รายงานสัมมนาเรื่อง

การนำเสนอการตรวจพิสูจน์อุปกรณ์สื่อสาร บนระบบปฏิบัติการ Windows Mobile

(Introduction to Windows Mobile Forensics)

ผู้ให้สัมมนา นายสมาจารย์ กษณะ

รหัสประจำตัว 52312338

อาจารย์ที่ปรึกษา พันตำรวจเอกศิริพงษ์ ติมุลา

วันที่ให้สัมมนา วันเสาร์ที่ 14 สิงหาคม พ.ศ. 2553

สถานที่ ห้อง 4205 **อาคาร** ว.4 **เวลา** 9.00-12.00 น.

วิชา 510 701 **สัมมนาสำหรับนิติวิทยาศาสตร์** 1

ภาคต้น ปีการศึกษา 2553

คำนำ

รายงานฉบับนี้เป็นส่วนหนึ่งของ วิชาสัมมนาสำหรับนิติวิทยาศาสตร์ 1 รหัสวิชา 510701 หลักสูตรระดับปริญญามหาบัณฑิต คณะวิทยาศาสตร์ สาขาวิชานิติวิทยาศาสตร์ ภาคเรียนที่ 1 ประจำปีการศึกษา 2553 โดยผู้ให้สัมมนาได้ทำการแปลและเรียบเรียงบทความต้นฉบับภาษาอังกฤษ เรื่อง Introduction to Windows Mobile Forensics เกี่ยวกับการนำเสนอการตรวจพิสูจน์อุปกรณ์สื่อสารบนระบบปฏิบัติการ Windows Mobile

เนื้อหาของรายงานสัมมนาฉบับนี้กล่าวถึง อุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile ซึ่งระบบปฏิบัติการดังกล่าวเป็นแหล่งข้อมูลสำคัญในการใช้เป็นพยานหลักฐานของการสืบสวนในหลายๆ ด้าน อุปกรณ์สื่อสารเคลื่อนที่ดังกล่าวสามารถเก็บบันทึกข้อมูลต่างๆ ของผู้ใช้ได้ เช่น การติดต่อสื่อสารทางโทรศัพท์ของผู้ใช้ รายชื่อผู้ติดต่อ ปฏิทิน การติดต่อสื่อสารทางอื่นที่นอกเหนือจากการโทรศัพท์ (อินเทอร์เน็ต) และการระบุถึงฐานที่อยู่ของผู้ใช้ในชั่วขณะหนึ่งๆ บทความนี้ได้นำเสนอภาพรวมเกี่ยวกับการตรวจพิสูจน์ระบบปฏิบัติการ Windows Mobile อธิบายถึงการใช้วิธีการต่างๆ ในการได้มาและการตรวจสอบข้อมูลที่ได้จากระบบปฏิบัติการดังกล่าว ซึ่งในที่นี้จะได้บรรยายถึงบริเวณของพื้นที่ในการจัดเก็บข้อมูลและชนิดของไฟล์ข้อมูลที่ถูกเก็บบันทึกบนระบบ รวมไปถึงข้อความสั้นข้อความรูปภาพ อีเมลล์ ประวัติการใช้อินเทอร์เน็ต และการนำเข้า Registry บนระบบด้วย บทความนี้ยังได้มีการสรุปผลที่เกี่ยวเนื่องจากการใช้โปรแกรม MobileSpy monitoring ไว้เช่นเดียวกัน

ขอขอบคุณ พันตำรวจเอกศิริพงษ์ ติมุลา ที่กรุณาช่วยให้คำปรึกษาแนะนำ อาจารย์ผศ.ดร. ธงชัย เตโชวิศาล และรศ.พ.ต.อ.หญิงดร.พัชรา สินลอยมา ที่ช่วยให้ข้อเสนอแนะ ทำให้การสัมมนาและรายงานฉบับนี้สมบูรณ์ สำเร็จลุล่วงไปด้วยดี ขอขอบคุณผู้เข้าร่วมสัมมนาทุกท่าน

ท้ายนี้ ผู้จัดทำหวังเป็นอย่างยิ่งว่า รายงานฉบับนี้จะเป็นประโยชน์ต่อท่านผู้อ่านที่มีความสนใจและต้องการศึกษาค้นคว้า ตลอดจนเป็นการเพิ่มพูนความรู้ในเรื่องดังกล่าวได้ไม่มากก็น้อย

ผู้จัดทำ

นายสมาจารย์ กษณะ

บทคัดย่อ

อุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile เริ่มเป็นที่แพร่หลายขึ้นอย่างกว้างขวางในปัจจุบันนี้ ซึ่งระบบปฏิบัติการดังกล่าวเป็นแหล่งข้อมูลสำคัญในการใช้เป็นพยานหลักฐานของการสืบสวนในหลายๆ ด้าน อุปกรณ์สื่อสารเคลื่อนที่ดังกล่าวสามารถเก็บบันทึกข้อมูลต่างๆ ของผู้ใช้ได้ เช่น การติดต่อสื่อสารทางโทรศัพท์ของผู้ใช้ รายชื่อผู้ติดต่อ ปฏิทิน การติดต่อสื่อสารทางอื่นที่นอกเหนือจากการโทรศัพท์ (อินเทอร์เน็ต) และการระบุถึงฐานที่อยู่ของผู้ใช้ในชั่วขณะหนึ่งๆ แม้ว่านักวิเคราะห์จะสามารถนำความรู้จากระบบปฏิบัติการ Windows มาใช้กับระบบปฏิบัติการ Windows Mobile ได้ แต่ก็มีหลายจุดสำคัญที่ต้องใช้ความรู้ความสามารถและเครื่องมือที่จำเพาะเจาะจงในการค้นหา แปลความจากพยานหลักฐานที่ได้ บทความนี้จึงได้นำเสนอภาพรวมเกี่ยวกับการตรวจพิสูจน์ระบบปฏิบัติการ Windows Mobile อธิบายถึงการใช้วิธีการต่างๆ ในการได้มาและการตรวจสอบข้อมูลที่ได้จากระบบปฏิบัติการดังกล่าว ซึ่งในที่นี้จะได้บรรยายถึงบริเวณของพื้นที่ในการจัดเก็บข้อมูลและชนิดของไฟล์ข้อมูลที่ถูกเก็บบันทึกบนระบบ รวมไปถึงข้อความสั้นข้อความรูปภาพ อีเมลล์ ประวัติการใช้อินเทอร์เน็ต และการนำเข้า Registry บนระบบด้วย บทความนี้ยังได้มีการสรุปผลที่เกี่ยวเนื่องจากการใช้โปรแกรม MobileSpy monitoring ไว้เช่นเดียวกัน

Abstract

Windows Mobile devices are becoming more widely used and can be a valuable source of evidence in a variety of investigations. These portable devices can contain details about an individual's communications, contacts, calendar, online activities, and whereabouts at specific times. Although forensic analysts can apply their knowledge of other Microsoft operating systems to Windows Mobile devices, there are sufficient differences that require specialized knowledge and tools to locate and interpret digital evidence on these systems.This paper provides an overview of Windows Mobile Forensics, describing various methods of acquiring and examining data on Windows Mobile devices. The locations and data formats of useful information on these systems are described, including text messages, multimedia, e-mail, Web browsing artifacts, and Registry entries. This paper concludes with an illustrative scenario involving MobileSpy monitoring software.

สารบัญ

1.บทนำ

อุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile มีอยู่ในปัจจุบันมากมายจึงเป็นโอกาสและสิ่งที่ท้าทายสำหรับผู้ปฏิบัติงานด้านการตรวจวิเคราะห์ ซึ่งอุปกรณ์เหล่านี้เป็นส่วนประกอบที่สำคัญของคอมพิวเตอร์ โดยผู้ใช้ได้พกพาติดตัวใส่ไว้ในกระเป๋าของพวกเขา อุปกรณ์เหล่านี้ได้บรรจุข้อมูลที่สำคัญรวมทั้งหมด ด้วยเหตุนี้จึงสามารถนำไปใช้ประโยชน์ได้โดยอาศัยความคิด มุมมอง ทัศนคติในการตรวจวิเคราะห์ รวมทั้งการติดต่อสื่อสาร มัลติมีเดีย และข้อมูลของตำแหน่งที่ตั้ง อุปกรณ์เหล่านี้สามารถเป็นแหล่งข้อมูลพยานหลักฐาน ในช่วงของการแพร่หลายของอาชญากรรม รวมทั้ง การฆาตรกรรม การหลอกหลวง และการโจรกรรมข้อมูล ซึ่งข้อมูลที่เกี่ยวกับลักษณะนิสัยส่วนบุคคลของผู้ที่ใช้อุปกรณ์นี้อยู่สามารถให้ข้อมูลในรูปของตัวเลขแก่ผู้สอบสวน พร้อมกับมีความสำคัญอย่างมากในความเข้าใจเกี่ยวกับวิธีการทำงาน(*modus operandi*)ของผู้ต้องสงสัยและกิจกรรมของผู้ที่ถูกหลอก นอกจากนั้น ผู้สอบสวนในงานเกี่ยวกับอาชญากรรม เกี่ยวกับบริษัท และทางทหาร จะต้องมีความสามารถในการเข้าใจความหมายของข้อความ มีทักษะที่ดี ในการสืบค้นโปรแกรมที่มีอยู่ เพราะว่าอนุญาตให้มีการควบคุมติดตามจากระยะไกลของอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile วิธีการที่ได้มาใหม่นี้เหมาะสมกับผู้ปฏิบัติงานด้านการตรวจวิเคราะห์ ซึ่งสามารถนำไปใช้ประโยชน์ ในการดึงข้อมูลจากอุปกรณ์เก็บข้อมูลต่างๆ ทำให้ได้ข้อมูลจำนวนที่มากขึ้นบนอุปกรณ์เหล่านี้ รวมถึงที่มีการลบข้อมูล

ในขณะเดียวกันอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile ค่อนข้างใหม่ และการจัดรูปแบบข้อมูล เป็นสิ่งที่ผู้ปฏิบัติงานด้านการตรวจวิเคราะห์ยังไม่คุ้นเคย ตัวอย่างเช่น ปริมาณ ความจุของไฟล์ และการฝังตัวของฐานข้อมูล(คลังข้อมูล) เครื่องมือสำหรับแปลคำสั่งและวิเคราะห์ข้อมูลบนระบบปฏิบัติการ Windows Mobile มีการแข่งขันกันไปพร้อมกับความก้าวหน้าในเทคโนโลยี นักตรวจวิเคราะห์จำเป็นต้องเข้าใจถึงสิ่งที่สำคัญและซ่อนอยู่ในเทคโนโลยี และการจัดรูปแบบข้อมูลเหล่านั้นที่มีอยู่ที่สำคัญกว่าคือการใช้ประโยชน์อันหลากหลายของเครื่องมือไปสู่การคัดลอก ดึงเอาข้อมูลออกมาใช้ประโยชน์ได้

บทความนี้ได้ครอบคลุมถึงวิธีการอันหลากหลาย ในการได้มาและการวิเคราะห์ข้อมูลอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile การใช้ประโยชน์ทั้งในด้านเกี่ยวกับการค้า และเปิดเผยแหล่งข้อมูลของเครื่องมือ รายละเอียดเกี่ยวกับการทดสอบอุปกรณ์ที่เคยใช้สำหรับบทความนี้ดังในตารางที่ 1

Table 1 – Summary of test device characteristics.

