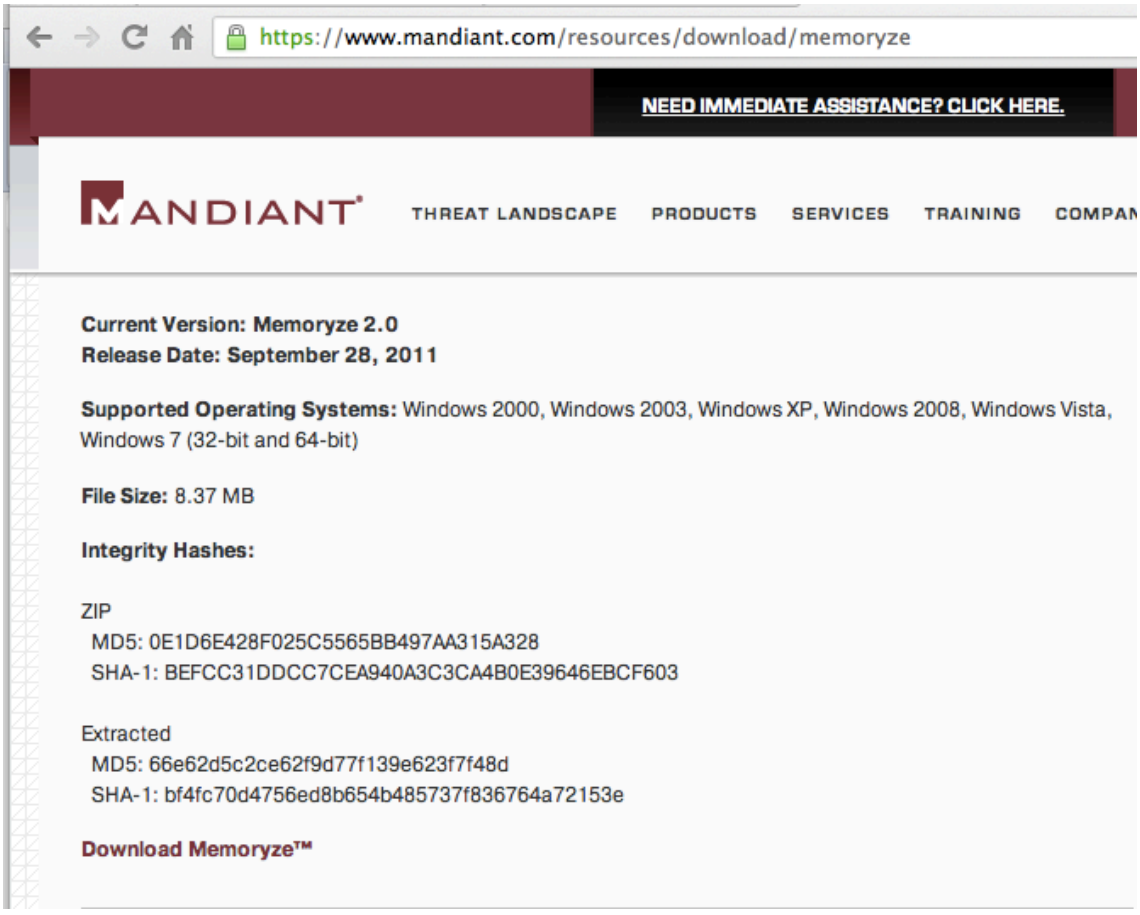
Project 19: RAM Capture dan Analisis

Kebutuhan Project

- Komputer Windows 7, real atau virtual.

