

Forensik Digital

SEMESTER GENAP T.A 2023/2024

LAB 1

Memory Image Forensic



**Program Studi Informatika
Fakultas Teknologi Industri
Universitas Atma Jaya Yogyakarta**



REQUIREMENT

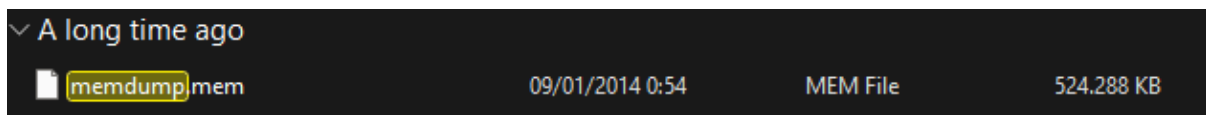
1. Autopsy (instalasi dapat dilihat di tutorial instalasi yang ada di situs kuliah)
2. Memory Image: klik [disini](#) untuk mendownload memory image

PENJELASAN

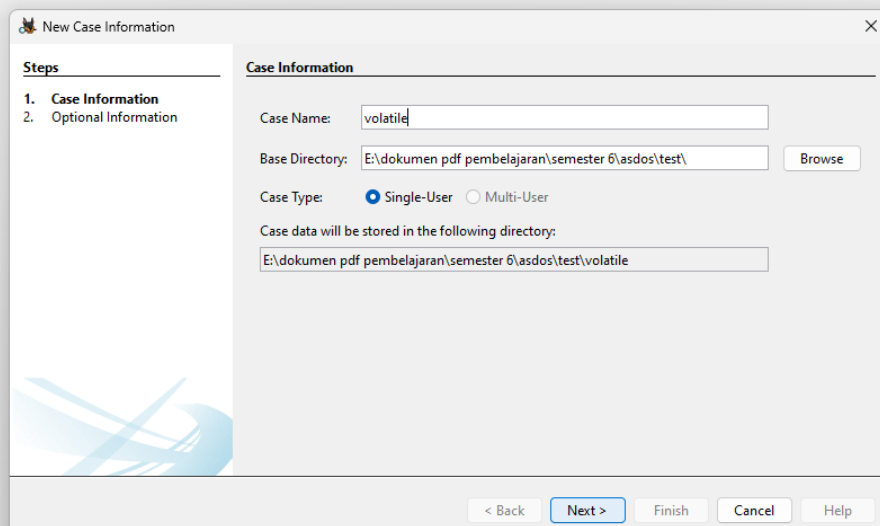
Memory Image adalah proses pengambilan snapshot dari memori yang volatile pada sebuah sistem komputer pada titik waktu tertentu. Tujuan dari Memory Image sendiri adalah meekam kondisi memori sistem pada waktu tertentu, yang kemudian dapat digunakna untuk analisis atau investigasi. Dalam kesempatan kali ini kita akan menggunakan autopsy untuk melakukan Memory Image Forensic.

TUTORIAL

Extract lah file yang sudah didownload pada requirement diatas.



File akan memiliki extensi mem file, setelah itu buka autopsy teman-teman dan buatlah sebuah case baru dengan penamaan bebas.



New Case Information

Steps

1. Case Information
2. Optional Information

Optional Information

Case Number:

Examiner

Name:

Phone:

Email:

Notes:

Organization

Organization analysis is being done for: Not Specified Manage Organizations

< Back Next > **Finish** Cancel Help

Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

Hosts are used to organize data sources and other data.

