บทที่ ๓
จัดการไวรัสคอมพิวเตอร์

ดังที่ทราบแล้วว่า ไวรัสคอมพิวเตอร์เป็นโปรแกรมชนิดหนึ่งที่ผู้สร้าง ทำขึ้นมาเพื่อประสงค์ร้ายต่อคอมพิวเตอร์ส่วนบุคคล หรือระบบเครือข่ายคอมพิวเตอร์ ดังนั้นเราก็จัดการลบไฟล์ไวรัสคอมพิวเตอร์ทิ้ง หรือลบที่ซ่อนของไวรัสคอมพิวเตอร์ทิ้งไป ไวรัสคอมพิวเตอร์ก็จะทำอะไรไม่ได้

แต่ตามที่ได้กล่าวมาในบทก่อนหน้าแล้วว่าไวรัสคอมพิวเตอร์นั้น ผู้อ่านจะมองไม่เห็นในขณะที่อยู่ในระบบปฏิบัติการวินโดวส์ หรือลบไม่ได้ในขณะที่อยู่ในระบบปฏิบัติการวินโดวส์ ดังนั้นเทคนิคในการจะลบของเราก็คือเราจะใช้ระบบปฏิบัติการอูบุนตู (Ubuntu) มาใช้ในการลบ ทั้งนี้อันเนื่องมาจากระบบปฏิบัติการอูบุนตู มีแพลตฟอร์มต่างกับระบบปฏิบัติการวินโดวส์ และระบบปฏิบัติการอูบุนตูสามารถมองเห็นทุกไฟล์และโฟลเดอร์ของระบบปฏิบัติการวินโดวส์ทั้งหมด อีกทั้งยังสามารถลบไฟล์และโฟลเดอร์ต่างๆ ของระบบปฏิบัติการวินโดวส์ทั้งหมดได้

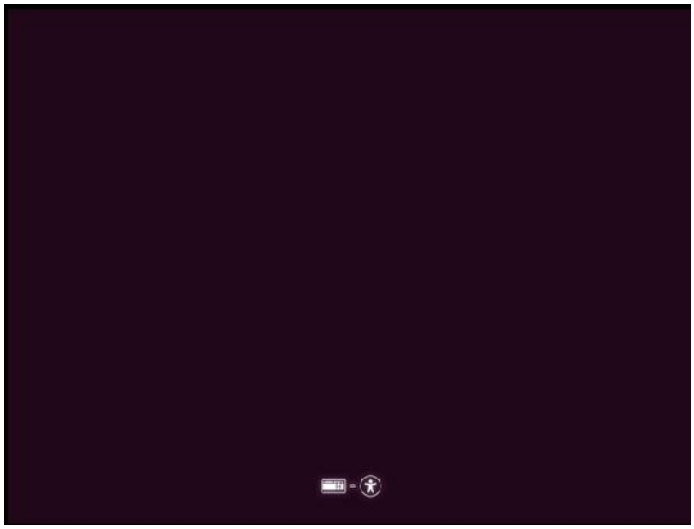
๑. ระบบปฏิบัติการอูบุนตู (Ubuntu)

อูบุนตู เป็นระบบปฏิบัติการคอมพิวเตอร์ที่เป็นระบบปฏิบัติการแบบเปิด ซึ่งมีพื้นฐานบนลีนุกซ์ดิสทรีบิวชัน ที่พัฒนาต่อมาจากเดเบียน การพัฒนาสนับสนุนโดยบริษัท Canonical Ltd. ซึ่งเป็นบริษัทของ นายมาร์ก ชัทเทิลเวิร์ธ ชื่อ Ubuntu มีความหมายในภาษาอังกฤษ คือ “humanity towards others” มาจากคำในภาษาซูลู และภาษาโคซา (ภาษาในแอฟริกาใต้) อูบุนตูออกรุ่นใหม่ทุก ๖ เดือน ในขณะที่ผู้เขียน เขียนหนังสือเล่มนี้ออกรุ่น ๑๔.๑๐ มาแล้ว ผู้อ่านสามารถดาวน์โหลดโปรแกรมได้ที่ www.ubuntu.com แล้วคลิกที่ Download Ubuntu แล้วเลือกคลิกที่ Download Ubuntu Desktop แล้วเลือกสิ่งที่ต้องการ นำไฟล์ที่ได้ซึ่งเป็นไฟล์ iso มาทำการเขียนเป็นแผ่น DVD สำหรับใช้ในการบูตเครื่องคอมพิวเตอร์

