Android 和 iOS 多媒体分发过程追踪

Yu-Min Jeon 韩国首尔
KITRI 第九届“最佳中的最佳”项目
邮箱：men1999@naver.com

Won-Mu Heo 韩国大邱天主教大学计算机软件学院 邮箱：
hwm1308@gmail.com

Jong-Min Kim 韩国高丽大学计算机科学与工程系
邮箱：
dakuo@korea.ac.kr

Kyounggon Kim 沙特阿拉伯王国利雅得阿拉伯纳伊夫安全科学大学网络犯罪与数字取证卓越中心 邮箱：
kkim@nauss.edu.sa

arXiv:2304.03848v1 [cs.MM] 7 Apr 2023

摘要——**在全球范围内，非法拍摄并传播图像或视频的犯罪活动日益增多。随着智能手机普及率不断提高，偷拍他人身体并通过即时通讯应用传播的犯罪也有所增加。然而，关于这些相关问题的研究很少。利用全球热门即时通讯应用 WhatsApp 和 Telegram 传播媒体的犯罪活动持续增加。为逃避调查网络追查，犯罪分子通过各种即时通讯应用传播非法影像的情况也很常见。随着这类犯罪增多，对专业调查人员的需求将持续存在，刑事调查所需时间也将不断延长。本文提出一种多媒体取证方法，通过检查使用智能手机拍摄的图像和视频经即时通讯应用传输时发生变化的媒体信息，追踪数字足迹。我们选取了全球最受欢迎的 11 款即时通讯应用和两款安全即时通讯应用，并选取了智能手机上使用最广泛的 Android 和 iOS 操作系统。通过本研究，我们确认，可以通过分析传输的图像和视频，追踪与即时通讯应用分发相关的数字足迹。因此，当视频经多个即时通讯应用传输时，可以确定用于传播该视频的即时通讯应用。**

一、引言

随着智能手机普及率的提高，利用智能手机针对在线社交网络（OSN）实施模拟和欺诈等犯罪行为也不断演变。Patel 等人开展的研究表明，社交媒体和即时通讯平台目前正被用作网络犯罪工具。因此，进一步研究 OSN 和即时通讯平台被认为十分重要 [1]。

现有关于刑事调查的研究主要聚焦于从特定应用程序中提取伪迹、文本挖掘和图像质量分析。虽然现有研究能够检索通过特定应用程序中的伪迹传输的记录，但对于设备上未留存记录时，如何识别图像和视频等媒体的来源及传播路径，相关研究仍然不足。这一研究空白表明，当前方法可能不足以应对非法拍摄影像的分发这一犯罪行为。色情内容的传播尤其令人担忧，因为这类内容很容易在即时通讯应用的聊天室中分享。根据 [2] 报告，近期一项研究发现，超过42%的成年人日常使用两个或更多社交媒体平台。因此，此类内容很可能会在其他应用程序上再次传播。

鉴于调查人员不可能手动检查每张图像或每段视频，因此有必要通过媒体分析来识别媒体的来源和传播路径。本研究考察了一种方法，用于调查移动设备上通过即时通讯应用收到的图像的来源。这些信息对于调查人员追溯在嫌疑人移动设备上发现的媒体的来源至关重要。这是因为，除非媒体是用该设备拍摄的，否则设备上发现的媒体要么是从他人处接收的，要么是从其他地方获取的。

在本研究的初期阶段，我们考虑了四个问题：i）特定应用中会留下哪些媒体伪迹？；ii）不同智能手机上的伪迹是否有所不同？；iii）能否识别媒体通过哪个平台传输？；iv）媒体在传输过程中的修改会如何影响刑事调查?

据我们所知，尚无其他研究分析特定即时通讯应用经过多个即时通信平台传递时发生的媒体变化。本文的贡献如下：

1) 首先，我们对十一款最受欢迎的即时通讯应用和两款安全即时通讯应用中的编码媒体伪迹进行了分类。2) 其次，我们分析了在一款即时通讯应用中编码一次的媒体经过另一款即时通讯应用后，其状态发生的变化。3) 最后，我们根据分析结果提出了调查方法。

本文其余部分结构如下：第2节介绍现有研究，第3节阐述我们的研究方法，第4节评估研究结果，最后，第5节总结结论并讨论未来方向。

II. 相关工作

现有的即时通信软件（IM）相关研究主要集中于痕迹分析、图像质量分析，以及分析即时通讯应用中文本的文本挖掘研究 [3]。过去 10 年间，随着社交网络服务（SNS）和即时通信应用日益普及，许多研究开展了痕迹分析 [4]。这些研究成功识别了特定应用程序中的伪迹，例如账户信息、短信、照片、通话和聊天记录；与 iOS 相比，这些伪迹在 Android 上尤为明显。

[5] 发现了 Instagram 中包含用户账户、关注者账户和亲密好友账户相关信息的用户配置。 [6]展示了从 Facebook Messenger 收集的证据，包括文本、照片、视频传输和通话。其他应用程序也开展了类似研究，例如 Discord（[7]）、LINE（[8, 9, 10, 11]）、WhatsApp（[12, 13]）、Telegram（[14, 15,16, 17, 18]）、KakaoTalk（[19, 20]）、Facebook（[21]）、Skype（[22, 23]）、Signal（[24, 25]）、微信（[26, 27]）、QQ（[28, 29]）、ChatON（[30]）、Kik（[31, 32]）和 Wickr（[33, 34, 35]）。

如上述研究所示，目前正在对特定应用进行痕迹分析。然而，由于即时通信应用种类繁多，而且大多数人会使用多种即时通讯应用，因此仍需开展进一步研究。[36] 探讨了 PNG 图像的消息传输问题：传输采用端到端加密保护，并按照预定义规则进行压缩。本研究通过比较和分析经 WhatsApp 发送的 PNG图像与传输前的 PNG图像，分析了 PNG图像压缩和阿尔法通道。不过，本研究未探讨其修辞含义。

另一方面， [37] 为 WhatsApp 构建了一个网络系统，采用文本挖掘方法提供与他人干预相关指令的信息。该方法使用词频-逆文档频率和余弦相似度，计算传输文档中每个词的权重，以识别消息。