Download dan Install Mandiant Memoryze

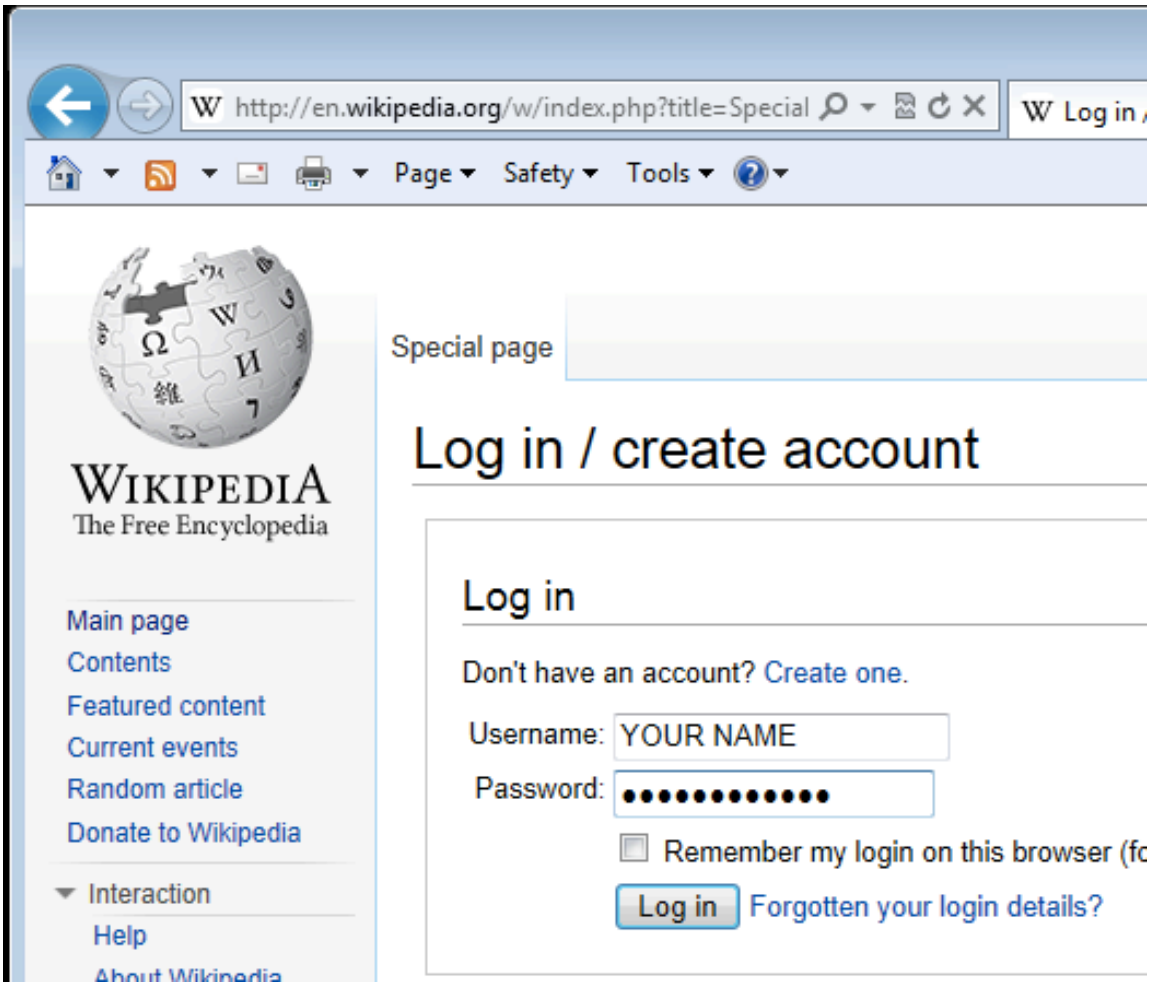
1. Pada browser, arahkan ke
   https://www.mandiant.com/resources/download/memoryze
   Click link "Download Memoryze" (Bisa download juga di elerning), seperti berikut. Verifikasi hash menggunakan HashCalc atau tool yang sama.



2. Klik kanan file **Memoryze.zip** dan click "**Extract All...**". Pada kotak "Extract Compressed (Zipped) Folders", click **Extract**.
   Jendela "Memoryze" terbuka. Double-click folder "Memoryze".
   Double-click file **MemoryzeSetup2.0.msi**.
   Install software dengan default options.

Membuat Prosess Internet Explorer dengan Data

3. Buka Internet Explorer.
4. Arahkan ke http://wikipedia.org dan click **English**.
   Pada bagian atas , click "**log in**".
   Masukan nama kalian untuk user name, masukkan password **SWORDFISH123**, sperti berikut.



