ANALYZING AND SEARCHING PROCESS OF INTERNET USERNAME AND PASSWORD STORED IN RANDOM ACCESS MEMORY (RAM)

SASITHORN THONGJUL 5537201 EGCO/M

M.Eng. (COMPUTER ENGINEERING)

THESIS ADVISORY COMMITTEE: SURATOSE TRITILANUNT, Ph.D., NOPPADOL WANICHWORANANT, Ph.D., VASIN SUTTICHAYA, Ph.D.

ABSTRACT

The main objective of this research is to develop the criteria for searching and extracting a username and password, which are stored in the physical memory while the computer is operating. The result from the first step is used to develop pattern searching that is suitable for matching the username and password. The output of this step is used to trace back to the websites that the user accesses. The researcher used the signature pattern from known accounts in order to extend the searching and linking to the account to be found. We linked the signature of the username and the search criteria stored in the physical memory. We set up the experiment to harvest and match the search criteria by browsing some social networks, webmail, Internet banking, and online business shopping websites. By using these search criteria obtained as a result from the second step, we developed software for searching the evidence stored in RAM. From the experiment, which we tested on some well known websites, our software was able to successfully search unencrypted usernames and passwords and then link to other artifacts, which were useful for the forensic investigation process.

KEY WORDS: RANDOM ACCESS MEMORY (RAM) / PHYSICAL MEMORY / VOLATILE DATA / LIVE MEMORY FORENSIC

138 pages

กระบวนการวิเคราะห์และค้นหารายชื่อผู้ใช้และรหัสผ่านของการใช้งานอินเทอร์เน็ตที่อยู่ในหน่วยความจำแรม

ANALYZING AND SEARCHING PROCESS OF INTERNET USERNAME AND PASSWORD STORED IN RANDOM ACCESS MEMORY (RAM)

ศศิธร ทองจุล 5537201 EGCO/M

วศ.ม. (วิศวกรรมคอมพิวเตอร์)

คณะกรรมการที่ปรึกษาวิทยานิพนธ์: สุรทศ ไตรติลานันท์, Ph.D., นภดล วณิชวรนันท์, Ph.D., วศิน สุทธิฉายา, Ph.D.

บทคัดย่อ

จุดประสงค์ของงานวิจัยนี้ เพื่อพัฒนาเกณฑ์ที่ใช้สำหรับการค้นหาและเก็บชื่อผู้ใช้และรหัสผ่านที่ถูกเก็บอยู่ในหน่วยความจำแรมในขณะที่เครื่องคอมพิวเตอร์เปิดใช้งานอยู่ ผลลัพธ์ของขั้นตอนแรกที่ได้จากการค้นหาจะถูกนำไปใช้ในการพัฒนารูปแบบที่เหมาะสมสำหรับจับคู่ชื่อผู้ใช้และรหัสผ่านเพื่อเชื่อมโยงกลับไปยังเว็บไซต์ที่ผู้ใช้งานนั้นเปิดใช้งานอยู่ ผู้พัฒนาได้ใช้รูปแบบของชื่อผู้ใช้และรหัสผ่านที่ผู้พัฒนาทราบ เพื่อค้นหาและเชื่อมโยงไปยังข้อมูลที่เป็นเกณฑ์ในการค้นหาชื่อผู้ใช้และรหัสผ่านที่เก็บอยู่ในหน่วยความจำแรม โดยในงานวิจัยนี้ผู้พัฒนาได้รวบรวมและสร้างเกณฑ์ของเว็บไซต์ที่เกี่ยวข้องกับ เครือข่ายสังคมออนไลน์, เว็บไซต์ที่ให้บริการจดหมายอิเล็กทรอนิกส์, ธนาคารออนไลน์, เว็บไซต์ซื้อขายออนไลน์ ผู้พัฒนาได้พัฒนาโปรแกรมสำหรับการค้นหาหลักฐานที่เก็บอยู่ในหน่วยความจำแรมโดยใช้จากเกณฑ์ที่ได้จากขั้นตอนแรกค้นหาชื่อผู้ใช้และรหัสผ่าน จากการทดสอบโปรแกรมโดยนำไปใช้ค้นหาชื่อผู้ใช้และรหัสผ่านจากเว็บไซต์ที่ได้รวบรวมมา สามารถค้นหาหลักฐานที่เป็นชื่อผู้ใช้และรหัสผ่านที่อยู่ในรูปแบบที่ไม่ได้เข้ารหัสและเชื่อมโยงไปยังข้อมูลอื่นๆที่เป็นประโยชน์กับกระบวนการทางนิติวิทยาดิจิทัลได้อย่างถูกต้อง

138 หน้า