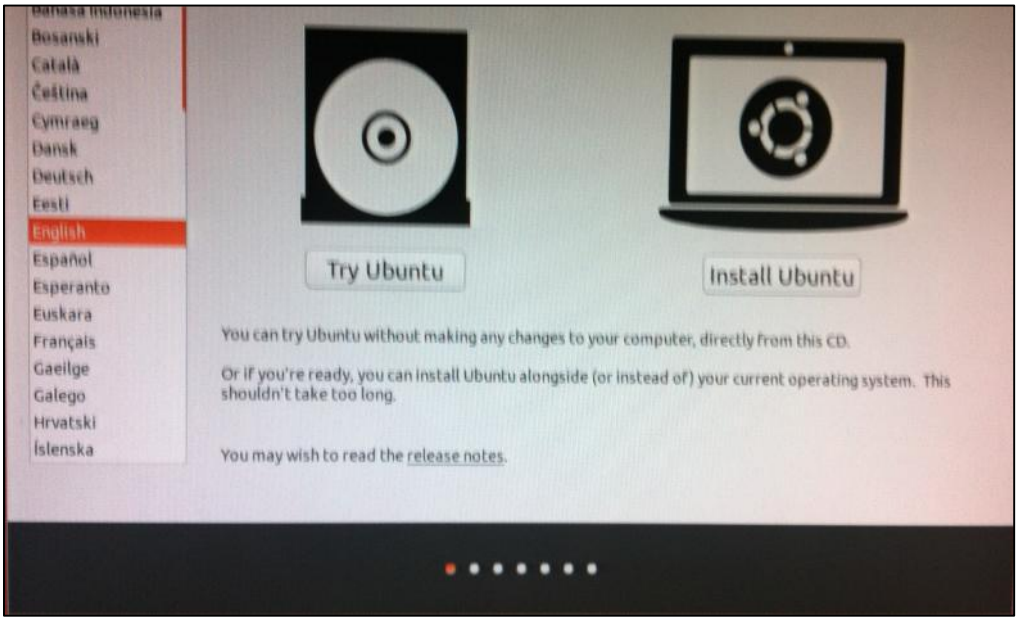
ทำไมต้องพูดถึงระบบปฏิบัติการอูบุนตู ก็เพราะเราจะใช้อูบุนตูในการบูตเครื่องคอมพิวเตอร์ด้วยแผ่นระบบปฏิบัติการอูบุนตู หลังจากนั้นเราก็จะสามารถดูไฟล์และโฟลเดอร์ต่างๆ ในเครื่องคอมพิวเตอร์ได้ และทีนี้เราจะจัดการ ค้นหาและลบไฟล์หรือโฟลเดอร์ที่เป็นไวรัสคอมพิวเตอร์ หรือสงสัยว่าน่าจะเป็นที่อยู่ของไวรัสคอมพิวเตอร์ได้

๒. การจัดการไวรัสคอมพิวเตอร์

เมื่อเราได้แผ่นบูตอูบุนตูแล้ว การที่จะจัดการกับไวรัสคอมพิวเตอร์ในเครื่องคอมพิวเตอร์ใดๆ เราต้องทำการให้เครื่องคอมพิวเตอร์เครื่องนั้นสามารถบูตจากแผ่น DVD เป็นอันดับแรกก่อน เมื่อใส่แผ่นอูบุนตูเข้าไปและคอมพิวเตอร์บูตระบบปฏิบัติการอูบุนตู (ผู้เขียนใช้ Ubuntu ๑๔.๑๐) ขึ้นมาจะได้ตามรูป ๓.๑ ก่อน หลังจากนั้นรอจนถึงหน้าต่าง Welcome ตามรูป ๓.๒ ให้เลือกระหว่างทดลองอูบุนตู (Try Ubuntu) กับลงระบบปฏิบัติการอูบุนตูไปในเครื่อง (Install Ubuntu)