Manufacturer/model	OS version	OS build	Radio version
HTC S620 (Dash)	Windows Mobile 6 Standard, 5.2.1236	17741.0.2.1	4.1.13.61_03.21.90
Motorola Q	Windows Mobile 5.0, 5.1.195	14960.2.4.0	Q2-BP_C_06.0B.11P, Q2 Portable
Samsung i607 (Blackjack)	Windows Mobile 5.0 with Messaging and Security Feature Pack, 5.1.342	15100.3.0.2	

Manufacturer/model : HTC S620 (Dash)

Manufacturer/model : Motorola Q

Manufacturer/model : Samsung i607 (Blackjack)

เพื่อทำให้เป็นการง่ายขึ้นสำหรับผู้ปฏิบัติงานด้านการตรวจวิเคราะห์ ในการใช้ประโยชน์ เพื่อเป็นพยานหลักฐาน จากอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile บทความนี้ได้เริ่มต้นตั้งแต่ เกี่ยวกับลักษณะทั่วไปของ Windows Mobile ครอบคลุมถึงผลที่ได้ ที่เป็นที่ยอมรับกันโดยทั่วไป ในการปฏิบัติสำหรับการได้มาของข้อมูลจากระบบปฏิบัติการนี้ ส่วนที่เหลืออยู่ของบทความนี้ได้บรรยายในเรื่องของการใช้ประโยชน์ของข้อมูล คือการเก็บข้อมูล และทำอย่างไรถึงจะตรวจสอบแหล่งข้อมูลที่สำคัญเหล่านี้ได้ บทความนี้ยังได้มีการสรุปผลที่เกี่ยวเนื่องจากการใช้โปรแกรม MobileSpy monitoring ส่วนอุปสรรคทั่วๆไป ซึ่งได้อภิปรายถึงวิธีการช่วยผู้ปฏิบัติหาหนทางจัดการกับสิ่งยุ่งยาก นำไปสู่การตีพิมพ์ออกมา อาทิเช่น การแปลข้อมูลที่ผิดพลาด

บทความนี้ได้ทำการทดสอบกับอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile ที่ไม่มีรหัสผ่านป้องกัน เป็นที่ทราบว่า อุปกรณ์ที่มีรหัสผ่านป้องกัน อาจจะมีวิธีการวางแผนในการใช้อุปกรณ์ต่างๆ ไปจนถึงการลบข้อมูลที่ผู้ใช้ได้สร้างขึ้น หลังจากการใส่ตัวเลขล้มเหลว ในการพยายามเริ่มทำงาน (logon) ยิ่งกว่าความก้าวหน้า สิ่งที่ได้มาคือวิธีการที่คล้ายกันกับ การคัดลอกชิฟ(chip) อาจจะสามารถนำไปสู่การเข้าถึงรหัสผ่านป้องกันโดยทางอ้อม และเนื่องจากการใช้ Flash memory และการติดเครื่องมือวัดระดับในอุปกรณ์เหล่านี้ สามารถทำให้ง่ายขึ้นสำหรับนักตรวจวิคราะห์ ในการดึงข้อมูลจากอุปกรณ์เก็บข้อมูลต่างๆ ที่ถูกลบได้มากกว่า ดังวิธีการรายละเอียดในบทความของ(van der Knijff, 2009; Klaver, 2010)

2.ลักษณะทั่วไปของ Windows Mobile

จำนวนมากของตัวอย่างที่เป็นบทเรียน เกี่ยวกับการเรียนรู้จากกระบวนการตรวจพิสูจน์โดยระบบปฏิบัติการ Microsoft Windows ที่แตกต่างกัน ซึ่งสามารถนำไปสู่การประยุกต์ใช้กับ Windows Mobile รวมถึงความเข้าใจเกี่ยวกับระบบของไฟล์ FAT และไฟล์ index.dat เช่นเดียวกับคอมพิวเตอร์แบบตั้งโต๊ะ (desktop) หรือคอมพิวเตอร์ชนิดที่เป็นแบบกระเป๋าหิ้วที่ใช้แบตเตอรี่ (laptop) อุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile จะเก็บข้อมูลที่สำคัญเกี่ยวกับกิจกรรมของผู้ใช้ ซึ่งสามารถที่จะเกี่ยวเนื่องกันกับการแสดงข้อมูลในรูปของตัวเลขในการสืบสวน คล้ายกับโปรแกรมค้นผ่านเว็บ (Web browsing) ผู้ใช้ได้สร้างแฟ้มข้อมูล และการลงทะเบียนเข้า (Registry entries) เมื่อไม่นานมานี้มีชื่อของคอมพิวเตอร์ที่ทำให้เชื่อมต่อกันพร้อมทั้ง WiFi ในการเข้าถึงจุดตำแหน่ง ยิ่งกว่านั้นสามารถเก็บไว้ที่อุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile ซึ่งสามารถใช้ประโยชน์ได้บางส่วนของการแสดงข้อมูลในรูปของตัวเลขในการสืบสวน อย่างไรก็ตาม ประเด็นนั้นก็พอเพียงที่บอกถึงความแตกต่างระหว่างระบบ Windows Mobile และระบบปฏิบัติการของ Windows อื่น จนถึงต้องการศึกษาเป็นพิเศษในข้อมูลเฉพาะบางเรื่อง และเครื่องมือไปสู่การหาแหล่งที่ตั้ง และแปลคำสั่งการแสดงข้อมูลในรูปของตัวเลขเพื่อเป็นหลักฐาน

การใช้ประโยชน์ของ Windows Mobile ในรูปแบบที่เปลี่ยนแปลงของระบบไฟล์ FAT เรียกว่าระบบไฟล์Transaction-safe FAT (TFAT) ซึ่งมีบางส่วนของการกู้ข้อมูลเป็นลักษณะเฉพาะของกรณีที่อุปกรณ์เกิดการปิดระบบอย่างกะทันหัน ดังแสดงไว้ในรูปที่ 1 ระบบไฟล์ลำดับชั้นบนอุปกรณ์อย่างนี้มีความคล้ายคลึงกันกับระบบปฏิบัติการของ Microsoft อื่น อันซึ่งใครก็ตามน่าจะคุ้นเคย ผู้ที่ปฏิบัติงานด้านการตรวจพิสูจน์ มีการตรวจสอบด้วย Windows ของระบบคอมพิวเตอร์

ส่วนใหญ่ของผู้ใช้ที่สร้างแฟ้มข้อมูลขึ้นมา รวมทั้งรูปถ่ายดิจิตอล และถ่ายวีดีโอด้วยอุปกรณ์กล้องถ่ายภาพ โดยเก็บไว้ในโฟลเดอร์ ‘‘My Documents’’ ซึ่งตรงกันข้ามกับ อุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile เก็บส่วนที่เหลือเกี่ยวกับกิจกรรมของผู้ใช้ในลักษณะที่หลากหลายของตำแหน่งที่เก็บ เหล่านี้การใช้สิ่งที่สร้างขึ้นรวมทั้งไฟล์ index.dat เกี่ยวเนื่องกับการใช้ Internet Explorer และการฝังตัวของฐานข้อมูล ไฟล์ที่ลงท้ายด้วย ‘‘.vol’’ ส่วนนามสกุลของแฟ้มได้แสดงในช่องหน้าต่างทางขวามือของรูปที่ 1 นอกจากนั้น การลงทะเบียนของอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile สามารถเก็บข้อมูลเกี่ยวกับผู้ใช้และกิจกรรมของเขาเหล่านั้น ดังที่แสดงในหัวข้อ ‘‘Examining Registry hives’’ ของบทความนี้

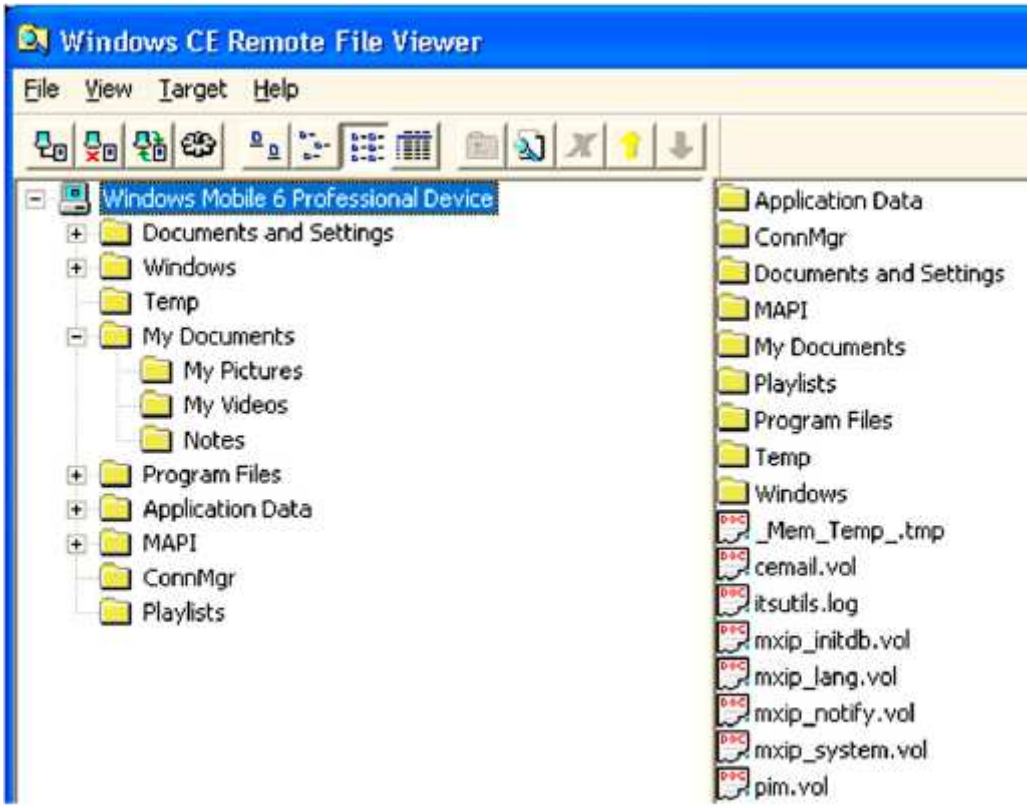

Fig. 1 – File system hierarchy on a Samsung i607 (Blackjack).

2.1 ตำแหน่งที่ตั้งของไฟล์ข้อมูลบนอุปกรณ์ Windows Mobile

อย่างไรก็ตาม ไฟล์บางอย่างที่คล้ายกันกับ cemail.vol สามารถพบได้ในทุกๆ อุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile ตำแหน่งที่ตั้งของการใช้สิ่งที่ประดิษฐ์บนความหลากหลายของแบบอุปกรณ์ Mobile สามารถเปลี่ยนแปลงได้ ดังในตารางที่ 2 ส่วนลักษณะทั่วไปของความเป็นไปได้ในการใช้ประโยชน์จากแหล่งที่มาของหลักฐานบนอุปกรณ์ Samsung i607 (Blackjack), HTC S62 (Dash) และ Motorola Q โดยจำนวนมากของแหล่งที่ตั้งเหล่านี้ จะพบประเภทของอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile อื่นด้วย ชื่อที่เพิ่มต่อท้ายในส่วนของ ชื่อและนามสกุลของไฟล์กลายเป็นเรื่องที่น่าสนใจ อาจจะพบในแหล่งที่ตั้งอื่นเหมือนกับโฟลเดอร์ ‘‘\Temp’’

นอกจากนี้รายละเอียดเกี่ยวกับรายชื่อพื้นที่ ดังในตารางที่ 2 ซึ่งได้จัดทำเมื่อไม่นาน โดยแสดงไว้ในบทความนี้ พร้อมด้วยตัวอย่างของวิธี ที่จะสามารถนำข้อมูลไปใช้ประโยชน์จากมุมมอง ทัศนคติของการตรวจวิเคราะห์

Table 2 – Potentially useful sources of evidence on Windows Mobile devices.

File	Description
\cemail.vol	An embedded database that stores information relating to communications, including text messages and portions of e-mails, not including file attachments.
\pim.vol	An embedded database that includes call logs (clog.db), address book information, calendar items, speed dial details (speed.db), and to do tasks.
\ReplStorVol	A file replication database used to synchronize items on the device with data in another location (Microsoft, 2008a).
\My Documents\My Pictures	A repository of photographs taken or downloaded by the user. This is the default download location for pictures.
\My Documents\UAContents	A folder with artifacts of user activities, including portions of MMS in ".dat" files and an MMS log file.
\Documents and Settings\default\user.hv	The User Registry hive.
\Documents and Settings\default.hv OR system.hv[a]	The System Registry hive.
\Windows\Messaging	A repository of viewed SMS and e-mail messages, stored in ".mpb" files.
\Windows\Messaging\Attachments	A repository of downloaded e-mail attachments in ".att" files.
\Windows\Profiles\guest	Contains Internet Explorer history, as well as cache and cookie files, including `index.dat` files.
\Windows\Favorites	Internet Explorer bookmarks.
Windows\eT9Cdb.Cdb and eT9Rudb.Rdb	Custom user T9 dictionary files.

a The location of the system Registry hive may vary. The Registry value under HKEY_LOCAL_MACHINE\init\BootVars\SystemHive contains the full path of the system hive.