III. 方法论

通过分析经即时通讯应用传播的媒体，我们提出了一种识别与“媒体由某个特定即时通讯应用分发”这一特征相关数字足迹的方法。我们设计了相关场景，假设用智能手机拍摄的媒体通过该应用程序进行分发。此外，媒体传播还涉及云端、驱动器、USB 和软件等多种途径，具体的传播过程并不明确。不过，通过检查特定即时通讯应用留下的媒体伪迹，就可以通过数字足迹追踪来追踪分发媒体的即时通讯应用。

我们使用 MediaInfo 20.09 版作为媒体分析工具。iOS 支持高效率格式和高兼容性格式。不过，由于高效率格式要求操作系统版本为 11 或更高，且设备为 iPhone 7 或更新机型，为了使实验结果更具普适性，我们选择高兼容性格式进行实验。对于 Android，我们采用两种方法进行实验：一种是新款 Galaxy S 系列主要使用的默认 4:3（12MP）4032x3024 分辨率，另一种是旧款 Galaxy Note 系列主要使用的默认 16:9（16MP）5312x2988 分辨率。图像媒体的原始信息见表 I。

表 I：原始图像信息

分发平台	iOS	Android
扩展名	JPG	JPG
格式	JPEG	JPEG
分辨率	4032x3024	4032x3024 5312x2988

我们将 iOS 中的相机选项设为 1080p HD – 30fps，在 Android 中则设为 FHD 1920x1080 分辨率。iOS 和 Android 之间的主要区别在于扩展名和编解码器 ID。扩展名方面，iOS 使用 MOV 扩展名，Android 使用 MP4 扩展名。使用 HxD 查看文件签名时，iOS 的编解码器 ID 显示为 ftypqt，Android 的则显示为 ftypmp42，如图 1 所示。此外，每个视频都有特定的文件大小；例如，30 秒的视频大小约为 50–60 MB。视频格式配置文件可分为 High（高画质）、Main（中等画质）和 Baseline（低画质）。表 II 展示了原始视频媒体信息。

表 II：原始视频信息

分发平台	iOS	Android
扩展名	MOV	mp4
格式	MPEG-4	MPEG-4
格式配置文件	QuickTime	基础媒体版本 2
编解码器 ID	qt	mp42 (isom/mp42)
视频格式配置文件	High@L4	High@L4
分辨率	1920x1080	1920x1080

IV. 实验

我们总结了从 Android 和 iOS（两种智能手机操作系统）上的 13 个即时通讯应用发送的图像和视频所发生的变化。本研究选取 KakaoTalk 和 Facebook Messenger 作为第 N个即时通讯应用，并进一步分析了媒体作为第 N+1 个即时通讯应用传输至其余即时通讯应用时发生变化的媒体信息。

A. 实验环境

为进行媒体工件分析，我们在智能手机（Android、iOS）上开展了实验；这些设备通常用于即时通讯应用。表 III 列出了目标测试设备及其版本。

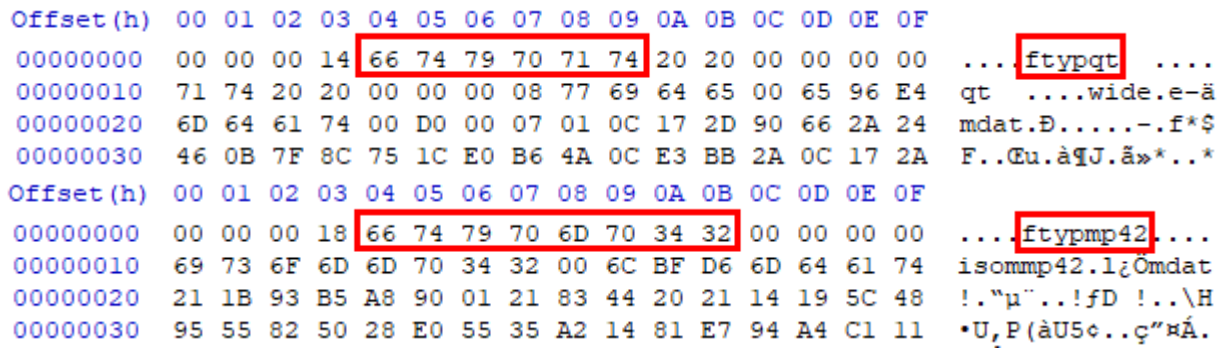

图 1：编解码器 ID（上方为 iOS，下方为 Android）

表 III：实验设备和版本

制造商	型号名称	操作系统版本
Apple	A1687	14.2
Apple	A1905	14.2
SAMSUNG	SM-N916L	6.0.1
三星	SM-G906K	6.0.1
三星	SM-G930S	8.0.0

本研究分析了 13 个平台上媒体的变化，其中包括 WhatsApp、Facebook Messenger 和 Telegram 等常用即时通讯应用，以及一些安全性较高、知名度较低的平台。实验中使用的移动即时通讯应用列于表 IV。

表 IV：移动即时通讯应用信息

应用名称	版本（iOS）	版本（Android）
KakaoTalk	9.1.2	9.1.3
Facebook Messenger	291.2	291.2.0.22.114
Facebook	297.0	297.0.0.36.116
Instagram	167.0	167.1.0.25.120
WhatsApp	2.20.121	2.20.205.16
微信	7.0.18	7.0.17
Telegram	7.2.1	7.2.1
Skype	8.66.76	8.66.0.76
Discord	49.0	49.16
NateOn	4.0.5	4.0.8
LINE	10.19.0	10.20.1
Signal	3.22.0	4.78.5
Wickr Me	5.66.10	5.66.8

Facebook Messenger、Facebook 和 Instagram 主要通过网页浏览器而非软件在 PC 环境中使用。因此，我们使用软件从 10 个即时通讯应用中下载了媒体，并通过网页浏览器从 3 个即时通讯应用中下载了媒体。本研究中使用的软件和网页浏览器信息如表 V 所示。

B. 发送即时通讯应用时的图像变化

在图像的媒体信息中，只有通过即时通讯应用传输的图像分辨率可以通过数字足迹追踪进行追踪。这是因为比较 Android 图像和 iOS 图像的媒体信息时，它们的扩展名和格式相同，不像视频媒体那样。因此，

