บทที่ 2
พื้นฐานและทฤษฎีที่เกี่ยวข้อง

2.1 พื้นฐานและทฤษฎีที่เกี่ยวข้องกับเว็บไซต์

2.1.1 PHP มี function ที่ใช้งานดังนี้

1. new ZipArchive() คือ การเรียกใช้ function สำหรับการ Zip file Zip file คือ การทำให้ ไฟล์หรือรูปภาพมีขนาดเล็กลง เพื่อประหยัดพื้นที่ในการเก็บรักษา แต่คุณภาพทุกอย่างยังเหมือนเดิม new ZipArchive() มี mode การใช้งานดังนี้

- ZipArchive::CREATE ใช้สำหรับสร้างไฟล์ zip
- ZipArchive::OVERWRITE ใช้เมื่อมีไฟล์เดิมอยู่แล้วให้สามารถบันทึกทับ

2. Function hash_file() คือ function ที่ใช้ในการนำเอาข้อมูลอิเล็กทรอนิกส์ต้นฉบับที่จะส่ง มาผ่านกรบวนการทางด้านคณิตศาสตร์ที่เรียกว่า Hash Function เพื่อให้ได้ข้อมูลที่สั้น ที่เรียกว่า Digest หรือ ข้อมูลย่อย โดยใช้กระบวนการ MD5 (Message-Digest algorithm 5) การเข้ารหัสแบบ Hash (Cryptographic hash) คือ การแปลงรูปแบบของข้อมูลที่รับเข้ามาไม่ว่าขนาดเท่าใดก็ตาม ให้อยู่ในอีกรูปแบบหนึ่งที่มีขนาดคงที่ เพราะฉะนั้น จะไม่สามารถเรียกดูข้อมูลต้นฉบับได้ (Decrypt) ทำได้เพียงตรวจสอบว่าข้อมูลที่ให้มาแต่ละครั้งเหมือนกันหรือไม่ ความปลอดภัยจึงค่อนข้างสูง

สามารถทำให้ข้อมูลย่อลงแต่มีลักษณะจำเพาะของข้อมูลนั้น โดยอาจกระทำโดยการแบ่งข้อมูลออกเป็นส่วนๆ ผ่านวิธีการใดๆแล้วนำกลับมารวมกัน เรียกว่า ค่าแฮช (hash value)

คุณสมบัติของฟังก์ชันแฮช (Hash function)

- ข้อมูลแต่ละตัวเมื่อผ่านฟังก์ชันแฮชแล้วจะต้องมีค่าไม่เท่ากัน มีลักษณะที่จำเพาะแต่ล่ะข้อมูล
- หาค่าแฮชจากข้อมูลควรทำได้ง่ายและรวดเร็ว
- เมื่อข้อมูลผ่านฟังก์ชันแฮชแล้วไม่ควรทำย้อนกลับได้
- การบวนการแฮชควรมีการกระจายตัวสูง ข้อมูลใดๆที่ผ่านฟังก์ชันแฮชควรมีขนาดเท่ากัน แต่ไม่เหมือนกัน

ชนิดของฟังก์ชันแฮช

- MD2 (128bits) คิดค้นโดย Ronald Rivests
- MD4 (128bits) คิดค้นโดย Ronald Rivests

- MD5 (128bits) คิดค้นโดย Ronald Rivests

- MD6 (0~512 bits) คิดค้นโดย Ronald Rivests Team

- SHA0 (160bits) คิดค้นโดย National Security Agency : NSA

- SHA1 (160bits) คิดค้นโดย National Security Agency : NSA

- SHA2 (SHA-224, SHA-256, SHA-384, SHA-512) คิดค้นโดย National Security Agency : NSA

ในที่นี้ MD5 เป็นการเข้ารหัสแบบ 128-bit ให้ค่าเป็นตัวเลขฐาน 16 (0123456789abcd) ขนาด 32 ตัวอักษร แต่ก็มีบางประเภทที่ให้ค่าเป็น binary และ base64

2.1 ประโยชน์ของการ HASH

1. นำไปตรวจสอบความถูกต้องของไฟล์ สมมติว่ามีไฟล์สองไฟล์ ถ้าเนื้อหาในไฟล์เหมือนกันทุกประการก็จะได้ค่า MD5 เหมือนกัน แต่หากว่า ค่า MD5 ไม่ตรงกัน นั้นแสดงว่าต้องมีไฟล์ใดๆไฟล์หนึ่งที่ไม่สมบูรณ์ ซึ่งการตรวจสอบเป็นการลดรูปของข้อมูลเพื่อให้ง่ายต่อการตรวจสอบ

2. นำไปใช้ในการเก็บข้อมูลที่ไม่ต้องการเปิดเผย เช่น เก็บรหัสผ่านไว้ในฐานข้อมูล

3. เพื่อใช้ตรวจสอบว่าข้อมูลมีการเปลี่ยนแปลงหรือไม่

4. เพื่อใช้เก็บข้อมูลสำหรับเปรียบเทียบ โดยการเปรียบเทียบข้อมูลจะทำได้รวดเร็วขึ้น

5. ทำให้เป็นภาษาที่มนุษย์อ่านไม่เข้าใจ

6. หากข้อมูลที่จะใช้เปรียบเทียบมีขนาดใหญ่มาก จะช่วยย่อข้อมูลให้เล็กลงได้มาก แต่ขึ้นอยู่กับวิธีของฟังก์ชันแฮช