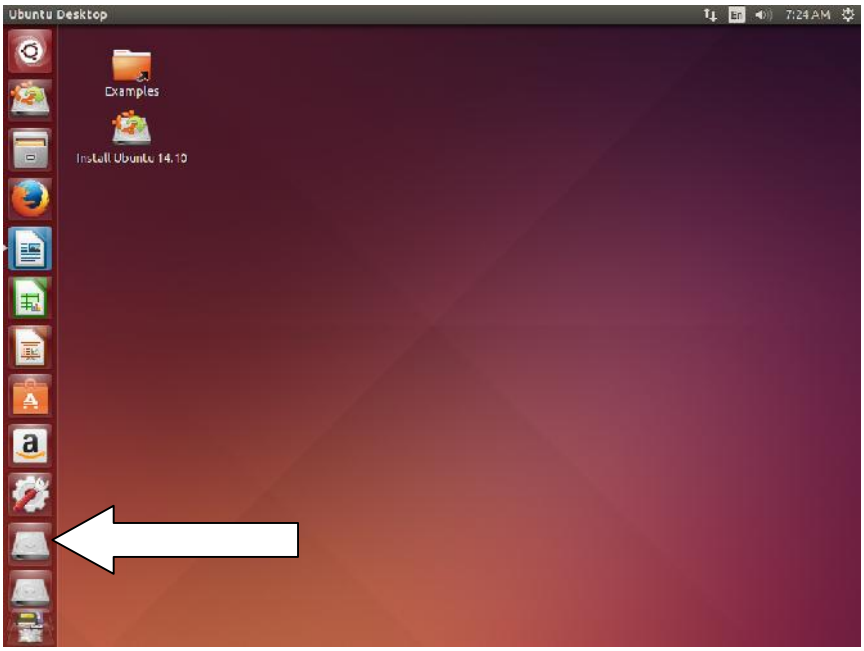


รูป ๓.๑ หน้าต่างบูตระบบปฏิบัติการอูบุนตู ๑๔.๑๐



รูป ๓.๒ หน้าต่าง Welcome ให้เลือกระหว่างทดลองอูบุนตูกับติดตั้งลงเครื่อง

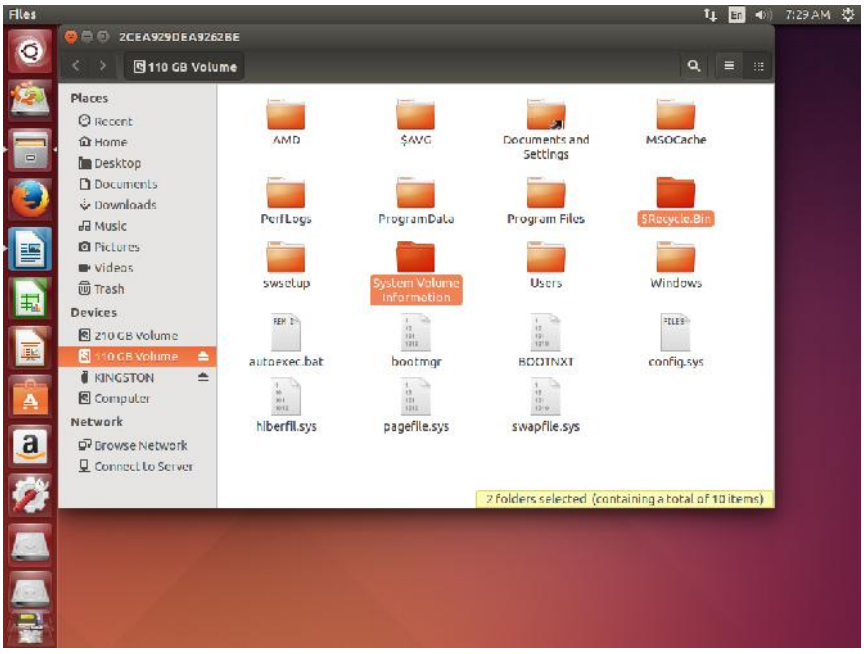
ให้เราเลือกทดลองอูบุนตู (Try Ubuntu) ระบบปฏิบัติการอูบุนตู ก็จะใช้อูบุนตูจากแผ่น DVD นั้น จนได้หน้าจอของระบบปฏิบัติการอูบุนตู ๑๔.๑๐ ตามรูป ๓.๓ (หรือถ้าผู้อ่านมีอูบุนตูก่อนหน้าก็สามารถนำมาใช้ได้ เช่น อูบุนตู ๑๑.๐๔ , อูบุนตู ๑๒.๑๐ หรือ อูบุนตู ๑๓.๐๔ ก็ได้ แต่หน้าจอ Desktop ที่ได้ก็จะแตกต่างออกไปบ้าง)



รูป ๓.๓ หน้าต่าง Desktop ของอูบุนตู ๑๔.๑๐

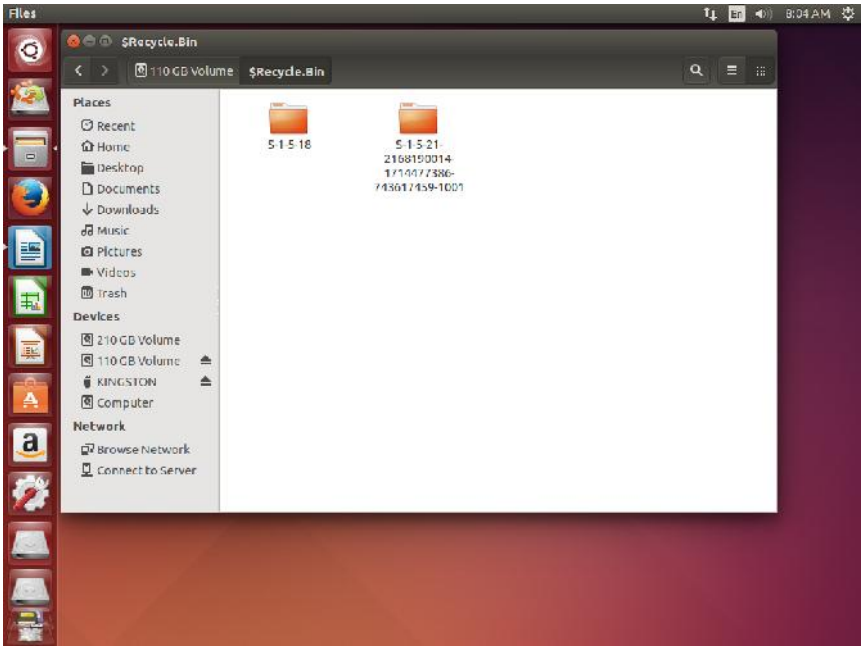
เมื่อบูตระบบปฏิบัติการอูบุนตู ๑๔.๑๐ ได้ตามรูป ๓.๓ แล้ว ตอนนี้เครื่องคอมพิวเตอร์ก็จะอยู่ในแพลตฟอร์มของอูบุนตู ผู้อ่านสามารถเข้าไปดูไฟล์หรือโฟลเดอร์ใดๆ ก็ได้ อีกทั้งยังสามารถลบไฟล์และโฟลเดอร์ใดๆ ก็ได้เช่นกัน ซึ่งการลบไฟล์และโฟลเดอร์นั้น ตอนที่อยู่ในสถานะของระบบปฏิบัติการวินโดวส์จะไม่สามารถทำได้ แต่ในสถานะที่อยู่ในระบบปฏิบัติการอูบุนตูสามารถทำได้หมด

เมื่อดำเนินการมาถึงตรงนี้ให้เข้าไปดูที่ไดรฟ์ C: โดยนำเมาส์ไปคลิกตามลูกศรชี้ในรูปที่ ๓.๓ จะได้ตามรูป ๓.๔ ซึ่งเป็นที่ติดตั้งระบบปฏิบัติการ Windows ๘ ให้สังเกตที่โฟลเดอร์ที่ชื่อ $Recycle.Bin กับ System Volume Information เราจะเข้าไปดูที่โฟลเดอร์ทั้ง ๒