表 V：软件和网页浏览器信息

应用名称	版本（软件）	浏览器（网页）
KakaoTalk	3.1.9.2626	
WhatsApp	2.2047.11	
微信	3.0.0.57	
Telegram	2.4.7	
Skype	15.66.77.0	
Discord	0.0.308	
NateOn	7.0.3.1	
LINE	6.4.0.2388	
Signal	1.37.2	
Wickr Me	5.65.4	
Facebook Messenger		谷歌浏览器
Facebook		谷歌浏览器
Instagram		谷歌浏览器

区分它们的唯一方法是查看分辨率。对于每个即时通信平台，我们都针对普通画质、高清和原图等所有选项进行了实验。实验结果表明，许多平台都可以通过为每个即时通信软件指定特定分辨率来进行数字足迹追踪。然而，有些平台会以原始分辨率传输图像，或者以不规律的方式改变分辨率，因此无法追踪数字足迹。

在正文中，我们排除了分辨率不规则变化或以通用原始图像形式传输的图像结果。图像分辨率结果的误差范围约为 ±10的情况也存在，但非常罕见。表 VI 总结了实验涉及的 13 个即时通信平台的图像分辨率变化。

4.2.1. KakaoTalk

KakaoTalk 在传输图像时提供三种图像质量选项：普通、高画质和原始画质。通过实验，我们发现，除原始画质外，普通和高画质选项都可以通过特定分辨率进行数字足迹追踪。然而，原始画质选项的分辨率与普通原始图像相同，因此无法通过数字足迹进行追踪。

表 VI：即时通讯应用中的更改图像

应用名称	图像选项	iOS		Android (4032x3024)		Android (5312x2988)	
		宽度	长度	宽度	长度	宽度	长度
KakaoTalk	通用	960x720	720x960	960x720	720x960	960x540	540x960
	High	1440x1080	1080x1440	1440x1080	1080x1440	1440x810	810x1440
Facebook 即时通讯应用	默认	无法区分				2048x1152 3984x2241	1151x2048 2240x3984
Facebook	默认	960x720	720x960	无法区分			
Instagram	无法区分						
WhatsApp	默认	1600x1200	1200x1600	1600x1200	1200x1600	1328x747	747x1328
微信	通用	1440x1080	1080x1440	1080x1440	1080x1440	1920x1080	1080x1920
Telegram	通用	1280x960	960x1280	1280x960	960x1280	1280x960	960x1280
Skype	默认	2048x1536	1536x2048	2016x1512	1512x2016	1992x1121	1121x1992
Discord	无法区分						
NateOn	最小化	无法区分				664x374	374x664
	标准					1328x747	747x1328
LINE	通用	1478x1108	1108x1478	1477x1108	1108x1477	1706x960	960x1706
	标准	2365x1774	1774x2365				
Signal	通用	1536x1152	1152x1536	无法区分		4096x2304	2304x4096
Wickr Me	无法区分						

此外，由于从 iOS 和 Android 传输的媒体分辨率相同（4032x3024），因此无法区分这两种操作系统。

4.2.2. Facebook Messenger

在 Facebook Messenger 中，无法选择图像质量，因此只能使用基本图像质量。对于 iOS 和 Android（4032x3024），分辨率会不规则地变化，或与普通原始图像的分辨率相同，因此无法通过数字足迹进行追踪。不过，由于 Android（5312x2988）使用特定分辨率，因此可以通过数字足迹进行追踪。分辨率结果有两种情况，这与其他即时通讯应用不同。虽然结果取决于媒体传播过程，但如果得到与表 VII 所示相同的结果，就可以将其识别为通过 Facebook Messenger 传输的媒体。

4.2.3. Facebook

Facebook 没有图像质量选项，因此只提供默认图像质量。在 iOS 中，可以通过特定分辨率利用数字足迹进行追踪。然而，在 Android 中，分辨率会不规则地变化，因此无法通过数字足迹进行追踪。从分辨率结果可以看出，KakaoTalk 的普通分辨率与 Facebook 的默认分辨率相同。当出现相同分辨率时，可以通过附加文件大小区分具体平台。KakaoTalk 通用清晰度媒体的文件大小约为 100KB，而 Facebook 基本清晰度媒体的文件大小约为 50KB。两个文件的误差范围约为 ±10KB。

4.2.4. Instagram

Instagram 没有质量选项，因此只有默认图像质量。此外，iOS 和 Android 的分辨率都不规则，无法通过数字足迹进行跟踪不可能。

4.2.5. WhatsApp

WhatsApp 没有画质选项，因此只有默认图像质量。iOS 和 Android 都会使用特定分辨率，以便通过数字足迹进行追踪。此外，从 iOS 和 Android 传输的媒体分辨率相同（4032x3024），因此无法区分操作系统。

4.2.6. 微信

微信提供普通画质和原画质两种传输选项。可以通过特定分辨率，利用数字足迹追踪通用图像质量。不过，由于整体图像质量与通用原始图像分辨率相同，因此无法区分整体图像质量，也无法通过数字足迹进行追踪。通过分析分辨率结果可以看出，微信的普通分辨率与 KakaoTalk 的高清分辨率会产生相同结果。如上所述，当分辨率相同时，可以通过附加文件大小来区分具体平台。

KakaoTalk 高清媒体的文件大小约为 500KB，微信普通清晰度媒体的文件大小约为 200KB。两个文件的误差范围约为±100KB。根据传播过程的不同，结果可能会有所差异，但这种情况非常罕见。

4.2.7. Telegram

Telegram 可通过选择两种选项进行传输：普通画质和原图。通用图像质量可以通过特定分辨率进行数字足迹追踪。然而，由于原图选项与普通原图分辨率相同，无法加以区分，因此无法通过数字足迹追踪。此外，由于从 iOS 和 Android 传输的媒体具有相同的

分辨率，因此无法区分操作系统。

4.2.8. Skype

Skype 没有图像质量选项，因此只有基本图像质量。iOS 和 Android 均使用特定分辨率，以便通过数字足迹进行追踪。

4.2.9. Discord

在 Discord 中下载图像时，可以选择预览选项或原图选项。使用预览选项时，iOS 和 Android 的分辨率都会不规则地变化，因此无法通过数字足迹进行追踪。而原图选项生成的结果与常规原图分辨率相同，因此也无法通过数字足迹进行追踪。