3. กระบวนการตรวจสอบทางนิติวิทยาศาสตร์สำหรับ Windows Mobile

ในทัศนคติของนิติวิทยาศาสตร์แล้ว เป็นเรื่องที่ไม่ง่ายเลยในการได้มาและตรวจสอบข้อมูลจากอุปกรณ์สื่อสารบนระบบปฏิบัติการ Windows Mobile บางครั้งเป็นเรื่องยากในการได้มาและคัดลอกซึ่งไฟล์ข้อมูลที่ระบบปฏิบัติการได้ทำการป้องกันไว้ โปรแกรมที่ใช้สำหรับการคัดลอกไฟล์ซึ่งขึ้นอยู่กับ Windows Mobile APIs ยังไม่สามารถทำการคัดลอกไฟล์บางอย่างได้เช่น cemal.vol pim.vol หรือ Registryของระบบปฏิบัติการ จากเหตุดังกล่าวทำให้โปรแกรมในการคัดลอกไฟล์ไม่สามารถทำการคัดลอกไฟล์ออกมาได้ทั้งหมด ซึ่งโปรแกรมบางชนิดก็อาจทำการคัดลอกไฟล์ได้มากกว่าอีกโปรแกรมหนึ่ง

ยิ่งไปกว่านั้นโปรแกรมที่ใช้ในการตรวจพิสูจน์ยังมีปัญหาในการแปลค่าที่ได้จากระบบปฏิบัติการ ซึ่งปัญหาดังกล่าว อาจเกิดขึ้นจากระบบของการบันทึกไฟล์ข้อมูลแบบ TFAT หรือการได้มาซึ่งข้อมูลที่ไม่เกี่ยวข้อง จึงต้องใช้นักตรวจวิเคราะห์ในการถอดรหัสของไฟล์ดังกล่าว ความขัดแย้งดังกล่าวอาจเกิดมาจากโปรแกรมที่ใช้ในการตรวจพิสูจน์ซึ่งในที่นี้ก็ได้มีการอภิปรายไว้ในส่วนของ “เครื่องมือและการแปลผล” ในบทความนี้ด้วย

ในขณะเดียวกัน ประเด็นดังกล่าว อาจเป็นเรื่องที่นักวิเคราะห์บางท่านคุ้นเคยและสามารถใช้เครื่องมือเดียวกันนี้ทำการตรวจสอบได้ ซึ่งปัจจุบันเครื่องมือที่ได้มีการนำมาใช้อ่านค่าแปลผลเช่น EnCase X-Ways และ FTK ดังรูปที่ 2 แสดงถึงโปรแกรม EnCase ที่นำมาใช้ในการอ่านค่าไฟล์ index.dat และ cache ของ Web บนอุปกรณ์สื่อสาร Samsung i607 (Blackjack)

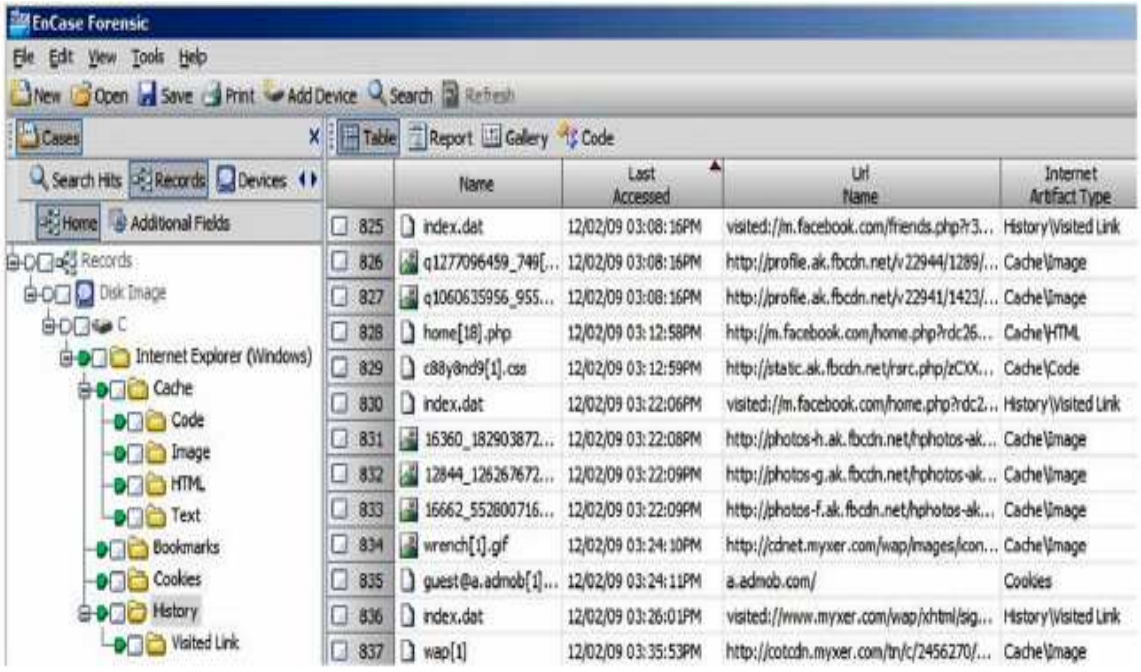

Fig. 2 – Remnants of Internet Explorer browsing activities on a Samsung i607 (Blackjack) device viewed using EnCase.

3.1 กระบวนในการได้มาซึ่งข้อมูล

ถึงแม้ว่าเครื่องมือที่ใช้ในการคัดลอกข้อมูลมีอยู่มาก แต่นักตรวจวิเคราะห์ก็ยังไม่มีวิธีการดึงข้อมูลโดยตรงจากหน่วยความจำแบบแฟลชในอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobileได้และถูกจำกัดในการได้มาซึ่งข้อมูลที่ผ่านทางฮาร์ดแวร์ ดังผลลัพธ์ตามวิธีการที่ได้อธิบายไว้ในบทความนี้ สามารถได้ข้อมูลจากแหล่งเก็บข้อมูล ในอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile แต่ไม่ได้สำเนาที่ครบถ้วนสมบูรณ์จากหน่วยความจำแบบแฟลช โดยมีข้อจำกัดของการป้องกันการเข้าไปลบข้อมูลที่มีอยู่ในหน่วยความจำแบบแฟลช เนื่องจากมีการเก็บข้อมูลในระยะเวลาไม่นาน

นอกจากนี้ การได้มาซึ่งแหล่งเก็บข้อมูลที่เหมาะสม บนอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile โดยเครื่องมือที่ใช้กันอยู่ในปัจจุบันได้ทำงาน แก้ไขตามคำสั่งของผู้จำหน่ายซอฟต์แวร์บนอุปกรณ์เป้าหมาย บางอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile ไม่ยินยอมให้โปรแกรมทำงานในกรณีที่ไม่ลงนามและจะต้องจัดรูปลักษณ์ใหม่ ถึงยอมให้เครื่องมือที่ใช้ในการคัดลอกข้อมูลทำงานได้อย่างถูกต้อง เหมาะสม

มีเครื่องมือสองอย่าง สำหรับการคัดลอกข้อมูลจากอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile คือ XACT จาก Microsystemation (http://www.msab.com) และ itsutils (http://wiki.xda-developers.com/index.php?pagename=XdaUtils) ซึ่งเครื่องมือทั้งสองต้องการ ActiveSync เพื่อติดตั้งเพิ่มเติมบนระบบ ก่อนสามารถที่จะได้ข้อมูลจากการเชื่อมกับอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile

โทรศัพท์เคลื่อนที่เป็นจำนวนมากมีการรองรับ สนับสนุน ย้ายที่จัดเก็บสื่อบันทึก ดังเช่น micro SD cards ซึ่งสามารถเก็บไฟล์ที่ใหญ่ๆ ได้ เช่น รูปภาพดิจิตอล วีดีโอ และเพลง อย่างไรก็ตามเครื่องมือที่ใช้ตรวจวิเคราะห์อาจจะสามารถได้ข้อมูลที่เกี่ยวกับตรรกวิทยา จากการย้ายสื่อบันทึกโดยผ่านทางอุปกรณ์ของตัวมันเอง กระบวนการนี้อาจจะเปลี่ยนข้อมูลบนสื่อบันทึกที่เก็บข้อมูล และจะไม่ให้นักตรวจวิเคราะห์เข้าไปลบข้อมูล เพราะฉะนั้น นอกจากการ์ดที่มีรหัสป้องกันหรือการเข้ารหัสลับ โดยทั่วไปสมควรย้ายสื่อบันทึกอย่างมากและสร้างสำเนาข้อมูล ซึ่งพวกเขาใช้เป็นวิธีมาตรฐานทางคอมพิวเตอร์ในการตรวจวิเคราะห์

ในด้านเกี่ยวกับการค้า เครื่องมือ XACT สามารถได้พื้นที่ของแหล่งเก็บข้อมูลเบื้องต้นมา มีการแบ่งออกเป็นส่วนๆ เท่าๆกันบนอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile ดังรูปที่ 3 แสดง XACT การประยุกต์ใช้ 4 พื้นที่ ที่เก็บข้อมูลบนอุปกรณ์ Motorola Q

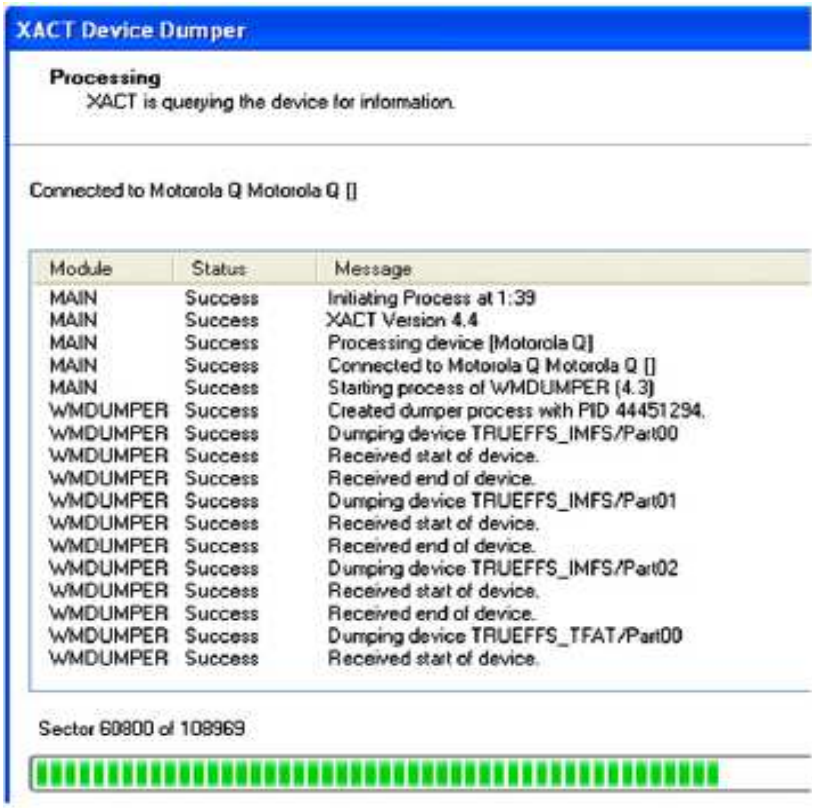

Fig. 3 – XACT acquisition screenshot of Motorola Q.