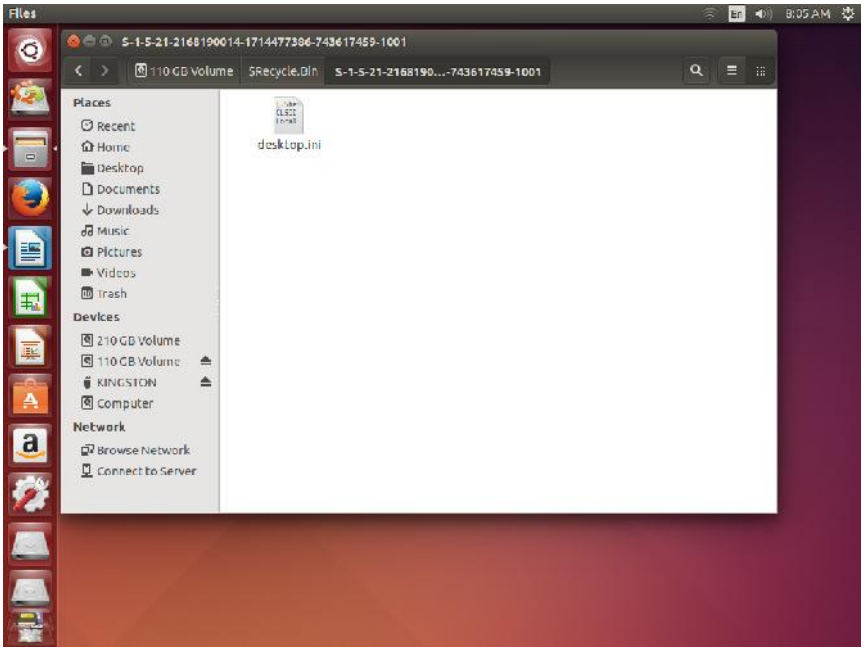
รูป ๓.๔ ไดรฟ์ C: ที่ติดตั้งระบบปฏิบัติการ Windows ๘

โดยเข้าไปที่โฟลเดอร์ $Recycle.Bin จะได้ดังรูป ๓.๕



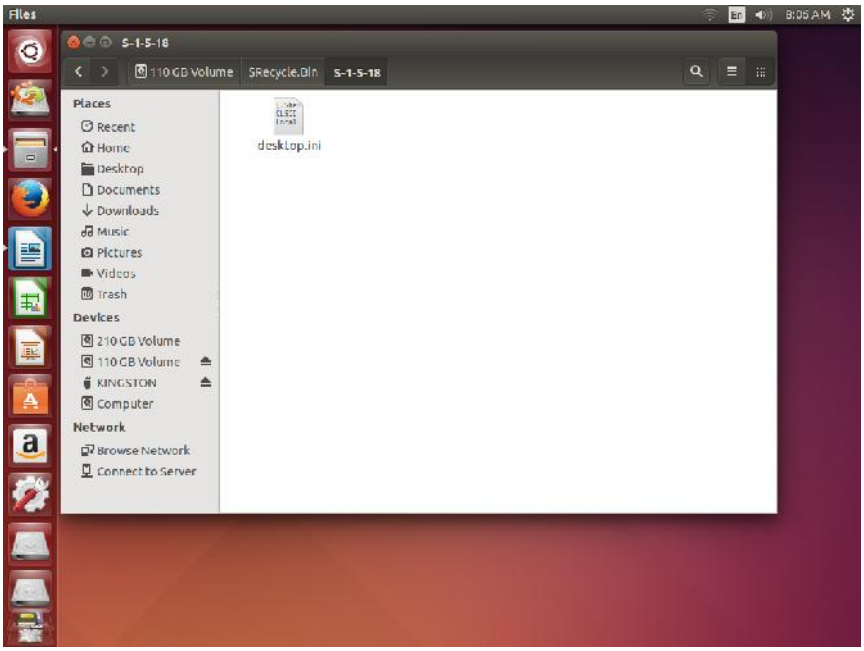
รูป ๓.๕ ภายในโฟลเดอร์ $Recycle.Bin ที่เปิดด้วยระบบปฏิบัติการอูบุนตู

ผู้อ่านจะพบว่าในโฟลเดอร์ $Recycle.Bin นั้น ตอนที่เรามองในระบบปฏิบัติการวินโดวส์ เราจะเห็นโฟลเดอร์ S-๑-๕-๑๘ กับโฟลเดอร์ Recycle.Bin แต่ในที่นี้ผู้อ่านจะพบว่าแท้จริงแล้ว โฟลเดอร์ Recycle.Bin นั้น เมื่อมามองในระบบปฏิบัติการอูบุนตู ผู้อ่านจะเห็นเป็นค่า SID (แตกต่างกันตามเครื่องคอมพิวเตอร์) ซึ่งเมื่อเข้าไปภายในโฟลเดอร์ดังกล่าวจะเป็นตามรูป ๓.๖



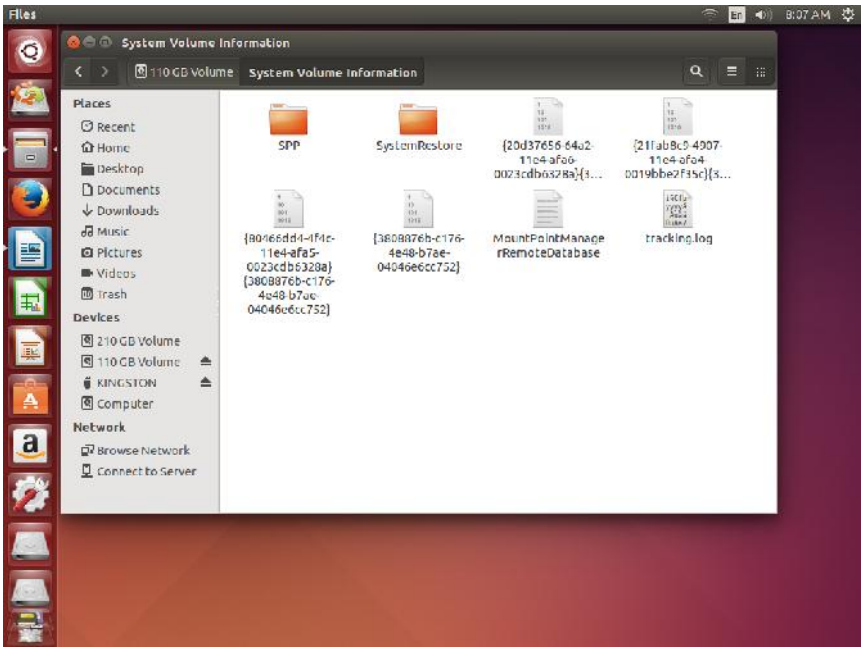
รูป ๓.๖ ภายในโฟลเดอร์ตามค่า SID (ใน Windows ๘ คือโฟลเดอร์ Recycle.Bin)