4.2.10. NateOn

在 NateOn 中发送图像时，iOS 用户可以选择两种选项：常规图像质量和原始图像质量；Android 用户则可以从三种选项中选择：最低质量、标准质量和原始质量。对于分辨率为 4032x3024 的 iOS 和 Android 设备，分辨率会不规则地变化，或与常规原图分辨率相同，因此无法通过数字足迹进行追踪。不过，分辨率为 5312x2988 的 Android 设备会使用特定分辨率，因此可以通过数字足迹进行追踪。

4.2.11. LINE

在 LINE 中，可以从三种选项中选择：普通画质、标准画质和原始画质。由于 iOS 和 Android 对普通画质和标准画质均使用特定分辨率，因此可以通过数字足迹追踪进行追踪。不过，由于原始图像质量与通用的原始图像分辨率相同，因此无法通过数字足迹追踪进行追踪。

4.2.12. Signal

Signal 仅提供基本图像质量，因为它没有提供画质选项。iOS 和 Android 均允许通过特定分辨率（5312x2988）利用数字足迹进行追踪。不过，在 Android 上（4032x3024）无法通过数字足迹追踪，因为该分辨率与原始图像分辨率相同。

4.2.13. Wickr Me

Wickr Me 仅提供基本图像质量，没有图像质量选项。此外，由于 iOS 和 Android 的分辨率均与普通原始图像的分辨率相同，因此无法通过数字足迹追踪进行追踪。

C. 通过即时通讯应用发送时的视频变化

通过即时通信应用传输视频时，我们确认可以通过数字足迹追踪来追踪视频，方法是分析各种媒体信息，例如扩展名、格式配置文件、编解码器 ID、视频格式配置文件和分辨率，编码器及特定信息。大多数文件大小都较小，而且在即时通信平台的编码过程中，分辨率发生了变化。一些即时通信平台会提供各平台对应的编码器和特定信息。综合分析各即时通信应用的特定分辨率、编码器信息、媒体信息等，可以识别特定即时通信平台产生的伪迹，并通过数字足迹追踪进行追踪。不过，我们也发现少数平台的媒体信息与原始视频一致，因此无法通过数字足迹追踪进行追踪。我们分析了 iOS 和 Android 上默认分辨率为 1920x1080 的视频，并在正文中排除了与原始视频相同的结果。表 VII 和表 VIII 总结了对 13 个受测即时通信平台的视频变化情况。

4.3.1. KakaoTalk

KakaoTalk 可通过选择普通画质或高画质两种选项之一来发送。尽管结果可能因传播过程而异，但传播后的媒体始终会呈现这两种结果之一。如果使用编码器，则可以查看每种图像质量对应的不同编码器信息，并已确认 KakaoTalk 使用了专属编码器。编码后的文件在即时通讯应用内重新分发后，变化很小。如果使用编码器，则可以确认 KakaoTalk 专属编码器：普通画质使用“Lavf57.56.101”，高画质使用“Lavf57.83.100”。通过 KakaoTalk 分发时，可以汇总分辨率等伪迹及其他媒体信息，并通过数字足迹追踪进行追踪。

4.3.2. Facebook Messenger

Facebook Messenger 没有视频质量选项，因此只有基本视频质量。Facebook Messenger 带有“Lavf58.20.100”信息，这是 Facebook 和 Instagram 共用的编码器信息。此外，iOS 会定期改变分辨率，而 Android 改变分辨率的时间不规律。通过 Facebook Messenger 分发时，无法在 Android 上指定分辨率。不过，可以结合其他媒体信息来确定分辨率，并通过数字足迹进行追踪。随后，iOS 会汇总分辨率等伪迹及其他媒体信息，并可根据结果通过数字足迹进行追踪。

4.3.3. Facebook

Facebook 没有视频质量选项，因此只有默认图像质量。与上文所述的 KakaoTalk 一样，结果会因传播过程而异，但分发的视频始终会产生两种结果之一。Facebook 的编码器信息与 Facebook Messenger 和 Instagram 相同，而 Facebook 特有的信息（如“影片名称”）会留下与帖子编号相关的信息。通过 Facebook 分发时，分辨率等伪迹及其他媒体信息可以

表 VII：即时通讯应用中的 iOS 视频变化

应用程序 name	视频质量	扩展名	格式配置文件	编解码器 ID	视频格式 配置文件	宽度	长度	编码器	附加信息 信息
KakaoTalk	通用	mp4	基础媒体	isom (isom/iso2/avc1/mp41)	基线配置@L4.1	720x404	404x720	Lavf57.56.101	
			基础媒体版本 2	mp42 (isom/mp41/mp42)					
	High	mp4	基础媒体	isom（isom/iso2/mp41）	Main@L4@Main	1920x1080	1920x1080	Lavf57.83.100	
			基础媒体版本 2	mp42 (isom/mp42)	Baseline@L4				
Facebook 即时通讯应用	默认	MP4，MOV	基础媒体	isom (isom/iso2/avc1/mp41)	Main@L3.1	1280x720	720x1280	Lavf58.20.100	
Facebook	默认	mp4							影片名称
Instagram	默认	MP4、MOV	基础媒体	isom (isom/iso2/avc1/mp41)	Baseline@L3	480x270 640x360	480x854 640x1138	Lavf58.20.100	
WhatsApp	默认	mp4	基础媒体版本 2	mp42 (mp42/isom)	Baseline@L3.1	848x480	848x480		
微信	默认	mp4	基础媒体版本 2	mp42 (isom/mp41/mp42)	High@L3.1	960x544	544x960		Movie More
Telegram	1080p	MOV	基础媒体版本 2	mp42 (isom/mp41/mp42)	High@L4	1920x1072	1072x1920		
	720p				High@L3.1	1280x720	720x1280		
	480p				High@L3.1	848x464	464x848		
	360p				高配置@L3	640x352	352x640		
	240p				高配置文件@L2.1	480x256	256x480		
Skype	默认	MOV	基础媒体版本 2	mp42 (isom/mp41/mp42)	Main@L3.1	1280x720	720x1280		
Discord	默认	MOV	QuickTime	qt	Main@L3.1	960x540	960x540		
NateOn	默认	mp4	基础媒体版本 2	mp42 (isom/mp41/mp42)	High@L4	1920x1080	1920x1080		录制日期
LINE	默认	mp4	基础媒体版本 2	mp42 (isom/mp41/mp42)	High@L4	960x540	960x540		影片名称
Signal	默认	mp4	基础媒体版本 2	mp42 (isom/mp41/mp42)	Main@L3	568x320	568x320		
Wickr Me	默认	MOV	QuickTime	qt	Main@L3	568x320	568x320		

