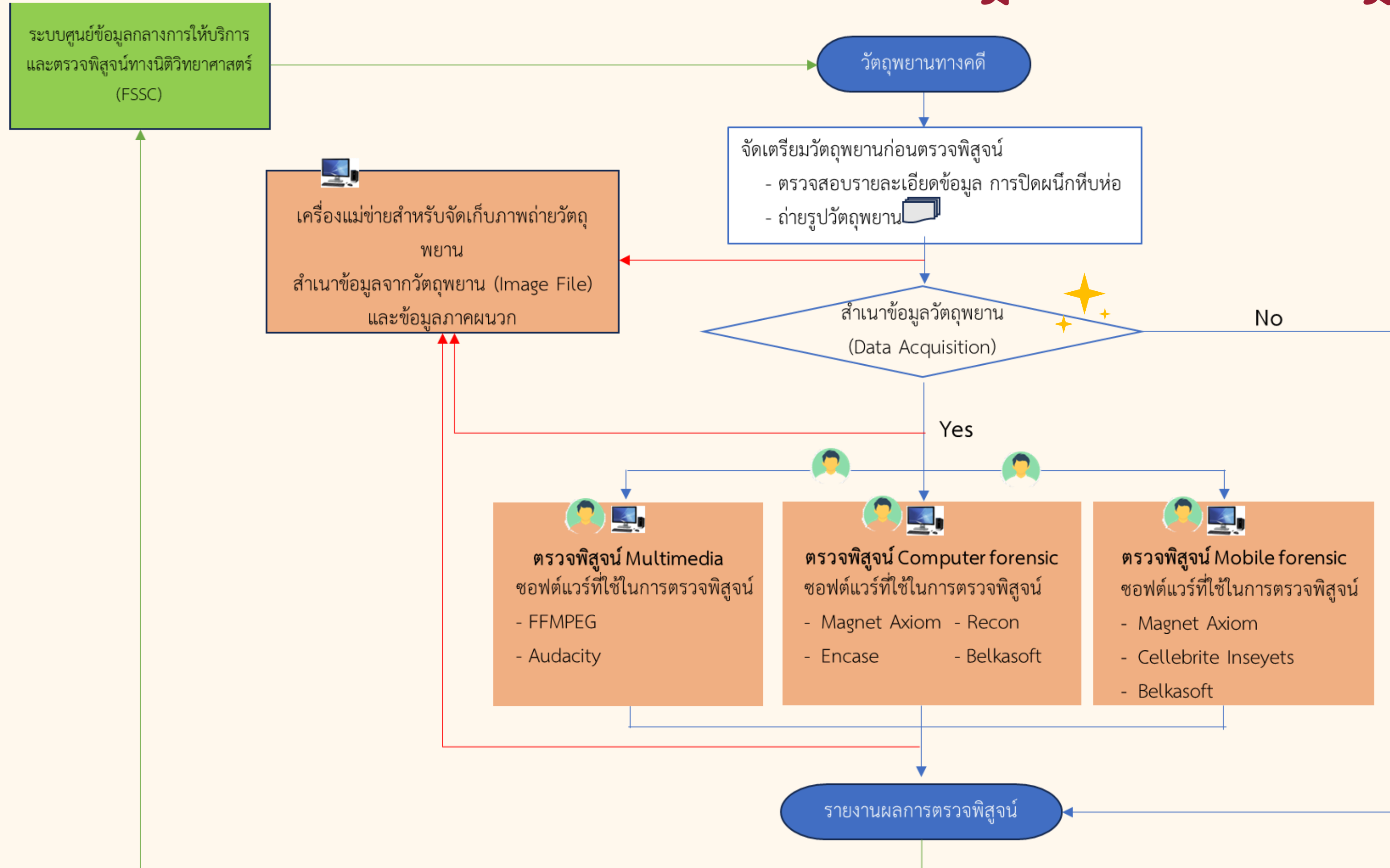


Software or Hardware

เอ๊ะ !!!! แบบไหนดีกว่ากันนะ ???



