บทที่ 3

การรวบรวมพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์

คอมพิวเตอร์เป็นสิ่งประดิษฐ์ที่มนุษย์ได้สร้างขึ้นและก่อให้เกิดการเปลี่ยนแปลงในโลกอย่างกว้างขวางในทุกสาขา คอมพิวเตอร์นั้นมีความยุ่งยากซับซ้อนอยู่ในตัวของมันเอง และมีขีดความสามารถสูง นิยมใช้กันอย่างแพร่หลายจนทำให้ผู้มีความรู้ทางด้านคอมพิวเตอร์อาศัยความรู้ที่ตนเองมีอยู่ประกอบอาชญากรรมขึ้น เจ้าหน้าที่ผู้รักษากฎหมายจึงต้องติดตามรวบรวมพยานหลักฐานนั้นไปแสดงต่อศาลเพื่อให้ศาลเชื่อว่าผู้ต้องหาหรือจำเลยได้กระทำผิดจริงและตัดสินลงโทษ การสืบสวนสอบสวนในคดีที่เกี่ยวข้องกับคอมพิวเตอร์จึงไม่ใช่เรื่องง่ายที่เจ้าหน้าที่คนใดคนหนึ่งจะกระทำได้เหมือนคดีอาชญากรรมธรรมดา แต่ต้องเป็นเจ้าหน้าที่มีความรู้ความเข้าใจในระบบต่าง ๆ ของคอมพิวเตอร์ด้วย จึงจะทำให้การดำเนินงานกับอาชญากรรมคอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพ

อาชญากรรมประเภทนี้เป็นอาชญากรรมที่มีเทคโนโลยีทางด้านคอมพิวเตอร์เข้ามาเกี่ยวข้อง เจ้าหน้าที่ผู้ทำการสืบสวนสอบสวนจึงจำเป็นที่จะต้องมีความรู้ความเข้าใจในระบบต่าง ๆ ของคอมพิวเตอร์ เครื่องมือและอุปกรณ์ในการตรวจสถานที่เกิดเหตุ ย่อมมีความแตกต่างจากคดีอาชญากรรมธรรมดาทั่ว ๆ ไป ในอาชญากรรมทั่วไปอาจมีพยานหลักฐานที่มองเห็นได้ เช่น มีดเปื้อนเลือด หรือยาเสพติด เจ้าหน้าที่รู้ว่าจะต้องไปค้นที่ใดและจะเก็บพยานหลักฐานเหล่านั้นอย่างไร แต่ในคดีอาชญากรรมคอมพิวเตอร์นอกจากพยานบุคคล พยานเอกสารและพยานวัตถุ ได้แก่ ลายพิมพ์นิ้วมือหรือสิ่งใด ๆ ที่มีความหมายในตัวเองแล้ว พยานหลักฐานที่เป็นเทคโนโลยีคอมพิวเตอร์ อันมีลักษณะเป็นอิเล็กทรอนิกส์ ย่อมสร้างปัญหาให้แก่เจ้าหน้าที่ผู้รักษากฎหมายในคดีอาญาทั่วไป จึงจำเป็นจะต้องจัดหน่วยงานหรือทีมงานซึ่งมีอำนาจหน้าที่โดยเฉพาะ รับผิดชอบในการรวบรวมพยานหลักฐานนี้โดยตรง

3.1 การจัดตั้งหน่วยสืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์

หน่วยงานที่มีอำนาจหน้าที่สืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์ อย่างน้อยควรมีคณะทำงานหรือสมาชิกดังนี้ (David Carter, 1996 : 16-3)

3.1.1 ผู้จัดการโครงการ/คดี (Case/Project Manager)

บุคคลซึ่งเป็นหัวหน้าคณะทำงานต้องมีความรู้และประสบการณ์เกี่ยวกับการสืบสวนสอบสวนคดีอาญาซับซ้อนประเภทต่าง ๆ และต้องมีความรู้เกี่ยวกับทางด้านคอมพิวเตอร์ควบคู่กันไปด้วย ผู้จัดการโครงการ/คดี มีหน้าที่บริหารงานภายในคณะทำงานดูแลและจัดเตรียม เครื่องคอมพิวเตอร์ อุปกรณ์และเครื่องมือเครื่องใช้ในการสืบสวนสอบสวนคดีอาญา บริหารงานและควบคุมการปฏิบัติงานของสมาชิกในคณะทำงาน

3.1.2 ผู้สืบสวนสอบสวนเกี่ยวกับอาชญากรรม (Criminal Investigator)

บุคคลที่มีความรู้ทั่วไปเกี่ยวกับระบบคอมพิวเตอร์ และพื้นที่ที่เป็นจุดที่ต้องระวังในระบบคอมพิวเตอร์ มีความชำนาญเกี่ยวกับพื้นฐานสิ่งที่เป็นประโยชน์ในการสืบสวนสอบสวน เช่น การเก็บลายนิ้วมือหรือวัตถุพยานทั่ว ๆ ไป การแจ้งสิทธิต่าง ๆ ตามที่กฎหมายบัญญัติ ผู้สืบสวนสอบสวนเกี่ยวกับอาชญากรรมมีหน้าที่เกี่ยวกับการปฏิบัติงานตามขั้นตอนของกฎหมาย เช่น ทำหน้าที่ขอหมายค้นจากศาล การสอบสวนปากคำผู้เสียหายและผู้ต้องหา ในสถานที่เกิดเหตุทำหน้าที่เก็บวัตถุพยานทั่ว ๆ ไป การควบคุมตัวผู้ต้องสงสัยหรือพยานไม่ให้เข้าไปยุ่งเกี่ยวกับพยานหลักฐานการถ่ายภาพและถ่าย V.D.O. การวาดแผนที่เกิดเหตุ เป็นต้น

3.1.3 พนักงานอัยการ (Prosecutor)

พนักงานอัยการจะต้องเป็นบุคคลที่เข้าใจในระบบคอมพิวเตอร์ เคยมีประสบการณ์ดำเนินคดีที่มีความซับซ้อน รวมถึงคดีเกี่ยวกับคอมพิวเตอร์เข้ามาร่วมในคณะทำงานเพื่อทำความเข้าใจกับพยานหลักฐานต่าง ๆ ซึ่งจะใช้นำเสนอในชั้นศาลเพื่อพิสูจน์ความผิดของจำเลยต่อไป

3.1.4 นักวิเคราะห์ระบบคอมพิวเตอร์ (Computer System Analyst)

บุคคลที่มีความรู้เชี่ยวชาญในด้านออกแบบและวิเคราะห์ระบบงานของคอมพิวเตอร์ทำหน้าที่ตรวจสอบโครงสร้างของระบบคอมพิวเตอร์ของกลาง ตั้งแต่โครงสร้างข้อมูลที่ได้นำเข้าและผลลัพท์ที่ได้ออกมาตลอดจนถึงขั้นตอนต่าง ๆ ตั้งแต่ต้นจนจบกระบวนการ นักวิเคราะห์ระบบต้องตรวจสอบให้ทราบว่าเครื่องคอมพิวเตอร์ได้ปฏิบัติการไปอย่างไร ผลลัพท์ที่ได้เป็นอย่างไร

เพื่อนำมาเป็นหลักฐานเชื่อมโยงกับการกระทำความผิดในคดี การตรวจค้นคอมพิวเตอร์ขนาดเมนเฟรมอาจต้องใช้นักวิเคราะห์ระบบของบริษัทผู้ผลิตหรือตัวแทนจำหน่ายด้วย

3.1.5 **เจ้าหน้าที่พัฒนาโปรแกรม** (Programmer)

บุคคลที่มีความรู้เชี่ยวชาญเกี่ยวกับการเขียนโปรแกรมทุกประเภท ทำหน้าที่ตรวจสอบโปรแกรมในคอมพิวเตอร์ของกลาง การแก้ไขปัญหาเมื่อไม่สามารถเข้าถึงโปรแกรมในคอมพิวเตอร์ของกลางได้ การตรวจค้นคอมพิวเตอร์ขนาดเมนเฟรมอาจต้องใช้เจ้าหน้าที่พัฒนาโปรแกรมของบริษัทผู้ผลิตเข้าร่วมในการทำงานด้วยเช่นกัน

3.1.6 **ผู้ตรวจสอบข้อมูลทางอิเล็กทรอนิกส์** (EDP Auditor)

บุคคลที่มีความชำนาญเป็นพิเศษเกี่ยวกับการจัดการข้อมูล มีความสามารถในการใช้โปรแกรมอรรถประโยชน์ได้ทุกประเภท ทำหน้าที่ในการค้นหาข้อมูลและคัดลอกข้อมูลใช้เป็นพยานหลักฐาน

3.1.7 **วิศวกรระบบ** (System Engineer)

บุคคลที่มีความรู้เรื่องเครื่องคอมพิวเตอร์, ระบบไฟฟ้าและระบบเครือข่ายคอมพิวเตอร์ ทำหน้าที่ดูแลโครงสร้างของคอมพิวเตอร์ การถอดชิ้นส่วนต่าง ๆ ของคอมพิวเตอร์ การตรวจค้นคอมพิวเตอร์ขนาดเมนเฟรมอาจต้องใช้วิศวกรระบบของบริษัทผู้ผลิตหรือตัวแทนจำหน่ายเข้าร่วมตรวจค้นด้วย

3.1.8 **ผู้เชี่ยวชาญทางการรักษาความปลอดภัย** (Security Specialist)

บุคคลที่ทำหน้าที่ตรวจสอบพื้นที่ที่ต้องระวังในระบบคอมพิวเตอร์ ทำการควบคุมระบบการเข้าถึงที่มีการกำหนดรหัสผ่านและระเบียบในการรักษาความปลอดภัย เป็นผู้รับผิดชอบการรักษาความปลอดภัยของระบบที่เข้าทำการตรวจค้นนั้น

3.1.9 **เสมียนข้อมูล** (Data Clerk)

บุคคลที่ทำหน้าที่บันทึกข้อมูลลงสื่อชนิดต่าง ๆ เมื่อได้รับคำสั่งอาจเป็นบุคคลเดียวกันกับพนักงานควบคุมเครื่องคอมพิวเตอร์ (Computer Operator)

3.2 **เครื่องมืออุปกรณ์ต่าง ๆ ที่จำเป็นในการปฏิบัติงาน** (Equipment Needs)

3.2.1 หน่วยประมวลผลกลาง CPU ซึ่งจะต้องเป็นรุ่นที่ใช้อยู่เป็นปัจจุบัน

3.2.2 RAM หน่วยความจำของ RAM จะต้องมีหน่วยความจำสูงสุดตามสเป็กของ CPU เพื่อใช้เป็นพื้นที่ทำงาน

3.2.3 สื่อบันทึก Disk Media

- จานขับแผ่น Floppy Disk ขนาด 5.25"
- จานขับแผ่น Floppy Disk ขนาด 3.5"
- จานขับ Back up ที่อยู่ข้างนอกตัวเครื่อง ใช้เชื่อมต่อจากจานขับหลัก
- จานขับหลัก (Hard Disk Drive) ขนาดความจำไม่ต่ำกว่า 12 GB

3.2.4 แผ่นดิสก์เก็ต Diskettes

- แผ่นดิสก์ซึ่งใช้สำหรับเก็บข้อมูลที่คัดลอกมาจากคอมพิวเตอร์ที่ถูกตรวจยึดควรจะทำแผ่นดิสก์เก็ตที่จัดรูปแบบเสร็จ (Formatted) ทุกขนาดและทุกประเภทที่นิยมใช้กันแพร่หลายทั่วไป เช่น ขนาด 5.25", 3.5"
- แผ่น CD ที่สามารถใช้บันทึกข้อมูลได้
- แถบบันทึก (Tape)
- แถบบันทึกคาร์ทริดจ์ (Cartridge) มีลักษณะคล้ายตลับเทป ใช้เก็บข้อมูลได้เหมือนเทปหรือดิสก์ ปัจจุบันไม่ค่อยนิยมใช้ นอกจากที่บรรจุเกมส์ต่าง ๆ เรียกว่าเกมคาร์ทริดจ์ (Game Cartridge)

ทีมงานสืบสวนสามารถใช้เทปหรือดิสก์ สำหรับเป็นอุปกรณ์เก็บข้อมูลสำรอง (Mass Storage) สำรองจากความจุของฮาร์ดดิสก์ เหมือนกับหน่วยเก็บข้อมูลของโปรแกรมประยุกต์และแฟ้มข้อมูล นอกจากนี้ทีมงานอาจจะเลือกใช้สื่อบันทึกสำรองชนิดอื่น ๆ เช่น Hard Disk ภายนอกตัวเครื่องหรือจานบันทึกแบบแสงหรือเลเซอร์