และในโฟลเดอร์ S-๑-๕-๑๘ *(ชื่อนี้อาจแตกต่างกันตามแต่ละเครื่องคอมพิวเตอร์)* เมื่อเข้าไปภายในโฟลเดอร์ดังกล่าวก็จะพบตามรูป ๓.๗



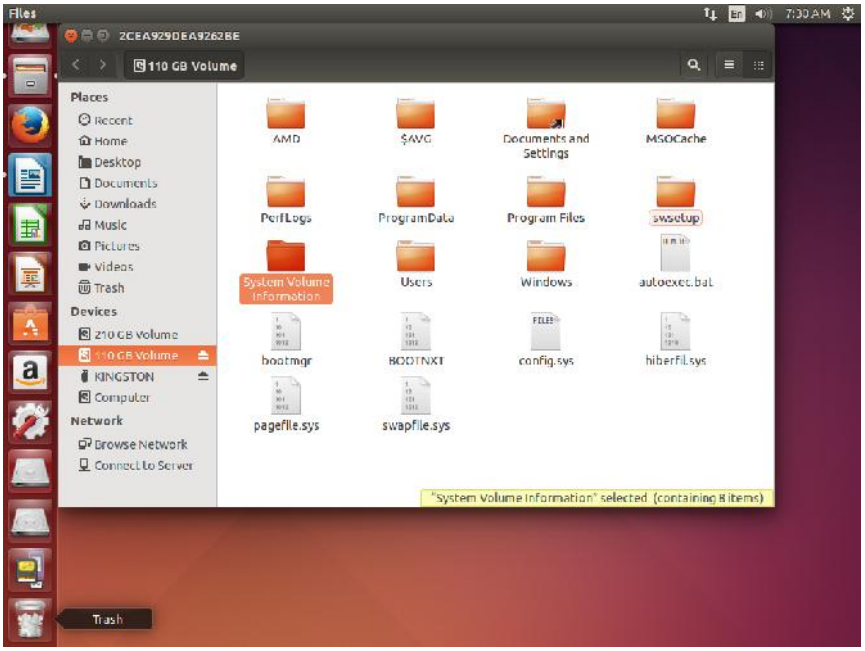
รูป ๓.๗

ทั้งโฟลเดอร์ S-๑-๕-๑๘ และโฟลเดอร์ตามค่า SID นั้น ถ้าไม่มีอะไรที่ตอนเราใช้ระบบปฏิบัติการวินโดวส์แล้วลบไปเพื่อต้องการกู้คืน ผู้อ่านสามารถลบได้ทั้งหมด หรือจะลบทิ้งทั้งโฟลเดอร์ $Recycle.Bin เลยก็ได้โดยคลิกขวามี่โฟลเดอร์ที่ต้องการลบแล้วเลือก Move to Trash เป็นอันว่าถูกลบไป และเช่นเดียวกันในโฟลเดอร์ System Volume Information เมื่อเข้าไปดูในโฟลเดอร์ดังกล่าว จะเห็นตามรูป ๓.๘ ซึ่งลบทิ้งไปเลยก็ได้โดยคลิกขวาเลือก Move to Trash เช่นเดียวกัน



รูป ๓.๘ ในโฟลเดอร์ System Volume Information

หรือจะลบไฟล์ โฟลเดอร์อะไรก็ตาม สามารถลบได้โดยการใช้เมาส์คลิกเลือกแล้วลากไปใส่ในถังขยะ (Trash) ที่อยู่ทางด้านล่างซ้ายมือ ตามรูป ๓.๙ ก็ได้

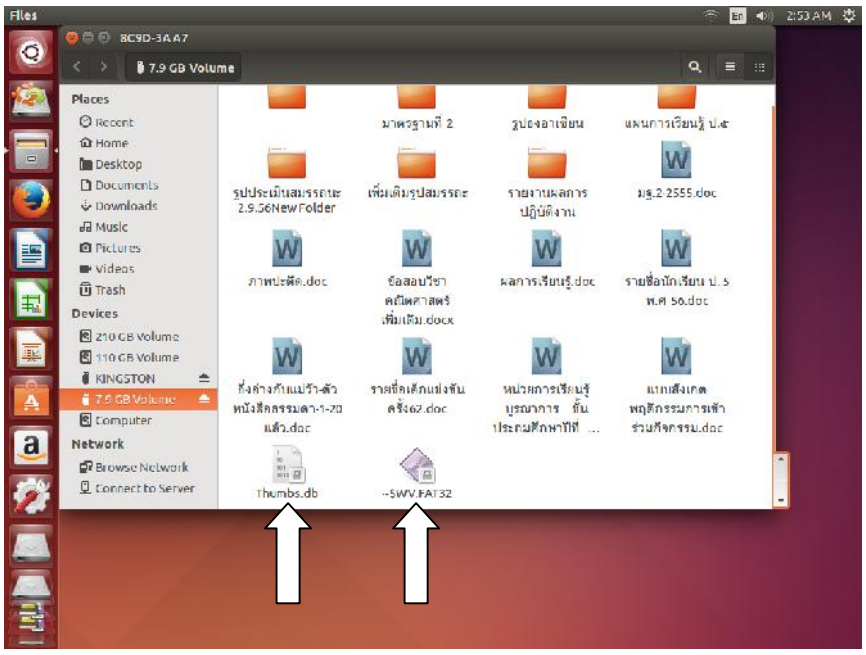


รูป ๓.๙ ลากไฟล์หรือโฟลเดอร์ที่ต้องการลบไปใส่ในถังขยะ (Trash)