5. Click tombol "**Log In**".
   Akan terlihat pesan "Login error". Tidak masalah – kita hanya ingin meletakkan password ke RAM.
6. Biarkan Internet Explorer terbuka.

Menganalisis Live RAM

7. Kita bisa mengkopi RAM image dengan MemoryDD.bat, tapi memakan banyak disk space, maka kita bisa analisa live RAM.

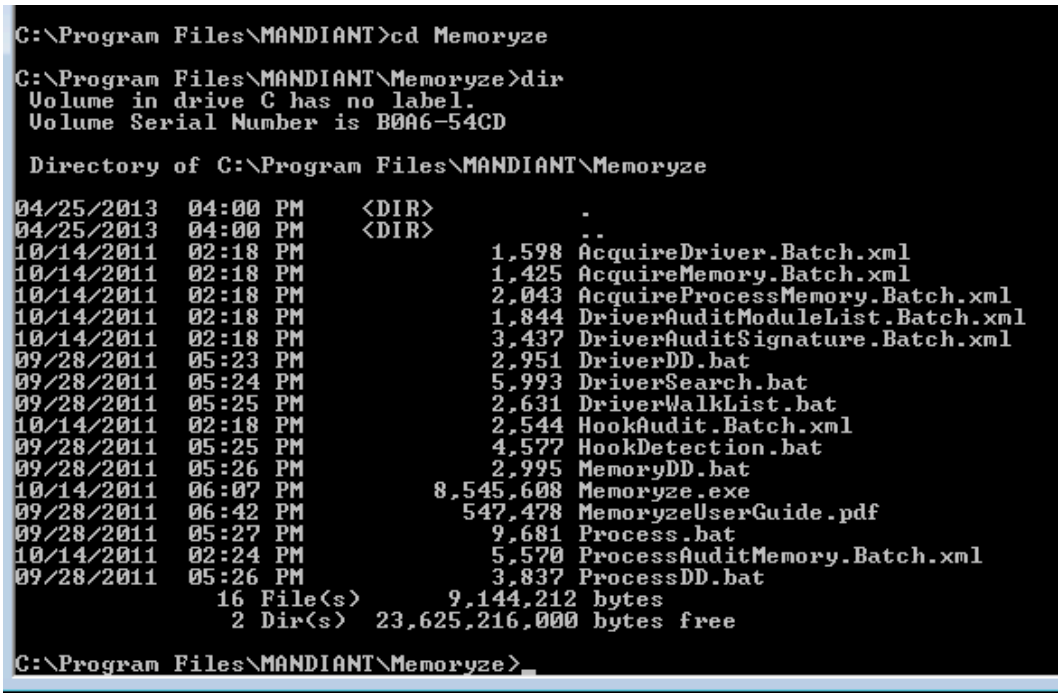
Pada real investigasi, kita harus mengcapture RAM dan setelah itu dianalisis.

Listing Semua Proses

8. Click **Start**, ketikkan **CMD**, dan tekan **Shift+Ctrl+Enter**.
   Pada kotak "User Account Control", click **Yes**.
   Pada jendela Administrator Command Prompt, jalankan perintah berikut diakhiri dengan Enter tiap barisnya:

   ```
   cd \Program Files
   cd MANDIANT\Memoryze
   DIR
   ```

   Maka akan terlihat beberapa programs yang tersedia, termasuk MemoryDD.bat, seperti berikut:

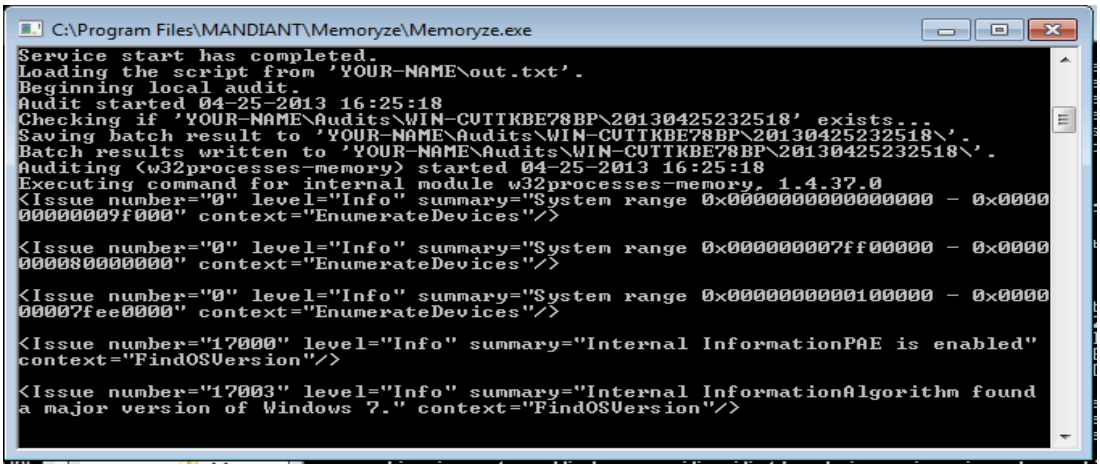


```
C:\Program Files\MANDIANT>cd Memoryze

C:\Program Files\MANDIANT\Memoryze>dir
 Volume in drive C has no label.
 Volume Serial Number is B0A6-54CD

 Directory of C:\Program Files\MANDIANT\Memoryze

04/25/2013  04:00 PM    <DIR>          .
04/25/2013  04:00 PM    <DIR>          ..
10/14/2011  02:18 PM             1,598 AcquireDriver.Batch.xml
10/14/2011  02:18 PM             1,425 AcquireMemory.Batch.xml
10/14/2011  02:18 PM             2,043 AcquireProcessMemory.Batch.xml
10/14/2011  02:18 PM             1,844 DriverAuditModuleList.Batch.xml
10/14/2011  02:18 PM             3,437 DriverAuditSignature.Batch.xml
09/28/2011  05:23 PM             2,951 DriverDD.bat
09/28/2011  05:24 PM             5,993 DriverSearch.bat
09/28/2011  05:25 PM             2,631 DriverWalkList.bat
10/14/2011  02:18 PM             2,544 HookAudit.Batch.xml
09/28/2011  05:25 PM             4,577 HookDetection.bat
09/28/2011  05:26 PM             2,995 MemoryDD.bat
10/14/2011  06:07 PM         8,545,608 Memoryze.exe
09/28/2011  06:42 PM           547,478 MemoryzeUserGuide.pdf
09/28/2011  05:27 PM             9,681 Process.bat
10/14/2011  02:24 PM             5,570 ProcessAuditMemory.Batch.xml
09/28/2011  05:26 PM             3,837 ProcessDD.bat
              16 File(s)      9,144,212 bytes
               2 Dir(s)  23,625,216,000 bytes free

C:\Program Files\MANDIANT\Memoryze>_
```

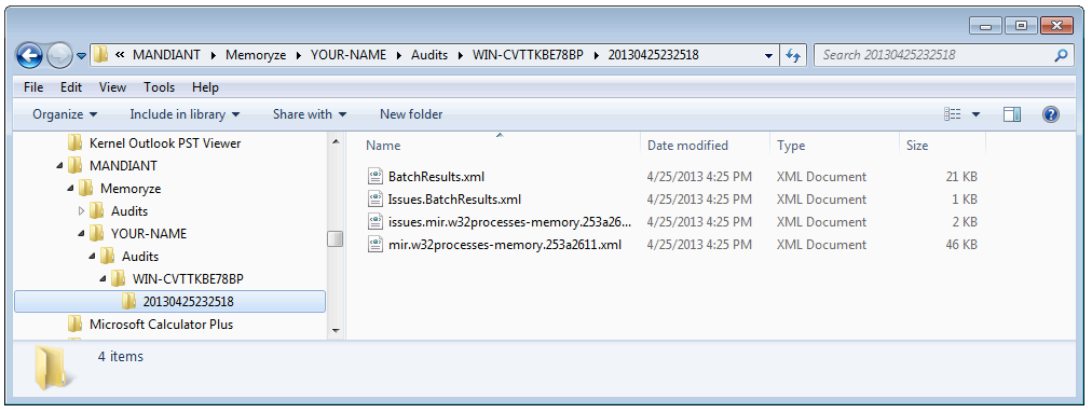
   Pada jendela Administrator Command Prompt, jalankan perintah berikut, diakhiri Enter tiap barisnya.
   Ganti "YOUR-NAME" dengan nama masing-masing, tulis tanpa spasi.