สำหรับบางอย่างของอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile ผู้แทนจำหน่ายซอฟต์แวร์ XACT สามารถใส่ไว้บนการ์ดหน่วยความจำ และใส่ไว้ในอุปกรณ์ ดังนั้นการทำให้มากขึ้น เพื่อความถูกต้อง โดยลดขนาดลงให้มากที่สุด จำนวนปริมาณที่เปลี่ยนไปทำให้เกิดความสามารถปฏิบัติตามคำสั่งโดยต่อเนื่องกันภายใต้การควบคุมของระบบ

ส่วนโปรแกรม itsutils จัดให้มีการเปิดแหล่งข้อมูล เพื่อเป็นทางเลือกสำหรับพื้นที่ ที่เก็บข้อมูลจากอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile ใช้ psdread เป็นส่วนประกอบของโปรแกรมนี้ร่วมกับ –l ทางเลือกได้ให้ไว้ในรายการของพื้นที่จัดเก็บข้อมูล ดังได้แสดงไว้ข้างล่างนี้ ของอุปกรณ์ Motorola Q

D:\itsutils>psdread -l

C: - TOSHIBA MK6021GAS

Drive geometry: 0x1e48 cyls, 240 t/cyl 63 s/t 512 b/s - 55.89 Gbyte

disknr = 0 fixed disk

D: - SONY DVD+RW DW-P50A

remote disk 1 has 135576 sectors of 512 bytes -66.20 Mbyte

SerialNr: 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

remote disk 2 has 112392 sectors of 512 bytes -54.88Mbyte

SerialNr: 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

อันดับแรก ในการเข้าทั้งสองทาง ในรายการข้างบนอ้างข้อมูลถึงเฉพาะที่ฮาร์ดดิสก์ของระบบข้อมูลที่ได้มา ภายหลังจากการที่เข้าทั้งสองทางซึ่งเกี่ยวโยงไปถึงรีโมทดิสก์บนอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile ซึ่งคือระบบและพื้นที่ในการจัดเก็บข้อมูลตามลำดับ หลังจากสั่งการก็ได้ทางเลือกของพื้นที่จัดเก็บข้อมูลซึ่งที่บรรจุข้อมูลสำคัญมาก จากทัศนคติการวิเคราะห์ (รีโมทดิสก์ 2 บนอุปกรณ์นี้ได้แสดงไว้ข้างต้น) เริ่มต้นที่ 0 และคัดลอก 57544704 bytes (112392 sectors ×512 bytes)

D:\itsutils>psdread – 2 0 57544704 E:\Samsung-i607.bin

remote disk 2 has 112392 sectors of 512 bytes- 54.88 Mbyte

SerialNr:01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

CopySDCardToFile (remote, 2, 0x0, 0x36e1000, C:\Samsung-i607.bin)

เมื่อ psdread ไม่ทำงานร่วมกับอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile อาจจะยังคงเป็นไปได้ที่จะได้ข้อมูลมาโดยใช้ pdocread ซึ่ง pdocreadไม่เพียงแต่เป็นโปรแกรมอรรถประโยชน์เท่านั้น ยังได้มาซึ่งข้อมูลของแต่ละบุคคลแบ่งออกเป็นส่วนๆ และบางครั้งต้องอาศัยวินโดว์ดิสก์บน chip API ซึ่งอาจจะจำกัดปริมาณของข้อมูลเพราะว่าสามารถได้มาในภายหลัง

3.2 การกู้ไฟล์ข้อมูลที่ถูกลบ

ถึงแม้ว่าเครื่องมือที่ใช้จะสามารถกู้ชื่อไฟล์ข้อมูลที่ถูกลบจาก TFAT เป็นจำนวนมากของอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile นักตรวจวิเคราะห์อาจจะพบกับอุปสรรคไปถึงการกู้คืนของไฟล์ข้อมูล ตัวอย่างเช่น ความล้มเหลวจากการแก้ไข สร้างใหม่โดยประกอบเรื่องจากข้อมูลของระบบไฟล์ TFAT บนอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile สามารถทำให้ไม่พบไฟล์และโฟลเดอร์ได้ ดังรูปที่ 4 แสดงถึงระบบไฟล์ที่ได้จาก HTC S620 (Dash) ในภายหลังที่ได้มาโดยใช้ psdread ไม่พบโฟลเดอร์ย่อย (subfolder) ภายใต้ ‘‘Documents and Settings’’

ในบางกรณี ไฟล์ที่สำคัญเช่น pim.vol ไม่พบจากระบบไฟล์ตรวจสอบ การสร้างขึ้นใหม่ไม่สมบูรณ์ด้วยระบบไฟล์ ซึ่งไม่จำกัดถึงอุปกรณ์เคลื่อนที่ และเกิดขึ้นในระบบไฟล์เครื่องมือวิเคราะห์ (Casey,2005) อุปสรรคของการสร้างขึ้นใหม่ในระบบไฟล์บนอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการWindows Mobile ทำให้แย่ลง โดยแสดงให้เห็นถึงการทำซ้ำ ‘‘DON’T DEL’’ รายนามการเข้า และธรรมชาติที่เปลี่ยนแปลงอย่างรวดเร็วของอุปกรณ์เคลื่อนที่ เหล่านี้ประเภทที่ไม่ตรงกันเน้นความสำคัญของการทดสอบความถูกต้องมากเท่าที่เครื่องมือวิเคราะห์อุปกรณ์เคลื่อนที่มีอยู่ขณะนี้ ได้อภิปรายไว้ในหัวข้อ ‘‘Tool Validation’’ ของบทความนี้

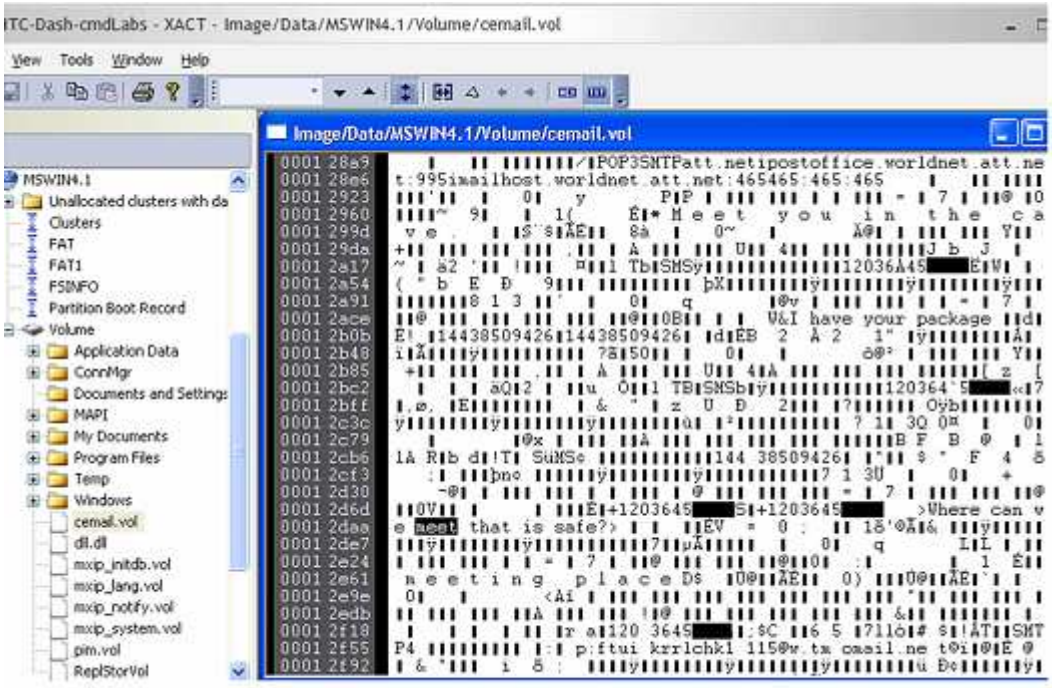

Fig. 4 – Windows Mobile file system viewed using XACT with missing folders.

สำหรับอุปสรรคอื่นจนถึงการกู้ข้อมูลไฟล์ที่ถูกลบ บางอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile ปรากฏว่ามีการเขียนทับเนื้อความของไฟล์ที่ถูกลบด้วยการทำซ้ำเป็นแบบ 0xFF จำไว้ว่าเนื้อหาต้นฉบับเดิมของไฟล์ที่ถูกลบ อาจจะกู้ข้อมูลคืนได้โดยใช้เทคนิคการตรวจวิเคราะห์ที่ก้าวหน้า ซึ่งมีวิธีเข้าถึงข้อมูลที่บรรจุอยู่อย่างครบถ้วน ด้วยหน่วยความจำแบบแฟลช

ส่วนเทคนิคการตัดแยกไฟล์ การที่จะประสบความสำเร็จถูกจำกัด ถ้าเนื้อหาของไฟล์ที่ลบถูกเขียนทับ เว้นแต่ว่าจะใช้เทคนิคที่ก้าวหน้ามากกว่า ซึ่งทั่วไปคุ้นเคยกับการได้จากหน่วยความจำแบบ dump (ที่ทิ้งขยะ) ถึงแม้ว่าไฟล์ที่ถูกลบอาจจะยากในการกู้คืน คัดลอก อาจะมีอยู่ที่อื่นบนอุปกรณ์ ดังที่ในสิ่งที่แนบมากับข้อความ MMS หรือข้อความ e-mail ดังได้ทอลองให้เห็นจริงไว้ในบทความนี้ จำไว้ว่าคำสำคัญให้ตรวจสอบอย่างละเอียด อาจจะมีผลอย่างมากที่สุดในวิธีการเข้าไปค้นหาข้อมูลส่วนที่ยังไม่สมบูรณ์ ในเรื่องที่ทำให้สนใจในบางคดี

3.3 การตรวจสอบฐานข้อมูลถาวร

อุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile เก็บข้อมูลบางส่วนที่สำคัญไว้ในความจุของไฟล์ ซึ่งเอาเฉพาะใจความที่สำคัญหลายอย่างฝังตัวในฐานข้อมูล รวมทั้งรายละเอียดเกี่ยวกับการติดต่อสื่อสาร ช่องทางการติดต่อ และการสนทนาทางโทรศัพท์ (Microsoft, 2005, 2010) ตัวอย่างเช่น pim.vol มีการฝังตัวของฐานข้อมูลสารสนเทศ อาทิเช่น ประวัติการสนทนาทางโทรศัพท์ และช่องทางการติดต่อข่าวสารผ่านไปตาม clog.db และฐานข้อมูลที่ใช้ในการติดต่อ ถึงแม้ว่าการจัดรูปแบบข้อมูลไม่เป็น

ตามรูปแบบเอกสาร หลายลักษณะของไฟล์ pim.vol และ cemail.vol ได้ถูกสำรวจตรวจค้นโดยผู้พัฒนาโปรแกรมคอมพิวเตอร์ ความสัมพันธ์ระหว่างฐานข้อมูลภายใน cemail.vol ได้บรรยายไว้ในรูปที่ 5

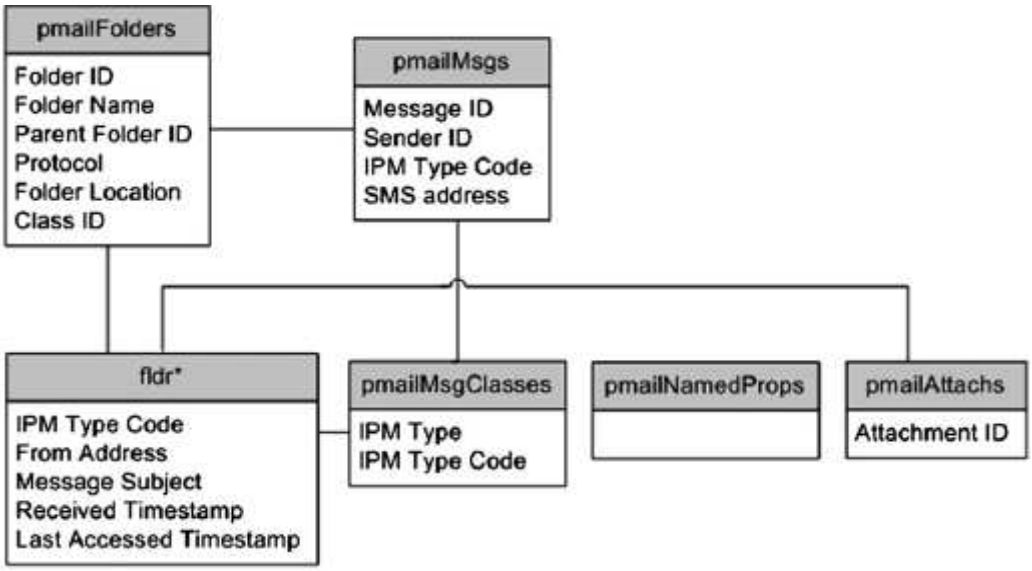

Fig. 5 – Overview of `cemail.vol` file.