3.2.5 ระบบปฏิบัติการ (Operating Systems) ควรใช้ระบบ

- ไมโครซอฟท์ (Microsoft) ใช้ซอฟท์แวร์ของ MS-DOS, MS-Windows

- ระบบ OS/2 (Operating System 2) เป็นระบบปฏิบัติการของ IBM ใช้กับเครื่องคอมพิวเตอร์ส่วนบุคคลหรือพีซี

- ระบบยูนิกซ์ (Unix Type) โปรแกรมระบบปฏิบัติการซึ่งใช้กันมากในระบบคอมพิวเตอร์ที่มีผู้ใช้ร่วมกันหลายราย (Multi-Users) พัฒนาขึ้นโดยศูนย์วิจัยเบลล์ ของบริษัท AT&T

- ระบบแอปเปิล (Apple) เป็นซอฟท์แวร์ของบริษัทแอปเปิลคอมพิวเตอร์ที่ได้รับความนิยมและใช้กันแพร่หลาย ได้แก่ ซอฟท์แวร์ของเครื่องคอมพิวเตอร์รุ่นแมคอินทอช

3.2.6 ระบบโปรแกรมอรรถประโยชน์ (Utilities) ซึ่งเป็นโปรแกรมที่ใช้กู้และคัดลอกแฟ้มข้อมูล

โปรแกรมอรรถประโยชน์ หมายถึง ซอฟท์แวร์ต่าง ๆ ที่สร้างขึ้นไว้เพื่อให้ผู้ใช้เพิ่มสมรรถนะในการใช้เครื่องคอมพิวเตอร์ โปรแกรมอรรถประโยชน์ไม่ใช่โปรแกรมใช้งานหรือโปรแกรมที่จะนำมาใช้ผลิตงานใด ๆ ออกมาด้วยตนเอง เพียงแต่เป็นโปรแกรมที่ทำให้การใช้โปรแกรมอื่น ๆ สะดวกขึ้น เดิมเรียกโปรแกรมประเภทนี้ว่า เป็นเครื่องมือในการทำซอฟท์แวร์ เพราะเป็นโปรแกรมที่ช่วยนักเขียนโปรแกรมอีกขั้นหนึ่ง ซึ่งทีมสืบสวนควรจะใช้โปรแกรมอรรถประโยชน์ ซึ่งสามารถนำไปดูแลแก้ไขดิสก์ได้ทุกตารางนิ้ว คือโปรแกรม PC Tools หรือโปรแกรม Norton Utilities

3.2.7 โปรแกรมป้องกันไวรัส ซึ่งจะช่วยป้องกันระบบต่าง ๆ ของทีมสืบสวนซึ่งอาจจะติดโปรแกรมไวรัสจากอุปกรณ์และคอมพิวเตอร์ของกลางและตรวจเช็คระบบปฏิบัติการดิสก์เก็ตให้สมบูรณ์ปราศจากไวรัส ส่วนใหญ่แล้วอาชญากรมักจะเขียนโปรแกรมป้องกันสำหรับแผ่นดิสก์เก็ต เมื่อระบบถูกเปิดโดยบุคคลอื่น เพื่อให้ข้อมูลในแผ่นดิสก์นั้นถูกทำลายไป ทีมงานจึงต้องมีโปรแกรมป้องกันและตรวจเช็คระบบก่อนปฏิบัติการ

3.2.8 คู่มือระบบปฏิบัติการและเอกสารที่จำเป็นอย่างอื่นสำหรับระบบปฏิบัติการที่เป็นเป้าหมาย รวมทั้งคู่มือภาษาโปรแกรม

3.2.9 เครื่องพิมพ์ (Printer) ควรใช้เครื่องพิมพ์เลเซอร์ และจัดเตรียมกระดาษสำหรับการพิมพ์

3.2.10 เครื่อง Pen Registers อุปกรณ์ที่ใช้สำหรับเก็บและดักข้อมูลที่เป็นตัวเลข

เป็นอุปกรณ์ที่ใช้สำหรับเก็บและดักข้อมูลที่เป็นตัวเลขและนำมาประมวลผลโดยทีมสืบสวนจะใช้เครื่อง Pen Registers ในการคัดลอกรหัสและตัวเลขที่บรรจุอยู่ในหน่วยความจำของคอมพิวเตอร์, โมเด็มหรือโปรแกรมการใช้โทรศัพท์

3.2.11 กล้องถ่ายรูป, วีดีโอ เพื่อช่วยในการเก็บรายละเอียดของที่เกิดเหตุ

3.2.12 อุปกรณ์สำหรับติดป้ายและผูกป้ายกำกับพยานหลักฐาน

ในที่เกิดเหตุจะมีพยานหลักฐานที่เป็นเทปและดิสก์จำนวนมาก ทีมงานจะต้องเตรียมอุปกรณ์สำหรับติดป้ายกำกับเพื่อป้องกันการสับสน ซึ่งอาจจะเป็นกระดาษกาวหรือฉลากและควรจะมีหลากสีเพื่อแยกแยะประเภท

การผูกป้ายติดกับพยานหลักฐาน ควรจะเป็นป้ายจำแนกสีเพื่อเป็นประโยชน์ในการจำแนกพยานหลักฐาน โดยตรวจสอบให้ชัดเจนว่าป้ายที่นำมาใช้นั้นเป็นป้ายที่มีความแตกต่างกันในพยานหลักฐานแต่ละประเภท เช่น การตรวจยึดแผ่นดิสก์ ติดป้ายหรือฉลากที่เตรียมมาลงบนแผ่นดิสก์แต่ละชิ้น และเขียนกำกับไปในระหว่างการตรวจค้น เช่น แฟ้มข้อมูลที่ถูกค้นพบ คำสั่งที่ใช้ในการเข้าถึงแฟ้มข้อมูล, ชื่อของระบบปฏิบัติการและรายละเอียดอื่นที่น่าเชื่อถือ ซึ่งถูกบรรจุอยู่ในแฟ้มข้อมูลนั้น

3.2.13 อุปกรณ์ที่ใช้ในการสืบสวนสอบสวนคดีอาญาทั่วไป เช่น อุปกรณ์ตรวจหาลายพิมพ์นิ้วมือแฝง

3.2.14 อุปกรณ์อื่น ๆ เช่น กล่องบรรจุแผ่นดิสก์, พลาสติกสำหรับหีบห่ออุปกรณ์คอม-พิวเตอร์ กล่องบรรจุ เป็นต้น

3.3 การรวบรวมพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์

3.3.1 การวางแผนในการตรวจค้น (Search Planning)

การวางแผนในการตรวจค้นเป็นสิ่งจำเป็นในคดีอาชญากรรมคอมพิวเตอร์ การวางแผนที่ดี จะนำไปสู่ความสำเร็จในการรวบรวมพยานหลักฐาน เนื่องจากการจัดเก็บพยานหลักฐานที่เป็นเทคโนโลยีคอมพิวเตอร์ต้องใช้วิธีพิเศษโดยเฉพาะ ในการตรวจค้นประการแรกที่จะ

ต้องพิจารณาในการวางแผนคือ ต้องทราบรูปแบบของอาชญากรรมคอมพิวเตอร์ว่าเป็นรูปแบบของอาชญากรรมที่เกี่ยวข้องกับฮาร์ดแวร์ (Hardware) ซอฟท์แวร์ (Software) หรือการสื่อสารโทรคมนาคม (Telecommunication) ซึ่งอาจแยกพิจารณาได้ดังนี้

3.3.1.1 รูปแบบของอาชญากรรมที่เกี่ยวข้องกับฮาร์ดแวร์ (Hardware) หากเป็นอาชญากรรมคอมพิวเตอร์ที่เกี่ยวข้องกับฮาร์ดแวร์ จะต้องพิจารณาว่าเป็นฮาร์ดแวร์คอมพิวเตอร์ขนาดใด เช่น เป็นฮาร์ดแวร์ ไมโครคอมพิวเตอร์ มินิคอมพิวเตอร์ เมนเฟรมคอมพิวเตอร์หรือซุปเปอร์คอมพิวเตอร์ โดยเฉพาะเครื่องขนาดใหญ่ หากทราบข้อมูลถึงระบบปฏิบัติการ (OS) โปรแกรมของตัวแทนจำหน่ายหรือบริษัทผู้ผลิตย่อมเป็นประโยชน์ต่อการตรวจค้นเป็นอย่างมาก เพราะคอมพิวเตอร์ขนาดใหญ่ไม่สามารถตรวจยึดเข้าไปสู่ห้องปฏิบัติการได้ การวางแผนและการตรวจค้นจึงต้องมีนักวิเคราะห์ระบบโปรแกรมเมอร์ หรือวิศวกรของบริษัทผู้ผลิตเข้าร่วมดำเนินการในการแก้ไขปัญหาและอุปสรรคของการตรวจค้นด้วย

3.3.1.2 รูปแบบของอาชญากรรมที่เกี่ยวข้องกับซอฟท์แวร์ (Software)

อาชญากรรมที่เกี่ยวข้องกับซอฟท์แวร์จะต้องพิจารณาว่าเป็นการกระทำผิดในลักษณะใด เช่น การละเมิดลิขสิทธิ์ (Copyright) ซอฟท์แวร์ หรือการใช้ซอฟท์แวร์เพื่อประกอบอาชญากรรมโดยตรง (Criminal Tools) เช่น การถอดรหัสผ่าน (Password) การคัดลอกข้อมูล ในการเข้าตรวจค้นซอฟท์แวร์เป้าหมายจะต้องมีโปรแกรมเมอร์ของบริษัทผู้ผลิตเข้าดำเนินการด้วย

3.3.1.3 รูปแบบของอาชญากรรมที่เกี่ยวข้องกับการสื่อสารโทรคมนาคม (Telecommunication)

อาชญากรรมคอมพิวเตอร์อาศัยระบบการสื่อสารโทรคมนาคมจึงต้องพิจารณาว่า การทำงานของเครื่องคอมพิวเตอร์เป็นการทำงานแบบอิสระ (Stand Alone) หรือเป็นคอมพิวเตอร์ที่เชื่อมกับระบบเครือข่าย เช่น ระบบ LAN (Local Area Network) ระบบ WAN (Wide Area Network) หรือระบบอินเตอร์เนต (Internet) การวางแผนในการตรวจค้นจึงต้องมีการเตรียมการสำหรับการตรวจค้นระบบเครือข่ายด้วย เช่น การหาข้อมูลเกี่ยวกับผู้ให้บริการ (ISP) ข้อมูลที่ใช้ในการเชื่อมต่อระบบ เช่น ชื่อผู้ใช้ (User Name), รหัสผ่าน

(Password), หมายเลขโทรศัพท์ของ ISP, ชื่อเครื่องบริการของ ISP และหมายเลขประจำเครื่อง (IP Address) และชุดโปรแกรมสำหรับติดตั้งพร้อมคู่มือ

วัตถุประสงค์ของการทราบรูปแบบอาชญากรรมก็เพื่อที่จะได้มีข้อมูลในการดำเนินการขอหมายค้นต่อศาล การเตรียมบุคลากรและเครื่องมือในการปฏิบัติงานและวิธีการรวบรวมพยานหลักฐานในขั้นตอนต่อไป

3.3.2 อำนาจในการตรวจค้น

เนื่องจากการตรวจค้นพยานหลักฐานที่เป็นเทคโนโลยีคอมพิวเตอร์นั้นจะต้องเกี่ยวข้องกับสิทธิส่วนบุคคล ข้อมูลที่เป็นความลับทางด้านเศรษฐกิจ การเมือง การทหารและความเจริญก้าวหน้าทางวิทยาศาสตร์ ในการตรวจค้นจึงต้องอาศัยอำนาจของศาลเข้าดำเนินการ ทั้งนี้ เพื่อเป็นการคุ้มครองสิทธิส่วนบุคคลไม่ให้ถูกละเมิดโดยเจ้าหน้าที่ของรัฐจนทำให้เกิดความเสียหายแก่เจ้าของระบบ (David Icove, 1995 : 185) กฎหมายของประเทศสหรัฐอเมริกา 18 USC, Ch 119, Section 2522 กำหนดว่าในการบังคับใช้กฎหมายเกี่ยวกับระบบสื่อสารโทรคมนาคมของเจ้าพนักงานจะต้องได้รับอนุญาตจากศาล ส่วน Ch 206, Section 3121 การใช้อุปกรณ์ดักฟัง อุปกรณ์ติดตามและอุปกรณ์บันทึกเลขหมาย (Pen Register) จะต้องดำเนินการโดยได้รับอนุญาตจากศาล และ 42 USC, Ch 21A, Section 2000aa กำหนดว่าเพื่อเป็นการคุ้มครองสิทธิส่วนบุคคล การตรวจค้นและยึดพยานหลักฐานในการสืบสวนดำเนินคดีจะต้องได้รับอนุญาตจากศาลจึงจะดำเนินการได้ (David Icove, 1995 : 78) ส่วนกฎหมาย Computer Misuse Act 1990 ของประเทศอังกฤษ Section 14 กำหนดให้การตรวจค้นพยานหลักฐานจะต้องได้รับอนุญาตจากศาล โดยให้มีอำนาจในการตรวจค้นจำนวน 28 วัน และระบุให้อำนาจเจ้าพนักงานที่จะเข้าไปในอสังหาริมทรัพย์, สิ่งปลูกสร้าง, วัตถุที่เคลื่อนไหวได้ทั้งที่มีรูปร่างและไม่มีรูปร่าง, ยานพาหนะ, เรือ, อากาศยาน และยานสะเทินบกสะเทินน้ำ (David Icove, 1995 : 347)

การรวบรวมพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์จะต้องดำเนินการโดยมีหมายหรือคำสั่งอนุญาตจากศาล จะต้องระบุบริเวณข่ายงานหรือคอมพิวเตอร์ที่จะทำการตรวจ

ค้นอุปกรณ์เครื่องมือที่จะใช้ พยานหลักฐานที่จะตรวจยึดและกำหนดระยะเวลาที่จะต้องปฏิบัติให้ชัดเจนและเมื่อได้รับอนุญาตแล้วจึงจะเข้าดำเนินการได้

3.3.3 วิธีการตรวจค้นสถานที่เกิดเหตุ

การตรวจค้นสถานที่เกิดเหตุในคดีอาชญากรรมคอมพิวเตอร์จะต้องระมัดระวังเป็นพิเศษในการรักษาอุปกรณ์และวัสดุที่เกี่ยวข้องนั้นไว้เป็นพยานหลักฐาน และเพื่อที่จะรักษาไว้ซึ่งสภาพที่มีความสมบูรณ์ของพยานหลักฐานเหล่านั้น

ถ้าอุปกรณ์คอมพิวเตอร์ปิดอยู่ขณะเข้าตรวจค้นที่เกิดเหตุ "อย่าเปิดรถยนต์ดขาด" มิฉะนั้นคอมพิวเตอร์จะถูกโปรแกรมทำลายพยานหลักฐานทั้งหมด ให้ดำเนินการถ่ายภาพหรือวีดีโอไว้แล้วตรวจยึดสู่ห้องปฏิบัติการ แต่ถ้าคอมพิวเตอร์เหล่านั้นเปิดและปฏิบัติการอยู่ขณะที่เข้าตรวจค้นในที่เกิดเหตุให้ดำเนินการ ดังนี้ (David Icove, 1995 : 183-186)

3.3.3.1 การปิดกั้นสถานที่เกิดเหตุ (Control Area) เมื่อเจ้าหน้าที่เข้าไปถึงในสถานที่เกิดเหตุ จะต้องแยกตัวบุคคลออกจากเครื่องคอมพิวเตอร์หรือส่วนประกอบให้เร็วที่สุดเพื่อป้องกันการทำลายพยานหลักฐาน

3.3.3.2 ปลดสายโทรศัพท์ (Disconnect any Phone Line) ปลดเส้นทางการสื่อสารกับคอมพิวเตอร์ที่เชื่อว่าเป็นเครื่องมือที่ใช้ในการกระทำผิด เช่น สายโทรศัพท์หรือเครื่องมือสื่อสารอื่น ๆ เพื่อป้องกันการควบคุมเครื่องจากระยะไกล

3.3.3.3 ถ่ายวีดีโอ (VDO) สถานที่เกิดเหตุ รูปภายนอกของระบบ สภาพ-ทำเลที่ตั้งของสถานที่เกิดเหตุ รวมทั้งสภาพอุปกรณ์ทุกอย่างในที่เกิดเหตุ

3.3.3.4 การวาดผังการต่อสายและผูกป้ายกำกับสายเชื่อม/ช่องเสียบ (Make a Diagram/Label) ให้ทำการวาดผังของการต่อเชื่อมสายเครื่องมืออุปกรณ์ในห้องที่เกิดเหตุไว้อย่างละเอียด พร้อมทั้งติดป้ายกำกับพยานหลักฐานทุกชิ้น รวมทั้งสายเชื่อม/ช่องเสียบและอุปกรณ์ต่อพ่วงทุกอย่างในที่เกิดเหตุ

3.3.3.5 ทำการถ่ายภาพสถานที่เกิดเหตุ (Photograph) เน้นให้เห็นบริเวณสายเชื่อมต่อ ช่องเสียบที่ทำป้ายผูกกำกับไว้ และที่สำคัญคือถ่ายภาพข้อมูลที่ปรากฏบนจอภาพ

(Screen Displays) ของเครื่องคอมพิวเตอร์ทุกเครื่องขณะที่เข้าทำการตรวจค้นหรือยึดก่อนการถอดประกอบสายเชื่อมต่อ

3.3.3.6 อย่าสัมผัสคีย์บอร์ด เพราะในระบบเครือข่าย การสัมผัสกับคีย์บอร์ดอาจจะเป็นการเข้าสู่โปรแกรม (Run Programs) และถ่ายเทข้อมูลที่ต้องการออกไป และอย่าสัมผัสทุกสิ่งทุกอย่าง โดยปราศจากความเข้าใจว่ากำลังทำอะไร ห้ามปลดสายไฟหรือแหล่งพลังงานและห้ามเปลี่ยนแปลงสภาพคอมพิวเตอร์ขณะปฏิบัติงานอยู่ ควรดำเนินการดังนี้

- ให้ผู้เชี่ยวชาญดำเนินการคัดลอกทุกสิ่งทุกอย่างที่แสดงผลอยู่บนจอคอมพิวเตอร์ในลักษณะคำต่อคำ

- ถ้าตรวจพบแฟ้มข้อมูลที่สามารถใช้เป็นพยานหลักฐานในการกระทำผิดแล้วจะต้องสำรอง (Back up) ข้อมูลเหล่านั้นไว้ เพราะข้อมูลที่เก็บไว้ในสภาพแม่เหล็ก อาจเสื่อมหรือสูญหายได้ง่าย

- ควรเก็บรายละเอียดที่เกี่ยวข้อง เช่น หมายเลขโทรศัพท์ คู่มือการใช้เครื่องและเครื่องมือสื่อสารที่ใช้กับเครื่องคอมพิวเตอร์ พร้อมกับบันทึกลักษณะการต่อสายไฟฟ้าระหว่างอุปกรณ์ต่าง ๆ ในที่เกิดเหตุ นอกเหนือจากตัวกลางซึ่งใช้บันทึกข้อมูล เช่น เทปดิสก์, ซีดี (CD), เอกสารจากเครื่องพิมพ์

- การอ่านข้อมูลในจานบันทึกอ่อน (Floppy Disk) หรือจานบันทึกแข็ง (Hard Disk) ควรใช้โปรแกรมของผู้ตรวจพิสูจน์เอง เพราะโปรแกรมในเครื่องคอมพิวเตอร์ที่ยึดมาอาจมีหลุมพลางซ่อนอยู่ เช่น คำสั่ง DIR อาจกลายเป็นคำสั่งลบทิ้ง (Delete) หลักฐานต่าง ๆ ก็อาจถูกทำลายไปโดยไม่รู้เท่าทัน

- บางครั้งทีมสืบสวนพยายามที่จะเข้าสู่โปรแกรม (Run Program) ในที่เกิดเหตุ เพื่อที่จะได้รายละเอียดเกี่ยวกับแฟ้มข้อมูลและระบบปฏิบัติการของคอมพิวเตอร์ จะต้องระมัดระวังอย่างยิ่งเมื่อจะกระทำการดังกล่าวนั้น เพราะว่าโปรแกรมคอมพิวเตอร์บางชนิดอาจจะสร้างขึ้นมาเพื่อแก้ไขเปลี่ยนแปลงข้อมูลในจานบันทึกแข็ง (Hard Disk) หรือข้อมูลบนจานบันทึกอ่อน (Floppy Disk) ทำให้พยานหลักฐานอาจจะถูกเปลี่ยนแปลงไป ส่งผลให้พยานหลักฐานเหล่านั้นฟังไม่ขึ้น จึงเป็นเรื่องสำคัญมากที่จะต้องรักษาพยานหลักฐาน ตามเงื่อนไขในการ

เข้าตรวจค้น ก่อนจะทำการเข้าสู่โปรแกรม (Run Program) ทุก ๆ สิ่ง ต้องมั่นใจว่าผู้เชี่ยวชาญด้านเทคนิคได้ตรวจพิสูจน์ทุกโปรแกรมหมดแล้ว

- ให้ผู้เชี่ยวชาญตรวจสอบหน่วยความจำของคอมพิวเตอร์แบบชั่วคราว (RAM Drive) ว่ามีข้อมูลที่ต้องสงสัยหรือไม่ ก่อนปิดไฟฟ้าที่เครื่องคอมพิวเตอร์

3.3.3.7 การกู้ข้อมูลคอมพิวเตอร์บางลักษณะจะต้องอาศัยผู้เชี่ยวชาญทางคอมพิวเตอร์โดยเฉพาะ จึงจะสามารถแยกรายละเอียดข้อมูลที่ต้องการออกมาได้ โดยผู้เขียนจะนำเสนอต่อไปในหัวข้อการพิสูจน์ทราบพยานหลักฐานโดยผู้เชี่ยวชาญ

3.3.3.8 การตรวจยึดพยานหลักฐานในที่เกิดเหตุ

- ตรวจยึดฮาร์ดแวร์ทั้งหมดที่พบในที่เกิดเหตุ
- ตรวจยึดโปรแกรมทั้งหมดในที่เกิดเหตุ
- แผ่นดิสก์, เทปหรือสื่อบันทึกชนิดอื่น ๆ
- เอกสารทั้งหมดที่พบในที่เกิดเหตุ
- อุปกรณ์ต่อพ่วงทั้งหมดที่ค้นพบ เช่น เครื่องพิมพ์, อุปกรณ์สื่อสาร สายเชื่อม, ลำโพง เป็นต้น
- เอกสารที่ถูกทิ้ง เอกสารจากคอมพิวเตอร์และเอกสารพิมพ์ต่อเนื่องจากเครื่องพิมพ์ที่สำคัญจะต้องตรวจดูเอกสารในถังขยะในระหว่างการตรวจค้นด้วย

3.3.3.9 ในกรณีของการหลอกล่อคนร้ายที่ชอบขโมยข้อมูล เจ้าหน้าที่อาจสร้างกับดัก เช่น โปรแกรม Virus ชนิดพิเศษไว้ในข้อมูลที่คนร้ายต้องการ เพื่อเป็นหลักฐานในการจับกุมคนร้ายและฟ้องร้องต่อศาล

3.3.3.10 การตรวจหาและเก็บลายพิมพ์นิ้วมือแฝงในที่เกิดเหตุ รวมทั้งการดำเนินในกรณีอื่น ๆ เช่น การวิเคราะห์แยกแยะพยานบุคคลที่เกี่ยวข้อง

3.3.4 วิธีการตรวจยึดพยานหลักฐานทางคอมพิวเตอร์

3.3.4.1 การตรวจยึดฮาร์ดแวร์ (Hardware) ไมโครคอมพิวเตอร์ (David Icove, 1995 : 190)