2.1.2 FTP (File Transfer Protocol) คือ โปรโตคอลเครือข่ายชนิดหนึ่ง ถูกนำใช้ในการถ่ายโอนไฟล์ ระหว่างเครื่องคอมพิวเตอร์ อย่างการถ่ายโอนไฟล์ระหว่าง ไคลเอนต์ (client) กับเครื่องคอมพิวเตอร์ที่เป็นแม่ข่าย เรียกว่า โฮสติง (hosting) หรือ เซิร์ฟเวอร์ ซึ่งทำให้การถ่ายโอนไฟล์ง่ายและปลอดภัยในการแลกเปลี่ยนไฟล์ผ่านอินเตอร์เน็ต การใช้ FTP ที่พบบ่อยสุด ก็เช่น การดาวน์โหลดไฟล์จากอินเทอร์เน็ต ความสามารถในการถ่ายโอนไฟล์ ทำให้ FTP เป็นสิ่งจำเป็นสำหรับทุกคนที่สร้างเว็บเพจ ทั้งมือสมัครเล่นและมืออาชีพ โดยที่การติดต่อกันทาง FTP เราจะต้องติดต่อกันทาง Port 21 ซึ่งก่อนที่จะเข้าใช้งานได้นั้น จะต้องเป็นสมาชิกและมีชื่อผู้เข้าใช้ (User) และ รหัสผู้เข้าใช้ (password) ก่อน และโปรแกรมสำหรับติดต่อกับแม่ข่าย (server) ส่วนมากจะใช้โปรแกรมสำเร็จรูป เช่น โปรแกรม Filezilla,CuteFTP หรือ WSFTP ในการติดต่อ เป็นต้น

FTP (File Transfer Protocol) แบ่งเป็น 2 ส่วน

1. FTP server เป็นโปรแกรมที่ถูกติดตั้งไว้ที่เครื่องเซิฟเวอร์ ทำหน้าที่ให้บริการ FTP หากมีการเชื่อมต่อจากไคลแอนเข้าไป

2. FTP client เป็นโปรแกรม FTP ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของ user ทั่วๆไป ทำหน้าที่เชื่อมต่อไปยัง FTP server และทำการอัพโหลด, ดาวน์โหลดไฟล์ หรือ จะสั่งแก้ไขชื่อไฟล์, ลบไฟล์ และเคลื่อนย้ายไฟล์ก็ได้เช่นกัน

2.1.3 MYSQLi (MySQL Improved) ส่วนขยายมากจากฐานข้อมูล MySQL โดยถ้ากล่าวอย่างง่าย MySQLi คือ MySQL เวอร์ชั่นใหม่ที่มีคุณสมบัติต่าง ๆ มากขึ้น และมีประสิทธิภาพมากยิ่งขึ้นการเลือกใช้ MySQLi ไม่มีผลต่อการ Query ของโปรแกรมเมอร์ หรือว่าการเข้าไปใน PhpMyAdmin แต่อย่างใด และในรีวิวของต่างประเทศ ก็มีการพูดถึงเรื่อง Security ที่เพิ่มขึ้นของ MySQLi ด้วยเช่นกัน ส่วนที่โดดเด่นขึ้นมาจากเดิมของ MySQLi ก็คือในเรื่องของการเรียกใช้คำสั่งในรูปแบบของ OOP

คุณสมบัติของ MySQLi (MySQL Improved)

- เป็นแบบ object-oriented
- สนับสนุนคำสั่ง prepared (ป้องกัน SQL Injection)
- สนับสนุนหลายคำสั่งพร้อมกัน (multiple statements)
- สนับสนุนคำสั่ง transactions
- เพิ่มเติมการสนับสนุน debugging
- เพิ่มเติมการสนับสนุนบน Server ต่าง ๆ โดยมีการใช้งานคำสั่งดังนี้

$conn = new mysqli($servername, $username, $password, $dbname) คือ คำสั่งที่ใช่สร้างการเชื่อมต่อไปยังฐานข้อมูล

$conn->connect_error คือ คำสั่งที่ใช้สำหรับการตรวจสอบการเชื่อม

$conn->query() คือ คำสั่งที่ใช้สำหรับดึงข้อมูลตามคำสั่งภาษา SQL

Update ตัวอย่างคำสั่ง

- UPDATE table_name
- SET column1 = value1, column2 = value2, ...
- WHERE condition;

Insert ตัวอย่างคำสั่ง

- INSERT INTO table_name (column1, column2, column3, ...)
- VALUES (value1, value2, value3, ...);