☒ Generate new host name based on data source name

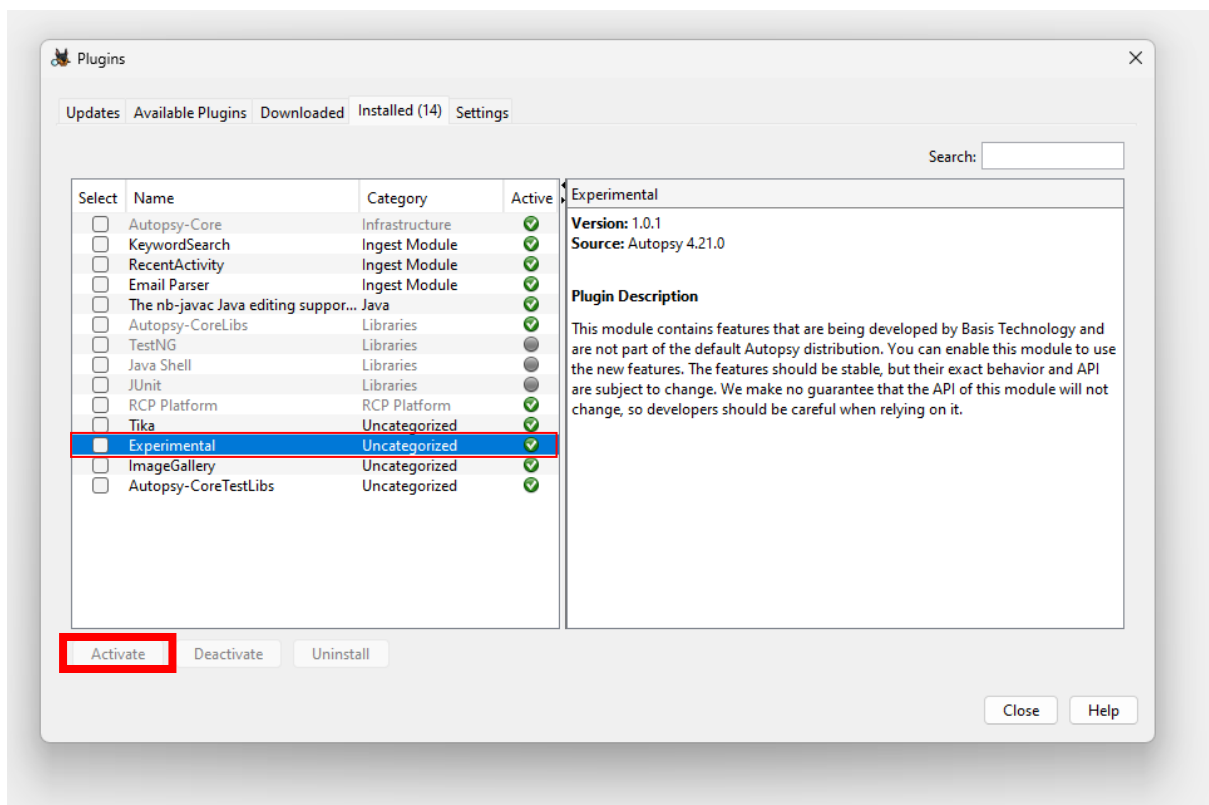
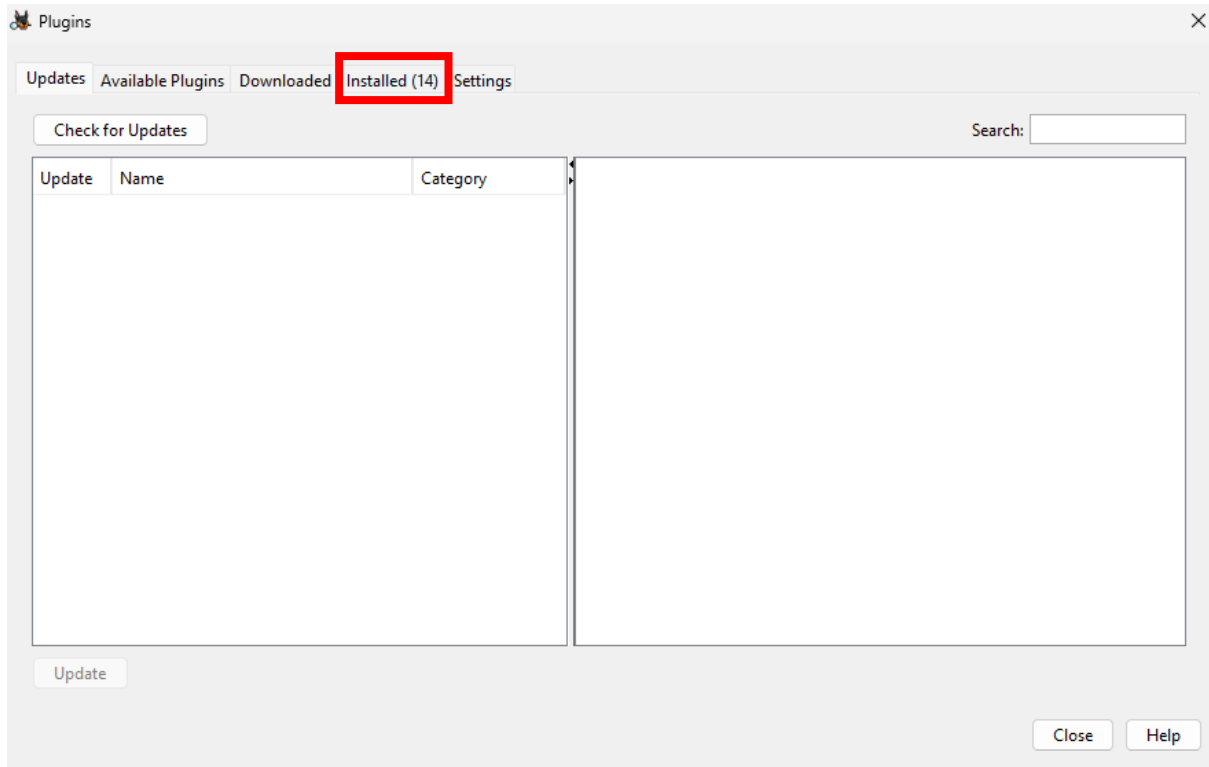
☐ Specify new host name