แต่ละฐานข้อมูลบรรจุข้อความที่บันทึกไว้มากมายที่ทันสมัยของแต่ละคนที่เป็นเจ้าของ OID (object identifier) ซึ่งจัดหาวิธีการทำงานอย่างรวดเร็วสำหรับผลของการสืบค้นโดยเฉพาะสิ่งที่บันทึกไว้ในไฟล์ cemail.vol แต่ละข้อความที่บันทึกไว้มีขอบเขตของความสามารถในการจุ (a.k.a. properties) โดยเก็บข้อมูลซึ่งมีอยู่ในขณะนี้

ไฟล์ cemail.vol เก็บข้อมูลรายละเอียดเกี่ยวกับแต่ละข้อความ และมีการอ้างอิงเกี่ยวเนื่องไปถึงสิ่งที่บรรจุอยู่ในไฟล์อื่นๆบนอุปกรณ์ เหมือนกับส่วนใหญ่ของข้อความมากมาย และสิ่งที่แนบมา โดยทั่วไปส่วนประกอบของข้อความถูกเก็บไว้ในหลายตำแหน่ง ‘‘pMail*’’ และ ‘‘fldr*’’ ฐานข้อมูลในไฟล์ cemail.vol และ ‘‘.mpb’’ และ ‘‘.att’’ บนอุปกรณ์ ส่วนใหญ่ใช้ประโยชน์การฝังตัวของฐานข้อมูลภายใน cemail.vol ได้บรรยายไว้ในที่นี้

pmailFolders: ฐานข้อมูลนี้ให้คำจำกัดความของโฟลเดอร์ข้อความโดยการจัดระบบตามลำดับขั้น (ตัวอย่าง Inbox, Outbox, Drafts, Deleted Items และอื่นๆ) สำหรับแต่ละที่อยู่ (address) ซึ่งที่อุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile ได้จัดเตรียมหรือปรับแต่งฮาร์ดแวร์หรือซอฟต์แวร์สำหรับแต่ละโฟลเดอร์ข้อความ ได้บันทึกไว้ใน‘‘pmail Folder’’ ซึ่งแสดงฐานข้อมูล ‘‘fldr*’’ เกี่ยวเนื่องกับรายละเอียดของข้อความ

pmailMsgs: ฐานข้อมูลนี้บรรจุรายละเอียดใจความสำคัญเกี่ยวกับข้อความบนอุปกรณ์ รวมทั้ง ID ของข้อความ ประเภทของข้อความ และที่อยู่ของข้อความสารสนเทศ คุณประโยชน์ของฐานข้อมูลนี้บ่งบอกถึงฐานข้อมูล ‘‘fldr*’’ ของแต่ละข้อความที่เกี่ยวข้องกันกับฐาน ID ของโฟลเดอร์ เป็นแบบฉบับใน

วิธีการจัดรูปแบบของ“fldr” + “folder ID” (e.g. fldr31000026) ดังในตารางที่ 3 ได้บรรยายถึงบางคุณสมบัติ ที่นำไปใช้ประโยชน์ได้ เป็นตัวบอกลักษณะภายในแต่ละข้อความที่ได้บันทึกไว้

Table 3 – Property identifiers for useful items within the “pmailMsgs” database.

Property ID	Description
0x800C	Contains sender identification information, such as a phone number in the case of an SMS message.
0x8001	Contains the Interpersonal Message (IPM) type code, which indicates the type of message sent (e.g. SMS, MMS, e-mail). The lookup table for IPM type code resides within the “pmailMsgClasses” database.
0x0E09	Contains the Folder ID in decimal form. This must be converted into its hexadecimal equivalent to determine the containing “fldr*” database.

pmailMsgClasses: ฐานข้อมูลนี้จัดเตรียมไว้ให้พิจารณาในตารางของประเภท IPM ที่ใช้ในฐานข้อมูล“pmailMsgs” และฐานข้อมูล “fldr*” ตัวอย่างเช่น การรวมกันของ “pmailMsgClasses” บน HTC S620 (Dash) รายชื่อในที่นี้ร่วมกับประเภทของสิ่งที่บรรจุอยู่ทางซ้าย และความสัมพันธ์กันในการกำหนดชื่อให้แก่ข้อมูลอยู่ทางขวา

IPM.MMS	822083597
IPM.Note	822083598
IPM.SI	822083600
IPM.SL	822083601
IPM.SMStext	822083599
IPM.SMStext.SIM	855638066
REPORT.IPM.Note.DR	822083603
REPORT.IPM.Note.IPNNRN	822083606
REPORT.IPM.Note.IPNRN	822083605
REPORT.IPM.Note.NDR	822083604
REPORT.IPM.Note.Status	822083602

pmailNamedProps: ฐานข้อมูลนี้ มีให้พิจารณาอยู่ในตารางของ วัตถุประสงค์คุณสมบัติของชื่อ ที่มีอยู่ภายในอุปกรณ์ (ตัวอย่างเช่น SMS:SMSCAddress, Meeting:Reminder) องค์ประกอบจะคล้ายกันกับฐานข้อมูล“pmailMsgClasses” แต่ใช้เครื่องหมาย (:) สำหรับการกำหนดเขตภายในคุณประโยชน์แทนที่ระยะเวลาหนึ่ง fldr*: ฐานข้อมูลเหล่านี้บรรจุข้อมูลสารสนเทศอย่างมากมายเกี่ยวกับข้อความบนอุปกรณ์ รวมทั้งประเภทของ IPM ผู้ส่ง ที่อยู่ของผู้ส่ง และเมื่อได้รับข้อความ และการแก้ไขเปลี่ยนแปลงครั้ง

ล่าสุด เมื่อเนื้อเรื่องของข้อความมีขนาดเล็กพอสมควร บรรจุอยู่เต็มซึ่งเก็บข้อมูลไว้ภายในการฝังตัวของฐานข้อมูล คุณสมบัติเฉพาะอาจจะเก็บข้อมูลในบันทึกของฐานข้อมูล "fldr*" รายการดังในตารางที่ 4

Table 4 – Property identifiers for useful items within "fldr*" databases.

Property ID	Description
0x8005	OID used as a lookup value.
0x0C1F	From address (contact name unresolved)
0x0C1A	From address (contact name resolved)
0x003D	Denotes the message prefix, either "Re: ", "Fw: ", or "" denoting reply, forward, and null, respectively.
0x0037	Message subject or, when applicable, the message body if it is small enough.
0x0E06	Message received timestamp.
0x3008	Message last modified timestamp.
0x001A	Lookup field, which links this database to the "pmailMsgClasses" database.

ร่วมกับคุณลักษณะที่สัมพันธ์กันของการกำหนดชื่อให้แก่ข้อมูล ทุกๆคุณสมบัติอาจจะหรืออาจจะไม่แสดงให้เห็นขึ้นอยู่กับประเภทของข้อความที่ได้บันทึกไว้ ฐานข้อมูล "fldr*" ซึ่งไม่พัฒนาวิธีการเข้าถึงแหล่งเก็บข้อมูล เช่นนี้ เมื่อชื่อที่ใช้ในการติดต่อถูกลบออกจากอุปกรณ์ที่ใช้ในการติดต่อ ข้อความที่มีมาก่อนเก็บไว้ในชื่อผู้ติดต่อ ข้อความที่ตามมาภายหลังจะไม่มีชื่อผู้ติดต่อ และทั้งจากรายการที่อยู่ ดังในตารางที่ 4 จะมีคุณประโยชน์ที่เหมือนกัน สิ่งนี้สามารถมีรายละเอียดเรื่องที่น่าสนใจให้กับผู้สอบสวน ถ้าผู้ใช้ลบการติดต่อสื่อสารจากบันทึกสมุดที่อยู่ ในการพยายามปิดบังบุคคลที่มีความเกี่ยวข้องกัน

3.4 เครื่องมือและการแปลผล

เครื่องมือในการตรวจวิเคราะห์ได้ถูกพัฒนาไปถึงการแปลรหัสของบางข้อมูลสารสนเทศในไฟล์ cemail.vol ตัวอย่างดังในรูปที่ 6 แสดงข้อมูลที่มาจากไฟล์ cemail.vol บนอุปกรณ์ Samsung i607 (Blackjack) ทั้งในการแปลคำสั่ง และข้อมูลดิบโดยใช้รูปแบบ XACT รายชื่อแฟ้มข้อมูลทั้งหมดในด้านซ้ายตอนท้ายสุด แสดงผลการกู้คืนรายการข้อมูลรวมทั้งข้อความ SMS รายละเอียดของเนื้อหาข้อความที่เลือกไว้แล้วได้แสดงผลในหน้าต่าง (Node pane) ด้านขวาตอนท้ายสุด ส่วนด้านบนตอนขวาเช่นเดียวกันได้แสดงบางข้อมูลสารสนเทศในไฟล์ cemail.vol คือทั้งวิธีการจัดรูปแบบ hexadecimal และ ASCII

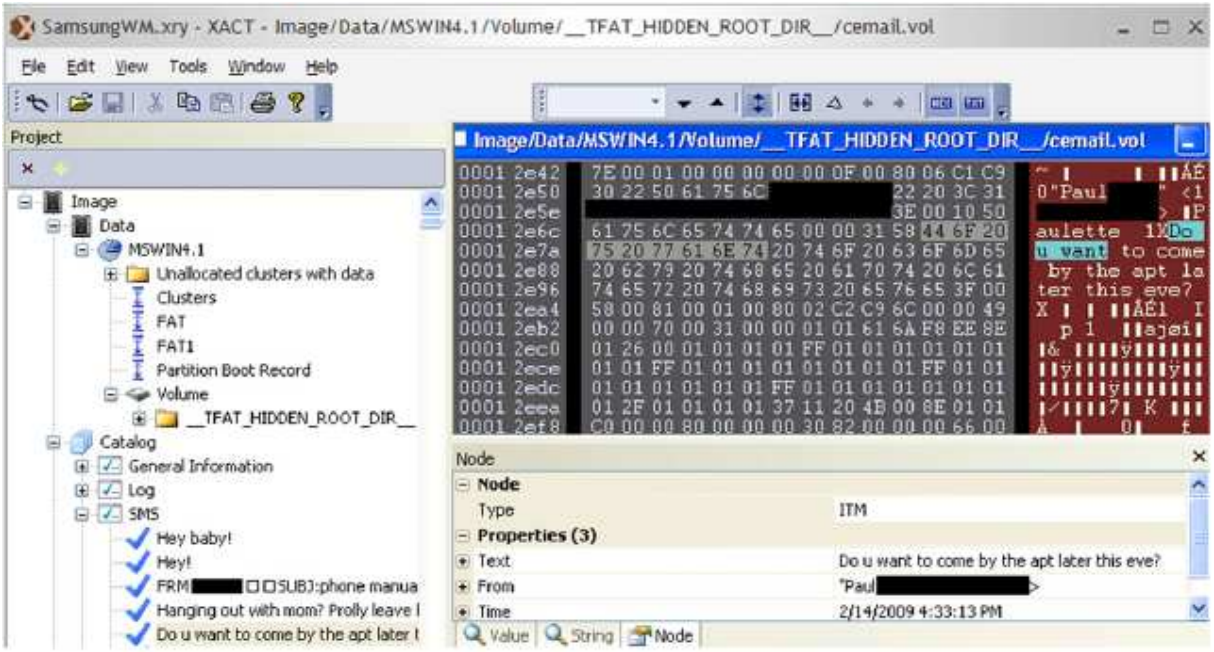

Fig. 6 – XACT showing data in `cemail.vol` file.

