

الجزائرية الديمقراطية الشعبية الجمهورية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للإعلام الآلي - 08 ماي 1945 - بسيدي بلعباس
Ecole Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbès



MEMOIRE

En Vue de l'obtention du diplôme de **Master**

Filière : **Informatique**

Spécialité : **Ingénierie des Systèmes Informatiques (ISI)**

Thème

Windows System Features Analysis for Digital Forensics

Présenté par :

- Mr Seddaoui Mhammed

Soutenu le : **24/09/2023**

Devant le jury composé de :

- | | |
|-----------------------------------|--------------|
| - M AZZA Mohamed | Président |
| - M KHALDI Miloud | Examineur |
| - M Belfedhal Alaa Eddine | Encadreur |
| - M LAHOUAZI Chamel Djamel Eddine | Co-encadreur |

Année Universitaire : 2022 / 2023

Abstract.

Digital forensics and Incident Response are vital aspects of cybersecurity. They play a crucial role in safeguarding organizations from the increasing threat of cyberattacks, which have become prevalent in the business world. Many services, including those connected to global networks, face the risk of attacks from hacker groups and malware. Fortunately, these services keep various logs.

Incident Response focuses on recovering from these attacks, relying on the forensic investigation, which, in turn, relies on these recorded logs. In this study, we explore modern methods and tools developed by the research community to simplify the analysis of these logs. our aim is to realize a state-of-art of recent studies considering Windows forensics investigations and using its features alongside with Windows event log. Finally, we give a useful comparison of performances and complexity by summarizing the empirical findings provided in each article and outlining the major contrasts between them.

ملخص

التحليل الرقمي واستجابة الحوادث هما جانبان حيويان في مجال أمن المعلومات. إنهما يلعبان دوراً حاسماً في حماية المؤسسات من تزايد تهديدات الهجمات الإلكترونية، التي أصبحت شائعة في عالم الأعمال. العديد من الخدمات، بما في ذلك تلك المتصلة بشبكات عالمية، تواجه خطر تعرضها للهجمات من قبل مجموعات الهاكرز والبرمجيات الخبيثة. لحسن الحظ، تحتفظ هذه الخدمات بسجلات متنوعة.

تركز استجابة الحوادث على استعادة الأوضاع بعد هذه الهجمات، وتعتمد على التحقيق الجنائي الرقمي، الذي بدوره يعتمد على هذه السجلات المسجلة. في هذه الدراسة، نقوم باستكشاف الأساليب والأدوات الحديثة التي طورتها مجتمعات البحث لتبسيط تحليل هذه السجلات. هدفنا هو التعرف على الأسباب الجذرية للحوادث، وضمان معالجة الثغرات، ومنع الهجمات المستقبلية. وأخيراً، نقدم مقارنة مفيدة للأداء والتعقيد عن طريق تلخيص النتائج التجريبية المقدمة في كل مقالة وتبسيط الضوء على الاختلافات الرئيسية بينها.

Résumé

La cybercriminalité et la réponse aux incidents sont des aspects essentiels de la cybersécurité. Ils jouent un rôle crucial dans la protection des organisations contre la menace croissante des cyberattaques, devenues courantes dans le monde des affaires. De nombreux services, y compris ceux connectés à des réseaux mondiaux, sont exposés au risque d'attaques de la part de groupes de pirates informatiques et de logiciels malveillants. Heureusement, ces services conservent divers journaux. La réponse aux incidents se concentre sur la récupération après ces attaques, en s'appuyant sur une enquête médico-légale qui, à son tour, s'appuie sur ces journaux enregistrés. Dans cette étude, nous explorons les méthodes et les outils modernes développés par la communauté de recherche pour simplifier l'analyse de ces journaux. Notre objectif est de réaliser un état de l'art des études récentes concernant les enquêtes médico-légales sous Windows et l'utilisation de ses fonctionnalités, ainsi que du journal des événements de Windows. Enfin, nous fournissons une comparaison utile des performances et de la complexité en résumant les conclusions empiriques de chaque article et en soulignant les principales différences entre eux.

Glossary

ELK elastic stack (Elasticsearch,logstash,kibana)
SIEM Security information and event management
SIM Security information management
OS Operating System
SEM Security event management
NIST National Institute of Standards and Technology
SANS SysAdmin, Audit, Network and Security
CSIRT Cyber Security Incident Response Team
DFIR Digital Forensics and Incident Response
RAM Random-access memory
NTFS New Technology File System
FAT File Allocation Table
HKCR HKEY CLASSES ROOT
HKLM HKEY LOCAL MACHINE
DLL Dynamic Link Library
DHCP Dynamic Host Configuration Protocol