Delete ตัวอย่างคำสั่ง

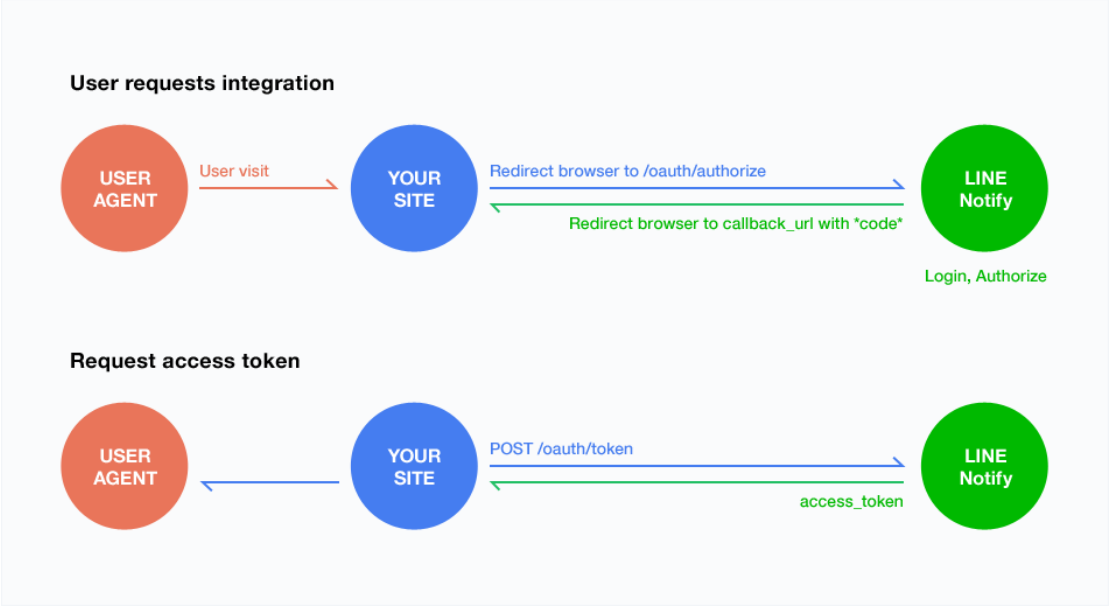
- DELETE FROM table_name
- WHERE condition;

2.1.4 Bootstrap คือ Front-end Framework ตัวหนึ่ง ที่จะช่วยให้การพัฒนาเว็บไซต์ของเราเร็วขึ้น ง่ายขึ้น และเป็นระบบมากขึ้น ซึ่งคำว่า Bootstrap นี้ในภาษาอังกฤษมันมักจะหมายถึง “สิ่งที่ช่วยทำให้ง่ายขึ้น” หรือ “สิ่งที่ทำได้ด้วยตัวของมันเอง” ซึ่งในที่นี้น่าจะหมายความว่า ถ้าเราใช้ Bootstrap แล้ว เราก็ไม่จำเป็นต้องไปหาอะไรมาเพิ่มอีก

รูปที่ 2.1 Bootstrap

จากรูปที่ 2.1 Bootstrap คือ Frontend Framework ที่รวม HTML, CSS และ JS เข้าด้วยกันสำหรับพัฒนา Web ที่รองรับทุก Smart Device หรือ เรียกว่า Responsive Web หรือ Mobile First

2.1.5 Line notify คือ บริการที่คุณสามารถได้รับข้อความแจ้งเตือนจากเว็บเซอร์วิสต่าง ๆ ที่คุณสนใจได้ทาง LINE โดยหลังเสร็จสิ้นการเชื่อมต่อกับทางเว็บเซอร์วิสแล้ว คุณจะได้รับการแจ้งเตือนจากบัญชีทางการของ “LINE Notify” ซึ่งให้บริการโดย LINE นั่นเอง คุณสามารถเชื่อมต่อกับบริการที่หลากหลาย และยังสามารถรับการแจ้งเตือนทางกลุ่มได้อีกด้วย ซึ่งบริการหลักๆ ที่สามารถเชื่อมต่อได้แก่ GitHub, IFTTT หรือ Mackerel เป็นต้น



รูปที่ 2.2 การทำงานระบบ LINE Notify

จากรูปที่ 2.2 เป็นทำงานของระบบ LINE Notify มี 2 ขั้นตอน ดังนี้

1. เป็นการขอสิทธิ์ใช้บริการจาก LINE(ไลน์) เพื่อให้เข้าถึงระบบการทำงานผ่านอินเทอร์เฟสของไลน์เพื่อเป็นช่องทางให้ไลน์ส่งแจ้งเตือนได้

2. เป็นการขอ Token เพื่อระบุตัวตนผู้ใช้ระบบไลน์ให้สามารถส่งข้อมูลไปยังผู้ใช้ได้อย่างถูกต้อง

2.1.6 LINE

รูปที่ 2.3 โปรแกรม LINE

จากรูปที่ 2.3 โปรแกรม LINE คือ แอพพลิเคชั่นที่ผสมผสานบริการ Messaging และ Voice Over IP นำมาผนวกเข้าด้วยกัน จึงทำให้เกิดเป็นแอพพลิชั่นที่สามารถแชท สร้างกลุ่ม ส่งข้อความ โพสต์รูปต่างๆ หรือจะโทรคุยกันแบบเสียงก็ได้ โดยข้อมูลทั้งหมดไม่ต้องเสียเงิน สามารถใช้งานโทรศัพท์ที่มีแพคเกจอินเทอร์เน็ตอยู่แล้ว แถมยังสามารถใช้งานร่วมกันระหว่าง iOS และ Android รวมทั้งระบบปฏิบัติการอื่น ๆ ได้อีกด้วย การทำงานของ LINE นั้น มีลักษณะคล้าย ๆ กับ WhatsApp ที่ต้องใช้เบอร์โทรศัพท์เพื่อยืนยันการใช้งาน แต่ LINE ได้เพิ่มลูกเล่นอื่นๆ เข้ามา ทำให้ LINE มีจุดเด่นที่เหนือกว่า WhatsApp และโปรแกรมอื่น มีส่วนเสริมที่สามารถนำมาพัฒนาใช้ประโยชน์ต่อยอด เช่น Line notify เป็นต้น