โชคดีที่มีเนื้อหาข้อมูลจำนวนมากใน cemail.vol คือ ASCII รวมทั้ง เนื้อหาข้อความสั้นๆของ SMS เนื่องจากการลบหลักฐานที่บันทึกไว้ ไม่หมดไปจากไฟล์ cemail.vol โดยทันที จึงสมควรที่จะตรวจสอบไฟล์ cemail.vol ใน hexviewer ค้นหาเนื้อหาข้อความที่เกี่ยวเนื่องกับรายการที่ถูกลบ โดยไม่มีรหัสเข้าถึง ซึ่งวิธีการดังที่ได้กล่าวมาก่อนแล้ว

ด้วยวิธีแนวทางปฏิบัติของการสืบสวนการรับส่งข้อมูลด้วยตัวเลข ซึ่งเลี่ยงไม่ได้ โดยถอดรหัสข้อมูลที่มีอยู่ แล้วตรวจแก้ไขแปลโดยนักตรวจวิเคราะห์ ใช้เครื่องมือคัดลอกข้อความออกมา ทางหนึ่งของวิธีการปฏิบัติไปถึงยืนยันความถูกต้องนั้น คุณค่าสำคัญคือการแปลคำสั่งที่มีอยู่ตรวจแก้ไข ซึ่งใช้การสำรวจในรูปแบบ Hexadecimal ได้จัดหาไว้ให้นักตรวจวิเคราะห์เพื่อให้เข้าใจถึงรูปแบบของการจัดข้อมูล ส่วนวิธีการอื่นที่ตรวจค้นหาความผิดพลาดการถอดรหัสที่ถูกตรวจจับคือเปรียบเทียบข้อมูลกับเครื่องมืออื่นหรือในโปรแกรมเลียนแบบ

ทางหนึ่งของการสำรวจไฟล์ cemail.vol ในเฉพาะเรื่องที่ถูกหุ้มห่อ ปกปิดอยู่ คือสกัด คัดลอกไฟล์ออกมาจากหัวข้อของระบบ เก็บมันไว้ในโฟลเดอร์บนคอมพิวเตอร์ที่ตรวจสอบ และหลังจากนั้นใช้ โปรแกรมเลียนแบบวินโดว์จัดการทำตามกระบวนการ ซึ่งโฟลเดอร์เช่นเดียวกับ virtual Storage Card (Casey, 2009) ในวิธีการนี้ โปรแกรมเลียนแบบสามารถใช้เปิดไฟล์ cemail.vol ซึ่งเป็นพยานหลักฐาน โดยใช้เครื่องมือคล้ายกับ itsutils หรือ Pocket dbExplorer อีกวิธีการหนึ่งคือสกัด คัดลอกไฟล์จาก หัวข้อของระบบและโหลดเข้าไปข้างในโปรแกรมเลียนแบบ แล้วเขียนทับไฟล์ cemail.vol สำหรับอุปสรรคของวิธีนี้คือค่าโดยปริยาย (default) ของไฟล์ cemail.vol ไม่สามารถเขียนทับได้โดยง่าย เพราะถูกว่าปิดกั้นโดย

ระบบปฏิบัติการ ความเป็นไปได้ซึ่งเกี่ยวข้องกับงานทั่วไป สำหรับผลที่ตีพิมพ์ออกมานี้คือเหมาะที่จะใช้กับผู้พัฒนาถึงวิธีการอภิปรายปัญหา(XDA, 2006)

เมื่อก่อนไฟล์ cemail.vol ถูกติดตั้งอยู่ในในโปรแกรมเลียนแบบ ส่วนประกอบอื่นของโปรแกรม itsutils เรียกว่า pdblist สามารถใช้วิเคราะห์คำในประโยค(ทางไวยากรณ์) ที่เป็นเนื้อหาของฐานข้อมูลถาวร (Casey, 2009) ที่จะกล่าวต่อไปคือผลลัพธ์จากคำสั่งสำหรับฐานข้อมูล ‘‘fldr31000028’’

T:\itsutils>pdblist -d fldr31000028 330007ec (332 13 8)

8005 T13 L0000 F0000 UI4 **1006634986**

8011 T13 L0000 F0000 UI4 74

001a T13 L0000 F0000 UI4 822083597

0e07 T13 L0000 F0000 UI4 40

0c1f T1f L0000 F0000 STR [00172838](12)

‘+14431234567’

0c1a T1f L0000 F0000 STR [00172854](12)

‘+14431234567’

003d T1f L0000 F0000 STR [00172870](4) ‘FW:’

0037 T1f L0000 F0000 STR [0017287c](26)

‘FWD:FW: FWD:Fw: FWD:Fw:Fw:’

0e08 T13 L0000 F0000 UI4 41057

0e17 T13 L0000 F0000 UI4 64

0e06 T40 L0000 F0000 FT 2009-04-15 15:37:23.000

3008 T40 L0000 F0000 FT 2009-04-15 15:37:23.000

8001 T13 L0000 F0000 UI4 855640044

ผลลัพธ์ที่แสดงนี้เป็นเพียงแค่หนึ่งบันทึกรายงานในเวลานี้ ในความต้องการฐานข้อมูลซึ่งก็คือข้อความ MMS(IPM ID 822083597) ข้อความ ID ของรายการนี้สามารถกำหนดโดยใช้ตัวเลขที่แสดงนี้ (1006634986) เปลี่ยนกลับไปสู่ hexadecimal (0x3C0007EA) และเปลี่ยนหมวดสุดท้ายสองดิจิตไปยังข้างหน้า(0xEA3C0007) ค่าเหล่านี้ถูกใช้สำหรับตำแหน่งที่อยู่ของข้อมูลเกี่ยวข้องกับไฟล์บนอุปกรณ์เคลื่อนที่ดังที่แสดงไว้ในหัวข้อ “การตรวจ E-mail และ MMS ที่เครื่องเก็บบันทึก” ของบทความนี้

เมื่อใช้โปรแกรมเลียนแบบวินโดว์ค้นหาข้อมูลในไฟล์ cemail.vol เป็นที่ทราบว่าบางเครื่องมือใช้การตั้งค่าเขตเวลาไปถึงการประทับวัน เวลา ขณะที่อันอื่นทำไม่ได้ ตัวอย่างเช่น การเปรียบเทียบรายละเอียดข้อความที่ได้สกัด คัดลอกออกมา แสดงให้เห็นโดยใช้เครื่องมือหลายอย่าง ซึ่ง Pocket dbExplorer ใช้ประยุกต์ตั้งค่าเขตเวลาได้ภายในโปรแกรมเลียนแบบประทับวัน เวลา ในทางตรงกันข้าม pdblist และ XACT แปลวัน เวลา ในรูปแบบข้อมูลดิบ

3.5. การตรวจสอบ Registry ในระบบ

การ Registry บนระบบอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile ประกอบด้วยรายละเอียดที่หลากหลายเกี่ยวกับองค์ประกอบ และอุปกรณ์ที่ใช้ ซึ่งการ Registry บนระบบอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile เป็นลำดับชั้น โดยจัดลำดับลดหลั่นกันไป โดยที่สิ่งหนึ่งอยู่เหนืออีกสิ่งหนึ่งเหมือนกับระบบปฏิบัติการไมโครซอฟต์อื่นๆ ดังแสดงในรูปที่ 7

Fig. 7 – Registry values on a Samsung i607 (Blackjack) device.

ใช้ Microsoft Remote Registry Editor ซึ่งระบบ Registry ที่อยู่เป็นกลุ่มประกอบด้วยข้อมูลสารสนเทศ อย่างเช่น การเชื่อมต่อของระบบเครือข่าย ตัวอย่างเช่น ข้อมูลเกี่ยวกับการเชื่อมต่อ WiFi เมื่อไม่นานมานี้ โดยตำแหน่งที่เข้าคือการใส่ข้อมูลภายใต้ “HKLM\Comm\ConnMgr\Providers” ผู้ใช้ Registry ที่อยู่เป็นกลุ่มมีข้อมูลที่สัมพันธ์กันกับรายละเอียดประวัติโดยย่อของผู้ใช้บนอุปกรณ์ อย่างเช่น รายละเอียดของการเข้าติดต่อสื่อสารโดยเจ้าของอุปกรณ์ดังแสดงในรูปที่ 7

ตัวอย่างของการป้อนข้อมูลอื่นๆที่มีประโยชน์ ซึ่งที่ผู้ใช้ Registry ในระบบตามรายการในตารางที่ 5

Table 5 – Items in the user Registry hive on Windows Mobile devices of potential interest.

Registry key	Description
HKCU\ControlPanel\Owner	Contact details entered by user
HKCU\System\State\Shell	Most recently used (MRU) items
HKCU\Software\Microsoft\pMSN\SavedUsers	Windows Live ID
HKCU\ControlPanel\Home\CurBgImageName	Home screen background image
HKCU\Comm\EAPOL\Config	WiFi access point information

3.6. การตรวจสอบ e-mail และ MMS ที่เครื่องเก็บบันทึก

เมื่อข้อความ MMS และ e-mail ถูกรับและเปิดออก หรือถูกสร้างและส่ง บนอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile บางอย่างที่ประดิษฐ์ขึ้นด้วยฝีมือมนุษย์กิจกรรมเหล่านี้ถูกสร้างขึ้นมา สิ่งประดิษฐ์เหล่านี้สามารถนำไปใช้ประโยชน์ให้กับนักตรวจวิเคราะห์ได้เพราะพวกเขาชี้ให้เห็นว่าเมื่อข้อความพิเศษถูกสร้างหรือสำรวจบนอุปกรณ์ แม้กระทั่งหลังจากที่ข้อความต้นฉบับได้ถูกลบ นอกจากนั้น แม้ว่าจัดการลบข้อความ สิ่งประดิษฐ์ที่เกี่ยวข้องกันสามารถคงอยู่บนอุปกรณ์ซึ่งไม่มีขีดจำกัดและอาจจะมีข้อมูลที่เกี่ยวข้องกับข้อความต้นฉบับอยู่ รายละเอียดหัวข้อความ E-mail รวมทั้ง ถึง จาก หัวเรื่อง และชื่อสิ่งที่แนบมา ถูกเก็บไว้ในไฟล์ cemail.vol เมื่อข้อความเหล่านี้ถูกเปิดบนอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile ไฟล์ ‘‘.mpb’’ ถูกสร้างขึ้นในโฟลเดอร์ ‘‘\Windows\Messaging’’ กับข้อความที่บรรจุอยู่ นอกจากนั้น เมื่อ e-mail ที่แนบถูกเปิดออกบนอุปกรณ์ ไฟล์ ‘‘.att’’ ถูกสร้างขึ้นในโฟลเดอร์ ‘‘\Windows\Messaging\Attachments’’ ข้อมูลจากการสำรวจ ข้อความ SMS/MMS เก็บไว้ใน ‘‘\Windows\Messaging’’ ในไฟล์ ‘‘.mpb’’ สามารถรวมส่วนที่เหลืออยู่ของรายการซึ่งที่ถูกลบจากไฟล์ cemail.vol file ดังรูปที่ 8