ขั้นตอนการปฏิบัติงานในห้องปฏิบัติการ



สำเนาข้อมูลวัตถุดิบ (Data Acquisition)

สร้างสำเนาที่เหมือนจริงของข้อมูลทั้งหมดบนอุปกรณ์นั้นๆ
โดยไม่ทำการเปลี่ยนแปลงข้อมูลต้นฉบับ
เพื่อนำไปตรวจสอบพิสูจน์วิเคราะห์หาหลักฐานที่เกี่ยวข้อง



Image



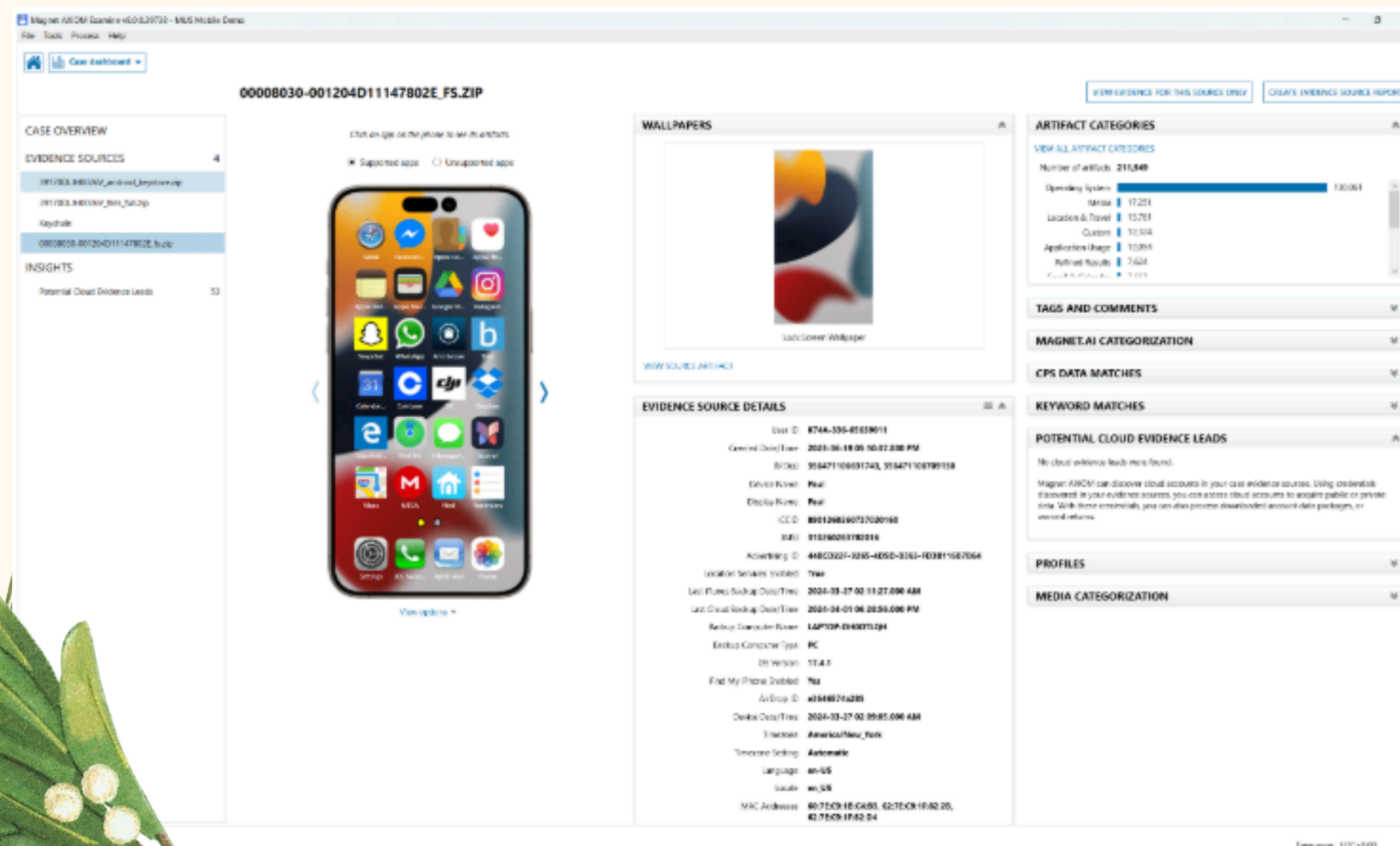
Forensic Imager TX1

เป็นเครื่องมือที่ออกแบบมาโดยเฉพาะสำหรับการเก็บรวบรวมหลักฐานดิจิทัลจากอุปกรณ์ต่างๆ เช่น ฮาร์ดดิสก์ แฟลชไดรฟ์ หรือสมาร์ทโฟน โดยการสร้างข้อมูล Image ของข้อมูลทั้งหมดบนอุปกรณ์นั้นอย่างครบถ้วนและแม่นยำ





Magnet Axiom



เป็นซอฟต์แวร์ที่ได้รับความนิยมอย่างสูงในวงการ Digital Forensics ใช้สำหรับวิเคราะห์ข้อมูลจากอุปกรณ์อิเล็กทรอนิกส์ต่างๆ เพื่อค้นหาหลักฐานที่เกี่ยวข้อง เช่น คอมพิวเตอร์ โทรศัพท์มือถือ แท็บเล็ต และอุปกรณ์จัดเก็บข้อมูลอื่นๆ

เปรียบเทียบการสกัดข้อมูลจากโทรศัพท์มือถือ

ระบบปฏิบัติการ IOS และ ANDROID

โดยการใช้เครื่องมือ TX1 และ ซอฟต์แวร์ MAGNET AXIOM



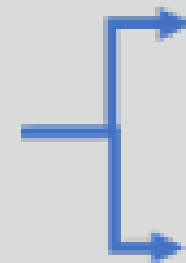
VS



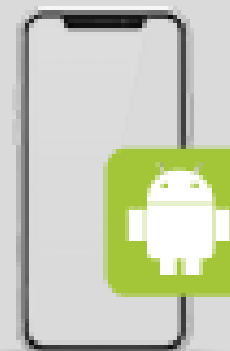
Method



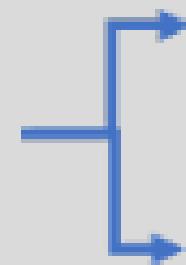
Brand: Apple
Model Number: A1586
Model name: iPhone 6
iOS version: 12.5.7



+



Brand: Samsung
Model Number: SM-A750GN
Model name: Galaxy A7
Android version: 10.0



+