2.2 พื้นฐานและทฤษฎีที่เกี่ยวข้องกับการ Backup

Backup คือ การสำรองข้อมูล เป็นการคัดลอกแฟ้มข้อมูลเพื่อทำสำเนา เพื่อหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย โดยสามารถนำข้อมูลที่สำรองไว้มาใช้งานได้ทันที ลักษณะการสำรองข้อมูล

1. Backup ข้อมูลไปยัง Storage ภายนอก ที่เครื่องแม่ข่ายหรือลูกข่ายไม่สามารถเข้าถึงข้อมูลได้เองโดยตรงแบบ Volume หรือ Folder การสำรองข้อมูลไปยัง Volume ที่ทำการ Mount จาก NAS หรือ File Sharing Server มาเป็นลักษณะ Folder หรือการ Mount iSCSI/FC มาเป็น Volume สำหรับทำการสำรองข้อมูลนั้น ไม่สามารถป้องกัน Ransomware ได้เลย เพราะหากเครื่องลูกข่ายหรือแม่ข่ายของคุณเกิดติด Ransomware ขึ้นมาจริงๆ ไฟล์ที่เครื่องนั้นๆ มองเห็นทั้งหมดก็จะถูกทำการเข้ารหัสไปด้วย ซึ่งก็จะรวมถึงไฟล์ที่ถูกบันทึกอยู่ใน NAS, File Sharing Server และ SAN Storage ด้วยเช่นกัน

แนวทางที่ปลอดภัยจาก Ransomware มากกว่านั้น ก็คือการสำรองข้อมูลไปยัง Volume ปลายทางผ่านทาง API, การเรียกใช้ Object Storage หรือบริการต่างๆ บน Backup Software โดยเฉพาะ ซึ่งไม่ได้มีการเปิดให้เครื่องแม่ข่ายหรือลูกข่ายเข้าถึงไฟล์เหล่านั้นได้ในลักษณะ Folder หรือ Volume นั่นเอง เพราะ Ransomware จะไม่สามารถโจมตีไปถึงไฟล์เหล่านั้นได้ ทำให้ข้อมูลที่สำรองเอาไว้ของเรายังคงปลอดภัยอยู่เสมอ

2. Backup ข้อมูลให้บ่อย เมื่อถูก Ransomware โจมตีจะได้ไม่เสียข้อมูลไปเยอะสำหรับนโยบายการสำรองข้อมูลในสมัยนี้ อาจต้องมีการสำรองข้อมูลให้ถี่ขึ้นซักนิด โดยอาจจะทำการสำรองข้อมูลรายวัน หรือถี่กว่านั้นสำหรับระบบที่มีความสำคัญสูง เนื่องจากหากเกิดเหตุการณ์ที่ Ransomware โจมตีและเข้ารหัสจริงๆ ความสูญเสียที่จะเกิดขึ้นกับไฟล์ที่เรายังไม่ได้สำรองข้อมูลจะได้มีน้อยที่สุด และกู้คืนข้อมูลย้อนหลังกลับมาได้มากที่สุดเท่าที่จะเป็นไปได้นั่นเอง ซึ่งการสำรองข้อมูลบ่อยๆ ในสมัยนี้ที่มักใช้การทำ Incremental Backup นั้นก็ไม่ได้ทำให้กินพื้นที่บนระบบจัดเก็บข้อมูลสำรองแต่อย่างใด อีกทั้งยังลดโอกาสที่จะเกิดเหตุการณ์ Traffic Spike ในระบบเครือข่ายได้อีกด้วย

3. ทำ Snapshot สำหรับข้อมูลใน Backup Storage และ Virtual Machine เพื่อเป็นการป้องกันอีกชั้น การทำ Snapshot บน Backup Storage โดยตรงเองก็เป็นทางเลือกที่ดี อีกทั้งสำหรับองค์กรที่ไม่ได้มีระบบ Backup Storage แบบอื่นๆ นอกจาก NAS หรือ SAN นั้น หากระบบ Storage เหล่านั้นสามารถทำ Snapshot จัดเก็บเอาไว้ในพื้นที่ซึ่งเครื่องลูกข่ายหรือแม่ข่ายที่มาเชื่อมต่อใช้งานไม่สามารถเข้าถึงได้ ก็จะทำให้สามารถย้อนข้อมูลกลับไปยัง Snapshot ใดๆ ก่อนที่ข้อมูลจะถูก Ransomware ทำการเข้ารหัสไปได้ เป็นวิธีการป้องกัน Ransomware ขั้นพื้นฐานสำหรับเหล่า Shared Storage นั่นเอง ทั้งนี้เทคนิคนี้ก็สามารถนำไปประยุกต์ใช้กับ Virtual Machine (VM) ทั้งบนระบบ Virtualization และ Cloud ได้ด้วยเช่นกัน เพราะการทำ Snapshot ในระดับ VM นั้นก็จะทำให้เราย้อน VM นั้นๆ กลับไปสภาพก่อนที่จะถูกโจมตีได้ แต่ก็ต้องจัดการอุดช่องโหว่ที่ Ransomware เหล่านั้นใช้โจมตีมาให้เรียบร้อยก่อนที่จะถูกโจมตีซ้ำสองด้วย