จากการที่เราบูตระบบปฏิบัติการอูบุนตูจากแผ่น DVD เพื่อให้อ่านไฟล์และโฟลเดอร์ต่างๆ ในไดรฟ์ C: หรือไดรฟ์อื่นๆ ในคอมพิวเตอร์ได้นั้น เราก็จะสามารถลบไฟล์หรือโฟลเดอร์ที่ไม่ต้องการได้ (แต่อย่าไปลบไฟล์และโฟลเดอร์ระบบในไดรฟ์ C: นะครับ) เมื่อผู้อ่านได้ประสบพบเห็นในไดรฟ์ C: บ่อยๆ ผู้อ่านก็จะพอทราบได้ว่าอะไรควรจะลบ แต่ดังที่ได้กล่าวไว้ในบทที่ ๒ แล้วว่า ถ้าเราตั้ง UAC ไว้ดีแล้ว และกระบวนการใช้วินโดวส์ของเราเมื่อมีการถามจาก UAC ว่ามีโปรแกรมใดๆ ต้องการติดตั้งแล้วเราอ่านก่อน โอกาสที่จะมีไฟล์ใดๆ ติดตั้งไปในไดรฟ์ C: โดยไม่ได้รับอนุญาตย่อมไม่มี ดังนั้นในไดรฟ์ C: ถ้าผู้อ่านจะลบก็สามารถลบโฟลเดอร์ $Recycle.Bin และโฟลเดอร์ System Volume Information ได้ แต่ในไดรฟ์อื่นๆ ท่านสามารถเข้าไปดูไฟล์และโฟลเดอร์ต่างๆ ได้หมด โดยตั้งข้อสังเกตไว้ว่าไฟล์หรือโฟลเดอร์ใดที่ชื่อไม่สื่อความหมายและยาวมากๆ ผู้อ่านลบไปได้เลย เพราะไฟล์และโฟลเดอร์ลักษณะเช่นนี้ย่อมไม่น่าไว้ใจอยู่แล้ว อีกทั้งในไดรฟ์อื่นๆ ที่ไม่ใช่ไดรฟ์ C: ย่อมไม่ใช่สถานที่ติดตั้งไฟล์ระบบอยู่แล้ว ยิ่งไฟล์และโฟลเดอร์จำพวก $Recycle.Bin หรือ System Volume Information ในไดรฟ์อื่นๆ ลบทิ้งให้หมด โฟลเดอร์ Recycler หรือ Recycled ใน External Harddisk หรือในแฟลชไดรฟ์ ลบได้หมด เพราะมักเป็นที่ซ่อนตัว (อีแอบ) ของไวรัสคอมพิวเตอร์ตัวดีทั้งหลาย

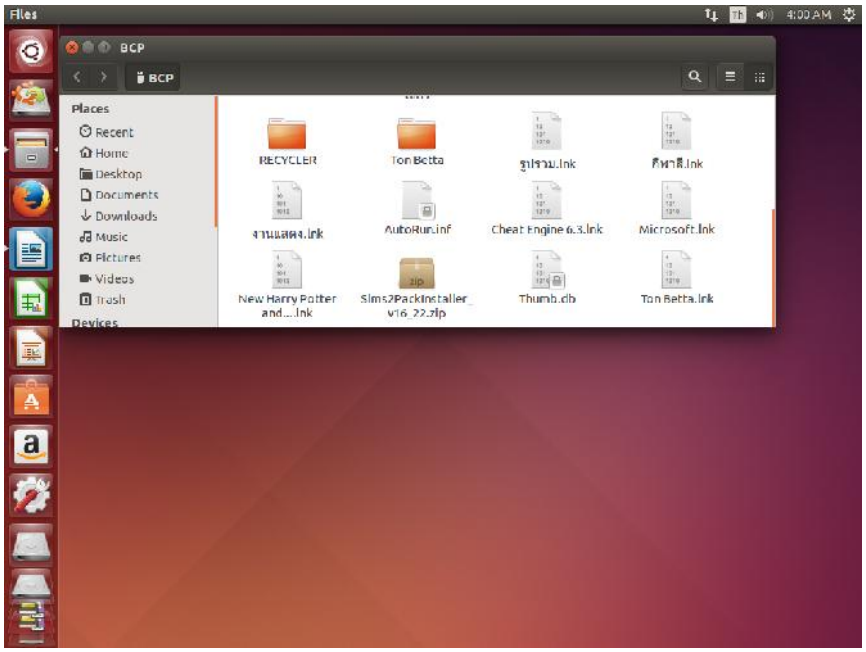
ที่นี้มาลองดูตัวอย่างของสิ่งที่ไม่น่าจะเป็นประโยชน์และตัวอย่างของไวรัสคอมพิวเตอร์ที่อยู่ในแฟลชไดรฟ์ กันบ้าง แล้วเราจะลบทิ้ง

ตัวอย่างแรกจากแฟลชไดรฟ์อันหนึ่ง เมื่อเราใช้ระบบปฏิบัติการอูบุนตู มองจะพบว่าในแฟลชไดรฟ์ตามรูป ๓.๑๐ มีไฟล์ที่น่าสงสัยอยู่คือ Thumbs.db และ ~$WV.FAT๓๒ ตามที่ลูกศรชี้ ถ้าเราคิดว่าไม่น่าจะเป็นประโยชน์ใดๆ ก็ลบทิ้งไปได้เลย



