며, 통화녹음파일의 파일 구조에서도 2가지 특징이 나타난다. 이에 대해서는 4.2 절에서 자세히 설명한다. 따라서, 파일 구조 분석만을 통해 해당 파일이 일반 녹음파일인지 혹은 통화 녹음파일인지 구분이 가능하다.



(a) File structure format of general audio recordings

(b) File structure format of call recordings

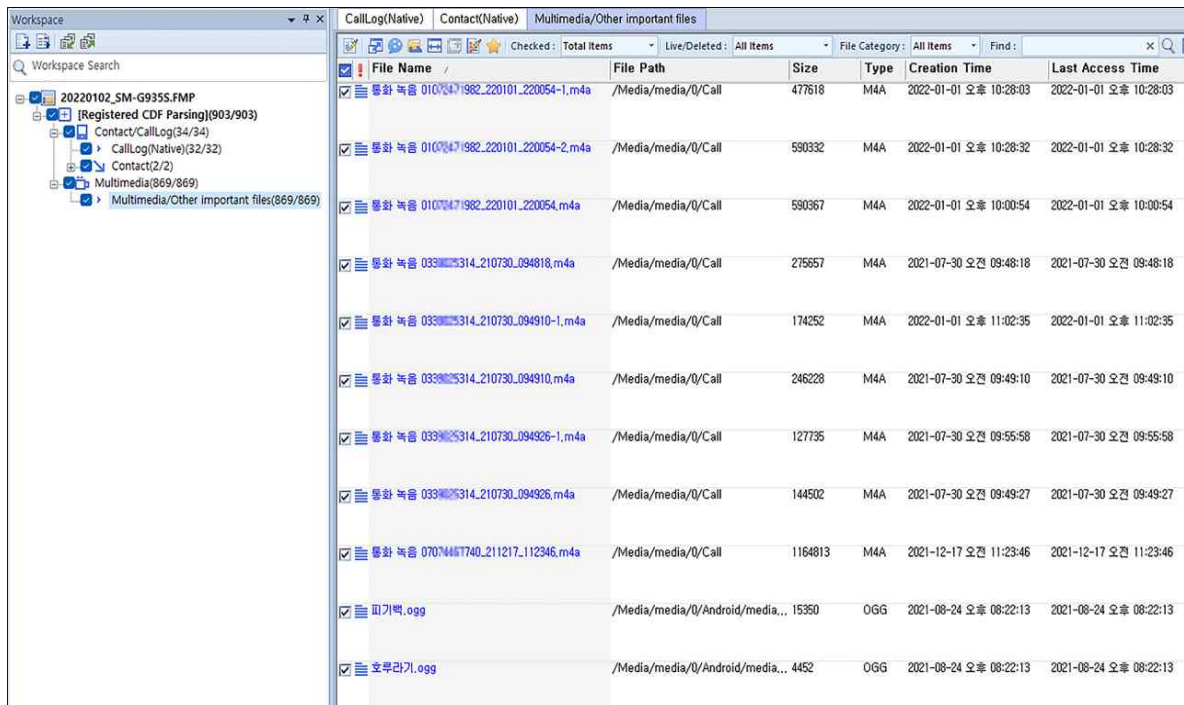
〈Figure 4〉 File structure comparison of audio recordings and call recordings.



⟨Figure 5⟩ Metadata included in file structure of call recordings.

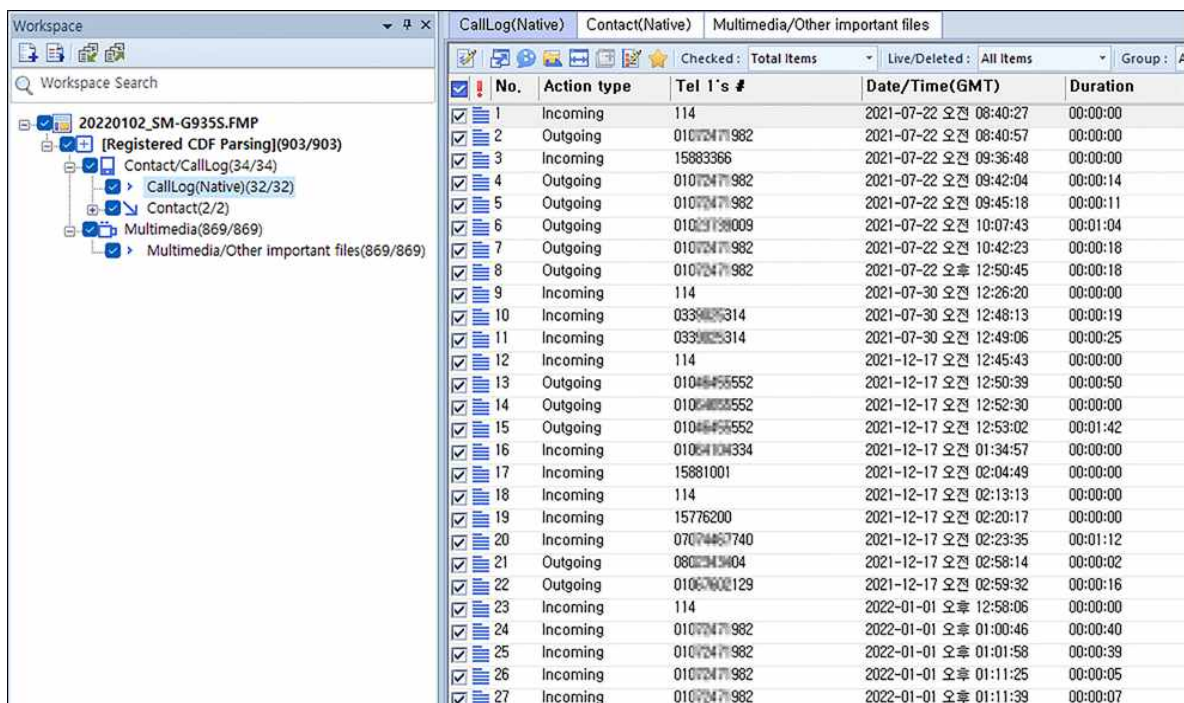
[그림5]는 통화녹음파일의 파일 구조 및 통화녹음파일에서 확인되는 메타데이터를 보여준다. 일반적으로 통화녹음파일의 메타데이터로 해당 통화녹음파일이 저장된 시점이 “\moov\trak\tkhd” atom에 기록된다. 그림에서 해당 파일이 최초 종료되어 저장된 시점은 시계협정시(UTC)기준 [2021-07-30 00:49:24]로 확인되며, 이를 한국표준시(KST)로 변환하면 +9시간을 적용하여 [2021-07-30 09:49:24]이다. 또한, “\moov\udta\smrd” atom에는 “TRUEBLUE”라는 삼성 스마트폰으로 녹음된 오디오 파일에서 나타나는 고유 식별자가 확인되며, 최종적으로 “\moov\meta” atom에는 해당 삼성 스마트폰의 안드로이드 버전 정보가 기록되어 있다. 현재 안드로이드 버전 정보는 “8.0.0”으로 확인된다.