A. หน่วยประมวลผลกลาง (CPU)

การตรวจยึดฮาร์ดแวร์ของไมโครคอมพิวเตอร์ ถ้าเครื่องเปิดอยู่และกำลังประมวลผลหรือปฏิบัติงานใดอยู่ปล่อยให้เครื่องทำงานจนเสร็จ แล้วดำเนินการถ่ายภาพหรือ V.D.O. ภาพข้อมูลที่ปรากฏบนจอภาพ นำดิสก์ออกจากหน่วยขับ เก็บข้อมูลจากความจำของ RAM โดยใช้ดิสก์ที่เตรียมมาให้ผู้เชี่ยวชาญทางการรักษาความปลอดภัยตรวจสอบระบบและรหัสผ่านถ้าสามารถเข้าไปสู่จานบันทึกแข็ง (Hard Disk) และเปิดแฟ้มข้อมูลได้จะต้องสำรองข้อมูลเหล่านั้นไว้โดยใช้ดิสก์ที่เตรียมมาเช่นกัน เมื่อเก็บข้อมูลเรียบร้อยแล้วจึงปิดเครื่องคอม-พิวเตอร์ ห้ามเคลื่อนย้ายส่วนประกอบภายในออกจากเครื่องคอมพิวเตอร์ ให้ถอดสายเชื่อมระหว่างอุปกรณ์ต่อพ่วงออก ผูกป้ายกำกับบริเวณปลายสายและบันทึกไว้ที่ป้ายกำกับว่าเป็นช่องเสียบเข้า/ออก สำหรับตัว CPU ติดป้ายกำกับเพื่อแยกแยะ CPU โดยบันทึกไว้ที่ป้ายเรียงตามลำดับตัวอักษรหรือตัวเลข เช่น CPU 1 หมายถึง CPU ที่ตรวจยึดเป็นตัวที่ 1 เป็นต้น และจะต้องบันทึกวันและเวลาที่ตรวจยึดลงบนป้ายกำกับด้วย การเคลื่อนย้ายให้หีบห่อฮาร์ดแวร์โดยใช้พลาสติกและบรรจุลงกล่องสำหรับส่งสู่ห้องปฏิบัติการตรวจหาข้อมูลอีกครั้งหนึ่ง

ส่วนเครื่องคอมพิวเตอร์ที่ปิดอยู่และเครื่องที่ไม่สามารถเข้าไปสู่จานบันทึกแข็ง (Hard Disk) ได้ ให้ทำการตรวจยึดลงสู่ห้องปฏิบัติการเช่นเดียวกัน

B. จอภาพ (Monitor)

ให้ผูกป้ายกำกับที่ปลายสายและบันทึกรายละเอียด เพื่อแสดงว่าเป็นสายเชื่อมหรือช่องเสียบเข้าออกอย่างไร ติดป้ายกำกับลงบนจอภาพและบันทึกว่าเป็นจอภาพที่ใช้กับ CPU เครื่องใด ระบุวันเวลาที่ตรวจยึด การเคลื่อนย้าย หีบห่อจอภาพด้วยพลาสติกและบรรจุลงกล่องส่งสู่ห้องปฏิบัติการ

C. แป้นพิมพ์ (Keyboard)

ให้ผูกป้ายกำกับที่ปลายสายและบันทึกรายละเอียดเพื่อแสดงว่าเป็นช่องเสียบเข้า/ออกอย่างไร ติดป้ายกำกับลงบนแป้นพิมพ์และบันทึกว่าเป็นแป้นพิมพ์ที่ใช้กับ CPU เครื่องใด ระบุวันเวลาที่ตรวจยึด การเคลื่อนย้ายหีบห่อแป้นพิมพ์ด้วยพลาสติกและบรรจุลงกล่องเพื่อส่งสู่ห้องปฏิบัติการ

D. หน่วยขับจานบันทึกแข็งจากภายนอก (External/Removable Hard Drives)

ให้ผู้เชี่ยวชาญตรวจสอบข้อมูลที่บรรจุอยู่ในจานบันทึกแข็ง (Hard Disk) ถ้าตรวจพบให้สำรองข้อมูลไว้ หน่วยขับจานบันทึกแข็งจากภายนอกในการเชื่อมกับคอมพิวเตอร์อาจจะต่อพ่วง โดยใช้คำสั่งจากโปรแกรมหรือไม่ต้องใช้โปรแกรมก็ได้ ดังนั้นในการจัดเก็บจึงต้องตรวจสอบก่อนว่าการต่อพ่วงต้องใช้โปรแกรมหรือไม่ หากใช้ให้ปิดโปรแกรมให้เรียบร้อยก่อนแล้วจึงถอดสายเชื่อม ผูกป้ายกำกับสายเชื่อมเพื่อแสดงว่าเป็นสายเชื่อมที่เสียบเข้า/ออกอย่างไร ติดป้ายกำกับลงบนหน่วยขับและบันทึกว่าเป็นหน่วยขับที่ใช้กับคอมพิวเตอร์เครื่องใด การกำกับอาจจะใช้ลำดับอักษรและหมายเลข ส่วนการเคลื่อนย้ายหีบห่อด้วยพลาสติกและบรรจุลงกล่องเพื่อส่งสู่ห้องปฏิบัติการ

E. หน่วยขับจานบันทึกอ่อนจากภายนอก (External Floppy Diskette Drive)

เคลื่อนย้ายดิสก์ออกจากหน่วยขับ ให้ผู้เชี่ยวชาญคัดลอกข้อมูลโดยใช้ดิสก์ที่เตรียมมาตรวจสอบว่าในการเชื่อมกับคอมพิวเตอร์ต้องใช้โปรแกรมหรือไม่ หากใช้ให้ปิดโปรแกรมให้เรียบร้อยแล้วจึงถอดสายเชื่อม ผูกป้ายกำกับสายเชื่อมเพื่อแสดงว่าเป็นสายเชื่อมที่เสียบเข้า/ออกอย่างไร ติดป้ายกำกับลงบนหน่วยขับและบันทึกว่าเป็นหน่วยขับที่ใช้กับคอมพิวเตอร์เครื่องใด การกำกับอาจจะใช้ลำดับอักษรและหมายเลข ส่วนการเคลื่อนย้ายหีบห่อด้วยพลาสติกและบรรจุลงกล่องเพื่อส่งสู่ห้องปฏิบัติการ

F. หน่วยขับเทปจากภายนอก (External Tape Drive)

ดำเนินการถ่ายภาพและวาดผังระบบติดตั้งสวิตช์ DIP (Dual In Line) โดยเน้นให้เห็นการทำงานของระบบว่าหมุนจากด้านใดไปทางใด ตรวจสอบว่าต้องใช้โปรแกรมในการเปิด-ปิดหน่วยขับหรือไม่ หากใช้ให้ปิดโปรแกรมให้เรียบร้อยแล้วจึงปลดแหล่งพลังงาน เคลื่อนย้ายตัวเทปออกจากหน่วยขับถอดสายเชื่อม ติดป้ายสายเชื่อมเพื่อแสดงทิศทางการเชื่อมต่อ ติดป้ายกำกับหน่วยขับและบันทึกว่าเป็นหน่วยขับที่ใช้กับคอมพิวเตอร์เครื่องใด การกำกับอาจจะใช้ลำดับอักษรและหมายเลข ส่วนการเคลื่อนย้ายหีบห่อด้วยพลาสติกและบรรจุลงกล่องเพื่อส่งสู่ห้องปฏิบัติการ

G. เครื่องพิมพ์ (Printer/Plotters)

ดำเนินการถ่ายภาพและวาดผังระบบติดตั้งสวิตช์ DIP แล้วเคลื่อนย้ายกล่องบรรจุผงหมึก (เครื่องพิมพ์ที่ใช้แบบผ้าหมึกบางชนิดสามารถอ่านได้) ออกจากเครื่องพิมพ์ ติดป้ายกำกับเครื่องพิมพ์และกล่องบรรจุผงหมึกว่าใช้กับคอมพิวเตอร์เครื่องใด การกำกับอาจจะใช้ลำดับอักษรและหมายเลข ส่วนการเคลื่อนย้ายหีบห่อด้วยพลาสติกและบรรจุลงกล่องเพื่อส่งสู่ห้องปฏิบัติการ

H. โมเด็ม (Modem)

โมเด็มจะต้องตัดการติดต่อจากโทรศัพท์ให้ผู้เชี่ยวชาญตรวจสอบที่โปรแกรมใช้งานโทรศัพท์อัตโนมัติว่าได้มีการติดต่อไปยังที่ใดบ้าง คัดลอกหมายเลขโทรศัพท์ที่คอมพิวเตอร์ได้ติดต่อผ่านโมเด็มออกไปและที่ได้รับการติดต่อผ่านโมเด็มเข้ามายังระบบ เพื่อนำมาใช้เป็นพยานหลักฐานและเชื่อมโยงกับแนวทางการสืบสวนสอบสวน ติดป้ายสายเชื่อมเพื่อแสดงทิศทางการเชื่อมต่อ ติดป้ายกำกับที่โมเด็มและบันทึกรายละเอียดว่าใช้กับคอมพิวเตอร์เครื่องใด การกำกับอาจจะใช้ลำดับอักษรและหมายเลข ส่วนการเคลื่อนย้ายหีบห่อด้วยพลาสติกและบรรจุลงกล่องเพื่อส่งสู่ห้องปฏิบัติการ

I. อุปกรณ์ต่อพ่วง/สายเชื่อม (Acoustic Couplers/Cables)

จัดเก็บอุปกรณ์ต่อพ่วงและสายเชื่อมทุกชนิดไว้เป็นพยานหลักฐาน จะต้องดำเนินการถ่ายภาพและวาดผังการเชื่อมต่อแล้วจึงถอดสายเชื่อมนั้น ติดป้ายกำกับที่ปลายสายและที่อุปกรณ์ต่อพ่วง โดยบรรยายสภาพการต่อเชื่อมสายไปสู่ PC เครื่องพิมพ์หรืออุปกรณ์อื่น ๆ การเคลื่อนย้ายอุปกรณ์ต่อพ่วงหีบห่อด้วยพลาสติกบรรจุลงกล่อง ส่วนสายเชื่อมไม่จำเป็นต้องหีบห่อให้บรรจุลงกล่องส่งไปสู่ห้องปฏิบัติการ

3.3.4.2 สื่อบันทึก (Magnetic Media) คอมพิวเตอร์ (David Icove, 1995 : 192)

A. แผ่นดิสก์ (Floppy Diskettes)

การเก็บพยานหลักฐานที่เป็นแผ่นดิสก์ติดป้ายกำกับลงบนแผ่นดิสก์บันทึกลำดับตามตัวอักษรหรือตัวเลข วันเวลาที่ทำการตรวจยึด นอกจากนี้ให้บันทึกชื่อแฟ้มข้อมูลที่ถูกค้นพบ คำสั่งที่ใช้ในการเข้าถึงชื่อของระบบปฏิบัติการหรือรายละเอียดปลีกย่อยอื่น ๆ หากเนื้อที่

บนป้ายกำกับแผ่นดิสก์ไม่พออาจจะบันทึกไว้ต่างหากอีกส่วนก็ได้ เก็บรักษาแผ่นดิสก์ให้ห่างจากสนามแม่เหล็กไฟฟ้าและบรรจุไว้ในกล่องบรรจุแผ่นดิสก์ ห้ามใช้พลาสติกหุ้มเพราะพลาสติกเป็นอันตรายต่อการระบายออกของระบบไฟฟ้าสถิตย์ให้ติดป้ายกำกับแผ่นดิสก์ว่า "ห้ามเอ็กซเรย์" เพื่อเตือนว่าพยานหลักฐานชิ้นนี้จะต้องเก็บรักษาให้ห่างจากสนามแม่เหล็ก รวบรวมนำส่งไปห้องปฏิบัติการ

B. ม้วนเทป (Tape)

การเก็บพยานหลักฐานที่เป็นม้วนเทป ติดป้ายกำกับลงบนม้วนเทป บันทึกลำดับตามตัวอักษรหรือตัวเลข วันเวลาที่ทำการตรวจยึด เก็บรักษาแผ่นดิสก์ให้ห่างจากสนามแม่เหล็กไฟฟ้า ห้ามใช้พลาสติกหุ้ม ติดป้ายกำกับที่ม้วนเทปว่า "ห้ามเอ็กซเรย์" เช่นกัน เพื่อรวบรวมนำส่งไปห้องปฏิบัติการ

3.3.4.3 พยานเอกสาร (Documentation)

A. คู่มือการปฏิบัติงานต่าง ๆ (Manuals/Hand Written Note)

การเก็บพยานหลักฐานที่เป็นเอกสาร เจ้าหน้าที่ผู้ปฏิบัติจะต้องสวมถุงมือเพื่อรักษาลายพิมพ์นิ้วมือแฝงในการตรวจพิสูจน์ ตรวจเก็บเอกสารทุกชนิดที่ต้องสงสัยว่าจะเกี่ยวข้องกับคดี เช่น สมุดคู่มือการใช้เครื่องคอมพิวเตอร์ การใช้โปรแกรมหรือเอกสารที่เป็นการจดบันทึกหรือบันทึกช่วยจำ อาจจะมีรหัสผ่านหรือข้อความที่ใช้เป็นพยานหลักฐานบรรจุลงกล่องติดป้ายกำกับบนกล่อง ระบุวันเวลาที่ทำการตรวจค้นแล้วส่งไปสู่ห้องปฏิบัติการ เพื่อตรวจหาลายพิมพ์นิ้วมือแฝงและใช้เป็นพยานหลักฐานในชั้นศาล

