1. **Tujuan Praktikum**
   1. Memahami konsep dasar forensik memori dan RAM, termasuk tujuan, manfaat, dan pentingnya dalam investigasi forensik digital.
   2. Menguasai teknik live memory acquisition (pengambilan citra memori secara langsung) dan metode pengamanan data memori.
   3. Menggunakan alat forensik untuk menganalisis citra memori dan mengidentifikasi berbagai artefak digital, termasuk proses aktif, koneksi jaringan, file yang diakses, dan aktivitas pengguna.
   4. Melaporkan temuan dari analisis memori dengan menyusun laporan yang lengkap dan terstruktur.
2. **Kompetensi Dasar**
   1. Menjelaskan proses dan teknik pengambilan memori dalam kondisi live.
   2. Menerapkan alat-alat forensik seperti Volatility untuk menganalisis citra memori.
   3. Mengidentifikasi bukti digital terkait aktivitas sistem dan pengguna dalam memori.
   4. Menyusun laporan hasil analisis memori yang dapat diinterpretasikan secara teknis dan non-teknis.
3. **Alat dan Bahan**
   1. Software:
      * Volatility Framework: Alat analisis forensik memori open-source.
      * Magnet RAM Capture atau FTK Imager: Alat untuk melakukan memory acquisition.
   2. Hardware:
      * Komputer atau laptop dengan RAM minimal 4 GB.
      * Sistem operasi Windows/Linux untuk pengambilan memori dan analisis.
   3. File Citra Memori: Jika pengambilan memori tidak dilakukan secara langsung, disediakan file citra memori yang berisi artefak untuk analisis.
   4. Dokumentasi: Buku catatan, log analisis, atau form laporan untuk mendokumentasikan setiap langkah dan hasil temuan.
4. **Dasar Teori**
   1. Forensik Memori: Bidang investigasi digital yang berfokus pada analisis data yang tersimpan di memori (RAM) sistem. RAM berisi data sementara yang dapat mencakup informasi yang sangat berharga seperti proses aktif, aplikasi yang sedang berjalan, sesi login pengguna, serta data sensitif lainnya yang tidak disimpan pada hard disk.
   2. Memory Acquisition: Proses menangkap data dari RAM sistem komputer saat komputer masih hidup (dalam kondisi live). Data yang ditangkap ini tidak akan tersedia lagi setelah sistem dimatikan, sehingga pengambilan memori sangat penting dalam investigasi langsung.
   3. Volatility Framework: Sebuah tool open-source yang dirancang khusus untuk analisis citra memori. Volatility menyediakan berbagai plugin yang memungkinkan ekstraksi data spesifik, seperti daftar proses aktif, daftar DLL yang sedang diakses, serta aktivitas jaringan yang mencurigakan.
5. Prosedur Praktikum
   1. Persiapan Praktikum
      * Pastikan Software Terinstal: Pastikan bahwa Volatility dan Magnet RAM Capture atau FTK Imager sudah terinstal di sistem.

- Cek Kapasitas Penyimpanan: Pastikan ada cukup ruang di penyimpanan untuk menyimpan citra memori.

- Dokumentasi Awal Sistem: Catat informasi awal tentang spesifikasi sistem (misalnya, sistem operasi, versi OS, dan ukuran RAM).

* 1. Proses Pengambilan Citra Memori (Memory Acquisition)
     + Langkah 1: Buka aplikasi Magnet RAM Capture atau FTK Imager.
       - Langkah 2: Pilih opsi untuk mengambil live memory. Setel penyimpanan hasil memory dump pada direktori yang telah ditentukan. Biasanya, format file .mem atau .bin digunakan.
     + Langkah 3: Catat informasi berikut:
       - Waktu pengambilan memori.
       - Versi sistem operasi dan informasi terkait.
       - Lokasi penyimpanan file citra memori.
       - Langkah 4: Selesaikan proses memory acquisition dan pastikan file citra memori aman serta tidak mengalami korupsi.
  2. Analisis Memori dengan Volatility
     + Langkah 1: Arahkan ke direktori Volatility di *command prompt* atau *terminal*.
     + Langkah 2: Identifikasi profile sistem yang sesuai untuk analisis menggunakan perintah berikut:

volatility -f path\_to\_memory\_image imageinfo

Contoh Outout

Suggested Profile(s) : Win7SP1x64, Win7SP0x64

* + - * Langkah 3: Lakukan analisis mendalam menggunakan plugin berikut untuk mengekstrak informasi spesifik:

1. Daftar Proses Aktif: Untuk melihat daftar proses yang berjalan di memori:

volatility -f path\_to\_memory\_image --profile=ProfileName pslist

Output yang relevan:

Offset(V) Name PID PPID Thds Hnds Time

---------- ----------- ---- ---- ---- ---- -----------

0x823c3808 svchost.exe 924 580 11 250 2023-11-06 12:20:01 UTC

1. Mendeteksi Koneksi Jaringan: Untuk melihat koneksi jaringan yang aktif:

volatility -f path\_to\_memory\_image --profile=ProfileName netscan

Output:

Offset(P) Local Address Foreign Address PID

--------- ----------------- ---------------- ---

0x120f0da0 192.168.1.2:52424 172.217.9.78:443 924

1. Daftar DLL yang Dimuat: Untuk melihat DLL yang dimuat oleh proses tertentu:

volatility -f path\_to\_memory\_image --profile=ProfileName dlllist

1. Registry dan Aktivitas Pengguna: Untuk melihat aktivitas pengguna (misalnya pada Windows registry dan shellbags):

volatility -f path\_to\_memory\_image --profile=ProfileName shellbags

* 1. Dokumentasi dan Interpretasi Temuan
     + Langkah Dokumentasi:
* Catat setiap perintah dan hasil yang relevan.
  + - * Temukan proses mencurigakan atau data yang tampak tidak biasa.
    - Interpretasi Hasil:
      * Cari tanda-tanda aktivitas mencurigakan seperti aplikasi yang tidak biasa, port terbuka, atau koneksi ke alamat IP yang tidak dikenal.
      * Jika menemukan aplikasi atau proses yang mencurigakan, lanjutkan dengan analisis lebih mendalam pada PID atau koneksi terkait.

1. Tugas Praktikum
   1. Penyusunan Laporan Analisis:
      * Buat laporan yang mencakup:
        + Detail sistem (waktu pengambilan memori, OS, RAM).
        + Langkah-langkah yang diambil dan alat yang digunakan.
        + Temuan terkait proses, koneksi, aktivitas DLL, dan aktivitas pengguna.
        + Kesimpulan dan rekomendasi berdasarkan temuan.
2. Evaluasi Praktikum

* Ketepatan dan Akurasi dalam Proses Pengambilan Memori: 20%
* Keakuratan dalam Penggunaan Volatility dan Interpretasi Hasil Analisis: 40%
* Kualitas Laporan dan Dokumentasi Hasil Temuan: 40%

1. Referensi dan Bacaan Tambahan
   1. Official Volatility Documentation: https://volatilityfoundation.org
   2. Guide to Computer Forensics and Investigations, 6th Edition, by Bill Nelson, Amelia Phillips, Christopher Steuart.
   3. Tutorial dan Sumber Video di YouTube tentang penggunaan Volatility untuk analisis memori.