3.3. 스마트폰 내의 미디어로그 및 통화 내역 분석



File Name	File Path	Size	Type	Creation Time	Last Access Time
통화 녹음 01072471982_220101_220054-1.m4a	/Media/media/0/Call	477618	M4A	2022-01-01 오후 10:28:03	2022-01-01 오후 10:28:03
통화 녹음 01072471982_220101_220054-2.m4a	/Media/media/0/Call	580332	M4A	2022-01-01 오후 10:28:32	2022-01-01 오후 10:28:32
통화 녹음 01072471982_220101_220054.m4a	/Media/media/0/Call	580367	M4A	2022-01-01 오후 10:00:54	2022-01-01 오후 10:00:54
통화 녹음 0339025314_210730_094818.m4a	/Media/media/0/Call	275557	M4A	2021-07-30 오전 09:48:18	2021-07-30 오전 09:48:18
통화 녹음 0339025314_210730_094910-1.m4a	/Media/media/0/Call	174252	M4A	2022-01-01 오후 11:02:35	2022-01-01 오후 11:02:35
통화 녹음 0339025314_210730_094910.m4a	/Media/media/0/Call	246228	M4A	2021-07-30 오전 09:49:10	2021-07-30 오전 09:49:10
통화 녹음 0339025314_210730_094926-1.m4a	/Media/media/0/Call	127735	M4A	2021-07-30 오전 09:55:58	2021-07-30 오전 09:55:58
통화 녹음 0339025314_210730_094926.m4a	/Media/media/0/Call	144502	M4A	2021-07-30 오전 09:49:27	2021-07-30 오전 09:49:27
통화 녹음 07074457740_211217_112346.m4a	/Media/media/0/Call	1164813	M4A	2021-12-17 오전 11:23:46	2021-12-17 오전 11:23:46
피기백.ogg	/Media/media/0/Android/media...	15350	OGG	2021-08-24 오후 08:22:13	2021-08-24 오후 08:22:13
호무라기.ogg	/Media/media/0/Android/media...	4452	OGG	2021-08-24 오후 08:22:13	2021-08-24 오후 08:22:13

〈Figure 6〉 Example of media-log.



No.	Action type	Tel l's #	Date/Time(GMT)	Duration
1	Incoming	114	2021-07-22 오전 08:40:27	00:00:00
2	Outgoing	01072471982	2021-07-22 오전 08:40:57	00:00:00
3	Incoming	15883366	2021-07-22 오전 09:36:48	00:00:00
4	Outgoing	01072471982	2021-07-22 오전 09:42:04	00:00:14
5	Outgoing	01072471982	2021-07-22 오전 09:45:18	00:00:11
6	Outgoing	01072471982	2021-07-22 오전 10:07:43	00:01:04
7	Outgoing	01072471982	2021-07-22 오전 10:42:23	00:00:18
8	Outgoing	01072471982	2021-07-22 오후 12:50:45	00:00:18
9	Incoming	114	2021-07-30 오전 12:26:20	00:00:00
10	Incoming	0339025314	2021-07-30 오전 12:48:13	00:00:19
11	Incoming	0339025314	2021-07-30 오전 12:49:06	00:00:25
12	Incoming	114	2021-12-17 오전 12:45:43	00:00:00
13	Outgoing	0104455552	2021-12-17 오전 12:50:39	00:00:50
14	Outgoing	0104455552	2021-12-17 오전 12:52:30	00:00:00
15	Outgoing	0104455552	2021-12-17 오전 12:53:02	00:01:42
16	Incoming	0106104334	2021-12-17 오전 01:34:57	00:00:00
17	Incoming	15881001	2021-12-17 오전 02:04:49	00:00:00
18	Incoming	114	2021-12-17 오전 02:13:13	00:00:00
19	Incoming	15776200	2021-12-17 오전 02:20:17	00:00:00
20	Incoming	07074457740	2021-12-17 오전 02:23:35	00:01:12
21	Outgoing	0802343404	2021-12-17 오전 02:58:14	00:00:02
22	Outgoing	01067602129	2021-12-17 오전 02:59:32	00:00:16
23	Incoming	114	2022-01-01 오후 12:58:06	00:00:00
24	Incoming	01072471982	2022-01-01 오후 01:00:46	00:00:40
25	Incoming	01072471982	2022-01-01 오후 01:01:58	00:00:39
26	Incoming	01072471982	2022-01-01 오후 01:11:25	00:00:05
27	Incoming	01072471982	2022-01-01 오후 01:11:39	00:00:07

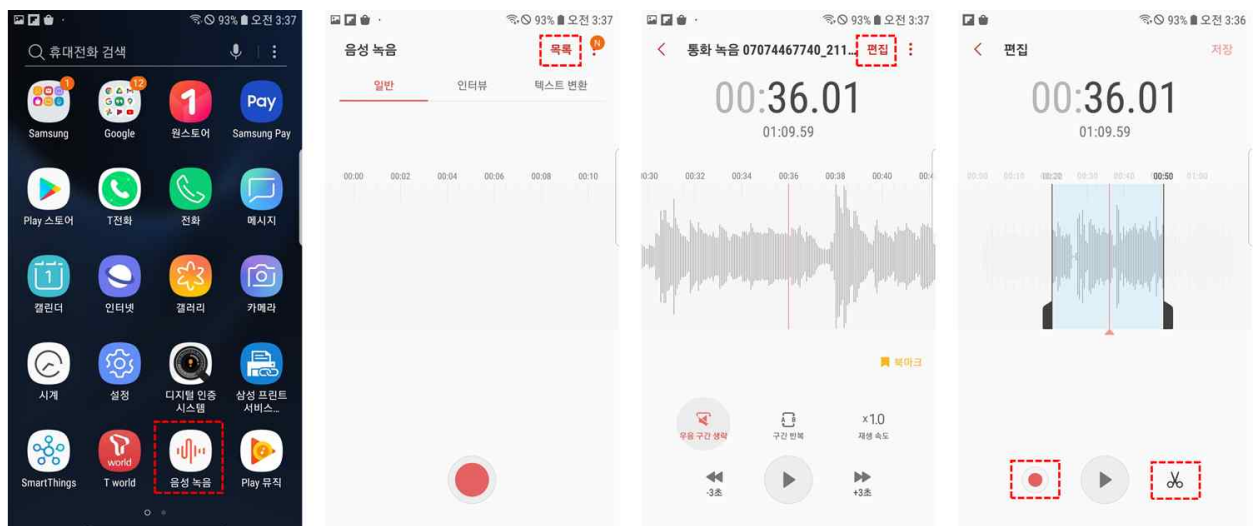
〈Figure 7〉 Example of call history.

