

ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่
ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
พ.ศ. ๒๕๖๘

โดยที่เป็นการสมควรปรับปรุงหลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ให้มีความเหมาะสมกับภารกิจหน้าที่และอำนาจของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และเพื่อให้การบังคับใช้กฎหมายมีประสิทธิภาพยิ่งขึ้น

อาศัยอำนาจตามความในมาตรา ๒๘ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จึงออกประกาศกำหนดหลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พ.ศ. ๒๕๖๘”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้ยกเลิก

(๑) ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๒) ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๙

ข้อ ๔ ในประกาศนี้

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“รัฐมนตรี” หมายความว่า รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ข้อ ๕ พนักงานเจ้าหน้าที่ ต้องมีคุณสมบัติ ดังต่อไปนี้

(๑) มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์

(๒) สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรีทางวิศวกรรมศาสตร์ วิทยาศาสตร์ วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ หรือรัฐประศาสนศาสตร์

(๓) ผ่านการอบรมทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) สืบสวน สอบสวน และการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) ตามภาคผนวกท้ายประกาศนี้

(๔) เป็นข้าราชการในสังกัดสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ซึ่งได้ปฏิบัติหน้าที่เกี่ยวกับการป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ หรืออาชญากรรมทางเทคโนโลยี หรือเป็นข้าราชการอื่นซึ่งได้ปฏิบัติหน้าที่ดังกล่าวมาแล้วเป็นเวลา ไม่น้อยกว่าสองปี และ

(๕) มีคุณสมบัติอื่นอย่างหนึ่งอย่างใด ดังต่อไปนี้

(ก) รับราชการหรือเคยรับราชการไม่น้อยกว่าสองปีในตำแหน่งเจ้าหน้าที่ตรวจพิสูจน์ พยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์หรือพยานหลักฐานอิเล็กทรอนิกส์

(ข) สำเร็จการศึกษาตามข้อ ๕ (๒) ในระดับปริญญาตรี และมีประสบการณ์ที่เป็นประโยชน์ ต่อการปฏิบัติงานตามพระราชบัญญัตินี้ นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสี่ปี

(ค) สำเร็จการศึกษาตามข้อ ๕ (๒) ในระดับปริญญาโท หรือสอบไล่ได้เป็นเนติบัณฑิต ตามหลักสูตรของสำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา และมีประสบการณ์ที่เป็นประโยชน์ ต่อการปฏิบัติงานตามพระราชบัญญัตินี้ นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสามปี

(ง) สำเร็จการศึกษาตามข้อ ๕ (๒) ในระดับปริญญาเอก หรือมีประสบการณ์ที่เป็นประโยชน์ ต่อการปฏิบัติงาน ตามพระราชบัญญัตินี้ นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสองปี

(จ) เป็นบุคคลที่ทำงานเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศ การตรวจพิสูจน์หลักฐาน ทางคอมพิวเตอร์ หรือมีประสบการณ์ในการดำเนินคดีเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ ไม่น้อยกว่าสองปี

ข้อ ๖ ในกรณีที่มีความจำเป็นเพื่อประโยชน์ของทางราชการในการสืบสวนและสอบสวน การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรืออาชญากรรมทางเทคโนโลยี จำเป็นต้องมีบุคลากร ซึ่งมีความรู้ ความชำนาญ หรือประสบการณ์สูง เพื่อดำเนินการสืบสวนและสอบสวนการกระทำผิด หรือคดีเช่นนั้น หรือเป็นบุคลากรในสาขาที่ขาดแคลน รัฐมนตรีอาจยกเว้นคุณสมบัติตามข้อ ๕ ไม่ว่าทั้งหมดหรือบางส่วนสำหรับการบรรจุและแต่งตั้งบุคคลใดเป็นการเฉพาะก็ได้

ข้อ ๗ การแต่งตั้งบุคคลหนึ่งบุคคลใดเป็นพนักงานเจ้าหน้าที่ให้แต่งตั้งจากบุคคล ซึ่งมีคุณสมบัติตามข้อ ๕ หรือข้อ ๖ โดยบุคคลดังกล่าวต้องผ่านการประเมินความรู้ความสามารถ หรือทดสอบตามหลักสูตรและหลักเกณฑ์ที่รัฐมนตรีประกาศกำหนด