B. เอกสารจากเครื่องพิมพ์/รายการบันทึก (Printout/Listings)

เก็บเอกสารที่ได้จากคอมพิวเตอร์เหล่านั้น โดยใช้ถุงมือเช่นกัน บรรจุใส่กล่องแยกออกมาเป็นพิเศษจากเอกสารชนิดอื่น ๆ ติดป้ายกำกับบนกล่องและบันทึกรายละเอียดว่าเป็นเอกสารจากเครื่องพิมพ์และคอมพิวเตอร์เครื่องใด เป็นข้อมูลที่เกี่ยวข้องในเรื่องใด ระบุวันเวลาที่ทำการตรวจค้นแล้วส่งไปสู่ห้องปฏิบัติการ เพื่อประมวลผลข้อมูลและพิมพ์ซ้ำข้อมูลออกมาเปรียบเทียบและใช้เป็นพยานหลักฐานในชั้นศาล

3.3.4.4 การตรวจยึดพยานหลักฐานที่ไม่สามารถเคลื่อนย้ายได้ (David Icove, 1995 : 187)

พยานหลักฐานที่เป็นเทคโนโลยีคอมพิวเตอร์บางประเภทที่ลักษณะทางกายภาพของพยานหลักฐานนั้นไม่อาจเคลื่อนย้ายไปได้ เช่น คอมพิวเตอร์ขนาดมินิหรือเมนเฟรมคอมพิวเตอร์ขึ้นไป การตรวจค้นจะต้องได้รับความยินยอมจากเจ้าของเครื่องหรือโดยคำสั่งศาลเข้าดำเนินการตรวจค้น การตรวจค้นคอมพิวเตอร์ขนาดใหญ่จึงต้องมีนักวิเคราห์ระบบ โปรแกรมเมอร์และวิศวกรของบริษัทผู้ผลิตเครื่องคอมพิวเตอร์นั้นเข้าดำเนินการตรวจค้น โดยขณะตรวจค้นจะต้องถ่ายภาพหรือถ่ายวีดีโอ (V.D.O.) ไว้ทุกขั้นตอนโดยมีวิธีปฏิบัติดังนี้คือ

A. การเข้าสู่ระบบ (Initial Approach)

การเข้าสู่ระบบอาจจะใช้เครื่องปลายทาง ซึ่งเป็นเครือข่ายของเมนเฟรมนั้นหรือใช้คอมพิวเตอร์ของทีมสืบสวนสอบสวนที่เตรียมไป การเข้าสู่ระบบหากต้องใช้หมายเลขโทรศัพท์ผ่านโมเด็มและรหัสผ่านจะต้องบันทึกหมายเลขโทรศัพท์และรหัสผ่านนั้นไว้เป็นพยานหลักฐาน เมื่อเข้าสู่ระบบได้แล้วให้ค้นหาสิ่งที่ต้องการถ่ายทอดข้อมูลออกมาทางเครื่องพิมพ์และสำรองเก็บใส่ดิสก์ ให้ผู้เกี่ยวข้องลงชื่อรับรองเอกสารจากเครื่องพิมพ์และลงชื่อบนป้ายกำกับแผ่นดิสก์ด้วยเช่นกัน

B. พยานหลักฐานที่ต้องตรวจยึด

- เอกสารจากเครื่องพิมพ์และดิสก์ที่ได้สำรองข้อมูลไว้
- ข้อมูลที่ต้องใช้เป็นพยานหลักฐานซึ่งอยู่ในรายการบันทึกของเครื่อง เช่น ชื่อผู้ใช้ (User name) รหัสผ่าน (Password) หมายเลขโทรศัพท์ที่ติดต่อเข้าระบบที่เป็นของผู้ต้องสงสัยหรือผู้กระทำผิด และข้อมูลปลีกย่อย ๆ อื่นที่ใช้เป็นพยานหลักฐาน ถ่ายทอดออกมาทางเครื่องพิมพ์และให้ผู้เกี่ยวข้องลงชื่อรับรองไว้เป็นหลักฐาน

C. การตรวจยึดพยานหลักฐานจากการใช้โปรแกรม BBS

ตามที่ได้กล่าวมาแล้วว่าโปรแกรม BBS (Bulletin Board System) เป็นโปรแกรมที่อาชญากรคอมพิวเตอร์ใช้รับส่งข้อมูลข่าวสารและลักลอบเข้าไปในโปรแกรม BBS เพื่อค้นหาข้อมูลที่ต้องการ เช่น ข้อมูลเกี่ยวกับผู้ถือบัตรเครดิต รายนามผู้ใช้โทรศัพท์และเลขหมายโทรศัพท์ ในทางธุรกิจมีโปรแกรม BBS มากมายที่ผู้ก่อตั้งได้รวบรวมข้อมูลที่น่าสนใจไว้เพื่อให้ผู้ที่สนใจได้คัดลอกไปโดยเสียค่าใช้จ่ายสำหรับข้อมูลนั้น เนื่องจากโปรแกรม BBS มีขนาดใหญ่และมีข้อมูลที่บรรจุไว้จำนวนมาก เป็นการยุ่งยากและไม่เกิดประโยชน์ที่ทีมสืบสวน

สอบสวนจะตรวจยึดไปทั้งหมด การตรวจยึดมีแนวทางในการปฏิบัติดังนี้คือ (David Icove, 1995 : 185)

- เข้าสู่โปรแกรม BBS หากมีรหัสผ่านให้จดบันทึกไว้เป็นพยานหลักฐาน ค้นหาข้อมูลที่เกี่ยวข้องกับการกระทำผิด หรือข้อมูลที่ต้องสงสัยว่าผู้ติดต่อ (Caller) ได้ใช้ประโยชน์หรือได้รับข้อมูลนั้นไป

- เข้าสู่ระบบปฏิบัติการของโปรแกรมแล้วเปิดระบบค้นหาวิธีการเข้าถึงระบบที่ทำให้ผู้ติดต่อได้ข้อมูลนั้นไป ซึ่งจะได้รายละเอียดเกี่ยวกับผู้ติดต่อ (Caller) เช่น หมายเลขโทรศัพท์ของเครื่องปลายทาง หรือ IP Address ในระบบเครือข่ายอินเตอร์เนต

- ถ่ายทอดข้อมูลออกมาทางเครื่องพิมพ์ เก็บ Printout หรือเอกสารใด ๆ ที่บรรจุข้อมูลที่เกี่ยวข้องกับการกระทำความผิดนั้นและสำรองข้อมูลเหล่านั้นโดยใช้ดิสก์ที่เตรียมไป ให้ผู้ที่เกี่ยวข้องลงชื่อรับรองเอกสารหรือดิสก์นั้นและนำไปใช้เป็นพยานหลักฐานในชั้นศาลต่อไป

D. การตรวจยึดพยานหลักฐานจากการใช้โปรแกรม Auto Dialers

ในระบบเครือข่ายอินเตอร์เนต การติดต่อสื่อสารจะต้องผ่านทางโทรศัพท์ ดังนั้นเลขหมายโทรศัพท์จึงเป็นพยานหลักฐานที่สำคัญ ที่สามารถชี้ชัดและโยงใยไปถึงตัวผู้กระทำความผิดได้ ดังนั้นการตรวจยึดหมายเลขโทรศัพท์จากโปรแกรม Auto Dialers, Speed Dialer, Programmable Telephone หรือโปรแกรมโทรศัพท์ประเภทอื่น ๆ ให้ดำเนินการดังนี้ (David Icove, 1995 : 185)

- ให้เชื่อมต่อการติดต่อทางโทรศัพท์ผ่านโปรแกรมไปสู่แหล่งที่มา

- เข้าถึงโปรแกรมและตรวจสอบค้นหาหมายเลขโทรศัพท์ที่ต้องสงสัยจากบันทึกรายการใช้โปรแกรม

- เมื่อได้หมายเลขที่ต้องสงสัยให้ดำเนินการติดต่อกลับไป หากสามารถเข้าระบบคอมพิวเตอร์ของเครื่องปลายทางได้ให้เข้าไปตรวจค้นหาข้อมูลหรือพยานหลักฐานที่ต้องการและถ่ายทอดข้อมูลเก็บไว้เป็นพยานหลักฐาน

- การดำเนินการดังกล่าวจะต้องได้รับอนุญาตจากศาลก่อนจึงจะสามารถใช้ข้อมูลที่ได้มานั้นเป็นพยานหลักฐานได้

3.4 การพิสูจน์พยานหลักฐานทางด้านคอมพิวเตอร์ (Examining Computer Evidence)

การตรวจพิสูจน์พยานหลักฐานทางด้านคอมพิวเตอร์ จะต้องดำเนินการอย่างเป็นระบบและมีขั้นตอนในการดำเนินการ ผู้ตรวจพิสูจน์จะต้องพิจารณารายละเอียดต่าง ๆ ของการบันทึกข้อมูลที่ค้นพบบนแผ่นดิสก์และฮาร์ดดิสก์ ตามที่ทีมสืบสวนได้บันทึกไว้ในเชิงเอกสารเป็นอันดับแรก และพิจารณาการปฏิบัติอื่น ๆ ต่อพยานหลักฐานในระหว่างที่ทีมสืบสวนได้ดำเนินการตรวจยึดพยานหลักฐานเหล่านั้นมาเพื่อตรวจดูประวัติความเป็นมาของพยานหลักฐานนั้น เมื่อได้ทำความเข้าใจรายละเอียดในเชิงเอกสารแล้ว ผู้ตรวจพิสูจน์จะดำเนินการอย่างเป็นขั้นตอน ดังนี้ (David Icove, 1995 : 192)

3.4.1 การตรวจรับพยานหลักฐาน

A. กำกับพยานหลักฐานทุกชิ้นเพื่อที่จะควบคุมและจัดแบ่งเข้าตรวจพิสูจน์
   - ใช้ระบบกำกับโดยใช้หลายเลข (ขึ้นบัญชี) และบันทึกวันและเวลาที่ได้รับพยานหลักฐาน
   - แยกแยะพยานหลักฐานเหล่านั้นเตรียมส่งผู้ตรวจพิสูจน์
   - ตระเตรียมเอกสารของพยานหลักฐานที่ได้มาจากทีมสืบสวนส่งให้ผู้ตรวจพิสูจน์

B. การเคลื่อนย้ายพยานหลักฐานไปสู่การตรวจพิสูจน์
   - กำหนดให้ชัดเจนว่า ผู้เชี่ยวชาญคนใดจะวิเคราะห์หรือตรวจพิสูจน์พยานหลักฐานชิ้นใด
   - ตระเตรียมวิธีการตรวจค้นและยึดพยานหลักฐานในลักษณะเชิงเอกสารให้ผู้เชี่ยวชาญใช้ประกอบในการตรวจพิสูจน์พยานหลักฐาน
   - ตรวจสอบให้แน่ชัดว่าชิ้นส่วนอุปกรณ์ที่ขึ้นบัญชีไว้ ได้มอบให้ผู้เชี่ยวชาญตรวจพิสูจน์ได้ถูกต้องตรงกับความเป็นจริง
   - ทำเครื่องหมายและกำกับอักษรลงบนพยานหลักฐานแต่ละชิ้นที่ต้องการตรวจพิสูจน์จากห้องปฏิบัติการ และเตรียมกระดาษสำหรับบันทึกการตรวจพิสูจน์

3.4.2 การตรวจพิสูจน์พยานหลักฐาน

เมื่อจะเปิดระบบของพยานหลักฐาน ห้ามใช้ซอฟท์แวร์ของระบบที่ถูกเปิดนั้น ใช้ในการตรวจพิสูจน์มิฉะนั้นจะเป็นการเสี่ยงต่อการทำลายพยานหลักฐาน ควรจะใช้ระบบของผู้ตรวจพิสูจน์ในการตรวจข้อมูลที่ต้องสงสัย

A. ตรวจสอบให้แน่ชัดว่าระบบที่ถูกส่งมานั้นสามารถใช้ได้
   - ตรวจดูระบบการสื่อสารเพื่อตรวจสอบให้แน่นอนว่าระบบนั้นสามารถใช้ได้ในขณะที่ตรวจยึด
   - นำระบบการแก้ไขปัญหาคอมพิวเตอร์มาใช้ทีละขั้นไปสู่การบูติการต่อระบบที่ใช้ได้นั้น