Result

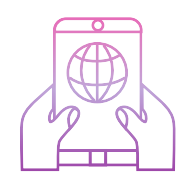
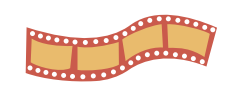


IOS



Android

Acquired and analyzed method	IOS		Android	
	TX1 Imager	Magnet AXIOM	TX1	Magnet AXIOM
Mobile Device Artifacts				
Geolocation Artifacts : GPS data, Cell tower connection, and timestamps	Wifi profile (30)	Wifi profile (30)	-	Wifi profile (344)
Communication Artifacts : include text message, Call logs, Emails, instant messaging posts and more	Contact (266) Call log (605) iMessage/SMS/MMS (771)	Contact (266) Call log (605) iMessage/SMS/MMS (771)	Contact (-) Call log (-) Android SMS/MMS (601)	Contact (1,941) Call log (546) Android SMS/MMS (601)
Application Artifacts	Installed app (471)	Installed app (893)	-	Installed app (113)
Media artifacts : Picture, VDO, Audio	Picture (7,125) Audio (5)	Picture (13,000) Audio (7)	Picture (23,025) Audio (326)	Picture (43,478) Audio (875)
Web Browser Activity Artifacts : Browsing History, Search queries, Bookmarks, Cached data, and Downloaded	Safari History (150) Google Search (24) Search Term (4) Bookmark (10)	Safari History (146) Google Search (24) Search Term (4) Bookmark (10)	Google Play Search (237)	Google Play Search (237)