   ```
   mkdir YOUR-NAME
   Process.bat -output YOUR-NAME
   ```

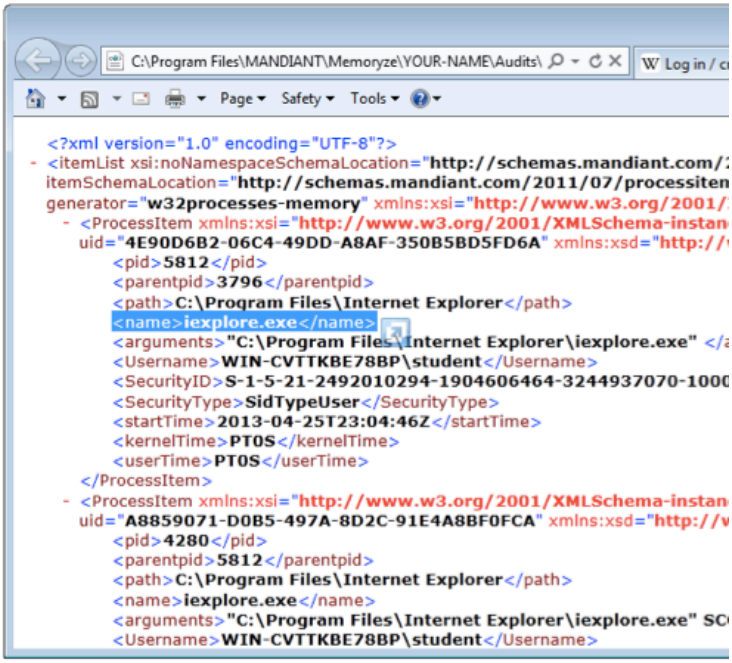
   Baris kedua jendela pops up akan tampil, memperlihatkan progress analysis, seperti berikut.
   Tunggu kotak menutup sendiri.



9. Untuk melihat hasilnya, click **Start**, **Computer**.
   Arahkan ke **C:\Program Files\MANDIANT\Memoryze\YOUR-NAME\Audits**
10. Buka folder di dalam folder Audits, dengan nama komputer di dalamnya.
11. Buka folder dengan nama awalan angka yang panjang dimulai dengan tahun ini.
    Akan terlihat beberapa files XML, seperti terlihat di bawah ini:



12. Double-click file dengan nama panjang yang berawalan **mir**.
    Sederetan proses yang terbuka di Internet Explorer, seperti berikut ini:



Cari proses dengan dengan nama **iexplore.exe** dan sorot baris tersebut, seperti terlihat di atas.