B. จานบันทึกอ่อน (Floppy Disk)
   - ปรับปุ่มกันบันทึกที่แผ่นดิสก์ทั้งหมด
   - แยกแยะคอมพิวเตอร์ที่ใช้ในการตรวจสอบแผ่นดิสก์ออกจากการใช้งานในสภาพปกติ
   - อาจจะต้องดำเนินการเปลี่ยนแปลงระบบบูติการตามระบบของดิสก์ของกลาง
   - สร้างสารบบ (Directory) และสารบบย่อยในการจัดเก็บข้อมูลเป็นกลุ่ม
   - ตรวจสอบหาแฟ้มข้อมูลที่ซ่อนอยู่หรือถูกลบทิ้งไป โดยใช้ซอฟท์แวร์ของบริษัทผู้ผลิต
   - ประมวลผลซ้ำและพิมพ์ข้อมูลใช้เป็นพยานหลักฐาน

C. จานบันทึกแข็ง (Hard Disk)
   - สร้างระบบกันบันทึก เพื่อป้องกันการทำซ้ำของฮาร์ดดิสก์โดยใช้ซอฟท์แวร์ป้องกัน
   - สร้างสารบบและสารบบย่อย และแบ่งฮาร์ดดิสก์ออกเป็นส่วน ๆ แต่ละส่วนสามารถควบคุมได้โดยโปรแกรม
   - ตรวจสอบหาข้อมูลที่ซ่อนอยู่หรือที่ถูกลบทิ้งไปจากแฟ้มข้อมูลสารบบและข้อมูลรายละเอียดอื่น ๆ ที่ถูกซ่อนไว้โดยใช้ซอฟท์แวร์ของบริษัทผู้ผลิต

- ประมวลผลซ้ำและพิมพ์ข้อมูลใช้เป็นพยานหลักฐาน

3.4.3 การรายงานผลการตรวจพิสูจน์พยานหลักฐาน

A. เตรียมรายงานเชิงเอกสารว่าได้ทำสิ่งใดไปบ้างและผลที่ได้เป็นอย่างไร

B. ส่งผลลัพท์จากคอมพิวเตอร์ และรายงานผลการตรวจพิสูจน์ไปยังพนักงานสอบสวนสำหรับการรวบรวมหลักฐานในทางคดี

C. ส่งหลักฐานกลับคืนไปเก็บรักษา

D. เก็บและบรรจุคอมพิวเตอร์และแผ่นดิสก์ทั้งหมดให้เหมือนเดิม

3.4.4 วิธีการพิสูจน์ทราบพยานหลักฐานของผู้เชี่ยวชาญ

จากเรื่องพื้นฐานทางด้านเทคนิคของระบบคอมพิวเตอร์ การประมวลผลข้อมูล การเก็บและเรียกข้อมูล ทำให้เราทราบว่าสื่อที่สำคัญที่ใช้ในการเก็บและเรียกข้อมูล ก็คือจานบันทึกอ่อน (Floppy Disk) และจานบันทึกแข็ง (Hard Disk)

ลักษณะการบันทึกข้อมูลลงในแผ่นดิสก์ (Disk) ที่มีลักษณะเป็นแผ่นกลม ๆ จะบันทึกข้อมูลเป็นวงแหวนซ้อน ๆ กันเหมือนแผ่นเสียง วงแหวนแต่ละวงเรียกว่าแทร็ก (Track) สำหรับ Floppy Disk หรือไซลินเดอร์ (Cylinder) สำหรับ Hard Disk แต่ละวงแบ่งออกเป็นส่วน ๆ เรียกว่าเซ็กเตอร์ (Sector) (Floppy Disk ขนาด 3.5 นิ้ว แบ่งเป็น 17 Sectors และ Hard Disk ส่วนใหญ่แบ่งเป็น 63 Sectors ต่อ Cylinder)

ในหน่วยขับ (Drive) แต่ละตัวอาจมีแผ่นดิสก์ที่ใช้บันทึกข้อมูลหลายหน้า แต่ละหน้าจะมีหัวอ่าน 1 หัว ใน Floppy Disk Drive มีหัวอ่าน 2 หัว แต่ใน Hard Disk Drive อาจมีหัวอ่านตั้งแต่ 2-16 หัว

หน่วยที่เล็กที่สุดที่ใช้ในการบันทึกข้อมูลเรียกว่า คัสเตอร์ (Cluster) และใน 1 Cluster อาจประกอบด้วย 2-6 Sectors ขึ้นอยู่กับขนาดของความจุของแผ่นดิสก์ ซึ่งระบบปฏิบัติการจะเป็นตัวจัดการในเรื่องนี้

เมื่อกล่าวถึงเครื่องคอมพิวเตอร์ สิ่งที่ขาดไม่ได้ก็คือระบบปฏิบัติการ หรือ OS (Operating System) ซึ่งเป็นระบบการจัดการที่มีประสิทธิภาพสูง ถูกต้อง แม่นยำและรวดเร็ว ในการ

- บันทึกข้อมูลไว้ในแผ่นดิสก์
- อ่านข้อมูลที่บันทึกไว้ออกมาใช้งาน
- แก้ไขข้อมูลที่บันทึกไว้ให้ถูกต้องเป็นปัจจุบัน
- ลบหรือยกเลิกข้อมูลที่บันทึกไว้

OS ที่ใช้อยู่ในเครื่องคอมพิวเตอร์มีอยู่มากมายหลายค่าย แต่ละค่ายมีการพัฒนา OS ของตนเอง ตามเทคโนโลยีที่เปลี่ยนไปอย่างสม่ำเสมอ เช่น PC-DOS หรือ MS-DOS ที่ใช้กับเครื่อง IBM PC Compatible เริ่มออกสู่ตลาดตั้งแต่ปี ค.ศ.1981 (Version 1.0) พัฒนาเป็น Version 2 ในปี ค.ศ.1982 และพัฒนาไปเรื่อย ๆ จนกระทั่งถึง Version 6 ในปี ค.ศ. 1992 ซึ่งแต่ละค่ายได้มีการคิดค้นและพัฒนาแข่งขันกันตลอดเวลาเพื่อชิงความได้เปรียบกันในทางธุรกิจ

OS แต่ละตัว มีวิธีการจัดการในการเก็บและเรียกข้อมูลแตกต่างกัน แต่มีหลักการใกล้เคียงกัน คือจัดแบ่งพื้นที่ของแผ่นดิสก์ เพื่อจัดระบบในการเก็บรายละเอียดและส่วนสำคัญของไฟล์ อาจแยกพื้นที่ต่าง ๆ ได้ดังนี้

- Boot Sector
- FAT (File Allocation Table)
- Data Area
- Directory Area

การบันทึกไฟล์ของ MS-DOS จะมีการแยกเก็บรายละเอียด ดังนี้

- ข้อมูลของไฟล์ทั้งหมดเก็บไว้ที่ Data Area
- ชื่อไฟล์ วันเดือนปีและเวลาที่บันทึก ขนาดไฟล์ ชนิดของไฟล์ และหมายเลข Cluster แรกที่ใช้เป็นพื้นที่ในการเก็บไฟล์ (Data Area) เก็บไว้ที่ส่วนของ Directory Area
- หมายเลขของ Cluster ต่าง ๆ ที่ใช้ในการบันทึกไฟล์นี้ จนถึง Cluster สุดท้าย แสดงไว้ในส่วนที่เรียกว่า FAT

การลบไฟล์ใน MS-DOS ไม่มีการลบข้อมูลของไฟล์ในส่วนที่บันทึกไว้ใน Data Area เพียงแต่ทำเครื่องหมายไว้ที่ชื่อไฟล์ใน Directory Area และใน FAT เพื่อให้ OS ทราบว่าไฟล์นี้ไม่ใช้งานแล้ว สามารถเขียนหรือบันทึกข้อมูลไฟล์อื่นทับได้ ดังนั้นหากยังไม่มีการเขียนหรือบันทึกข้อมูลทับ ข้อมูลของไฟล์ที่ถูกสั่งลบก่อนหน้านั้นยังคงอยู่โดยครบถ้วนสมบูรณ์ สามารถกู้คืนได้

ในการเขียนข้อมูลหรือไฟล์ใหม่ ทับไฟล์เดิมที่ถูกลบไป ก็เช่นเดียวกัน OS ไม่ได้ลบข้อมูลหรือไฟล์เก่า เพียงแต่เขียนหรือบันทึกไฟล์ใหม่ทับพื้นที่ที่ใช้เก็บไฟล์ที่ถูกลบ ดังนั้นหากไฟล์ที่บันทึกใหม่มีขนาดเล็กกว่าไฟล์เดิมที่ถูกลบ ย่อมมีข้อมูลบางส่วนของไฟล์หลงเหลืออยู่ในสื่อหรือแผ่นดิสก์ ซึ่งอาจเป็นข้อมูลหรือข้อความที่เป็นประโยชน์ต่อรูปคดี

โดยปกติแล้วระบบปฏิบัติการต่าง ๆ จะมีคำสั่งให้ผู้ใช้งาน ใช้ในการขอดูชื่อไฟล์ที่เก็บบันทึกไว้พร้อมรายละเอียดต่าง ๆ ที่เกี่ยวข้อง เช่น ขนาดของไฟล์ วันเดือนปีและเวลาที่บันทึก ชนิดของไฟล์ นอกจากนั้นยังมีโปรแกรมอรรถประโยชน์ (Utility Software) ที่มาพร้อมกับระบบปฏิบัติการ เพื่ออำนวยความสะดวกกับผู้ใช้งาน ในการจัดการกับไฟล์และสื่อที่ใช้ในการบันทึกข้อมูล เช่น ซ่อนไฟล์ (Hidden Filed), เปลี่ยนชื่อไฟล์ ฯลฯ แต่มีประสิทธิภาพสู้โปรแกรมอรรถประโยชน์ (Utility Software) โดยตรงเช่น PC Tools หรือ Norton Utility ซึ่งสามารถเข้าไปดูและแก้ไขดิสก์ได้ทุกตารางนิ้วไม่ได้

ในการใช้งานเครื่องคอมพิวเตอร์ ย่อมมีการบันทึก แก้ไขและลบข้อมูล ในการดำเนินการเหล่านั้นย่อมมีร่องรอยการใช้งานในแต่ละครั้งหลงเหลืออยู่ในสื่อที่ใช้บันทึก เนื่องจากในการลบแต่ละครั้ง ระบบปฏิบัติการไม่ได้ลบข้อมูลจริง ดังกล่าวข้างต้น หากเราใช้โปรแกรมอรรถประโยชน์ที่เหมาะสม ก็จะสามารถกู้ไฟล์หรือข้อมูลที่ถูกลบทิ้งคืนมา นอกจากนั้นยังสามารถเข้าไปดูข้อมูล ข้อความที่เคยถูกบันทึกไว้และยังถูกเขียนหรือบันทึกทับไม่หมด หรืออาจตรวจหาข้อมูลที่ผู้ใช้งานจงใจพิมพ์ซ่อนไว้ได้

ดังนั้น เมื่อมีอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์เกิดขึ้น โดยมีการยึดเครื่องคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้องมาเป็นของกลาง พนักงานสอบสวนจะต้องระมัดระวังในการจัดการกับสื่อต่าง ๆ ที่ใช้ในการบันทึกข้อมูลที่ยึดไว้ เพื่อมิให้ข้อมูลสูญหายและควรให้ผู้เชี่ยวชาญในระบบปฏิบัติการของเครื่องนั้น ๆ มาทำการตรวจสอบ ค้นหา กู้คืน ข้อมูลและ/หรือข้อความที่ถูกบันทึกหรือเคยถูกบันทึกในสื่อนั้น ๆ ทั้งหมด รวมทั้งไฟล์หรือข้อความที่ถูกสั่งให้ซ่อนไว้ (Hidden Files or Hidden Data) เพื่อให้ได้มาซึ่งข้อมูลบางอย่างที่อาจมีความเกี่ยวโยงกับการกระทำ

ความผิด เช่น หมายเลขโทรศัพท์ เลขบัญชีธนาคาร ชื่อบุคคล ชื่อสถานที่ ข้อความที่ใช้ติดต่อ ซึ่งสามารถใช้เป็นพยานหลักฐานที่สำคัญ ที่จะแสดงต่อศาล เพื่อเอาตัวผู้กระทำความผิดมาลงโทษต่อไปได้

3.5 การรักษาสภาพพยานหลักฐานอย่างปลอดภัย

3.5.1 การรักษาพยานหลักฐานที่เป็นเทปแม่เหล็ก (Magnetic Tape), ดิสก์ (Disk) หรือ ซีดี-รอม (CD-ROM)