4. ปกป้อง Backup Storage จากการถูก Ransomware โจมตีเองโดยตรงด้วย เป็นอีกประเด็นหนึ่งที่มักถูกมองข้ามกัน กับการที่เหล่า Backup Storage ไม่ว่าจะเป็น Windows File Sharing, Linux NAS Storage หรือ Software-defined Storage ค่ายต่างๆ นั้นถูก Ransomware ทำการเจาะช่องโหว่เข้าไปเข้ารหัสไฟล์ที่ถูกจัดเก็บอยู่บน Backup Storage ด้วย ทำให้ระบบงานอื่นๆ ที่ทำการสำรองข้อมูลมายัง Backup Storage เหล่านี้ไม่สามารถกู้คืนไฟล์ใดๆ ได้ และตกเป็นเหยื่อของ Ransomware ต่อไป

การรักษาความมั่นของปลอดภัยให้กับ Backup Storage นั้นทำได้หลายวิธี ไม่ว่าจะเป็นการหมั่น Patch อุดช่องโหว่ด้านความมั่นคงปลอดภัยต่างๆ, การกำหนด Firewall Rule ให้อุปกรณ์อื่นๆ สามารถเข้าถึง Backup Storage ได้เฉพาะจาก Protocol และ IP Address ที่จำเป็น, การติดตั้งระบบ Antivirus/Anti-malware และอื่นๆ เพื่อเสริมความมั่นคงปลอดภัยเพิ่มเติม และอื่นๆ อีกมากมาย เรียกได้ว่าทุกแนวทางที่ใช้ในการรักษาความมั่นคงปลอดภัยให้กับ Server นั้น ก็สามารถนำมาประยุกต์ใช้กับ Backup Storage ได้แทบทั้งหมดเลยก็ไม่ผิดนัก และเป็นสิ่งที่สมควรทำเป็นอย่างยิ่งด้วย

5. มีระบบวิเคราะห์ข้อมูลและตรวจสอบย้อนหลังกับความผิดปกติที่เกิดขึ้นกับข้อมูลที่ Backup เอาไว้ได้และการหมั่นตรวจสอบการทำงานของระบบสำรองข้อมูล และวิเคราะห์เหตุการณ์ต่างๆ ที่เกิดขึ้นกับระบบ Backup ทั้งหมดให้ได้อย่างต่อเนื่องนั้นก็ถือเป็นอีกประเด็นสำคัญ โดยปัจจุบันนี้เทคโนโลยี Backup นั้นเริ่มมีเทคโนโลยีตรวจจับ Ransomware ได้แล้วในตัว อีกทั้งในระบบที่ทำการสำรองข้อมูลแบบ Incremental Backup เองนั้น หากมีการสำรองข้อมูลที่ถูกเข้ารหัสไป ปริมาณข้อมูลที่ต้องสำรองนั้นก็จะเพิ่มขึ้นอย่างผิดสังเกตอยู่แล้ว ประเด็นต่างๆ เหล่านี้เองที่เหล่าผู้ดูแลระบบสามารถนำมาใช้เพื่อเป็นส่วนหนึ่งในการวิเคราะห์และค้นหาปัญหาต่างๆ ที่เกิดขึ้นในรายวันได้อย่างน่าสนใจ

ประโยชน์ของการสำรองข้อมูล ดังนี้

1. เพื่อป้องกันทั้งการ ลบ หรือ ทำข้อมูลสูญหาย ทั้งที่ตั้งใจและไม่ตั้งใจ

2. กู้ข้อมูลเก่า เพราะการแก้ไขข้อมูลปัจจุบันอาจทำให้มีปัญหา หรือไฟล์ที่มีใช้งานไม่ได้ ต้องการกลับไปใช้ต้นฉบับก่อนหน้านี้

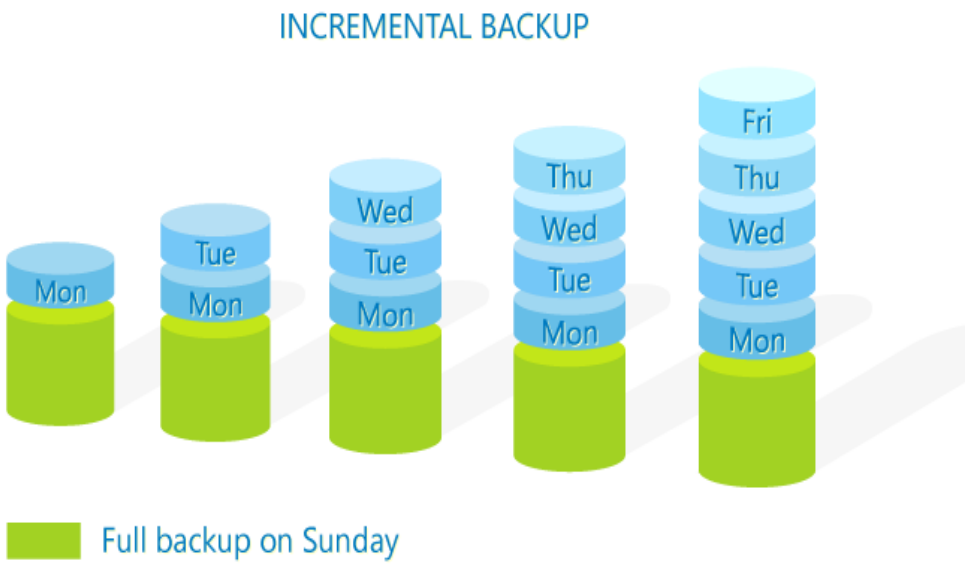
3. ป้องกัน อุปกรณ์เก็บข้อมูลเสียหาย หรือ โดนขโมย หากอุปกรณ์สำหรับเก็บข้อมูลหายไป เราก็สามารถใช้ข้อมูลที่เราสำรองไว้จากอุปกรณ์เก็บข้อมูลตัวอื่นแทนได้