통화녹음파일의 위변조 여부를 분석하기 위해, 가장 중요한 것은 해당 통화녹음파일을 실제로 녹음한 기기를 확보하는 것이다 [8]. 그 후, 검증된 모바일포렌식도구[13]을 통해, 해당 통화녹음파일에 대한 미디어로그를 분석해야 한다. [그림6]은 모바일포렌식도구를 통해 삼성 스마트폰에 기록된 미디어로그의 예시를 보여준다. 그림에서 보는 바와 같이, 통화녹음파일이 기록된 경로는 “/Media/media/0/Call”폴더에 기록되어 있으며, 본 논문에서 사용한 모바일포렌식도구에서는 “Creation Time”과 “Last Access Time”이라고 정의한 부분에는 통화녹음파일이 최초 생성된 시점 (녹음 시작 시점) 정보가 한국표준시(KST)로 기록되어 있다. 여기서, 기기의 시간 설정을 위한 위치 정보 혹은 사용자에게 의해 정의한 기기 시간 설정에 따라 시간 정보의 해석은 달라질 수 있다.

[그림7]은 모바일포렌식도구를 통해 삼성 스마트폰에 기록된 통화내역의 예시를 보여준다. 그림에서 보는 바와 같이, 송·수신 여부, 전화번호, 통화 시점 정보가 기록된다. 특히, 통화 시점 정보는 송신하는 시점 및 수신되는 시점의 시간 정보가 UTC 기준으로 기록되기 때문에, 본 예시에서는 9시간이 더해진 한국표준시(KST)로 변환해서 해석해야 한다. [그림6]과 [그림7]에 청색으로 표시된 항목은 통화녹음파일(“통화녹음_07074467740_20211217_112346.m4a”)의 미디어로그 및 통화내역을 보여준다. [그림6]과 [그림7]을 통해, 통화녹음파일(“통화녹음_07074467740_20211217_112346.m4a”)는 [2021-12-27, 11:23:35]경에 수신되었으며, 약 1분12초간 통화가 진행된 것이 통화내역에서 확인된다. 녹음된 통화녹음파일이 최초 생성된 시점 (녹음 시작 시점)은 미디어로그 상에서 [2021-12-27, 11:23:46]경이다.

IV. 통화녹음파일의 위변조에 대한 특징 변화

지금까지 정상적으로 녹음된 통화녹음파일의 스펙트로그램 특징, 파일 구조 특징 및 해당 통화녹음파일을 기록한 기기의 미디어로그 및 통화내역 분석에 대해 살펴보았다. 통화녹음파일은 스마트폰의 기본 탑재된 “음성 녹음” 어플리케이션을 통해 편집이 가능하다.

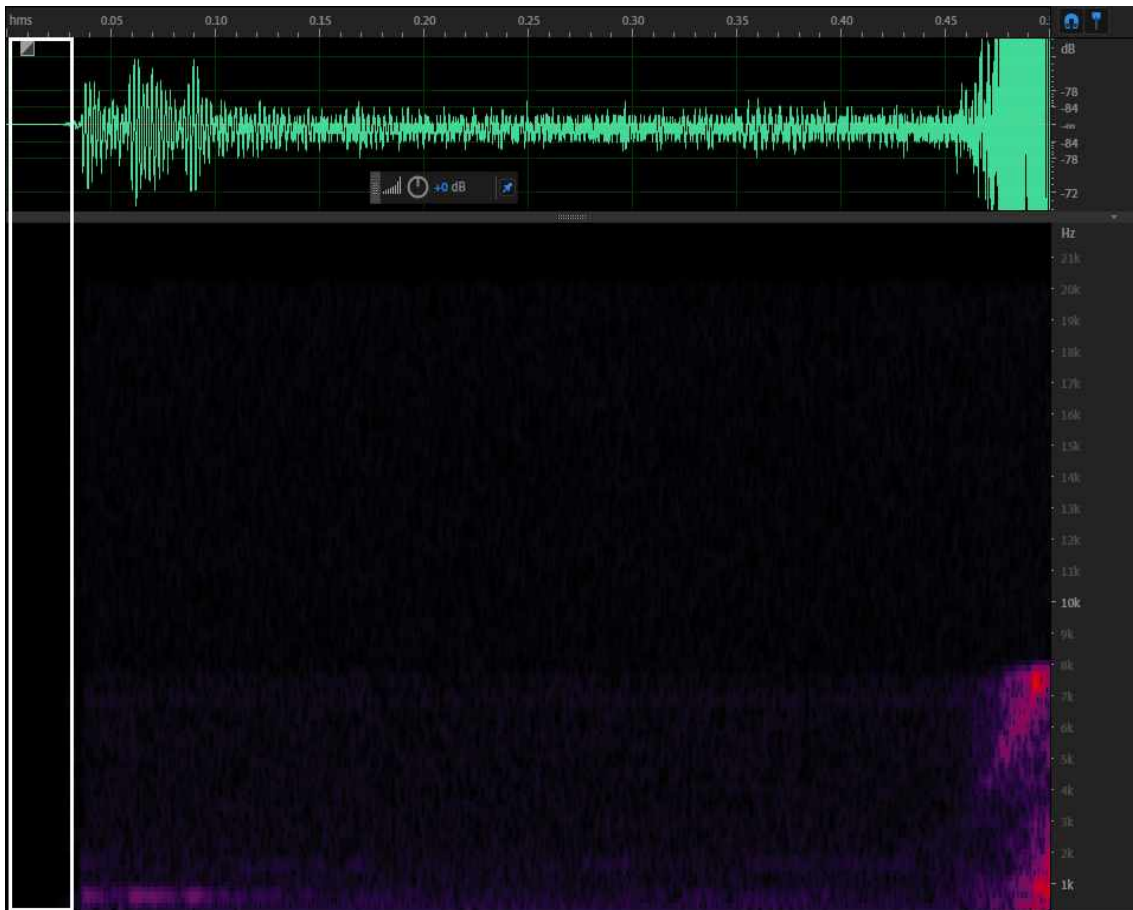


〈Figure 8〉 Manipulation method of call recordings by the built-in “Voice Recorder” application in Samsung smartphone.