- บรรจุเทป ดิสก์ หรือ แผ่นซีดี-รอม ไว้ในกล่องบรรจุโดยเฉพาะและห้ามใช้พลาสติกห่อหุ้ม เพราะว่าพลาสติกเป็นอันตรายต่อการระบายออกของระบบไฟฟ้าสถิตย์และติดป้ายกำกับว่า "ห้ามเอ็กซเรย์"

- จะต้องเก็บรักษาไว้ในสถานที่ที่ซึ่งรักษาอุณหภูมิให้คงที่ อยู่ในระหว่าง 50-80 องศาฟาเรนไฮน์ หรือระหว่าง 10-26 องศาเซลเซียส และเป็นสถานที่ที่มีความชื้นเล็กน้อย ในระหว่าง 35-50 เปอร์เซนต์

- การจัดวางต้องคำนึงถึงเรื่องกระแสแม่เหล็กที่อาจส่งออกมาจากเครื่องมือหรือชิ้นส่วนอุปกรณ์ใดไปทำลายหลักฐานหรือข้อมูลทางคดีที่ตรวจค้นยึดมา

3.5.2 การรักษาพยานหลักฐานที่เป็นฮาร์ดแวร์และอุปกรณ์ต่อพ่วง

- หีบห่อและบรรจุลงลัง

- เก็บให้ห่างจากน้ำ และควันไฟ

- อุปกรณ์บางชนิดจะต้องใส่แบตเตอรี่หรือถ่านให้พลังงาน จะต้องหมั่นตรวจสอบดูแลอยู่เสมอ โดยเขียนป้ายกำกับให้ชัดเจน

- เก็บไว้ในห้องคอมพิวเตอร์โดยเฉพาะ คือเป็นห้องที่มีการควบคุมอุณหภูมิให้อยู่ในระหว่าง 50-80 องศาฟาเรนไฮน์หรือ 10-26 องศาเซลเซียส

- ควบคุมความชื้นสัมผัสอยู่ที่ 35-50 เปอร์เซนต์

- ติดตั้งระบบเครื่องปรับอากาศโดยเฉพาะสำหรับห้องคอมพิวเตอร์

- ติดตั้งระบบอุปกรณ์วัดและส่งสัญญาณเตือนเมื่ออุณหภูมิและความชื้น มีการเปลี่ยนแปลงไป

- อุปกรณ์ระบบให้ความเย็นและความร้อน เพื่อรักษาอุณหภูมิและควรติดตั้งระบบกรองอากาศ เพื่อป้องกันฝุ่นละอองที่จะมาทำอันตรายต่อคอมพิวเตอร์อุปกรณ์ต่อพ่วงโดยเฉพาะแผ่นดิสก์และแผ่นพิมพ์

3.6 แนวทางในการสืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์

ในการสืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์ สิ่งแรกที่จะต้องพิจารณาคือรูปแบบหรือชนิดของอาชญากรรมคอมพิวเตอร์ โดยพิจารณาว่าอาชญากรรมที่เกิดขึ้นนั้นเป็นอาชญากรรมที่กระทำในรูปแบบใด คือ

- **ฮาร์ดแวร์** (Hardware)

  จะเป็นการกระทำผิดที่เกี่ยวกับส่วนอุปกรณ์ประกอบของเครื่องคอมพิวเตอร์ เช่น การขโมยชิ้นส่วนอุปกรณ์คอมพิวเตอร์ที่สำคัญบางประเภท ได้แก่ วงจรหน่วยความจำ (Memory), วงจรส่วนสมองกล (Chip), วงจรระบบควบคุม CPU ฯลฯ

- **ซอฟท์แวร์** (Software)

  จะเป็นการกระทำผิดที่เกิดขึ้นกับส่วนของโปรแกรมคำสั่งในการใช้งานเครื่องคอมพิวเตอร์ สามารถแบ่งได้เป็น 3 ประเภทย่อยคือ

  1. การละเมิดลิขสิทธิ์
  2. การคัดลอกข้อมูลอันเป็นความลับ ซึ่งมีความสำคัญ
  3. การใช้ Software เพื่อประกอบอาชญากรรมโดยตรงเช่น การถอดรหัสผ่าน (Password) เพื่อที่จะลักลอบเข้าไปสู่ฐานข้อมูลของผู้อื่น

- **ระบบการสื่อสาร** (Telecommunication)

  จะเป็นการกระทำความผิดที่เกี่ยวกับการสื่อสารโทรคมนาคมทุกประเภท เนื่องจากอุปกรณ์สื่อสารต่าง ๆ เหล่านี้มีลักษณะเป็นเครื่องคอมพิวเตอร์ประเภทหนึ่ง การ

ประกอบอาชญากรรมจึงสามารถที่จะกระทำได้โดยอาศัยเครือข่ายสื่อสารในด้านคอมพิวเตอร์

เมื่อพิจารณาได้ถึงรูปแบบหรือชนิดของอาชญากรรมคอมพิวเตอร์แล้ว ทีมสืบสวนจะวิเคราะห์หาผู้ต้องสงสัยหรือผู้กระทำผิดจากพยานหลักฐาน การสอบสวนปากคำผู้เสียหายและพยานบุคคลที่เกี่ยวข้อง ซึ่งจะทำให้การสืบสวนหาตัวผู้กระทำผิดแคบเข้าจนถึงการจับกุมตัวได้ในที่สุด ไอคอป, ซีเกอร์ และ วันสเตร์ ได้ให้แนวทางในการสืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์ว่าจะต้องวิเคราะห์หารูปแบบหรือวิธีการกระทำผิดต่อคอมพิวเตอร์ก่อนแล้วจึงรวบรวมพยานหลักฐานวิเคราะห์หาผู้ต้องสงสัย หรือผู้กระทำผิดต่อไปโดยได้ให้แนวทางวิเคราะห์การกระทำผิดต่อคอม-พิวเตอร์, วิธีการสืบสวน, พยานหลักฐานที่ต้องรวบรวมไว้ดังนี้ (David Icove, 1995 : 55)

3.6.1 **การเข้าไปคัดลอกหรือล้วงข้อความ** (Dumpster Diving)

หมายถึง การกระทำที่มีลักษณะเป็นการค้นหาเพื่อเข้าถึงรหัสหรือข้อมูลปลีกย่อยอื่น ๆ ในถังขยะอิเล็กทรอนิกส์ (ที่ซึ่งจัดไว้เป็นการเฉพาะสำหรับลากข้อมูลทิ้งลงไป) Crackers จะพยายามกู้ข้อมูลที่ถูกลบทิ้งไปจากเทปหรือดิสก์

ผู้ต้องสงสัย

(1) ผู้ใช้ระบบ

(2) บุคคลที่สามารถเข้าถึงถังขยะอิเล็กทรอนิกส์

(3) บุคคลที่เข้าถึงที่ตั้งของคอมพิวเตอร์ หรือบริเวณที่เก็บสำรองข้อมูล

วิธีสืบสวน

(1) ตามรอยหรือติดตามเจ้าของข้อมูลย้อนหลังไปสู่แหล่งที่มา (จากบันทึกชื่อหรือสัญลักษณ์ของบริษัท)

(2) โดยการสังเกต (สอบถามพนักงานรักษาความปลอดภัย อาจจะพบเห็นพฤติการณ์ของผู้บุกรุกผู้ต้องสงสัย)

พยานหลักฐาน

(1) ผลลัพท์คอมพิวเตอร์ที่ได้จากสื่อบันทึก (อาจจะมีชื่อผู้จำหน่าย, ผู้ขายหรือจำแนกจำนวนหน้า)

(2) ข้อความที่คล้ายกันซึ่งถูกผลิตหรือทำให้มีขึ้นในวิธีที่น่าสงสัยในรูปแบบอย่างเดียวกัน

(3) ลักษณะของแผ่นพิมพ์หรือข้อมูลที่ได้จากสื่อประเภทอื่น (ลักษณะตัวอักษรหรือเครื่องหมาย)

3.6.2 **การดักฟังและการลอบฟัง** (Wiretapping and Eavesdropping)

การดักฟัง (Wiretapping) หมายถึงการสกัดกั้นสัญญาณการสื่อสาร ด้วยจุดประสงค์เพื่อให้ได้รับข้อมูลและข้อความที่ถูกส่งทางวงจรการสื่อสาร

การลอบฟัง (Eavesdropping) หมายถึงการลอบฟังเสียงหรือข้อมูล ซึ่งถูกส่งสื่อสารโดยปราศจากอำนาจ

ผู้ต้องสงสัย

(1) ช่างเทคนิคและวิศวกรการสื่อสาร

(2) ฝ่ายตรงข้ามหรือคู่แข่งทางการค้า

(3) พนักงานการสื่อสาร, อดีตพนักงาน, ผู้จำหน่ายและผู้แทนทางการค้า

(4) หน่วยงานสืบราชการลับของต่างประเทศ

วิธีสืบสวน

(1) วิธีใช้ดักฟังเสียง

(2) สืบร่องรอยว่าเครื่องมือที่ใช้ในการกระทำผิดมาจากที่ใด

(3) สืบร่องรอยผลลัพท์คอมพิวเตอร์จากดิสก์และเทปไปสู่แหล่งที่มา

(4) โดยการสังเกตสิ่งผิดปกติ

(5) ค้นหาข้อมูลที่ถูกขโมยไป

พยานหลักฐาน

(1) เสียงซึ่งถูกลอบฟังเพื่อใช้เป็นพยานหลักฐาน

(2) รูปแบบผลลัพท์จากคอมพิวเตอร์

(3) เครื่องคอมพิวเตอร์ที่ใช้ตรวจสอบการบันทึกการปฏิบัติงานหรือเหตุการณ์ที่เกิดขึ้นตามลำดับ ซึ่งบันทึกทุกอย่างที่เกี่ยวข้องกับการทำงาน (Computer Audit Logs)

(4) สื่อบันทึกจากหน่วยเก็บข้อมูลของเครื่องคอมพิวเตอร์

(5) ลักษณะของแผ่นพิมพ์หรือข้อมูลที่ได้จากสื่อประเภทอื่น ลักษณะตัวอักษรหรือเครื่องหมายต่าง ๆ

(6) เอกสารที่ใช้สำหรับลงนามก่อนการใช้และหลังการใช้เครื่องคอมพิวเตอร์

3.6.3 การปลอมตัว (Masquerading)

หมายถึง การแสดงตัวว่าเป็นผู้ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ แต่ความจริงตนเองไม่ได้รับอนุญาต มักเกิดขึ้นในกรณีการพยายามเข้าสู่ระบบคอมพิวเตอร์โดยไม่มีอำนาจ

ผู้ต้องสงสัย

(1) บุคคลทั่วไปสามารถที่จะกระทำผิดได้ไม่จำกัดหรือชี้ชัดไปว่าจะเป็นบุคคลใดโดยเฉพาะ

วิธีสืบสวน

(1) จำแนกแยกแยะเพื่อตรวจสอบบันทึกการปฏิบัติงานและรายงานประจำวัน เช่น ในบันทึกรายการแสดงว่า ผู้ได้รับอนุญาตใช้คอมพิวเตอร์ได้เข้ามาใช้เครื่องคอมพิวเตอร์ แต่ปรากฏว่าขณะนั้นผู้ได้รับอนุญาตคนนั้นไม่อยู่

(2) โดยการสังเกต เช่น ในบันทึกรายการผู้ใช้เครื่องคอมพิวเตอร์ ปรากฏว่ามีผู้พยายามใช้รหัสผ่านที่ไม่ชอบเข้ามาซ้ำ ๆ กัน

(3) การฝ่าฝืนหรือละเมิดรหัสผ่าน เช่น บันทึกรายการจะแสดงว่ามีความล้มเหลวหลายครั้งในการพยายามใช้รหัสผ่านที่ไม่ถูกต้อง

(4) จากการรายงานของตัวบุคคล ผู้ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ตัวจริง ซึ่งถูกแอบอ้างเอาชื่อไปใช้ เช่น ผู้มีอำนาจใช้เครื่องตัวจริงต้องการเข้าสู่ระบบเพื่อใช้เครื่องแต่เครื่องแจ้งว่ามีการพยายามเข้าสู่ระบบแต่ไม่สำเร็จมาแล้วรวม 6 ครั้ง ตั้งแต่ครั้งสุดท้ายที่เข้าสู่ระบบได้

พยานหลักฐาน

(1) แฟ้มข้อมูลเพื่อเก็บไว้สำรองใช้

(2) การบันทึกการเข้าสู่ระบบ

(3) บันทึกการใช้โทรศัพท์ (สถิติจากเครื่องบันทึกหมายเลขโทรศัพท์อัตโนมัติ)