ปัจจัยที่ทำให้การสำรองข้อมูลสำคัญ ดังนี้

- อุปกรณ์เสียหาย
- ถูกไวรัสโจมตี
- ตกเป็นเป้าประสงค์ร้ายจากHackerหรือผู้ไม่หวังดี
- เกิดความผิดพลาดของซอฟต์แวร์ในระดับVolumeและDirectory
- เกิดความผิดพลาดในการส่งข้อมูล
- ปัญหาจากระบบไฟฟ้า
- การถูกขโมยอุปกรณ์หรือข้อมูล
- ภัยจากไฟหรือน้ำ
- เกิดความผิดพลาดจากผู้ใช้งานหรือผู้อื่น

2.2.1 Unstructured หรือ Full เป็นแบบง่ายๆ คือการ copy ไว้หลายๆ ชุด แต่มีข้อควรต้องระวังว่าไฟล์ไหนเป็นไฟล์ล่าสุด ต้องจัดระเบียบให้ดี เดี๋ยวไป merge/replace ทับไฟล์เดิม การทำแบบนี้จะได้ไฟล์ตามชุดข้อมูลที่ต้องการเป็นหลัก ส่วนใหญ่นิยมใช้การสำรองข้อมูลแบบนี้เพราะง่ายต่อการจัดการไม่ต้องใช้ซอฟต์แวร์พิเศษให้ยุ่งยากสามารถทำการ copy/paste ข้อมูลไปยังที่เก็บข้อมูลได้ทันที

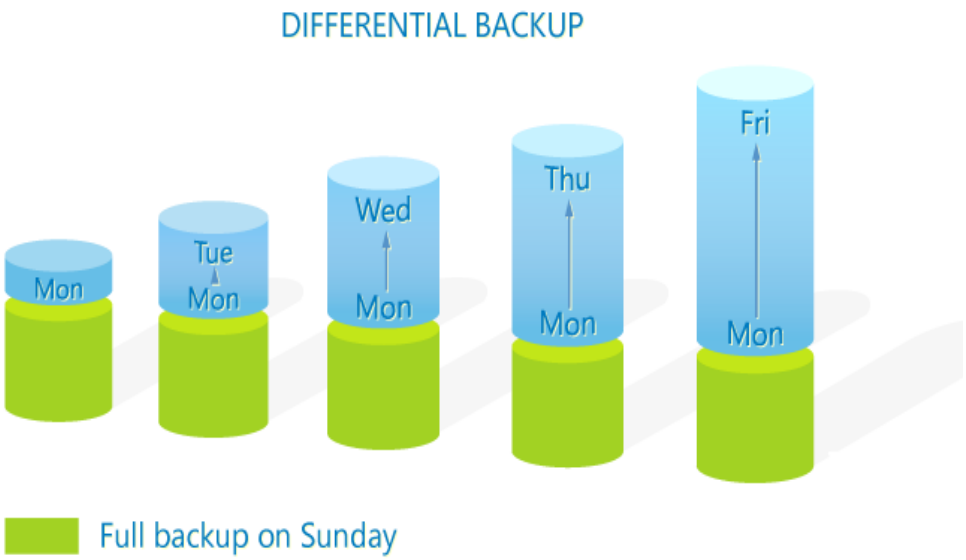
2.2.2 Full and Incrementals



รูปที่ 2.4 Full and Incremental

จากรูปที่ 2.4 backup Incremental การการทำงานคล้าย Unstructured แต่มีซอฟต์แวร์มาช่วยจัดการให้ โดยจะมีการทำ copy ข้อมูลไว้เป็นไฟล์ๆ ตามรูปแบบของแต่ละซอฟต์แวร์จัดการ อาจจะเป็นไฟล์เดียวหรือแบ่งย่อยเป็นหลายไฟล์ก็ได้เมื่อมีการสำรองข้อมูลครั้งต่อไปก็จะตรวจสอบเฉพาะไฟล์ที่มีการเปลี่ยนแปลงหรือถูกลบออกไปล่าสุดจากการสำรองข้อมูลครั้งก่อนหน้าแล้วทำการ mark/update เพื่อ Backup ไว้เป็นวันและเวลานั้นๆ ไปเรื่อย ๆ ต่อเป็นลูกโซ่ ซึ่งช่วยประหยัดพื้นที่ในการจัดเก็บได้มาก ถ้ามีการสำรองข้อมูลทุกวันแต่ไฟล์ที่ได้จากการ Backup แบบนี้มันเพิ่มขึ้นมาเรื่อยๆ เวลาจัดเก็บไฟล์พวกนี้ต้องอยู่ครบทุกไฟล์ ต้องระวังสักนิดและแนะนำว่าให้ครั้งละไม่มาก เพราะการเชื่อมไฟล์ Backup แบบนี้ ยิ่งเยอะยิ่งช้าและอ่านนานมาก ปรกติไม่ควรเกิน 14 ไฟล์ หรือขนาดไม่ใหญ่เกินไป สัก 100GB – 150GB กำลังพอไหว แต่ขึ้นอยู่กับซอฟต์แวร์และเครื่องที่เปิดไฟล์ Backup พวกนี้ด้วยว่าเปิดไหวไหมด้วย ตรงนี้ต้องระวังว่าซอฟต์แวร์ที่เราใช้มีเสถียรภาพในการรองรับจำนวนและขนาดไฟล์เท่าใด