表 VIII：即时通讯应用中的 Android 视频变化

应用程序 name	视频 质量	扩展名	格式配置文件	编解码器 ID	视频格式 配置文件	宽度	长度	编码器	附加信息 信息
KakaoTalk	通用	mp4	基础媒体	isom (isom/iso2/avc1/mp41)	Baseline@L3	852x480	852x480	Lavf57.56.101	
			基础媒体版本 2	mp42 (isom/mp41/mp42)	Baseline@L3.1				
	High	mp4	基础媒体	isom（isom/iso2/mp41）	Main@L4@Main	1920x1080	1920x1080	Lavf57.83.100	
			基础媒体版本 2	mp42 (isom/mp42)	Baseline@L4				
Facebook 即时通讯应用	默认	mp4	基础媒体	isom (isom/iso2/avc1/mp41)	Main@L3 Main@L4	分辨率异常		Lavf58.20.100	
Facebook	默认	mp4			Baseline@L3	400x224	224x400	Lavf56.40.101	影片名称
Instagram	默认	mp4	基础媒体	isom (isom/iso2/avc1/mp41)	Baseline@L3	480x270 640x360	480x852 640x1136	Lavf58.20.100	
WhatsApp	无法区分								
微信	默认	mp4	基础媒体版本 2	mp42 (isom/mp41/mp42)	High@L3.1	960x544	544x960		版权
Telegram	High	mp4	基础媒体	isom (isom/iso2/avc1/mp41)	High@L4 Baseline@L4	1920x1080	1080x1920		
	中等				Baseline@L3.1	1280x720	720x1280		
	介于中等和低				Baseline@L3.1	854x480	480x854		
	Low				基线配置文件@L2.1	480x270	270x480		
Skype	默认	mp4	基础媒体版本 2	mp42 (isom/mp42)	Baseline@L3.1	1280x720	720x1280		
Discord	无法区分								
NateOn	无法区分								
LINE	默认	mp4	基础媒体版本 2	mp42 (isom/mp42)	High@L3.1	960x540	540x960		
Signal	默认	mp4	基础媒体版本 2	mp42 (isom/mp42)	Baseline@L3.1	1280x720	720x1280		
Wickr Me	无法区分								

根据结果进行汇总，并通过足迹追踪。

4.3.4. Instagram

Instagram 没有视频质量选项，因此只有默认图像质量。Instagram 的编码器信息与 Facebook Messenger 或 Facebook 相同。因此，Facebook Messenger、Facebook 和 Instagram 的编码器信息相同，但可以通过综合检查编解码器 ID、视频格式配置文件等媒体信息，将它们识别为特定平台。通过 Instagram 分发时，可以通过数字足迹追踪汇总并追踪分辨率等伪迹及其他媒体信息。

4.3.5. WhatsApp

WhatsApp 没有视频质量选项，因此只有默认质量。iOS 可识别为 WhatsApp 平台，因此可以通过数字足迹进行追踪。不过，由于 Android 的媒体信息与通用原始视频相似，因此无法将其识别为特定平台，也无法通过数字足迹进行追踪。通过 WhatsApp 分发时，只有 iOS 能汇总分辨率等伪迹及其他媒体信息，并通过数字足迹进行追踪。

4.3.6. 微信

微信没有视频质量选项，因此只有基本图像质量。微信的 iOS 和 Android 版本均包含微信特有的具体信息，可供检查。在 iOS 中，仍保留与名为“Movie More”的微信版本相关的信息；在 Android 中，仍保留名为“Copyright”的版权信息。通过微信分发时，可以借助数字足迹追踪汇总并追踪分辨率等伪迹及其他媒体信息。

4.3.7. Telegram

Telegram 的 iOS 版有五种视频质量选项：1080p、720p、480p、360p 和 240p；Android 版有四种视频质量选项：高画质、中画质、中低画质和低画质。在 Telegram 中，只有 Android 上的高画质横向视频采用 High 视频格式配置文件；其余高画质竖向视频以及中画质、中低画质和低画质视频均采用基线配置文件。在 Android 上，高画质竖向视频采用基线视频格式配置文件。因此，Telegram 的每种视频质量都有不同的分辨率和配置文件，可以检查分发的视频质量。通过 Telegram 分发视频时，可以借助数字足迹追踪汇总并追踪分辨率等伪迹及其他媒体信息。

4.3.8. Skype

Skype 不提供视频质量选项，因此只有基本质量。Skype 可在 iOS 和 Android 上识别为特定平台。因此，通过 Skype 分发时，可聚合分辨率等伪迹及其他媒体信息，并通过数字足迹追踪进行跟踪。

4.3.9. Discord

Discord 不提供视频质量选项，因此只有基本质量可用。iOS 可以归类为特定平台，但 Android 会传输未经任何修改的原始视频，因此无法通过数字足迹进行追踪。因此，通过 Discord 分发时，只有 iOS 能够聚合分辨率等伪迹及其他媒体信息，以便通过数字足迹追踪进行跟踪。

4.3.10. NateOn

在 NateOn 中，iOS 提供两种视频质量选项：普通视频质量和原始视频质量；而 Android 仅提供基本视频质量，没有其他选项。在 iOS 上，可以根据具体平台区分这两种选项；但在 Android 上，原始视频会以原样传输，无法区分，也无法通过数字足迹追踪进行追踪。NateOn 的 iOS 特定信息会保留与视频录制日期相关的信息，称为“录制日期”。通过 NateOn 分发时，只有 iOS 可以汇总分辨率等伪迹及其他媒体信息，并通过数字足迹追踪进行追踪。