(4) รายงานการละเมิดหรือฝ่าฝืนจากโปรแกรมควบคุมการเข้าสู่ระบบ

(5) บันทึกและเอกสารซึ่งพบในความครอบครองของผู้ต้องสงสัย

(6) พยานบุคคลที่เกี่ยวข้อง

(7) ใบแจ้งหนี้การใช้โทรศัพท์ที่มากเกินปกติ

3.6.4 **การละเมิดลิขสิทธิ์** (Software Piracy)

หมายถึง การลักลอบทำสำเนาโปรแกรม ไม่ว่าจะเป็นทางการค้าหรือไม่ก็ตาม

ผู้ต้องสงสัย

(1) ผู้ซื้อและผู้ใช้โปรแกรมพาณิชย์, โปรแกรมทางการค้า

(2) ผู้ละเมิดลิขสิทธิ์

(3) พนักงานของบริษัทซึ่งขโมยโปรแกรมของคนอื่น

วิธีสืบสวน

(1) โดยการสังเกตสิ่งผิดปกติ

(2) ค้นให้การของผู้ซื้อโปรแกรมที่ถูกต้องตามกฎหมาย

(3) ตรวจค้นเครื่องใช้และเครื่องคอมพิวเตอร์ของผู้ใช้ระบบ

พยานหลักฐาน

(1) ภาพถ่ายจากจอคอมพิวเตอร์ขณะที่มีการใช้โปรแกรมที่ถูกละเมิดลิขสิทธิ์

(2) เนื้อหาในหน่วยความจำของเครื่องคอมพิวเตอร์ที่มีโปรแกรมที่ถูกละเมิดลิขสิทธิ์บันทึกไว้

(3) สำเนาของสื่อบันทึกที่พบว่ามีโปรแกรมละเมิดลิขสิทธิ์บันทึกไว้

(4) สิ่งที่พิมพ์ออกมาทางเครื่องพิมพ์โดยใช้โปรแกรมละเมิดลิขสิทธิ์

3.6.5 **ประตูกล** (Trap Doors)

หมายถึง โปรแกรมคอมพิวเตอร์ที่นักเขียนโปรแกรมได้เว้นตำแหน่งช่องว่างไว้ในชุดคำสั่งในการเขียนโปรแกรม เพื่อใช้ในการเพิ่มคำสั่งและใช้ในการปรับปรุงแก้ไขโปรแกรมในภายหลัง ตำแหน่งช่องว่างเหล่านี้อาจกลายเป็นประตูกลให้มีการซ่อนคำสั่งหรือรหัสคำสั่งสามารถทำให้เครื่องคอมพิวเตอร์ทำงานตามที่ต้องการได้

ผู้ต้องสงสัย

(1) นักเขียนโปรแกรม

(2) นักเขียนโปรแกรมประยุกต์

วิธีสืบสวน

(1) ตรวจสอบโปรแกรมโดยละเอียดเพื่อหาช่องว่างที่เว้นไว้

(2) ตรวจสอบตามหลักการหาพยานหลักฐาน

(3) เปรียบเทียบคุณลักษณะเฉพาะกับการปฏิบัติงานจริงว่าถูกต้องหรือไม่

พยานหลักฐาน

(1) โปรแกรมซึ่งทำงานได้ไม่ตรงตามที่ระบุไว้

(2) รายงานผลลัพท์ที่ได้มาไม่ตรงตามชนิดของงานที่โปรแกรมระบุไว้

3.6.6 **การจู่โจม** (Timing Attacks)

หมายถึง การจู่โจมเข้าสู่ระบบ ขณะที่เครื่องคอมพิวเตอร์กำลังทำงานเพื่อสามารถเข้าถึงระบบได้

ผู้ต้องสงสัย

(1) นักวิเคราะห์ระบบระดับสูงหรือเชี่ยวชาญ

(2) โปรแกรมเมอร์ระดับสูงหรือเชี่ยวชาญ

วิธีสืบสวน

(1) ตรวจสอบระบบถึงวิธีการจู่โจมที่น่าสงสัย

(2) คำให้การของผู้ใช้ระบบว่ากิจกรรมหรืองานที่เกี่ยวข้องกับคอมพิวเตอร์ไม่สามารถทำให้บรรลุแห่งความสำเร็จซึ่งการแสดงผลหรือเกิดผลได้

(3) ทบทวนการดำเนินงานที่ต้องปฏิบัติเป็นปกติประจำ

พยานหลักฐาน

(1) ผลลัพท์ซึ่งมีลักษณะที่ผิดปกติไปจากงานปกติประจำ

(2) บันทึกการปฏิบัติงานตามลำดับของคอมพิวเตอร์

3.6.7 การใช้โปรแกรมกระทำผิด

อุบายม้าไม้โทรจัน (Trojan Horse) เป็นโปรแกรมที่ผู้กระทำผิดจะทำการเพิ่มเติมหรือแก้ไขคำสั่งในโปรแกรมคอมพิวเตอร์ก่อนที่จะนำโปรแกรมนั้นไปใช้งานอันเป็นการแอบซ่อนคำสั่งลับไว้เพื่อให้คอมพิวเตอร์ทำงานบางอย่างให้ ในขณะเดียวกันก็ยังปล่อยให้โปรแกรมนั้นทำงานตามปกติของมันไปด้วย

ไวรัส (Viruses) เป็นโปรแกรมที่สามารถเผยแพร่ได้ด้วยตนเอง ที่ซึ่งเกาะติดไปกับซอฟท์แวร์เมื่อมีการทำงานของโปรแกรม เป็นโปรแกรมที่เขียนขึ้นมาเพื่อทำลายข้อมูลและรบกวนการทำงานของเครื่องขับแผ่นดิสก์ ทำให้เครื่องทำงานไม่เป็นปกติ

ซาลามิ (Salamis) เป็นโปรแกรมที่สั่งให้เครื่องคอมพิวเตอร์ทำซ้ำในการปัดเศษจุดทศนิยมของเงินตรา เป็นการหยิบเอาประโยชน์ของเลขทศนิยมในการคำนวณดอกเบี้ยของธนาคาร

ระเบิดลอจิก (Logic Bombs) เป็นโปรแกรมที่เขียนซ่อนไว้ในโปรแกรมที่ใช้ทำงานปกติและจะทำงานเมื่อมีเหตุการณ์อย่างใดอย่างหนึ่งที่ระบุไว้เกิดขึ้น

ผู้ต้องสงสัย

(1) นักเขียนโปรแกรมผู้ซึ่งมีความรู้ในรายละเอียดของโปรแกรม

(2) พนักงานปัจจุบันหรืออดีตพนักงาน

(3) ผู้จำหน่ายหรือนักเขียนโปรแกรมซึ่งเป็นคู่สัญญา

(4) นักเขียนโปรแกรมระบบทางการเงิน

(5) ผู้ใช้และปฏิบัติงานด้านคอมพิวเตอร์

(6) พวก Crackers

วิธีสืบสวน

(1) เปรียบเทียบรหัสคำสั่งโปรแกรมที่ใช้อยู่กับรหัสคำสั่งสำรองที่เก็บรักษาไว้

(2) ติดตามร่องรอยของเหตุการณ์ที่ไม่น่าจะเกิดขึ้นได้ ซึ่งเป็นผลที่เกิดขึ้นจากการกระทำที่สามารถสาวไปถึงผู้บุกรุกได้

(3) จำแนกรายละเอียดข้อมูล รวมทั้งจำแนกแยกแยะรหัสโปรแกรม เช่น อาจจะพบโปรแกรมไวรัส เพราะว่าแฟ้มข้อมูลมีขนาดใหญ่ขึ้นเนื่องจากถูกเปลี่ยนแปลงแก้ไขหรือเพราะว่าเนื้อที่ว่างของดิสก์ มีปริมาณที่ลดลง

(4) สังเกตติดตามพฤติกรรมทางด้านการใช้เงินของผู้ต้องสงสัย

(5) ตรวจสอบโปรแกรมที่น่าสงสัย

(6) ตรวจสอบการบันทึกรายการประจำวันของคอมพิวเตอร์ สำหรับโปรแกรมที่น่าสงสัยหรือข้อมูลที่เกี่ยวข้องกับการถูกนำเข้ามา เช่น บันทึกรายการการเข้าสู่ระบบที่แสดงว่าโปรแกรมจำนวนมากถูกปรับปรุงแก้ไขในช่วงเวลานั้น (ตรวจสอบเป็นพิเศษสำหรับโปรแกรมไวรัส)

พยานหลักฐาน

(1) ผลลัพท์จากคอมพิวเตอร์ในเชิงเอกสาร

(2) ผลลัพท์ที่เหนือคาดหมายของการทำงานของโปรแกรม

(3) รายการการใช้คอมพิวเตอร์และการเรียกใช้แฟ้มข้อมูล

(4) การทำงานที่ไม่ปรากฏว่ามีคำอธิบายว่าเป็นงานอะไร

(5) ผลลัพท์ที่ได้จากการวิเคราะห์แยกแยะการตรวจสอบโปรแกรม

(6) บันทึกรายการ การตรวจสอบการใช้ระบบประจำวัน

3.6.8 **การโกงข้อมูล** (Data Diddling)

หมายถึง การเปลี่ยนแปลงข้อมูลทั้งในเวลาก่อน, ระหว่างหรือหลังใส่ข้อมูลเข้าไปสู่ระบบคอมพิวเตอร์

ผู้ต้องสงสัย

(1) ผู้มีส่วนในการติดต่อดำเนินงานทางธุรกิจในระหว่างที่ใส่หรือปรับปรุงข้อมูล

(2) ผู้ให้ข้อมูลดิบ

(3) ผู้ตระเตรียมข้อมูล

วิธีสืบสวน

(1) การเปรียบเทียบของข้อมูลก่อนและหลังใส่ข้อมูลเข้าไปสู่ระบบคอมพิวเตอร์

(2) การวิเคราะห์แยกแยะรายงานความสมบูรณ์ของคอมพิวเตอร์

(3) การตรวจสอบความถูกต้องแท้จริงของข้อมูล

(4) ความสมบูรณ์ถูกต้องของเอกสาร

(5) วิเคราะห์แยกแยะการตรวจสอบรายการประจำวัน

(6) วิเคราะห์แยกแยะผลลัพท์ของคอมพิวเตอร์

พยานหลักฐาน

(1) เอกสารข้อมูลดิบและเอกสารการดำเนินงานทางธุรกิจอื่น ๆ

(2) บันทึกการตรวจสอบรายการประจำวัน

(3) ข้อมูลที่เก็บสำรองไว้และที่อยู่ในสื่อบันทึกประเภทอื่น เช่น เทปและดิสก์

(4) ผลลัพท์จากคอมพิวเตอร์ที่ไม่ถูกต้องใช้ควบคุมสัญญาณบอกเหตุการละเมิดได้

3.6.9 **การเจาะระบบ** (Scanning)

หมายถึง โปรแกรมที่พยายามประมวลผลหรือกำหนดลำดับการเปลี่ยนแปลงหมายเลข (โทรศัพท์หรือรหัสผ่าน) ไปสู่การกำหนดสิ่งซึ่งหรือรหัสซึ่งมีการขานรับหรือคำตอบที่แท้จริง

ผู้ต้องสงสัย

(1) ผู้บุกรุกซึ่งมีความประสงค์ร้ายหรือมุ่งร้าย

(2) สายลับที่พยายามเข้าถึงระบบโดยมีเป้าหมายอยู่ที่ข้อมูล

(3) อาชญากรที่มีเจตนากระทำความผิดในฐานฉ้อโกง

วิธีสืบสวน

(1) ตรวจสอบการบันทึกรายการประจำวันของคอมพิวเตอร์ ซึ่งจะแสดงว่ามีการติดต่อหรือพยายามติดต่อกับคอมพิวเตอร์ผ่านทางสายโทรศัพท์

(2) การสูญหายของข้อมูลหรือการรอนเงินหรือประโยชน์ที่เป็นทรัพย์สินในลักษณะอื่น ๆ

(3) ตรวจสอบบันทึกการใช้โทรศัพท์

พยานหลักฐาน

(1) บันทึกการใช้โทรศัพท์ของบริษัท (บันทึกหรือสถิติจากเครื่องบันทึกหมายเลขโทรศัพท์อัตโนมัติ)

(2) บันทึกรายการประจำวันของคอมพิวเตอร์

(3) การมีไว้ในครอบครองของสิ่งที่เรียกว่า "เปรียบเสมือนข้อมูลข่าวสาร" เพราะได้มาจากการสแกนภาพ รวมทั้งรายชื่อหมายเลขโทรศัพท์