2.2.3 Full and Differential



รูปที่ 2.5 Full and Differential

จากรูปที่ 2.5 การทำงานคล้าย Full and Incremental ต่างกันเล็กน้อยตรงที่ เมื่อมีการสำรองข้อมูลครั้งต่อไปก็จะตรวจสอบเฉพาะไฟล์ที่มีการเปลี่ยนแปลงหรือถูกลบออกไปล่าสุดจากการ Backup ตัว Full แล้วทำการ mark/update เพื่อ Backup ไว้เป็นวันและเวลานั้นๆ ไปเรื่อยๆ เวลากู้คืนกลับมาใช้ไฟล์ Full และตัวไฟล์ที่ Backup ตัวล่าสุด แค่ 2 ส่วนก็กู้คืนได้เร็ว การอ่านและเขียนไฟล์ก็เร็วกว่า รวมไปถึงความเสี่ยงต่อการสูญหายของไฟล์แต่ละส่วนก็น้อยกว่า แต่เสียพื้นที่เยอะกว่าแบบข้อที่ Full and Incrementals มาก

อุปกรณ์ที่ใช้สำหรับเก็บข้อมูลสำหรับการแบคอัพมีหลายประเภท เช่น เทป, CD/DVD, สตอเรจแบบภายนอก (External Storage) เป็นต้น ซึ่งสตอเรจโดยทั่วไปมีให้เลือกแบบทั้งที่เป็น DAS (Direct Attached Storage), NAS (Network Attached Storage), SAN (Storage Area Network) ขึ้นอยู่กับขนาดธุรกิจและสภาพแวดล้อมของระบบไอที

2.3 พื้นฐานและทฤษฎีที่เกี่ยวข้องกับการ Recory

Recovery คือการกู้คืนระบบให้กลับคืนมาทำงานได้อย่างปกติ ภายหลังที่เกิดวิตกฤตการณ์อย่างหนึ่งอย่างใดที่ทำให้ระบบไม่สามารถทำงานได้ตามปกติ สำหรับองค์กรที่ระบบ IT มีความสำคัญอย่างยิ่งยวด และต้องให้บริการอย่างต่อเนื่องไม่สามารถหยุดได้

การพิจารณาถึงความสำคัญของระบบที่ใช้สำหรับการดำเนินธุรกิจ องค์กรโดยทั่วไปจะกำหนด Service Level Agreement (SLA) ของแอพลิเคชั่นหลักๆ ซึ่งสามารถนำมาพิจารณากำหนดค่า RTO และ RPO เพื่อเลือกโซลูชั่น Backup & DR ที่เหมาะสมกับ SLA ที่ต้องการ

1. Recovery Time Objective (RTO) หมายถึงระยะเวลาที่ยอมรับได้ในการกู้คืนระบบให้ทำงานได้ตามปกติ หลังจากที่เกิดเหตุฉุกเฉินขึ้น ตัวอย่างเช่น ถ้าองค์กรกำหนดค่า RTO = 1 ชั่วโมง ก็จะหมายความว่า ระบบจะต้องถูกกู้คืนมาได้ภายในหนึ่งชั่วโมง