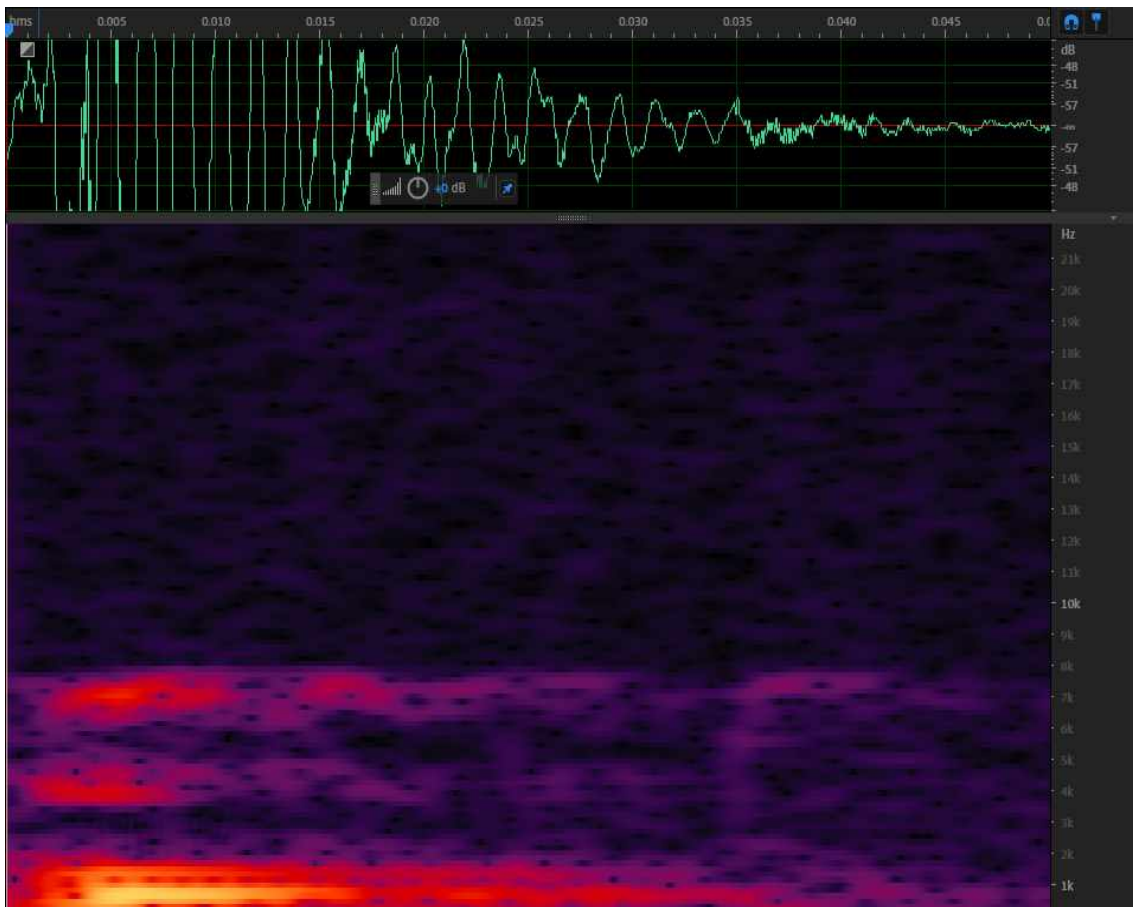
[그림8]에서 보는 바와 같이, 삼성 스마트폰에 기본 탑재된 “음성 녹음” 어플리케이션에서 “목록” 탭을 통해 통화녹음 파일을 불러올 수 있다. 그러면, 화면 상단에 “편집” 탭에 접근하면, 특정 지점에서 녹음 버튼을 통해 재녹음할 것인지 혹은 특정 구간을 삭제할 것인지 편집이 가능하다.

4.1. 통화녹음파일의 주파수 분포 변화

위변조 방법에 따라 주파수 분포의 특징은 크게 2가지 형태로 구분된다. 먼저, 통화녹음파일에서 앞부분을 삭제할 경우이다. [그림9](a)에서 보는 바와 같이, 편집되지 않은 정상적인 통화녹음파일은 약 23 ms의 zero-padding 구간이 발생한다. 그러나, [그림8]의 방법으로 통화녹음파일의 앞부분을 삭제할 경우, [그림9](b)에서 보는 바와 같이 zero-padding 구간이 삭제되기 때문에, 통화녹음파일의 스펙트로그램에서 최초 앞부분에 zero-padding이 존재하는지 여부가 위변조 검출 방법의 요소가 되기도 한다.



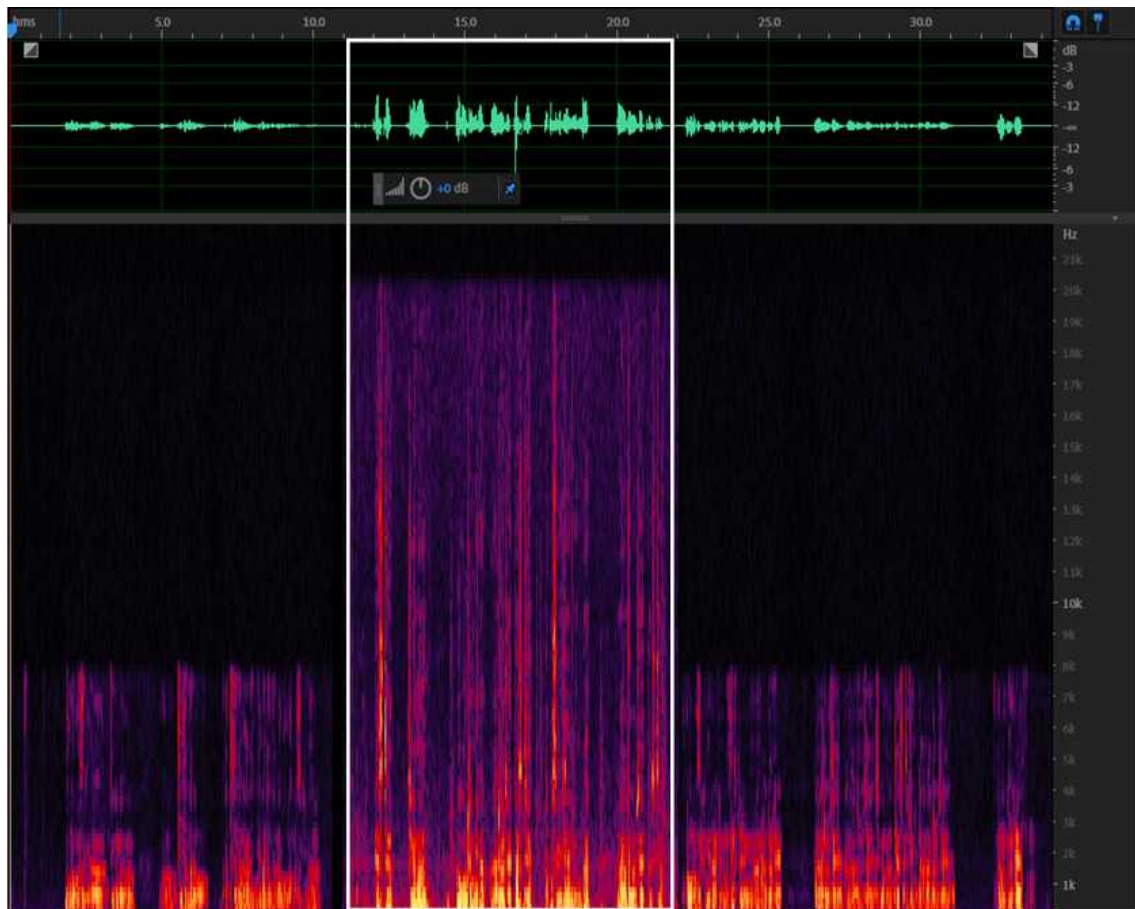
(a) Before manipulation



(b) After manipulation

〈Figure 9〉 Spectrogram characteristics when deleting the start part of call recordings.