4.3.11. LINE

在 LINE 中没有视频质量选项，因此只有基本视频质量。无论传播过程如何，iOS 都可归类为特定平台；而对于 Android，则取决于能否根据传播过程加以区分。本文仅考虑 Android 可以区分的情况。iOS 上的 LINE 视频包含名为“影片名称”的特定信息。通过 LINE 分发时，只有在 LINE 平台能够识别 Android 媒体信息的情况下，才能通过数字足迹追踪这些信息，此外，iOS 可以汇总分辨率等伪迹及其他媒体信息，以便通过数字足迹追踪。

4.3.12. Signal

Signal 不提供视频质量选项，因此只有基本视频质量。此外，使用 Signal 时，可以分别识别 iOS 和 Android 平台。通过 Signal 分发媒体时，可以汇总分辨率等信息和其他伪迹，并通过数字足迹追踪进行追踪。

4.3.13. Wickr Me

Wickr Me 不提供视频质量选项，因此只有基本视频质量。可以将 iOS 识别为特定平台，因此可以通过数字足迹进行追踪。然而，由于 Android 会原样传输原始视频且无法区分，因此也无法通过数字足迹进行追踪。通过 Wickr Me 分发时，只有 iOS 可以汇总分辨率等伪迹及其他媒体信息，并通过数字足迹进行追踪。

D. 通过即时通讯应用发送多条消息时的视频媒体切换

在上一节中，我们通过追踪一次分发视频媒体时留下的数字足迹，识别了即时通信软件的伪迹。本节仅关注普通和基本图像质量，分析媒体从一个即时通讯应用传输到另一个即时通讯应用时各自留下的伪迹。我们选择了全球两款热门即时通讯应用 KakaoTalk 和 Facebook Messenger 作为第N个分发站点，其余即时通讯应用则作为第N+1 个分发站点。基于研究结果，我们探讨能否通过数字足迹追踪第N个及第N+1个分发即时通讯应用。

4.4.1. 第N个即时通讯应用 KakaoTalk

本节重点介绍 KakaoTalk 作为第N个即时通讯应用、其余即时通讯应用作为第N+1 个即时通讯应用时发生的变化。实验得出三种情况。第一，可以部分查看第N个和第N+1个即时通讯应用的媒体信息，从而通过数字足迹追踪。第二，第N个即时通讯应用的媒体信息会被第N+1个即时通讯应用的媒体信息覆盖，导致无法追踪。最后，多个最终媒体信息结果相同，从而缩小调查网络的范围。本研究排除了无法通过数字足迹追踪的结果。表 IX 和表 X 展示了 iOS 和 Android 环境下 KakaoTalk 作为第N个即时通讯应用时发生的变化。

4.4.2. 第N个即时通讯应用 Facebook Messenger

本节分析将 Facebook Messenger 作为第N个即时通讯应用传递时发生的变化，以及

表 IX：即时通讯应用之间的视频媒体变化（KakaoTalk / iOS）

应用程序 name	扩展名	格式配置文件	编解码器 ID	视频格式 配置文件	宽度	长度	编码器	附加信息 信息
Facebook 即时通讯应用	mp4	基础媒体	isom (isom/iso2/avc1/mp41)	Main@L3	720x404	404x720	Lavf58.20.100	
		基础媒体版本 2	mp42 (isom/mp41/mp42)	基线配置@L4.1	720x404	720x404		
Facebook		基础媒体	isom (isom/iso2/avc1/mp41)	Main@L3	640x358	358x640	Lavf58.20.100	影片名称
Instagram	无法区分							
WhatsApp	mp4	基础媒体版本 2	mp42 (mp42/isom)	Baseline@L3	720x404	720x404		
微信			mp42 (isom/mp41/mp42)	高配置@L3		404x720		Movie More
Telegram	无法区分							
Skype	mp4	基础媒体版本 2	mp42 (isom/mp41/mp42)	基线配置@L4.1	720x404	720x404		
Discord								
NateOn								
LINE				High@L4		404x720		Line Video
Signal				Main@L2.1	480x268			
Wickr Me		QuickTime	qt	Main@L2.1				

表X：即时通讯应用之间的视频媒体变化（KakaoTalk / Android）

应用程序 name	扩展名	格式配置文件	编解码器 I D	视频格式 配置文件	宽度	长度	编码器	附加信息 信息
Facebook 即时通讯应用	mp4	基础媒体	isom (isom/iso2/avc1/mp41)	Main@L3	852x480	480x852	Lavf58.20.100	
Facebook								影片名称
Instagram	无法区分							
WhatsApp	mp4	基础媒体版本 2	mp42 (mp42/isom)	Baseline@L3.1	852x480	852x480		
微信				High@L3.1				
Telegram		基础媒体	isom (isom/iso2/avc1/mp41)	Baseline@L3.1		480x852		版权
Skype		基础媒体版本 2	mp42 (isom/mp42)					
Discord						852x480		
NateOn								
LINE				High@L3.1		404x720		
Signal	无法区分							
Wickr Me	mp4	基础媒体版本 2	mp42 (isom/mp42)	Baseline@L3.1	852x480	852x480		

T表 XI：即时通讯应用间的视频媒体变化（Facebook Messenger / iOS）

应用程序 name	扩展名	格式配置文件	编解码器 I D	视频格式 配置文件	宽度	长度	编码器	附加信息 信息
KakaoTalk	无法区分							
Facebook	mp4	基础媒体	isom (isom/iso2/avc1/mp41)	Main@L3.1	1280x720	720x1280	Lavf58.20.100	影片名称
Instagram	无法区分							
WhatsApp	mp4	基础媒体版本 2	mp42 (mp42/isom)	Main@L3.1	1280x720	720x1280		
微信	无法区分							
Telegram	无法区分							
Skype	MOV	基础媒体	isom (isom/iso2/avc1/mp41)	Main@L3.1	1280x720	720x1280	Lavf58.20.100	
Discord		QuickTime	qt		960x540	540x960		
NateOn	mp4	基础媒体版本 2	isom (isom/mp41/mp42)		1280x720	720x1280		
LINE	无法区分							
Signal	无法区分							
Wickr Me	MOV	QuickTime	qt	Main@L3	568x320	320x568	Lavf58.20.100	