การแต่งตั้งและการพ้นจากตำแหน่งของพนักงานเจ้าหน้าที่ให้ประกาศในราชกิจจานุเบกษา

ข้อ ๘ ให้สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นหน่วยงานรับผิดชอบ ในการนำเสนอต่อรัฐมนตรีเพื่อแต่งตั้งบุคคลให้เป็นพนักงานเจ้าหน้าที่และการให้พ้นจากตำแหน่ง ของพนักงานเจ้าหน้าที่

ข้อ ๙ พนักงานเจ้าหน้าที่ต้องไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) เป็นบุคคลล้มละลาย บุคคลไร้ความสามารถ หรือบุคคลเสมือนไร้ความสามารถ

(๒) เป็นสมาชิกสภาผู้แทนราษฎร สมาชิกวุฒิสภา ข้าราชการการเมือง สมาชิกสภาท้องถิ่น ผู้บริหารท้องถิ่น กรรมการหรือผู้ดำรงตำแหน่งที่รับผิดชอบในการบริหารพรรคการเมือง ที่ปรึกษาพรรคการเมือง หรือเจ้าหน้าที่ในพรรคการเมือง

(๓) เป็นผู้อยู่ระหว่างถูกสั่งให้พักราชการหรือถูกสั่งให้ออกจากราชการไว้ก่อน

(๔) ถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หน่วยงานของรัฐหรือรัฐวิสาหกิจเพราะทำผิดวินัย หรือรัฐมนตรีให้ออกจากการเป็นพนักงานเจ้าหน้าที่ เพราะมีความประพฤติเสื่อมเสียบกพร่องหรือไม่สุจริต ต่อหน้าที่หรือหย่อนความสามารถ

(๕) ได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษ สำหรับความผิด ที่กระทำโดยประมาทหรือความผิดลหุโทษ

(๖) ต้องคำพิพากษาหรือคำสั่งของศาลให้ทรัพย์สินตกเป็นของแผ่นดิน เพราะร่ำรวยผิดปกติ หรือมีทรัพย์สินเพิ่มขึ้นผิดปกติ

ข้อ ๑๐ พนักงานเจ้าหน้าที่พ้นจากตำแหน่งเมื่อ

(๑) ตาย

(๒) ออกจากราชการไม่ว่าด้วยเหตุใด

(๓) ถูกจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก

(๔) ขาดคุณสมบัติตามข้อ ๕ หรือมีลักษณะต้องห้ามตามข้อ ๙

(๕) รัฐมนตรีให้ออก

ข้อ ๑๑ ให้พนักงานเจ้าหน้าที่ซึ่งไม่ได้สังกัดสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และกองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีที่ได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่อยู่ในวันก่อนวันที่ประกาศนี้ใช้บังคับ มีหน้าที่รายงานหัวหน้าหน่วยงานต้นสังกัดของตน เพื่อพิจารณาแจ้งยืนยันการเป็นพนักงานเจ้าหน้าที่ให้สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทราบ ภายในสี่สิบห้าวันนับแต่วันที่ประกาศนี้ใช้บังคับ หากไม่มีการแจ้ง ภายในกำหนดระยะเวลาดังกล่าว ให้สถานะการเป็นพนักงานเจ้าหน้าที่ของบุคคลนั้นสิ้นสุดลง นับแต่วันที่พ้นกำหนดระยะเวลาดังกล่าว

เมื่อได้รับแจ้งจากหน่วยงานภายในกำหนดระยะเวลาตามวรรคหนึ่งแล้ว ให้สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมดำเนินการเสนอต่อรัฐมนตรีเพื่อพิจารณาแต่งตั้งบุคคลให้เป็นพนักงานเจ้าหน้าที่ต่อไปโดยเร็ว ทั้งนี้ ในระหว่างการดำเนินการดังกล่าวให้สถานะการเป็นพนักงานเจ้าหน้าที่ของบุคคลที่มีรายชื่อตามแจ้งยังคงอยู่ต่อไป

ข้อ ๑๒ ให้หัวหน้าหน่วยงานต้นสังกัดของพนักงานเจ้าหน้าที่ตามข้อ ๑๑ มีหน้าที่รายงานผลการปฏิบัติงานของพนักงานเจ้าหน้าที่ในสังกัดของตน พร้อมความเห็นและข้อเสนอแนะในการปฏิบัติงานต่อรัฐมนตรีอย่างน้อยปีละหนึ่งครั้ง