두 번째 경우는 [그림8]의 방법으로 재녹음하는 경우이다. 위 3.1절의 [그림2]와 [그림3]에서 설명한 바와 같이 통화녹음파일에서 기록가능한 오디오 대역폭은 약 4 kHz, 8 kHz 및 16 kHz 이내이고, 삼성 스마트폰에서 제공하는 “음성 녹음” 어플리케이션을 통해 녹음된 일반 녹음파일의 기록가능한 오디오 대역폭은 약 20 kHz 이하이다. 통화녹음파일에 대해 “음성 녹음” 어플리케이션을 통해 재녹음을 하게 되면, [그림10]에서 보는 바와 같이 기록가능한 오디오 대역폭의 차이가 확인된다.

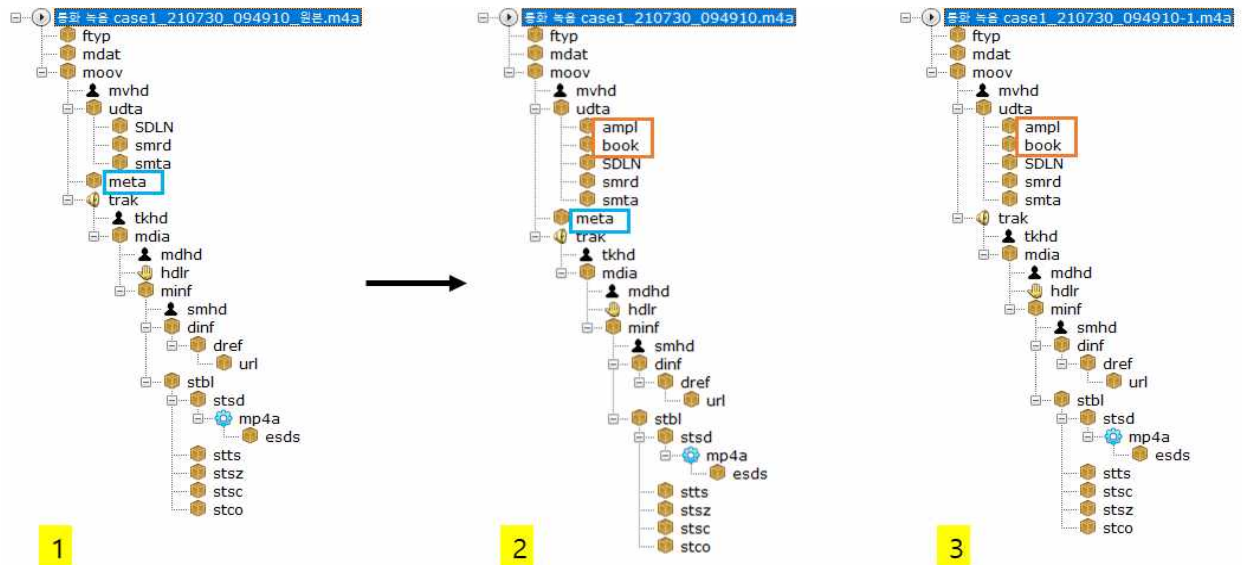


〈Figure 10〉 Spectrogram characteristics when re-recording the call recording at the specific part.

4.2 통화녹음파일의 파일 구조 변화

[그림11]은 통화녹음파일을 “음성 녹음” 어플리케이션을 통해 편집하였을 때의 파일 구조 특징을 보여준다. [그림11]의 1)은 편집없이 정상적으로 기록된 통화녹음파일의 파일 구조를 보여준다. [그림11]의 2)와 3)에 대한 파일 구조는 [그림11]의 1)을 “음성 녹음” 어플리케이션을 통해 편집한 후, “원본 파일 대체”가 아닌 “새 파일로 저장”할 경우, 생성되는 파일이다. 즉, [그림11]의 2)는 [그림11]의 1)과 서로 정확히 동일한 오디오 신호를 포함하고 있으며, [그림11]의 3)은 편집된 파일이다. 특히, “음성 녹음” 어플리케이션을 통해 편집을 수행할 경우, 원본([그림11]의 1))의 파일 구조가 [그림11]의 2)에서처럼 “\moov\udta”내의 sub-atoms의 변화가 되는 것을 확인할 수 있다. 또한, 편집된 파일 ([그림11]의 3)과 원본([그림11]의 1)과 2))와 비교했을 때, “\moov\meta” atom영역을 포함하고 있는지 여부에 따라 해당 통화녹음파일이 위변조 되었는지를 확인할 수 있다 [7].

[그림12]은 “음성 녹음” 어플리케이션을 통해 편집된 통화녹음파일에 기록된 시간정보를 보여준다. [그림12]에서 보는 바와같이, 최초 통화녹음은 세계협정시(UTC)기준 [2021-07-30 00:49:24]에 저장된 파일이며, 이후 [2022-01-01 14:02:35]에 수정되어 최종 저장된 파일이다. 이를 한국표준시(KST)로 변환하면 [2021-07-30, 09:49:24]에 최초 저장된 파일을 [2022-01-01 23:02:35]에 최종 수정되어 저장된 것으로 추정할 수 있다.



〈Figure 11〉 Type of file structure when manipulating the call recording through “Voice Recording”:
1) original, 2) target for manipulation, 3) manipulated call recording (“Save as new file”).

Item	Value
Box Information	
Type	tkhd
Description	Track Header Box
Version	0
Flags	15 (track_enabled, track_in_movie, track_in_p...
Size	92 bytes
Header Size	12 bytes
Data Size	80 bytes
Begin Position	172,304 (0x2A110)
End Position	172,395 (0x2A16B)
Path	\moov\trak\tkhd
Box Data	
Creation Time	UTC 2021-07-30 00:49:24
Modification Time	UTC 2022-01-01 14:02:35

〈Figure 12〉 Time information of manipulated call recording

4.3 스마트폰에서의 미디어로그 변화

[그림13]는 편집된 통화녹음파일의 미디어로그를 보여준다. 그림에서 “통화녹음 033xxxx314_210730_094910.m4a”는 미디어로그에서 한국표준시(KST)기준 [2021-07-30, 09:59:10]에 파일이 최초로 생성된 것으로 확인된다. [그림14]에서 보는 바와 같이 해당 녹음 파일의 파일 구조를 보면, 세계표준시(UTC)기준 [2021-07-30, 00:49:24]에 파일이 최종 저장된 것으로 확인되고, 이를 한국표준시(KST)로 변환하면 [2021-07-30, 09:49:24]이다.