Simpan Screen Image

13. Pastikan di layar terlihat **iexplore.exe** dipilih. Simpan screen image dengan nama file "**NamaKamu_ Proj19a**".

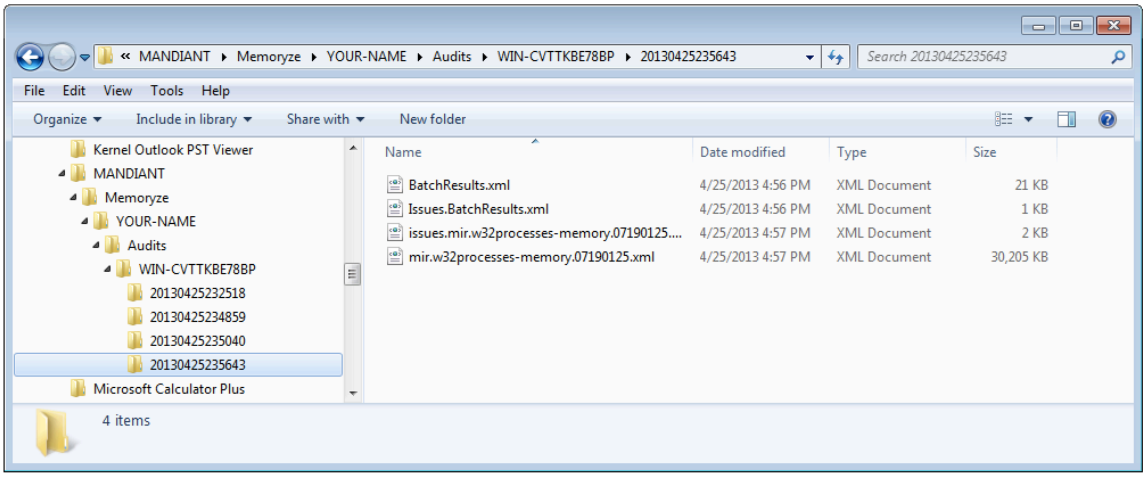
Capture Strings dari Internet Explorer Process Memory

14. Pada jendela Administrator Command Prompt, jalankan perintah berikut. Ganti "YOUR-NAME" dengan nama masing-masing, tanpa spasi.

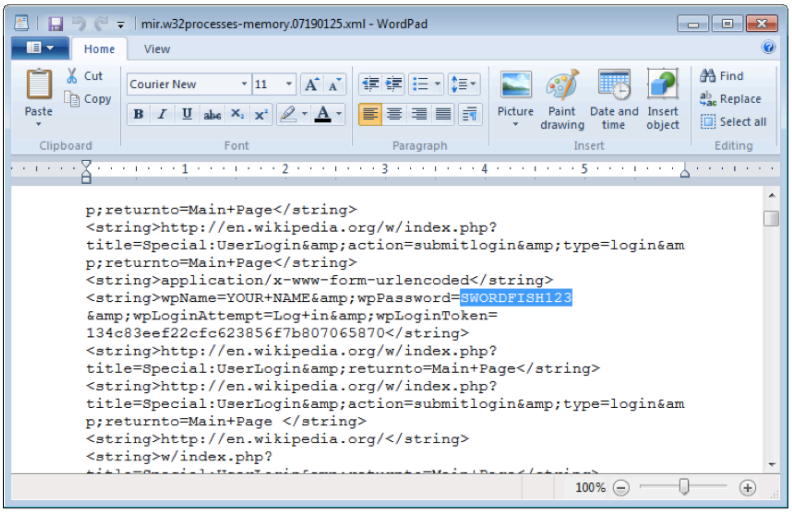
```
Process.bat -output YOUR-NAME -process iexplore.exe -strings true
```

Jendela command prompt pops up, memperlihatkan progress analysis. Tunggu hingga kotak tertutup. Untuk melihat hasil, click **Start**, **Computer**.

15. Arahkan ke **C:\Program Files\MANDIANT\Memoryze\YOUR-NAME\Audits**
16. Buka folder di dalam Audits folder, dengan nama komputer di dalamnya. Buka folder dengan nama berupa deretan angka yang bermula dengan tahun. Jika ada lebih dari satu folder, buka yang paling bawah.
    Akan terlihat beberapa file XML, seperti berikut.



17. Cari file berukuran besar (di contoh 30 MB) dengan nama panjang berawalan dengan **mir**.
    JANGAN DI DOUBLE-CLICK! Jika dilakukan akan membekukan Internet Explorer.
18. Yang dilakukan, click kanan dan buka dengan Wordpad.
    Click jendela Wordpad, dan tekan **Ctrl+F**.
    Cari kata string **SWORDFISH**
    Akan terlihat, seperti berikut.



Simpan Screen Image

19. Pastikan di layar terlihat **SWORDFISH123** yang disorot. Simpan screen image dengan namafile "**NamaKamu_ Proj19b**".

Mengumpulkan Project

20. Kirim melalui elearning.

Sumber

http://www.subhashdasyam.com/2011/10/mandiant-memoryze-is-free-memory.html

Last Modified: 28-5-13