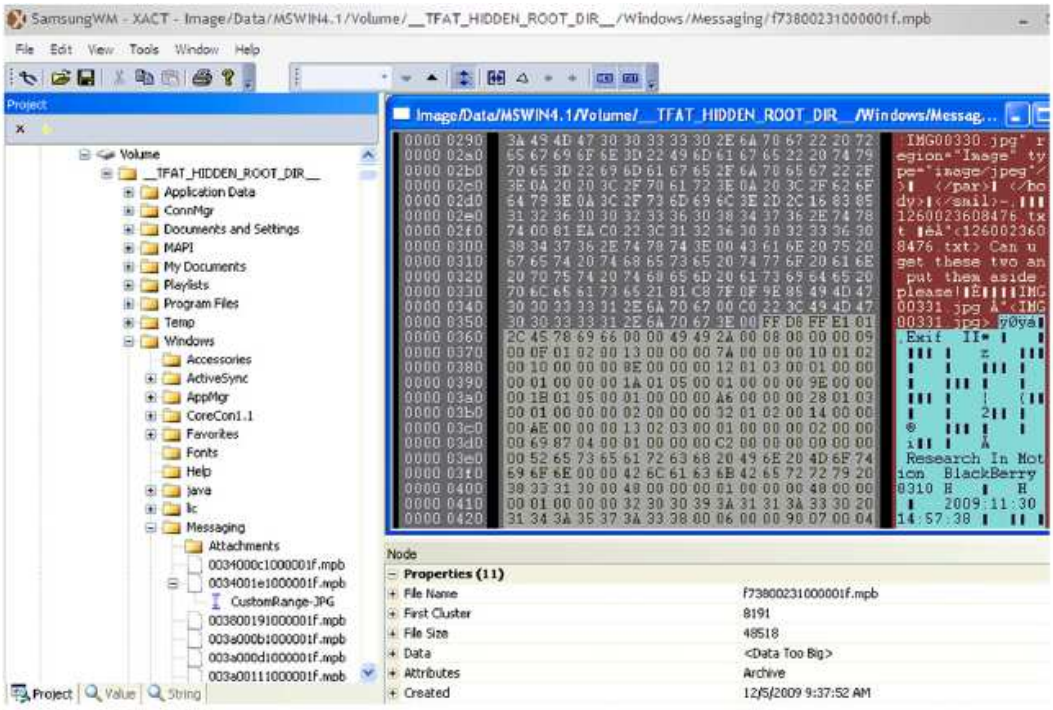

Fig. 8 – Message contents on a Windows Mobile device that contains a digital photograph with embedded EXIF header details from a Blackberry.

แสดงถึงไฟล์ ‘‘.mpb’’ ที่เกี่ยวข้องกับข้อความ MMS บนอุปกรณ์ Samsung i607 (Blackjack) พร้อมด้วยการสร้างไฟล์ ประทับวัน เวลา สิ่งนั้นบ่งบอกถึงว่าข้อความถูกเปิดวันที่ 5 เดือนธันวาคม ค.ศ. 2009 ไฟล์เหล่านี้ รวมทั้งภาพถ่ายดิจิตอลพร้อมด้วยแสดงการฝัง EXIF หัวเรื่องข้อมูล สิ่งนั้นถูกทำด้วย Blackberry

เมื่อวันที่ 30 เดือนพฤศจิกายน ค.ศ.2009 ของเดิมรับข้อความที่เกี่ยวกันกับไฟล์นี้ ‘‘.mpb’’ ได้ถูกลบทิ้ง

Object identifier (OID) ขององค์ประกอบข้อความ สามารถใช้ความสัมพันธ์กันเข้าสู่ในไฟล์ cemail.vol ร่วมกับไฟล์‘‘.mpb’’ ที่เหมือนกัน ในโฟลเดอร์ ‘‘\Windows\Messaging’’ ตัวอย่างเช่น เนื้อหาเกี่ยวข้องกับข้อความตัวอย่าง รายการในส่วนก่อนหน้านี้ถูกจัดเก็บใน‘‘\Windows\Messaging \EA3C00071000001f.mpb’’ ในที่ซึ่งชื่อของไฟล์ เริ่มด้วยข้อความ OID (0xEA3C0007) ท้ายสุด 8 อักษรของไฟล์‘‘.mpb’’ กำหนดโดยคุณสมบัติไมโครซอฟต์ คำลงท้ายมีค่าสำหรับไฟล์ กรณีนี้คือเนื้อหาของข้อความต้นฉบับ (Microsoft, 2008b)

บางอุปกรณ์มีไฟลเดอร์ ‘‘\My Documents\UAContents’’ ซึ่งมีส่วนที่เหลืออยู่ของข้อความที่ได้ส่งไปแล้ว โฟลเดอร์นี้มีไฟล์ ‘‘.dat’’ ร่วมกับการคัดลอกของรูปภาพที่ส่งโดยทาง MMS แม้กระทั่งหลังจากข้อความต้นฉบับได้ถูกลบทิ้ง ดังรูปที่ 9

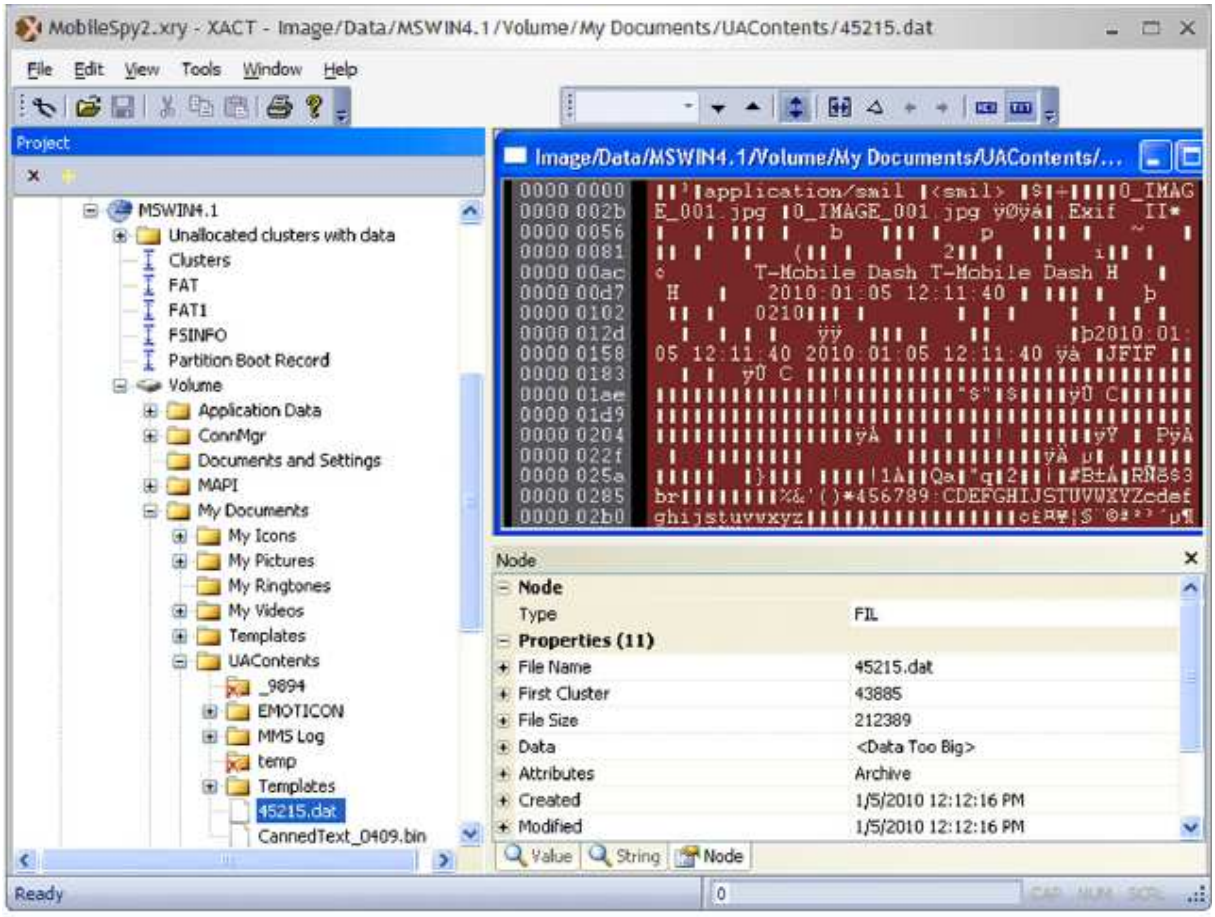

Fig. 9 – Example ‘‘.dat’’ file containing data associated with a sent MMS message.

แสดงถึงสิ่งที่บรรจุอยู่ของไฟล์ ‘‘\My Documents\UAContents\45215.dat’’ รวมทั้งภาพถ่ายดิจิตอล ซึ่งใช้ HTC S620 (Dash) และส่งในข้อความ MMS การสร้างวัน เวลา ประทับของไฟล์ ‘‘.dat’’ นี้แสดงเมื่อข้อความ MMS ถูกสร้าง รายละเอียดที่เพิ่มขึ้นเกี่ยวกับการส่งและรับ ข้อความ MMS ถูกบันทึกไว้ในเนื้อหาของไฟล์ในโฟลเดอร์ ‘‘\My Documents\UAContents\MMS Log’’

4.กรณีศึกษา การลักลอบเข้าถึงอุปกรณ์สื่อสารของผู้อื่นโดยมิชอบ

การวิวัฒนาการของโปรแกรม สามารถติดตามกิจกรรมโดยการควบคุมจากระยะไกล ของอุปกรณ์สื่อสารบนระบบปฏิบัติการ Windows Mobile เป็นการเพิ่มขีดระดับความลับและความปลอดภัยให้มากยิ่งขึ้น ทั้งในด้านที่เกี่ยวกับรัฐบาลและด้านธุรกิจ โปรแ MobileSpy และ FlexiSpy ทั้งสองโปรแกรมนี้ซึ่งสามารถติดตั้งไว้ใน อุปกรณ์สื่อสารบนระบบปฏิบัติการ Windows Mobile ทำให้ง่ายต่อการควบคุมเป็นเฉพาะราย ไปสู่การติดตามกิจกรรมของผู้ใช้ เช่น SMS และเสียงในการสนธนา โดยโปรแกรมนี้จะส่งข้อมูลจากอุปกรณ์เคลื่อนที่ ไปยังตัวบริการเว็บ (Web server) ที่ซึ่งอุปกรณ์ควบคุมระยะไกลของส่วนบุคคลสามารถตรวจสอบรวมรวมข้อมูลได้ ดังแสดงไว้ในรูปที่ 10

Fig. 10 – MobileSpy Web site showing SMS traffic on a monitored device.

โดยเฉลี่ยแล้วผู้ใช้จะไม่สังเกตเห็นสิ่งเช่นนั้นของโปรแกรม ที่กำลังทำงานบนอุปกรณ์ของเขา ถึงแม้ว่าระบบของโปรแกรม MobileSpy (Smartphone.exe) สามารถมองเห็นการทำงานในหน่วยความจำบนอุปกรณ์ โดยใช้ Remote Process Viewer ซึ่งมันไม่เกิดขึ้นใน Task Manager อย่างไรก็ตามโปรแกรมนี้ได้ทิ้งร่องรอยพอเพียง ในการนำไปสู่การสืบค้นโดยนักตรวจวิเคราะห์ การตรวจวิเคราะห์เกี่ยวกับอุปกรณ์สื่อสารบนระบบปฏิบัติการ Windows Mobile โดยการติดตั้ง MobileSpy แสดงให้เห็นร่องรอยบนระบบแฟ้มข้อมูล และการลงทะเบียน(Registry) ตัวอย่างเช่น โปรแกรม MobileSpy ถูกใส่ไว้ใน โฟลเดอร์ ‘‘Program Files\Applications\Smartphone’’ ดังแสดงไว้ในรูปที่ 11 โฟลเดอร์นี้ประกอบด้วยไฟล์ ‘‘smartphone.log’’ อันซึ่งเก็บรักษาบันทึกเกี่ยวกับกิจกรรมทั้งหลาย ซึ่งติดตามโดยโปรแกรม MobileSpy