File Name	File Path	Size	Type	Creation Time	Last Access Time
통화 녹음 010 982_220101_220054-1.m4a	/Media/media/0/Call	477618	M4A	2022-01-01 오후 10:28:03	2022-01-01 오후 10:28:03
통화 녹음 010 982_220101_220054-2.m4a	/Media/media/0/Call	590332	M4A	2022-01-01 오후 10:28:32	2022-01-01 오후 10:28:32
통화 녹음 010 982_220101_220054.m4a	/Media/media/0/Call	590367	M4A	2022-01-01 오후 10:00:54	2022-01-01 오후 10:00:54
통화 녹음 033 14_210730_094918.m4a	/Media/media/0/Call	275857	M4A	2021-07-30 오전 09:48:18	2021-07-30 오전 09:48:18
통화 녹음 033 14_210730_094910-1.m4a	/Media/media/0/Call	174252	M4A	2022-01-01 오후 11:02:35	2022-01-01 오후 11:02:35
통화 녹음 033 14_210730_094910.m4a	/Media/media/0/Call	246228	M4A	2021-07-30 오전 09:49:10	2021-07-30 오전 09:49:10
통화 녹음 033 314_210730_094926-1.m4a	/Media/media/0/Call	127735	M4A	2021-07-30 오전 09:55:58	2021-07-30 오전 09:55:58
통화 녹음 033 114_210730_094926.m4a	/Media/media/0/Call	144502	M4A	2021-07-30 오전 09:49:27	2021-07-30 오전 09:49:27
통화 녹음 070 740_211217_112346.m4a	/Media/media/0/Call	1164813	M4A	2021-12-17 오전 11:23:46	2021-12-17 오전 11:23:46

〈Figure 13〉 Example of media-log for manipulated call recording.

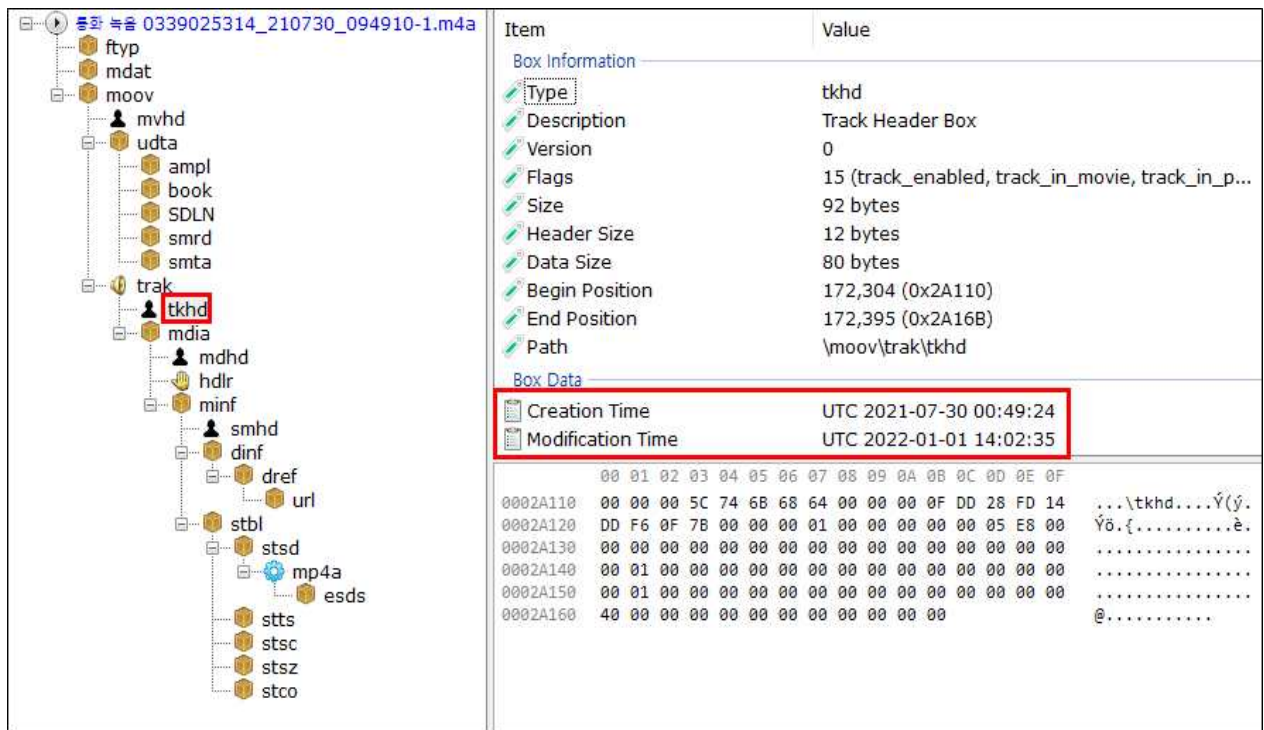
No.	Action type	Tel 1's #	Date/Time(GMT)	Duration
1	Incoming	114	2021-07-22 오전 08:40:27	00:00:00
2	Outgoing	010 1982	2021-07-22 오전 08:40:57	00:00:00
3	Incoming	15883366	2021-07-22 오전 09:36:48	00:00:00
4	Outgoing	010 1982	2021-07-22 오전 09:42:04	00:00:14
5	Outgoing	010 1982	2021-07-22 오전 09:45:18	00:00:11
6	Outgoing	010 3009	2021-07-22 오전 10:07:43	00:01:04
7	Outgoing	010 1982	2021-07-22 오전 10:42:23	00:00:18
8	Outgoing	010 1982	2021-07-22 오후 12:50:45	00:00:18
9	Incoming	114	2021-07-30 오전 12:26:20	00:00:00
10	Incoming	033 314	2021-07-30 오전 12:48:13	00:00:19
11	Incoming	033 314	2021-07-30 오전 12:49:06	00:00:25
12	Incoming	114	2021-12-17 오전 12:45:43	00:00:00
13	Outgoing	010 5552	2021-12-17 오전 12:50:39	00:00:50
14	Outgoing	010 5552	2021-12-17 오전 12:52:30	00:00:00

〈Figure 14〉 Information of call recording when extracting media-log.

Item	Value
Box Information	
Type	tkhd
Description	Track Header Box
Version	0
Flags	7 (track_enabled, track_in_movie, track_in_pr...
Size	92 bytes
Header Size	12 bytes
Data Size	80 bytes
Begin Position	243,521 (0x3B741)
End Position	243,612 (0x3B79C)
Path	\\moov\\trak\\tkhd
Box Data	
Creation Time	UTC 2021-07-30 00:49:24
Modification Time	UTC 2021-07-30 00:49:24

〈Figure 15〉 File structure of "CallRec 033xxxx314_210730_094910.m4a".

따라서, 본 논문에서 제안한 위변조 검출 방법에 의하면 총, 3가지 시간정보가 나오게 된다. 첫 번째, 파일 구조상에서 해당통화녹음파일이 최초 저장 완료된 시점 (T_{final}), 두 번째, 모바일포렌식을 통해 해당 기기를 분석했을 때, 통화내역상 송신 혹은 수신 시점($T_{t/r}$), 마지막으로 미디어로그에 기록된 통화녹음 파일이 최초로 생성된 시점 (T_{\in})을 확인할 수 있다. 따라서, 1) $T_{t/r}$ 은 T_{\in} 보다 최소한 같거나 빨라야 한다. 왜냐하면, 일반적으로 통화녹음은 상대방과 연결된 직후, 녹음이 되도록 하는 방법과 상대방과 연결 후, 사용자에게 의해 녹음하는 방법 2가지가 존재하기 때문이다. 추가적으로 저장된 시점이 파일 생성된 시점보다 나중에 발생하므로, 2) T_{\in} 시점이 T_{final} 보다 선행되어야 한다.