表XII：即时通讯应用之间的视频媒体变化（Facebook Messenger / Android）

应用程序 name	扩展名	格式配置文件	编解码器 I D	视频格式 配置文件	宽度	长度	编码器
KakaoTalk	mp4	基础媒体	isom (isom/iso2/avc1/mp41)	Main@L4	1920x1080	1080x1920	Lavf58.20.100
Instagram							
WhatsApp							
Telegram							
Discord							
NateOn							
LINE							
Wickr Me							
Facebook	无法区分						
微信							
Skype							
Signal							

其余即时通讯应用作为第N+1个即时通讯应用。实验得出了三种情况，与第4节4.1节类似。首先，可以部分检查第N个和第N+1个即时通讯应用的媒体信息，从而通过数字足迹追踪进行追踪。其次，第N个即时通讯应用的媒体信息会被第N+1个即时通讯应用的媒体信息覆盖，导致无法追踪。最后，多个最终媒体信息结果相同的情况会缩小调查网络的范围。与 KakaoTalk 的情况不同，在 Android 环境下使用 Facebook Messenger 时，有些情况下只能缩小调查网络的范围。某些即时通讯应用产生的结果也无法通过数字足迹追踪进行追踪。表XI和表XII展示了 iOS 和 Android 环境下 Facebook Messenger 的第N个即时通讯应用发生的变化。

五、结论

我们分析了在即时通讯应用中发送图像和视频媒体时，通过媒体信息分析进行数字足迹追踪的实验结果。研究证实，即时通讯应用在 iOS 和 Android 上的运行方式有所不同。此外，当媒体从一个即时通讯应用转发到另一个即时通讯应用时，由于传输过程中留下了相关即时通讯应用的伪迹，因此可以查明消息经过了哪些即时通讯应用。从数字取证的角度出发，我们得出以下结论：

当存在原始图像或相似图像时，可以通过比较分辨率确定传输图像的分发平台。除分辨率保持不变或不规则的即时通讯应用外，每种即时通讯应用传输的图像分辨率各不相同。此外，有些即时通讯应用在 iOS 和 Android 上的分辨率相同，而有些则不同。因此，可以通过数字足迹追踪图像的分发平台。

当存在原始视频或相似视频时，可以通过比较媒体信息来确认传输视频的分发情况。即时通讯应用传输的视频会保留各自不同的媒体信息，但媒体信息不发生变化的即时通讯应用除外。此外，与图像不同，只有当每种即时通讯应用在 iOS 和 Android 上的媒体信息不同时，才会有相应视频。因此，可以推测分发智能手机的操作系统，并追踪视频分发平台相关的数字足迹。

当一个即时通讯应用中的内容被转发至另一个即时通讯应用时，可以通过检查媒体信息来确认或推测所传输视频的分发情况，并缩小调查网络的范围。我们以 KakaoTalk 和 Facebook Messenger 作为第N个即时通讯应用，以其余即时通讯应用作为第N+1个即时通讯应用进行了实验。最后，我们根据实验得出了三项关键发现。

1) 第N个即时通讯应用和第N+1st个即时通讯应用的媒体信息部分保留。

因此，可以准确确认信息经过了哪些即时通讯应用，并通过数字足迹追踪所传输视频的分发情况。2) 第N个即时通讯应用的媒体信息被第N+1st个即时通讯应用的媒体信息覆盖。因此，无法准确确认信息经过了哪些即时通讯应用，也无法通过数字足迹进行追踪。3) 在许多情况下，最终的媒体信息结果都相同。在这种情况下，虽然无法准确确认信息经过了哪些即时通讯应用，但可以缩小调查网络的范围。

我们希望本研究能通过综合所呈现的信息，并追踪媒体的传播渠道，帮助数字取证调查人员迅速开展与媒体传播相关的刑事调查。

参考文献

[1] P.Patel、K.Kannoorpatti、B.Shanmugam、S. Azam 和 K. C. Yeo，“网络犯罪分子对社交媒体使用情况的理论综述”，载于*2017*年计算机通信与信息学国际会议*(ICCCI)*。IEEE，2017 年，第 1–6 页。[2]R. Roshan，“单个用户的多个社交媒体账户”，https://medium.com/@rajroshan26j/multiple-social-media-accounts-of-single-user-71f2f1cde31d，2020, [在线；访问日期：2020]年9月28日。[3] J. Son、Y. W. Kim、D. B. Oh 和 K. Kim，《即时通讯应用的取证分析：解密 Signal、Wickr 和 Threema》，《国际法医科学：数字调查》，第40卷，第301347页，2022年。[4] M. G. Campana 和 F. Delmastro，《Mydigitalfootprint：用于边缘普适计算应用的综合上下文数据集》，《普适与移动计算》，第70卷，第101309页，2021年。[5]C. Alisabeth 和 Y. R. Pramadi，《Android 上 Instagram 的取证分析》，载于 *IOP* 会议系列：材料科学与工程，第1007卷，第1期。IOP Publishing，2020年，第012116页。[6]M. S. Chang 和 C. P. Yen，《Android 上 Facebook Messenger 的证据收集》，《国际网络安全杂志》，第22卷，第5期，第828–837页，2020年。[7] M. Motyli´nski、A. MacDermott、F. Iqbal、M. Hussain 和 S. Aleem，《 Discord 应用程序的数字取证采集与分析》，载于*2020*年国际通信、计算、网络安全与信息学会议（*CCCI*）。IEEE，2020年，第1–7页。[8] M. S. Chang 和 C. Y. Chang，《Windows 10 上 Line Messenger 的取证分析》，《计算机杂志》，第30卷，第1期，第114–125页，2019年。[9] I. Riadi、A. Fadlil 和 A. Fauzan，《Android 设备上 Line Messenger 的证据收集与识别》，《国际计算机科学与信息安全杂志（*IJCSIS*）》，第16卷，第5期，第201–205页，2018年。