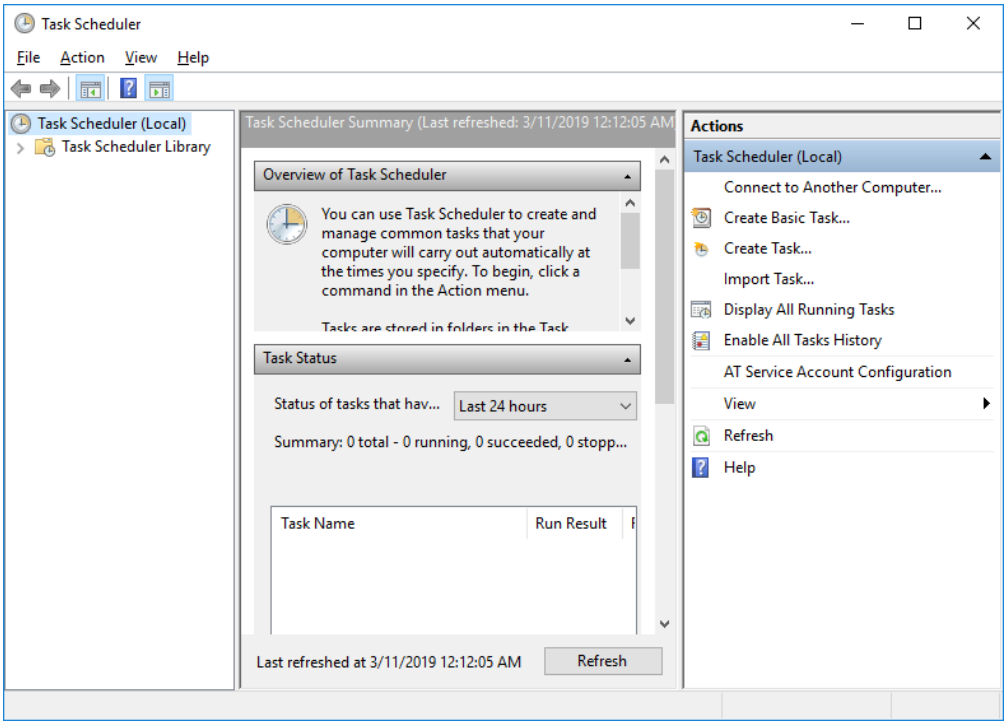
2. Recovery Point Objective (RPO) หมายถึง ปริมาณข้อมูลสูญหายในช่วงเวลาหนึ่งที่องค์กรยอมรับได้ (Acceptable Loss) ในกรณีที่เกิดเหตุฉุกเฉินขึ้น ตัวอย่างเช่น ถ้าองค์กรกำหนดค่า RPO = 2 ชั่วโมง ก็จะหมายความว่า องค์กรสามารถยอมรับได้ในกรณีที่ข้อมูลสูญหายไม่เกิน 2 ชั่วโมง ซึ่งถ้าหากทำการแบ็กอัพระบบเอาไว้ ณ เวลา 13.00 น. แต่เมื่อเวลา 14.50 น. เกิดเหตุขัดข้องกับระบบ ดังนั้นข้อมูลล่าสุดที่เราสามารถกู้คืนได้ก็คือข้อมูล ณ เวลา 13.00 น. ก็ยังถือว่าอยู่ในเวลาที่กำหนดไว้ตาม RPO คือไม่เกิน 2 ชั่วโมง เป็นต้น

2.4 ซอร์ฟแวร์ที่ใช้

รูปที่ 2.6 โปรแกรม 7zip

จากรูปที่ 2.6 **โปรแกรม 7zip** เป็นโปรแกรมในการบีบอัดไฟล์ (Compressed) ทำให้ไฟล์มีขนาดเล็กลง หรือสามารถบีบอัด ไฟล์หลาย ๆ ไฟล์เข้าเป็นไฟล์เดียว เพื่อสะดวกในการคัดลอกลงในอุปกรณ์เก็บข้อมูล หรือส่ง E-Mail โปรแกรมนี้มีหลักการทำงานเช่นเดียวกันกับโปรแกรมบีบอัดไฟล์ตามท้องตลาด คือ WinZIP และ WinRAR โปรแกรม 7-Zip เป็น Freeware สามารถทำงานกับไฟล์ สามารถใช้ฟังก์ชันบีบอัด (Add) และแตกไฟล์ (Extract) ไฟล์นามสกุล: **7z, ZIP, GZIP, BZIP2 และ TAR** ใช้ฟังก์ชันแตกไฟล์ (Extract) ได้อย่างเดียว (ไม่สามารถบีบไฟล์นามสกุลเหล่านี้ได้) กับไฟล์นามสกุล: **RAR, CAB, ISO,** ARJ, LZH, CHM, Z, CPIO, RPM, DEB และ NSIS
และสามารถใช้งานผ่าน command line มีคำสั่งดังนี้

ลำดับ	Switch	Description
1	--	Stop switches parsing
2	-ad	Show dialog box in GUI version (7zg)
3	-ai	Include archive filenames
4	-an	Disable parsing of archive_name
5	-ao	Overwrite mode
6	-ax	Exclude archive filenames
7	-bb[0-3]	Set output log level
8	-bd	Disable progress indicator
9	-bs{o|e|p}{0|1|2}	Set output stream for output/error/progress
10	-bt	Show execution time statistics
11	-i	Include filenames
12	-m	Set Compression Method
13	-o	Set Output directory
14	-p	Set Password
15	-r	Recurse subdirectories
16	-sa	Set Archive name mode
17	-scc	Set charset for for console input/output
18	-scrc	Set hash function
19	-scs	Set charset for list files
20	-sdel	Delete files after including to archive
21	-seml	Send archive by email
22	-sfx	Create SFX archive
23	-si	Read data from StdIn
24	-slp	Set Large Pages mode
25	-slt	Show technical information
26	-sni	Store NT security information
27	-sns	Store NTFS alternate Streams
28	-snc	Extract file as alternate stream, if there is ':' character in name
29	-snr	Replace ':' character to '_' character in paths of alternate streams



รูปที่ 2.7 โปรแกรม Task Scheduler

จากรูปที่ 2.7 โปรแกรม Task Scheduler บนระบบปฏิบัติการวินโดว์ Task Scheduler เป็นโปรแกรมที่มีอยู่ใน Windows ทำหน้าที่ตั้งเวลา การทำงานต่าง ๆ ซึ่งเหมือนโปรแกรมที่มีบนระบบปฏิบัติ Linux ก็คือ Cron tab หรือ Cron Jobs ที่ค่อยสั่งโปรแกรมทำงานอัตโนมัติ ตามวันเวลาที่กำหนด ในทุก ๆ วันซึ่งสามารถใช้ Task Scheduler ในการทำงาน เราสามารถเปิด Task Scheduler ได้โดยการ พิมพ์ ที่ start menu คำว่า Task Sc หรือ Scheduler