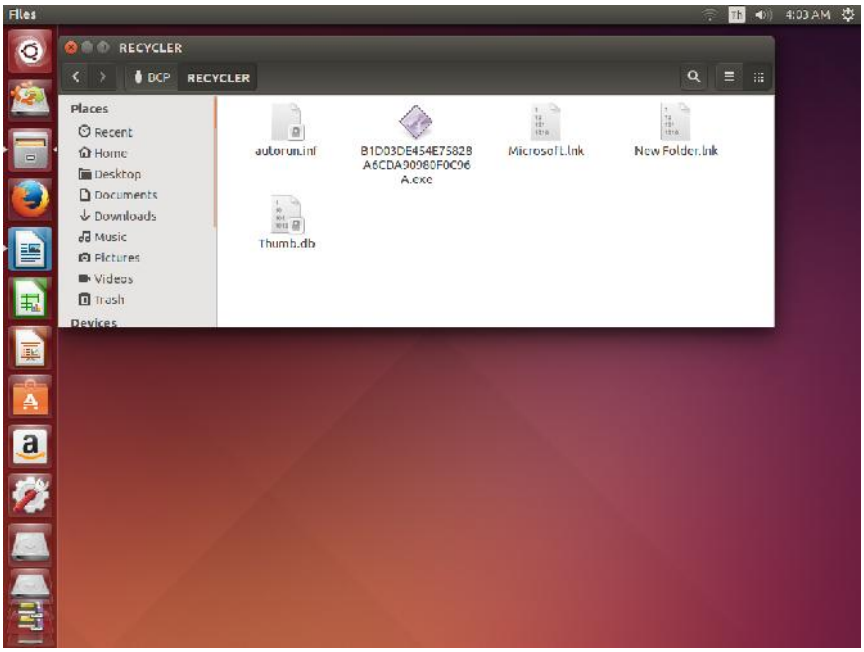
รูป ๓.๑๐ ไฟล์ที่ไม่น่าจะเป็นประโยชน์ในแฟลชไดรฟ์ตัวอย่าง

อีกตัวอย่างหนึ่งจากแฟลชไดรฟ์ชื่อ BCP ซึ่งมีไวรัสแน่นอนตามรูป ๓.๑๑ จะเห็นว่ามีโฟลเดอร์ชื่อ Recycler อยู่ *(ซึ่งเราได้กล่าวไว้แล้วว่าในแฟลชไดรฟ์ถ้ามีโฟลเดอร์พวกนี้อยู่ลบทิ้งได้เลย เพราะนี้คือที่อยู่ของไวรัสคอมพิวเตอร์ส่วนหนึ่ง)* และไฟล์อื่นๆ ที่มีนามสกุลเป็น .lnk คือไวรัสได้สร้างไฟล์เลียนแบบขึ้นมา อาการของไฟล์ที่โดนไวรัสคอมพิวเตอร์พวกนี้เล่นงาน คือเมื่อเราพยายามจะเรียกไฟล์พวกนี้ขึ้นมา จะพบว่าไม่เกิดอะไรขึ้น เพราะว่าในความเป็นจริง สิ่งที่เราเห็นเป็นไฟล์นามสกุล .lnk ตัวนี้ในระบบปฏิบัติการวินโดวส์ เราจะเห็นเป็นไฟล์ปกติ แต่ไฟล์ปกติจะถูกไวรัสคอมพิวเตอร์ซ่อนไว้ เมื่อเราคลิกเลือกก็เท่ากับเรียกให้ไวรัสคอมพิวเตอร์ทำงานนั่นเอง



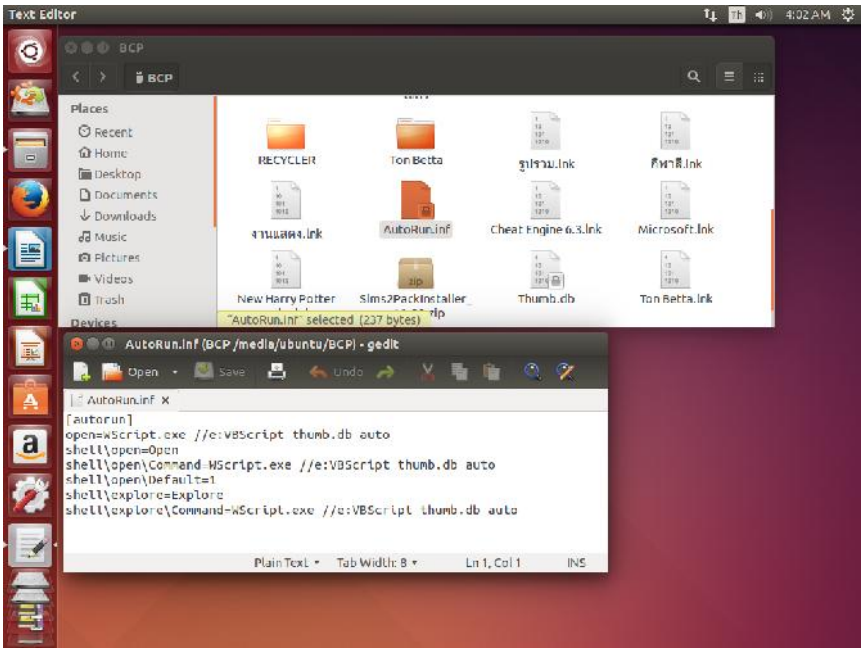
รูป ๓.๑๑ แฟลชไดรฟ์ที่ติดไวรัสคอมพิวเตอร์

ที่นี้เรามาดูไวรัสคอมพิวเตอร์ที่อยู่ในแฟลชไดรฟ์ตามรูป ๓.๑๑ คือ โฟลเดอร์ Recycler กันว่ามีอะไรอยู่ภายในบ้าง โดยคลิกเข้าไปดูในโฟลเดอร์ดังกล่าว จะได้ตามรูป ๓.๑๒