ข้อ ๑๓ ให้พนักงานเจ้าหน้าที่ซึ่งสังกัดสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีที่ได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่อยู่ในวันก่อนวันที่ประกาศนี้ใช้บังคับ พ้นจากตำแหน่งพนักงานเจ้าหน้าที่เมื่อพ้นกำหนดหนึ่งปีนับแต่วันที่ประกาศนี้ใช้บังคับ หรือเมื่อรัฐมนตรีมีประกาศให้พ้นจากตำแหน่งพนักงานเจ้าหน้าที่ก่อนกำหนดระยะเวลาดังกล่าว แล้วแต่กรณี

ข้อ ๑๔ ให้รัฐมนตรีมีอำนาจตีความและวินิจฉัยปัญหาอันเกิดจากการปฏิบัติตามประกาศนี้

ประกาศ ณ วันที่ ๒๗ ตุลาคม พ.ศ. ๒๕๖๘

ไชยชนก ชิดชอบ

รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ภาคผนวก

แนบท้ายประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พ.ศ. ๒๕๖๘

ผู้ที่จะได้รับการแต่งตั้งให้เป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ จะต้องผ่านการอบรมด้านจริยธรรม สืบสวน สอบสวน ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) และการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) แล้วแต่กรณี ดังต่อไปนี้

๑. หลักสูตรมาตรฐานสากล (International Standard Courses)

วัตถุประสงค์ : เพื่อใช้เป็นแนวทางในการจัดอบรมให้กับบุคคลซึ่งจะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ในกรณีทั่วไป (หลักสูตรเต็มเวลาประมาณ ๑ เดือน ทั้งภาคทฤษฎีและปฏิบัติ ทั้งนี้ ไม่รวมด้านที่สาม ข. และด้านที่สี่ ข. ซึ่งเป็นหลักสูตรความเชี่ยวชาญเฉพาะทาง)

เนื้อหาหลักสูตรที่อบรม :

- ด้านแรก การอบรมด้านจริยธรรม/จรรยาบรรณที่พึงมีในบทบาทและอำนาจหน้าที่ของพนักงานเจ้าหน้าที่
- ด้านที่สอง ความรู้พื้นฐานด้านการสืบสวนและสอบสวนเพื่อการบังคับใช้กฎหมาย (Law Enforcement)

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๑	กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๒	กฎหมายอาญาและวิธีพิจารณาความอาญาที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๓	รูปแบบการกระทำความผิดและกรณีศึกษา (Case Studies)
๔	การสืบสวนทางเทคนิค เช่น การตรวจสอบหมายเลข IP Address หรือแหล่งที่มาของการกระทำความผิด การขอข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) จากผู้ให้บริการการวิเคราะห์และเชื่อมโยงข้อมูล/พยานหลักฐานข้างต้น
๕	แนวทางปฏิบัติในการดำเนินคดี/การทำสำนวนคดี เช่น การร้องทุกข์กล่าวโทษ (การแจ้งความ) การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง การรวบรวมพยานหลักฐาน และแสวงหาข้อเท็จจริง การตรวจสอบสถานที่เกิดเหตุ การยื่นคำร้องต่อศาล การยึดอายัดและคืนพยานหลักฐาน การเก็บรักษาพยานหลักฐาน การเก็บรักษาพยานหลักฐานให้คงความน่าเชื่อถือในกระบวนการ การเปรียบเทียบปรับและการดำเนินคดี เป็นต้น
๖	การบริหารจัดการคดีให้เป็นไปอย่างมีประสิทธิภาพ

ด้านที่สาม ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security)

ก. เนื้อหาหลักสูตรภาคบังคับสำหรับพนักงานเจ้าหน้าที่

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๑	General security concepts
๒	Security Architecture
๓	Access Controls
๔	Applications Security
๕	Operation Security
๖	Security Management
๗	Cryptography
๘	Physical Security
๙	Telecommunications and Network Security
๑๐	Business Continuity Planning
๑๑	Law, Investigations, and Ethics

ข. หลักสูตรความมั่นคงปลอดภัยของระบบสารสนเทศขั้นสูง (Advanced Information Security Course) สำหรับพนักงานเจ้าหน้าที่สายผู้เชี่ยวชาญด้านเทคนิค

ลำดับ	เนื้อหาหลักสูตร (ความชำนาญเฉพาะทาง)
๑	Audit and Monitoring
๒	Risk, Response and Recovery
๓	Malicious Code Analysis
๔	Vulnerabilities Assessment & Penetration Testing