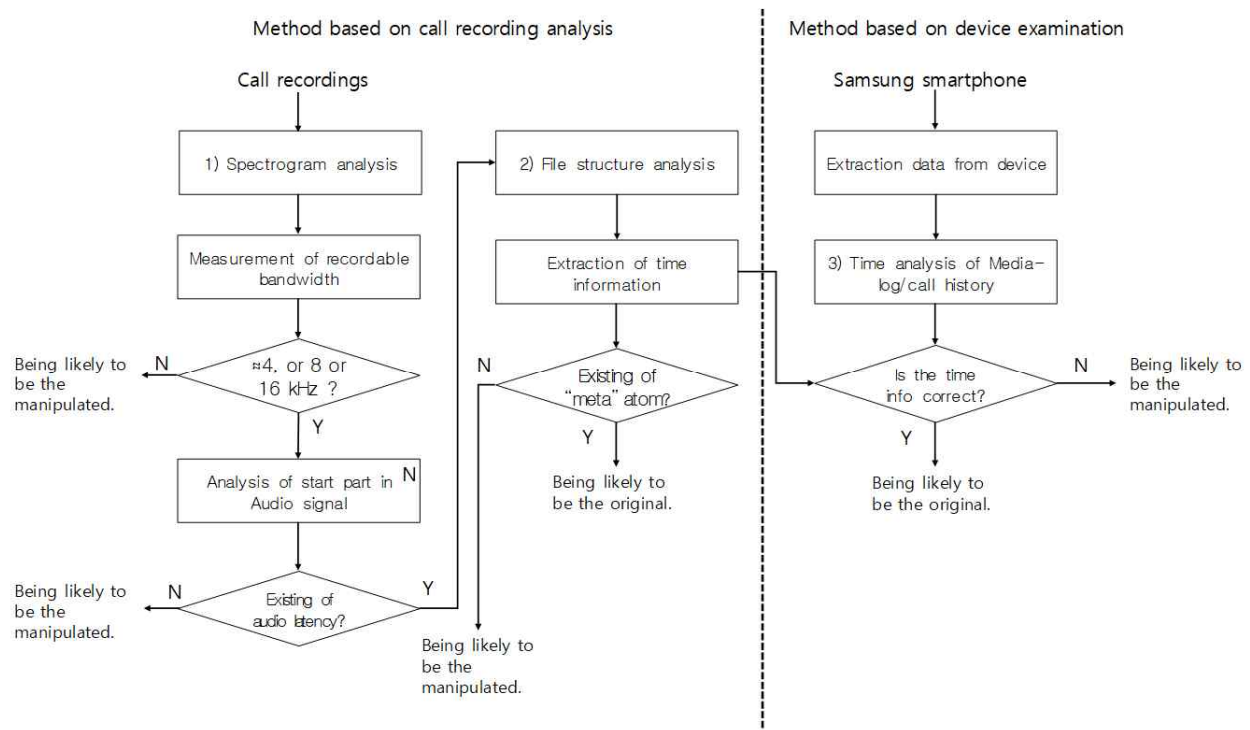
〈Figure 16〉 File structure of manipulated "CallRec 033xxxx314_210730_094910-1.m4a".

예를 들면, [그림13]의 적색박스로 표시한 "통화녹음 033xxxx314_210730_094910-1.m4a"은 "통화녹음 033xxxx314_210730_094910.m4a"의 통화녹음파일을 중간 일부를 삭제하여 편집한 파일이다. 편집된 "통화녹음 033xxxx314_210730_094910-1.m4a" 파일의 미디어로그상의 파일이 생성된 시점(T_{\in})은 한국표준시(KST)기준 [2022-01-01, 11:02:35]이다. [그림16]의 해당 파일의 구조에서도 최초 통화녹음이 저장 완료된 시점 (T_{final})은 한국표준시(KST)기준 [2021-07-30, 09:49:24]이며, 통화녹음파일이 최종 수정된 시점 (T_{\in})은 한국표준시(KST)기준 [2022-01-01, 23:02:35]으로 확인된다. 따라서 미디어로그상의 파일이 생성된 시점(T_{\in})이 파일의 구조에서도 최초 통화녹음이 저장 완료된 시점(T_{final}) 후에 발생한 것이기 때문에, 이러한 경우 통화녹음파일이 위변조의 가능성이 있음을 추정할 수 있다.

V. 통화녹음 파일에 대한 위변조 여부 분석 절차

3장과 4장에서 설명한 바와 같이 통화녹음파일의 위변조 여부에 대해 검출할 수 있는 절차를 [그림17]과 같이 도식화하였다. 먼저 통화녹음파일 분석 방법은 통화녹음파일의 스펙트로그램 분석을 통한 기록가능한 오디오 대역폭 측정 방법 및 음성지연구간 구간을 측정하기 위한 주파수 분석 방법이 존재한다. 먼저 통화녹음 파일에 대해 스펙트로그램 분석을 통해, 기록가능한 오디오 대역폭을 측정하고, 해당 대역폭이 약 4, 8, or 16kHz 이내의 범위를 가지고 있지 않으면, 위변조된 파일일 가능성이 크다. 만약 해당 대역폭이 조건을 만족하면, 음성지연구간을 존재하는지 여부를 알아본다. 만약 음성지연구간이 존재하지 않는다면, 이는 통화녹음파일의 앞부분을 조작했을 가능성이 있다. 그 후, 파일 구조 분석을 통해, 시간 정보(파일생성시간 및 수정시간)가 일치하는지 살펴보고, "meta" atom이 존재 여부에 따라 위변조를 판별하게 된다. 통화녹음파일을 기록한 것으로 추정되는 디바이스가 확보되면, 모바일포렌식툴을 통해 데이터를 추출하고, 미디어로그 및 통화내역 등의 시간

정보를 통화녹음파일에서 획득한 시간 정보와 4.3절에 기술된 조건에 부합하는지를 분석하여 위변조 가능성을 판단할 수 있다. 그러나, 디지털파일의 특성상 정교한 위변조가 가능하다는 것을 명심해야 한다.



〈Figure 17〉 The proposed forgery detection analysis procedure.