[10] M. S. Chang 和 C. Y. Chang，《Android 上 Line Messenger 的取证分析》，《计算机杂志》，第29卷，第1期，第11–20页，2018年。[11] I. Riadi、S. Sunardi 和 M. E. Rauli，《专有操作系统上 LINE 应用程序的实时取证分析》，*Kinetik*：游戏技术、信息系统、计算机网络、计算、电子与控制，第305–314页，2019年。[12] H. A. Ghannam，《Android 智能手机中巨型即时通讯应用“WhatsApp”伪迹的取证分析》，应用信息、通信与技术杂志，第5卷，第2期，第63–72页，2018年。[13]D. Orr 和 A. Castro，《Android 平台上的 WhatsApp 即时通信软件：对物理设备的取证检查》，法医科学方法与技术，第1卷，第4–19页，2018年。[14] C. Anglano、M. Canonico 和 M. Guazzone，《Android 智能手机上 Telegram 即时通信软件的取证分析》，数字调查，第23卷，第31–49页，2017年。[15] G. B. Satrya、P. T. Daely 和 M. A. Nugroho，《Android 设备上 Telegram 即时通信软件的数字取证分析》，载于*2016*年国际信息与通信技术及系统会议（*ICTS*）。IEEE，2016年，第1–7页。[16] D. Hintea、A. Sangins 和 R. Bird，《Android 设备上 Telegram 即时通信应用程序的取证分析》，载于欧洲网络战与安全会议。*Academic Conferences International Limited*，第12卷，2018年，第217–223页。[17] J. Gregorio、A. Gardel 和 B. Alarcos，《Windows Phone 上 Telegram 即时通信软件的取证分析》，数字调查，第22卷，第88–106页，2017年。[18] J. Gregorio、B. Alarcos 和 A. Gardel，《macOS 上 Telegram 桌面版即时通信软件的取证分析》，卷，第6卷，第39–48页，2018年。[19] J. Choi、J. Park 和 H. Kim，《KakaoTalk 即时通信软件备份数据库文件的取证分析》，载于*2017*年*IEEE*国际大数据与智能计算会议（*BigComp*）。IEEE，2017年，第156–161页。[20]J. Yoon 和 Y. Park，《KakaoTalk 即时通信服务的取证分析及 KakaoTalk 与 WhatsApp 伪迹比较研究》，韩国信息与通信工程学会杂志，第20卷，第4期，第777–785页，2016年。[21]A. K. Agrawal、A. Sharma 和 P. Khatri，《虚拟环境中 Facebook 应用程序的数字取证分析》，载于*2019*年第六届可持续全球发展计算国际会议（*INDIACom*）。IEEE，2019年，第660–664页。[22]M. I. Al-Saleh 和 Y. A. Forihat，《Android 设备上的 Skype 取证分析》，国际计算机应用杂志，第78卷，第7期，2013年。[23] M. Nicoletti 和 M. Bernaschi，《Microsoft Skype for Business 的取证分析》，数字调查，第29卷，第159–179页，2019年。[24] S. M. Judge，移动取证：消息分析 *ing* 应用程序 *Signal*。中俄克拉荷马大学，2018 年。[25] S. Krishnapriya、V. Priyanka 和 S. S. Kumar，“安卓手机中 Signal 应用程序的取证提取与分析”，载于 *2021* 年国际取证、分析、大数据与安全会议（*FABS*），第 1 卷。IEEE，2021 年，第 1–6 页。[26]S. Wu、Y. Zhang、X. Wang、X. Xiong 和 L. Du，“安卓智能手机上微信的取证分析”，数字调查，第 21 卷，第 3–10 页，2017 年。[27] L. Zhang、F. Yu 和 Q. Ji，“微信消息的取证分析”，载于 *2016* 年第六届国际仪器与测量、计算机、通信与控制会议（*IMCCC*）。IEEE，2016 年，第 500–503 页。[28] Q. Li、D. Du、Z. Yang、B. Liu 和 J. Yan，“安卓系统中 QQ 取证的一种灵活方法”，载于*2017* 年 *IEEE* 第二届先进信息技术、电子与自动化控制会议（*IAEAC*）。IEEE，2017 年，第 855–861 页。[29] Y. Gao 和 T. Cao，“实时系统中 QQ 的内存取证。”计算机杂志，第 5 卷，第 4 期，第 541–548 页，2010 年。[30] A. Iqbal、A. Marrington 和 I. Baggili，“ChatON 即时通信应用的取证痕迹”，载于*2013* 年第八届数字取证工程系统方法国际研讨会（*SADFE*）。IEEE，2013 年，第 1–6 页。[31] O. S. Adebayo、S. A. Sulaimon、O. Osho 和 S. M. Abdulhamid，“安卓设备上 Kik 即时通讯应用的取证分析。”联邦大学第二届国际工程会议……，2017 年。[32] K. M. Ovens 和 G. Morison，“iOS 设备上 Kik 即时通讯应用的取证分析 ”，数字调查，第 17 卷，第 40–52 页，2016 年。[33] T. Mehrotra 和 B. Mehtre，“安卓设备上 Wickr 应用程序的取证分析”，载于 *2013* 年 *IEEE* 国际计算智能与计算研究会议。IEEE，2013 年，第 1–6 页。[34] G. Kim、S. Kim、M. Park、Y. Park、I. Lee 和 J. Kim，“即时通信应用的取证分析：解密 Wickr 和私人短信数据”，《国际法医科学：数字调查》，第 37 卷，文章编号 301138，2021 年。[35] M. Azhar 和 T. E. A. Barton，“安卓平台上安全、阅后即焚即时通信应用的取证分析”，载于全球安全、安保与可持续发展国际会议。Springer，2017 年，第 27–41 页。[36] F. Anwar、A. Fadlil 和 I. Riadi，“通过 WhatsApp 即时通讯应用发送的 PNG图像的图像质量分析”，*Telematika*，第 14 卷，第 1 期，第 1–12 页，2021 年。[37] A. Marfianto 和 I. Riadi，“基于安卓的 WhatsApp 即时通讯应用取证分析：采用文本挖掘方法”，《国际网络安全与数字取证期刊》（*IJCSDF*），第 7 卷，第 3 期，第 319–327 页，2018 年。