ด้านที่สี่ การพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics)

ก. ความรู้ด้านการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics)

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๑	The needs for Computer Forensics
๒	Principles of Computer Forensics and Digital/Electronic Evidence
๓	Crime scene, Digital/Electronic Evidence and Chain of Custody

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๔	Capturing the Data Image and Volatile Data
๕	Extracting Information from Captured Data
๖	Breaking Password and Encryption
๗	Using Computer Forensics Tools
๘	Investigation and Interrogation
๙	Digital/Electronic Evidence Analysis and Synthesis
๑๐	Testify in Court, Admissibility requirements
๑๑	Different between Computer Forensics and Network/Internet Forensics
๑๒	Network/Internet Forensics
๑๓	Using Network/Internet Forensics Tools

ข. ความเชี่ยวชาญเฉพาะทางด้านการพิสูจน์หลักฐานทางคอมพิวเตอร์
(Professional Computer Forensics และ Certified Forensic Computer Examiner (CFCE))

ลำดับ	เนื้อหาหลักสูตร (ความชำนาญเฉพาะทาง)
๑	Using Computer Forensic Tools เช่น Encase, Forensics Toolkits, ILook
๒	Using Network / Internet Forensic Tools เช่น Encase Field Intelligence Model (FIM)
๓	Wireless Forensic Tools เช่น Netstumbler, Kismet, Aircrack
๔	Using Handheld Forensics Tools (Cell & PDA) Paraben, MobilEdit, Vogon
๕	Cryptology ได้แก่ Cryptography และ Cryptanalysis

๒. หลักสูตรเร่งรัด (Intensive Courses) (๕ วัน)

วัตถุประสงค์ : เพื่อใช้เป็นแนวทางในการจัดการอบรมระยะสั้นแบบเร่งรัดให้กับบุคคลซึ่งได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ในกรณีพิเศษ ซึ่งได้รับการยกเว้นตามหลักเกณฑ์ในการกำหนดคุณสมบัติของพนักงานเจ้าหน้าที่ตามปกติทั่วไป

เนื้อหาหลักสูตรที่อบรม :

ด้านแรก การอบรมด้านจริยธรรม/จรรยาบรรณที่พึงมีในบทบาทและอำนาจหน้าที่ของพนักงานเจ้าหน้าที่

ด้านที่สอง ความรู้พื้นฐานด้านการสืบสวนและสอบสวนเพื่อการบังคับใช้กฎหมาย (Law Enforcement)

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๑	กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๒	กฎหมายอาญาและวิธีพิจารณาความอาญาที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๓	รูปแบบการกระทำความผิดและกรณีศึกษา (Case Studies)
๔	การสืบสวนทางเทคนิค เช่น การตรวจสอบหมายเลข IP Address หรือแหล่งที่มาของการกระทำความผิด การขอข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) จากผู้ให้บริการ การวิเคราะห์และเชื่อมโยงข้อมูล/ พยานหลักฐานข้างต้น
๕	แนวทางปฏิบัติในการดำเนินคดี/การทำสำนวนคดี เช่น การร้องทุกข์กล่าวโทษ (การแจ้งความ) การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง การรวบรวมพยานหลักฐาน และแสวงหาข้อเท็จจริง การตรวจสอบสถานที่เกิดเหตุ การยื่นคำร้องต่อศาล การยึดอายัดและคืนพยานหลักฐาน การเก็บรักษาพยานหลักฐาน การเก็บรักษาพยานหลักฐานให้คงความน่าเชื่อถือในกระบวนการ การเปรียบเทียบปรับและการดำเนินคดี เป็นต้น
๖	การบริหารจัดการคดีให้เป็นไปอย่างมีประสิทธิภาพ

ด้านที่สาม การพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics)

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๑	The needs for Computer Forensics
๒	Principles of Computer Forensics and Digital/Electronic Evidence
๓	Crime scene, Digital/Electronic Evidence and Chain of Custody
๔	Capturing the Data Image and Volatile Data
๕	Extracting Information from Captured Data
๖	Breaking Password and Encryption
๗	Using Computer Forensics Tools
๘	Investigation and Interrogation
๙	Digital/Electronic Evidence Analysis and Synthesis
๑๐	Testify in Court, Admissibility requirements
๑๑	Different between Computer Forensics and Network/Internet Forensics
๑๒	Network/Internet Forensics
๑๓	Using Network/Internet Forensics Tools