Laboratorul 5 – Analiza Prefetch

**Scopul** acestui laborator este de a-i învăța pe studenți despre artefactele încorporate în fișierele Prefetch și despre modul de a utiliza aceste fișiere pentru a identifica malware și circumstanțele de infectare.

**Sarcina:**

1. Completați câmpurile libere de mai jos cu informația corespunzătoare, obținută în urma analizei fișierelor!

2. Pentru primele 3 întrebări, de mai jos, creați un writeup (descrieți pe pași cum ați aflat răspuns la întrebările selectate, obligatoriu includeți și capturi de ecran).

**Rezolvarea sarcinilor:**

1. Care fișier a fost executat de cele mai multe ori?
   1. Din ce cale a fost executat acest fișier?
   2. Când a fost pornit acesta pentru prima și ultima dată?
   3. Ce zonă de timp reprezintă?
2. Când a fost instalat Thunderbird?
   1. Când a fost folosit acesta pentru prima oară?
3. A fost vreo operațiune executată din medii detașabile? Ce anume și când? (Sugestie: Referință la Internet Lab.)

**\* Vă rugăm să treceți peste următoarele întrebări până după laboratorul Windows Event Log.**

1. Mergeți înapoi la Laboratorul Event Log, când a fost ultima acțiune de RDP?
   1. Există careva fișiere Prefetch de potențial interes în jurul acestui interval de timp?
   2. Ce este psexesvc.exe? De câte ori a fost executat acesta?
   3. Ce a fost executat cu exact 10 secunde înainte de 9129837.exe? Ce ar putea însemna acest lucru?
   4. Uitați-vă la panoul de jos al fișierelor accesate în primele 10 secunde după executarea 9129837.exe. Observați altceva anormal?

**2. Writeup: Întrebarea 1, 2, 3.**