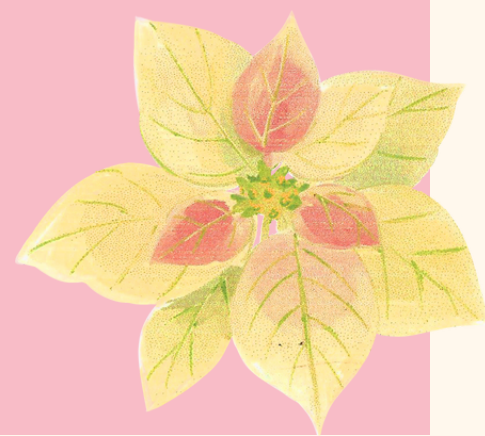
Discussion

ระบบปฏิบัติการ iOS:



ทั้งเครื่องมือ TX1 Imager และซอฟต์แวร์ Magnet Axiom

สามารถดึงข้อมูลได้หลากหลายประเภท โดย **Magnet Axiom** สามารถดึงข้อมูลได้มากกว่า TX1



Acquired and analyzed method	IOS	
	TX1 Imager	Magnet AXIOM
Mobile Device Artifacts		
Geolocation Artifacts : GPS data, Cell tower connection, and timestamps	Wifi profile (30)	Wifi profile (30)
Communication Artifacts : include text message, Call logs, Emails, instant messaging posts and more	Contact (266) Call log (605) iMessage/SMS/MMS (771)	Contact (266) Call log (605) iMessage/SMS/MMS (771)
Application Artifacts	Installed app (471)	Installed app (893)
Media artifacts : Picture, VDO, Audio	Picture (7,125) Audio (5)	Picture (13,000) Audio (7)
Web Browser Activity Artifacts : Browsing History, Search queries, Bookmarks, Cached data, and Downloaded	Safari History (150) Google Search (24) Search Term (4) Bookmark (10)	Safari History (146) Google Search (24) Search Term (4) Bookmark (10)

Discussion

ระบบปฏิบัติการ Android:



TX1 Imager มีข้อจำกัดในการดึงข้อมูลบางประเภทจากอุปกรณ์ Android

ซอฟต์แวร์ **Magnet Axiom** มีประสิทธิภาพเหนือกว่า TX1 Imager ในแง่ของปริมาณข้อมูล

	Android	
Acquired and analyzed method	TX1	Magnet AXIOM
Mobile Device Artifacts		
Geolocation Artifacts : GPS data, Cell tower connection, and timestamps	-	Wifi profile (344)
Communication Artifacts : include text message, Call logs, Emails, instant messaging posts and more	Contact (-) Call log (-) Android SMS/MMS (601)	Contact (1,941) Call log (546) Android SMS/MMS (601)
Application Artifacts	-	Installed app (113)
Media artifacts : Picture, VDO, Audio	Picture (23,025) Audio (326)	Picture (43,478) Audio (875)
Web Browser Activity Artifacts : Browsing History, Search queries, Bookmarks, Cached data, and Downloaded	Google Play Search (237)	Google Play Search (237)

Conclusion

iOS: ทั้งสองเครื่องมือสามารถดึงข้อมูลพื้นฐาน เช่น รายชื่อ บันทึกการโทร และ SMS

Android: TX1 มีข้อจำกัดในการดึงข้อมูลบางประเภท ข้อมูลที่ซับซ้อน แอปพลิเคชัน ข้อมูลบนคลาวด์ และโทรศัพท์ที่เข้ารหัส โดยรวมแล้ว Axiom ดึงข้อมูลได้มากกว่า TX1



Mobile Phone



Software
Magnet Axiom



Hardware
TX1 Imager