รูป ๓.๑๒ ภายในโฟลเดอร์ Recycler ในแฟลชไดรฟ์ตัวอย่าง

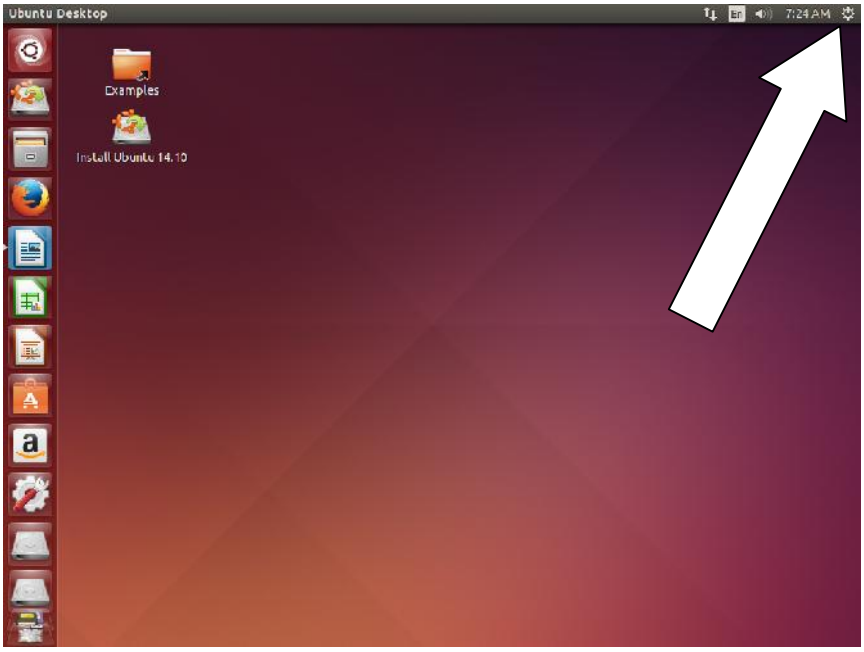
จะเห็นได้ว่าภายในโฟลเดอร์ Recycler ดังกล่าวนั้นมีไฟล์ autorun.inf และไฟล์ Thumb.db ตลอดจนไฟล์อื่นๆ อยู่ด้วย ตอนนี้เราลองย้อนกลับไปดูรูป ๓.๑๑ ผู้อ่านจะเห็นว่ามีไฟล์ autorun.inf อยู่ด้วย ผู้เขียนเปิดไฟล์ตัวนี้ให้ดูจะพบลักษณะการทำงานของไฟล์นี้ ตามรูป ๓.๑๓



รูป ๓.๑๓ คำสั่งหรือ Script ของไฟล์ autorun.inf

ผู้เขียนจะไม่ขออธิบายในส่วนของคำสั่งหรือ Script ของไฟล์พวกนี้ เนื่องจากจะต้องอธิบายอีกยาว แต่หนังสือเล่มนี้แนะเทคนิคการต่อกรกับไวรัสคอมพิวเตอร์ ดังนั้นมาถึงตรงนี้ผู้อ่านก็ลบทิ้งได้เลย ทั้งโฟลเดอร์ Recycler ไฟล์ autorun.inf ไฟล์ thumb.db และไฟล์ที่นามสกุล .lnk ไปได้ทั้งหมด

ก่อนจบขออธิบายวิธีการในการ Shut Down... ออกจากระบบปฏิบัติการอูบุนตู ๑๔.๑๐ ดังนี้ คือ ที่หน้าจอ Desktop ของระบบปฏิบัติการอูบุนตู ตามรูป ๓.๑๔ ให้นำเมาส์ไปชี้ที่สัญลักษณ์มุมบนด้านขวาของจอ (ลูกศรชี้) จะมีเมนูขึ้นมา ให้เลือก Shut Down... แล้วรอให้ระบบดีดแผ่น DVD ออกมาแล้วกด Enter เป็นอันเสร็จสิ้น



รูป ๓.๑๔ การปิดระบบปฏิบัติการอูบุนตู

๓. สรุป

ไวรัสคอมพิวเตอร์ก็คือไฟล์ชนิดหนึ่ง ที่เรามองด้วยวิธีปกติไม่เห็น ดังนั้นถ้าเรารู้ว่าไฟล์ใดเป็นไวรัสคอมพิวเตอร์ เราก็สามารถลบได้ แต่ปัญหาที่เกิดกับเราก็คือไม่รู้ว่าไฟล์ใดเป็นไฟล์ไวรัสคอมพิวเตอร์และอยู่ตรงไหน หรือถึงแม้ว่าจะรู้ว่าอยู่ตรงไหน เราก็ไม่สามารถลบมันออกไปได้ ในขณะที่เราอยู่ในสถานะของระบบปฏิบัติการวินโดวส์ ดังนั้นหลักการของเราก็คือการบูตระบบด้วยระบบปฏิบัติการอูบุนตู ในการเข้าไปในที่ ที่ไวรัสคอมพิวเตอร์ชอบไปซ่อนอยู่ และทำการลบออกเสียด้วยระบบปฏิบัติการอูบุนตู

แต่เทคนิคดังกล่าวนี้ไม่ใช่ยาวิเศษที่จะต่อกรกับไวรัสคอมพิวเตอร์ได้ทุกอย่าง ทั้งนี้ขึ้นอยู่กับตัวผู้ใช้เองด้วย ในการที่จะระแวดระวัง และใช้คอมพิวเตอร์ เพราะคนสร้างไวรัสคอมพิวเตอร์ย่อมมีวิธีการและอัลกอริทึ่มในการที่จะเขียนไวรัสคอมพิวเตอร์ใหม่ๆ มาอยู่เสมอ เพราะถ้าไวรัสคอมพิวเตอร์เข้าไปฝังในรีจิสตรี้ของระบบปฏิบัติการวินโดวส์แล้ว แน่นอนย่อมเป็นเรื่องยากที่จะกำจัด และเราต้องเรียนรู้และใช้เทคนิคขั้นสูงขึ้นอีกในการต่อกรกับไวรัสคอมพิวเตอร์