VI. 고찰 및 향후 계획

본 논문에서는 통화녹음파일에 대한 스펙트로그램, 파일 구조, 미디어로그 및 통화내역 분석을 통한 위변조 검출 분석 절차에 대해 제안하였다. 제안한 방법 중 스펙트로그램 분석에서는 일반 녹음파일과는 달리 통화녹음 파일에서만 기록되는 제한된 대역폭을 통해, 최초 원본 파일에 추가적으로 삽입된 부분이 있는지 확인이 가능하였다. 추가적으로 음성지연간의 존재여부에 따라 앞부분이 삭제된 것인지도 판별이 가능하였다. 파일구조에서는 통화녹음파일을 삼성 스마트폰에 기본 탑재되어 있는 “음성 녹음” 기능을 통해 편집하였을 경우, “meta” atom이 존재하는지 여부에 따라 위변조여부를 확인할 수 있다. 추가적으로 통화녹음파일이 기록된 삼성 스마트폰이 제시되면, 모바일 포렌식 툴로 데이터를 획득한 후, 미디어로그, 통화내역분석을 통한 시간 정보와 파일 구조에서 획득한 시간정보의 분석을 통해 4.3절에서 기술한 조건들과 부합하는 분석하여, 통화녹음파일이 위변조되었는지 판별할 수 있다. 본 연구는 삼성 스마트폰에서 한정하여 기술하고 있으며, 삼성 스마트폰 뿐만 아니라 LG 등 다른 안드로이드 기종에 대해 제안한 방법을 확장할 수 있는지에 대해 알아볼 필요가 있다. 또한 본 논문에서 사용한 삼성 스마트폰에 탑재된 음성 녹음 어플리케이션 이외에 구글스토어 등에서 내려받은 어플리케이션을 통해 편집하였을 때, 원본 녹음파일과 비교해서 편집된 녹음파일의 파일 구조 및 기록 가능한 대역폭 및 오디오 시간 지연 등에 변화가 있는지 확인해 볼 필요가 있다. 마지막으로 일부 특정 조건에서는 제안한 편집 여부 분석 절차로도 위변조 여부가 검출되지 않을 수 있으므로, 이를 해결하기 위한 정교한 분석 절차에 대한 연구가 필요하다.

참 고 문 헌 (References)

- [1] Park N.I., Shim K.-S. and Jeon O.-Y., A Study on Authentication Analysis Procedure of Digital Audio Files. *Journal of Digital Forensics*, 13(4), 2019.
- [2] Park N.I., Lee J.W. Jeon O.-Y., Kim Y.J. and Lee J.H., A Method of Forensic Authentication via File Structure and Media log Analysis of Digital Images Captured by iPhone. *Journal of Korea Multimedia Society*, 24(4), 2021.
- [3] THEELEC. <http://www.thelec.kr/news/articleView.html?idxno=15342>. Accessed 6 Dec. 2021.
- [4] Oh B.T., Moon B.J., and Lee D.I., The Trend of Digital Watermarking Technology for Digital Rights Management. *Electronics and Telecommunications Trends*, 17(6), 2002.
- [5] Lee J.W., Lee J.H., Shim K.-S., Byun J.S., Na G.-H., and Lee J., A Study on Limitation of Image Forgery Detection Methods. *Journal of Digital Forensics*, 12(1), 2018.
- [6] Yang I.-H., Kim K.-H., Kim M.-J., Baek R.-S., Heo H.-S., and Yu H.-J., An Automatic Method of Detecting Audio Signal Tampering in Forensic Phonetics. *Phonetics and Speech Sciences*, 6(2), 2014.
- [7] Kim K.H., A Study on the Forensic Application of Smartphone Recording Database. *Journal of Digital Forensics*, 15(1), 2021.
- [8] Park N.I., Lee J.W., Shim, K.-S., Byun J.S., and Jeon O.-Y., A Method of Forensic authentication of audio recordings generated using the Voice Memos application in the iPhone, *Forensic Science International*, 320(110702), 2021.
- [9] Adobe Audition. <https://www.adobe.com/>. Accessed 1 Dec. 2021.
- [10] Park N.I., Kang J.A., Lee S.R., Kim H.K. A packet loss concealment technique improving quality of service for wideband speech coding in wireless sensor networks. *International of Distributed Sensor Networks*, 10(4), 2014.
- [11] MP4 Inspector. <https://www.sourceforge.net/projects/mp4-inspector/>. Accessed 1 Dec. 2021
- [12] Park N.I., Lee J.W., Lim, S.H., Byun J.S., Na, G.-H., Jeon O.-Y., and Lee J.H., Energy-based linear PCM audio recovery method of impaired MP4 file stored in dashboard camera memory. *Forensic Science International: Digital Investigation*, 39(301274), 2021.
- [13] Final Mobile Forensics. <https://finaldata.com/mobile/>. Accessed 1 Nov. 2021.

저 자 소 개



박 남 인 (Nam In Park)

준회원

2007년 2월 : 광운대학교 전자통신공학과 공학사

2009년 2월 : GIST 정보통신공학과 공학석사

2013년 8월 : GIST 정보통신공학과 공학박사

2013년 8월~2014년 3월 : GIST 박사후연구원

2014년 4월~현재 : 국립과학수사연구원 디지털분석과

관심분야 : 화자인식, 음성합성, 음성/오디오 신호처리, 오디오포렌식, 머신러닝 및 딥러닝 등



이 지 우 (Ji Woo Lee)

준회원

2009년 2월 : 동국대학교 전자공학과 공학사

2017년 2월 : 동국대학교 대학원 전자공학과 공학박사

2017년 12월~현재 : 국립과학수사연구원 디지털과

관심분야 : 파일복원, 사진 위·변조 검출, 디지털포렌식, 모바일포렌식



김 진 환 (Jin-Hwan Kim)

준회원

2008년 2월 : 고려대학교 전기전자전파공학과 공학사

2010년 2월 : 고려대학교 대학원 전자전기공학과 공학석사

2015년 2월 : 고려대학교 대학원 전자전기공학과 공학박사

2015년 2월~2017년 12월 : 국방기술품질원 선임연구원

2017년 12월~현재 : 국립과학수사연구원 디지털과

관심분야 : 디지털포렌식, 영상개선, 특징검출 등



임 재 성 (Jae Sung Lim)

준회원

2012년 2월 : 한양대학교 전자전기공학과 공학사

2014년 2월 : 포항공과대학교 대학원 전자전기공학과 공학석사

2015년 9월~2018년 11월 : 국방기술품질원 지휘정찰센터

2018년 11월~현재 : 국립과학수사연구원 디지털과

관심분야 : 영상신호처리, 생체인식, 디지털포렌식 등



나 기 현 (Gi-Hyun Na)

준회원

1998년 2월 : 경북대학교 전자공학과 공학사

2000년 2월 : 경북대학교 대학원 전자공학과 공학석사

2016년 2월 : 광운대학교 대학원 전자공학과 공학박사

2001년 11월~현재 : 국립과학수사연구원 디지털분석과

관심분야 : 디지털포렌식, 파일복원, 사진 위·변조 검출, 비디오 재구성



전 옥 엽 (Oc-Yeub Jeon)

준회원

1998년 2월 : 부산대학교 물리학과 이학사

2000년 2월 : 부산대학교 물리학과 이학석사

2006년 8월 : 부산대학교 물리학과 이학박사

2006년 6월~현재 : 국립과학수사연구원 디지털분석과

관심분야 : 오디오 포렌식, 오디오 신호처리, 머신러닝 및 딥러닝 등