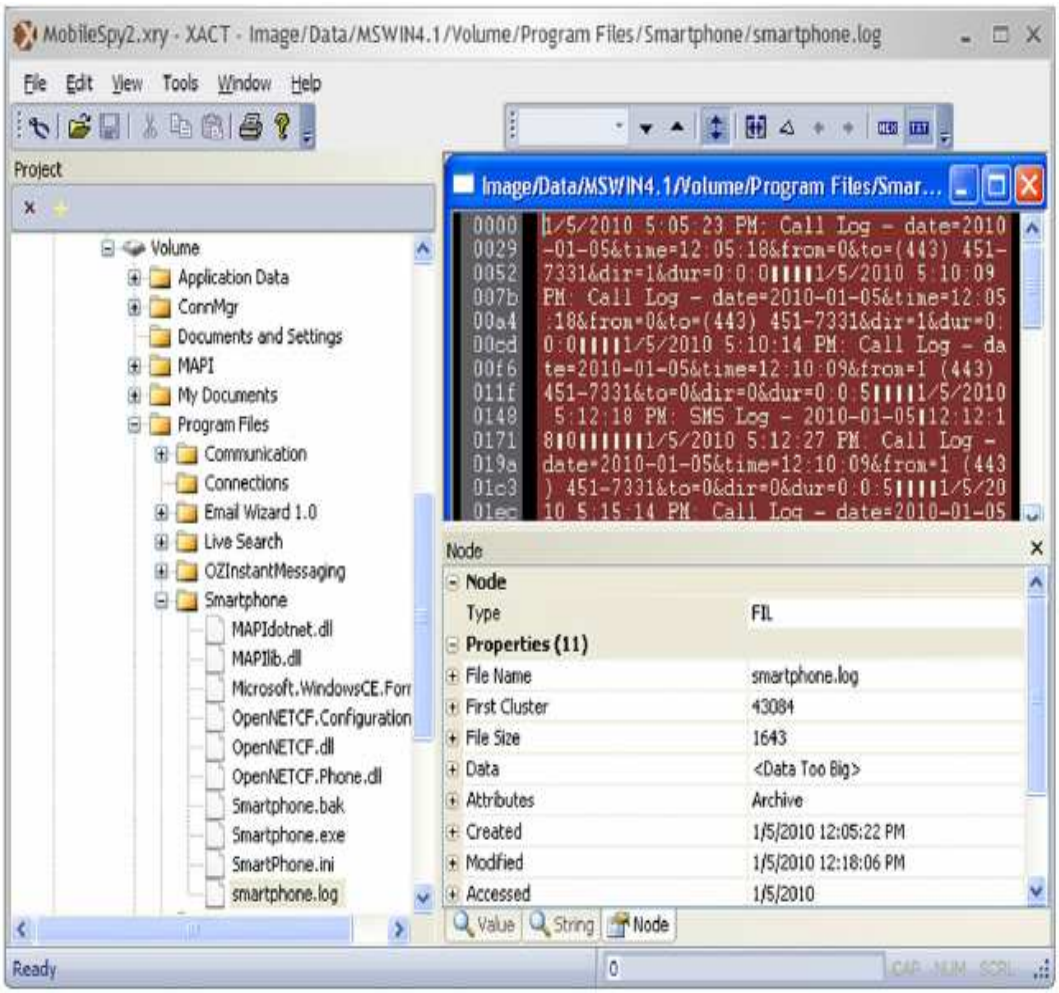

Fig. 11 – MobileSpy program installed in "Program Files\Applications\Smartphone" with "smartphone.log" file recording activities on the device.

นอกจากนั้น ยังได้ใส่ MobileSpy ไว้ในไฟล์ shortcut ใน "Windows\StartUp\" และสร้าง Registry entries ตามมาที่หลัง

[HKEY_CURRENT_USER\Software\RetinaxStudios]

"isLogUrl" = dword:1

"isLogSMS" = dword:1

"isLogPhoneCall" = dword:1

‘ ‘Username" = " ’ ’

"ReportTimer" = dword:f

"RememberUser" = dword:1

‘ ‘Password" = " ’ ’

‘ ‘BlackList" = "0010001’ ’

"AutoLogin" = dword:1

ซึ่งแต่ก่อนเวอร์ชั่นของ MobileSpy มีชื่อผู้ใช้ (username) และรหัสผ่าน (password) เพื่อเป็นการพิสูจน์ตัวจริง เปรียบเทียบระหว่างอุปกรณ์และตัวบริการเว็บ (Web server) ได้เก็บข้อมูลในการลงทะเบียนในข้อความธรรมดาที่ยังไม่เข้ารหัส (Fogie, 2007) ต่อมาได้มีเวอร์ชั่นป้องกัน ชื่อผู้ใช้ (username) และรหัสผ่าน (password) แต่มันยังคงสามารถได้ข้อมูลเหล่านี้ โดยการถ่ายเทข้อมูลจากหน่วยความจำของกระบวนการ ‘‘Smartphone.exe’’

สรุป

ถึงอย่างไรก็ตาม แม้ว่าอุปกรณ์สื่อสารจะมีขนาดเล็ก แต่ระบบปฏิบัติการบนอุปกรณ์สื่อสารมีความสามารถในการจัดเก็บข้อมูล ที่เกี่ยวข้องกับผู้ใช้งาน ได้เป็นจำนวนมาก รวมไปถึงข้อมูลของผู้ที่ติดต่อสื่อสารด้วย และกิจกรรมของผู้ใช้ในเวลาหนึ่งๆ ถึงแม้ว่าระบบปฏิบัติการ Windows Mobile จะเป็นที่คุ้นเคยสำหรับนักตรวจวิเคราะห์ แต่ระบบปฏิบัติการดังกล่าว ก็มีความเป็นเอกลักษณ์ ที่ต้องใช้เครื่องมือและเทคนิคในการตรวจพิสูจน์ที่จำเพาะเจาะจง อุปกรณ์สื่อสารบนระบบปฏิบัติการดังกล่าว กลายเป็นที่แพร่หลายในปัจจุบัน จึงมีความจำเป็นที่นักตรวจวิเคราะห์จะต้องมีการพัฒนาความสามารถในการตรวจวิเคราะห์ เพื่อให้ได้มาซึ่งพยานหลักฐาน จากอุปกรณ์สื่อสาร และมีการอ่านค่าได้อย่างถูกต้อง ทั้งนี้ในอนาคตยังต้องมีการวิจัยและพัฒนาขีดความสามารถ ในการจัดเก็บและคัดลอกข้อมูลบนระบบปฏิบัติการ Windows Mobile รวมถึงการเก็บกู้ไฟล์ข้อมูลที่สูญหายหรือถูกทำลายต่อไป

ข้อเสนอแนะ

บทความนี้เป็นเพียงการชี้นำวิธีการตรวจพิสูจน์ทางนิติวิทยาศาสตร์สำหรับอุปกรณ์สื่อสารที่ทำงานบนระบบปฏิบัติการ Windows Mobile ที่มีการใช้กันอย่างแพร่หลายในปัจจุบัน ซึ่งเนื้อหาของบทความได้มีการอธิบายถึงหลักการทำงานอย่างคร่าว ๆ ของ Windows Mobile ว่า มีการจัดเก็บไฟล์ข้อมูล วิธีการจัดเก็บไฟล์ข้อมูล รวมไปถึงความแตกต่างของระบบการจัดเก็บข้อมูลว่ามีความแตกต่างจากระบบปฏิบัติการ Windows ที่ใช้กับคอมพิวเตอร์ PC ทั่วไปอย่างไร เมื่อทราบถึงวิธีและระบบการจัดเก็บข้อมูลของระบบปฏิบัติการ Windows Mobile แล้ว ก็สามารถหาเครื่องมือหรือโปรแกรมที่เหมาะสมทางนิติวิทยาศาสตร์ มาใช้ในการคัดลอกไฟล์ข้อมูลที่เป็นประโยชน์ในการสืบสวนต่อไป โดยการได้มาซึ่งไฟล์ข้อมูลเหล่านี้ยังต้องมีการแปลผล อ่านค่าที่ถูกต้อง เพื่อให้ได้ข้อมูลที่ถูกต้องตามความเป็นจริงและครบถ้วนสมบูรณ์ เพื่อใช้เป็นพื้นฐานในการสืบสวนคดีต่อไป

จากบทความดังกล่าว เป็นเพียงจุดเริ่มต้นให้นักตรวจวิเคราะห์ได้รู้จักกับระบบปฏิบัติการดังกล่าว รวมถึงความแตกต่างกันกับระบบปฏิบัติการทั่วไป ซึ่งในการทดสอบ ได้ทำการทดสอบกับอุปกรณ์สื่อสารเพียงบางชนิด และใช้เครื่องมือทำการทดสอบเพียงบางอย่างเท่านั้น ยังไม่มีการต่อยอดในการตรวจพิสูจน์และอ่านค่าด้วยวิธีอื่นๆ ซึ่งเชื่อว่ายังมีอีกหลายวิธีที่สามารถนำมาใช้ในการตรวจพิสูจน์และอ่านค่าของผลที่ได้มาจาก การตรวจพิสูจน์ได้ แต่ก็นับว่าเป็นการชี้นำจุดเริ่มต้นให้กับนักตรวจวิเคราะห์ ในการตรวจพิสูจน์อย่างถูกแหล่ง และถูกต้องเพื่อประยุกต์ใช้ในการสืบสวน

เนื่องจากในโลกยุคปัจจุบันนี้ เป็นยุคแห่งการติดต่อสื่อสารและการพัฒนาที่ไม่หยุดนิ่ง เครื่องมือหรืออุปกรณ์สื่อสาร จึงมีความจำเป็นต่อการใช้ชีวิตของมนุษย์ ทำให้ผู้ผลิตอุปกรณ์สื่อสารมีการแข่งขันกันในการพัฒนาสินค้าของตนให้มีความเป็นเอกลักษณ์ สวยงาม ใช้งานง่าย สามารถตอบสนองความต้องการของลูกค้าได้อย่างครบครัน จึงเป็นเหตุผลหนึ่งที่ทำให้ระบบปฏิบัติการบนอุปกรณ์สื่อสารมีความแตกต่างกันไปด้วย เช่น ระบบปฏิบัติการ Mac OS x ระบบปฏิบัติการ Android ระบบปฏิบัติการ Symbian ระบบปฏิบัติการ Bada ระบบปฏิบัติการ RIM ฯลฯ ที่ได้เริ่มมีการใช้งาน เป็นที่แพร่หลายในปัจจุบัน ดังนั้นนักตรวจวิเคราะห์จึงควรศึกษาถึงระบบปฏิบัติการต่างๆ ทำความเข้าใจ และนำไปสู่การพัฒนาขีดความสามารถของเครื่องมือที่จะใช้ในการตรวจพิสูจน์ เพื่อเพิ่มศักยภาพในการตรวจวิเคราะห์อุปกรณ์สื่อสารต่างๆเหล่านี้ได้ เพื่อเป็นประโยชน์ในการสืบสวนคดีต่อไป

เอกสารอ้างอิง

1. Eoghan Casey, Michael Bann, John Doyle. *Digital Investigation 6*, (2010) 136-146

2. Casey. Digital evidence and computer crime. In: Byard R, Corey T,Henderson C, editors. The encyclopedia of forensic and legal medicine. Elsevier; 2005.

3. Casey. Recovering deleted text messages from Windows Mobile devices, https://blogs.sans.org/computer-forensics/2009/10/22/recovering-deleted-text-messages-from-windows-mobiledevices/; 2009.

4. Fogie S. Inside mobile-spy "spouseware", informIT. Indianapolis: Pearson Education, http://www.informit.com/articles/article.aspx?p=1077909; 2007.

5. Klaver C. Windows Mobile advanced forensics. Journal of Digital Investigation; 2010.

6. van der Knijff R. Embedded systems analysis in handbook of digital forensics and investigation. San Diego: Elsevier; 2009.

7. Microsoft. EDB data types and size limits, http://msdn.microsoft.com/en us/library/ ms885368. aspx; 2010.

8. Microsoft. Embedded database system technologies, http://msdn.microsoft.com/en-us/library/ ms838188.aspx; 2005.

9. Microsoft. File system boot process, http://msdn.microsoft.com/en-us/library/aa912276.aspx; 2008a.

10. Microsoft. Message content properties, http://msdn.microsoft.com/en-us/library/ bb446140. aspx; 2008b.

11. XDA. Backup and restore your cemail.vol easily, http://forum.xda-developers.com/ showthread.php?t=302909; 2006.