☐ Use existing host

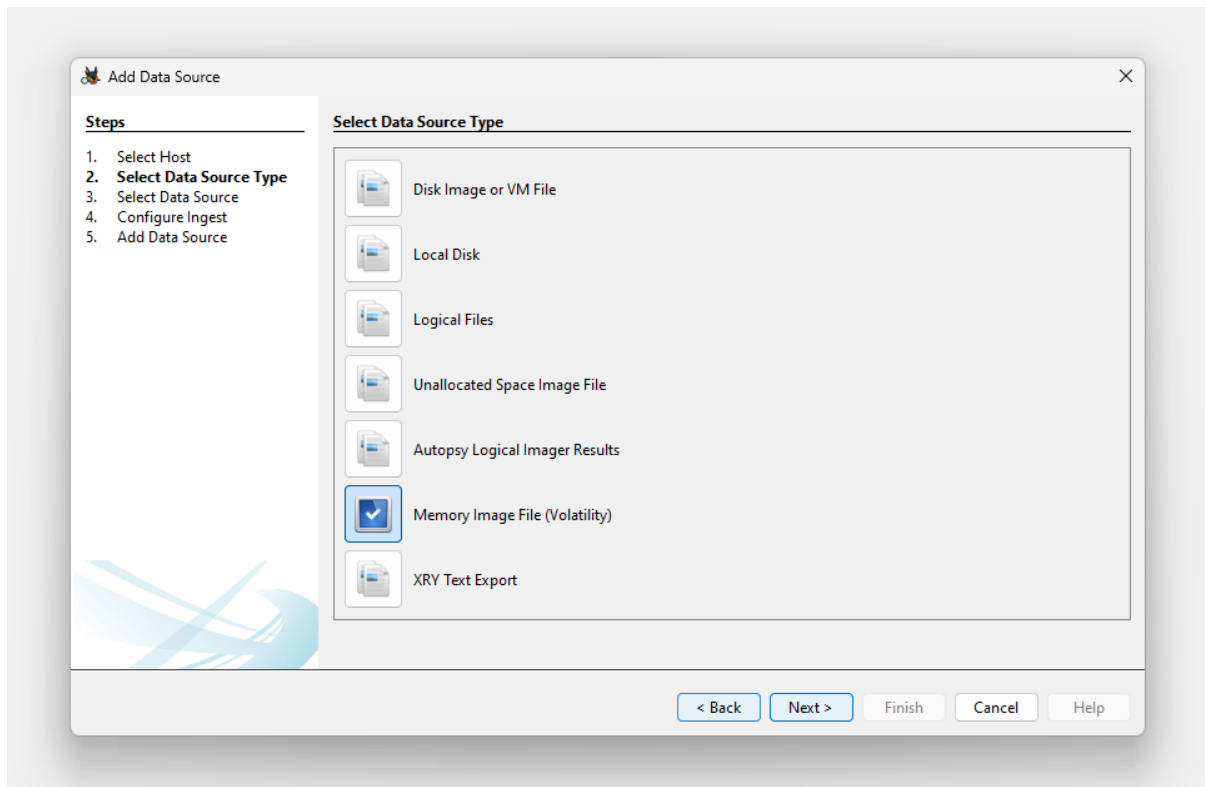
< Back **Next >** Finish Cancel Help

Setelah itu, pada bagian “Select Data Source Type” pilih Memory image disk(Volatility). Jika tidak ada opsi tersebut, teman-teman dapat mengatur nya di tool->Plugin->installed->experimental->Active

- Images/Videos
- Communications
- Geolocation
- Timeline
- Discovery
- Auto Ingest Dashboard
- File Search by Attributes
- Search Central Repository
- Find Common Properties
- Run Ingest Modules >
- Generate Report
- Plugins**
- Python Plugins
- Options
- Personas
- Make Live Triage Drive
- Open Case Folder
- Create Logical Imager



Setelah itu, maka Memory image disk(Volatility).

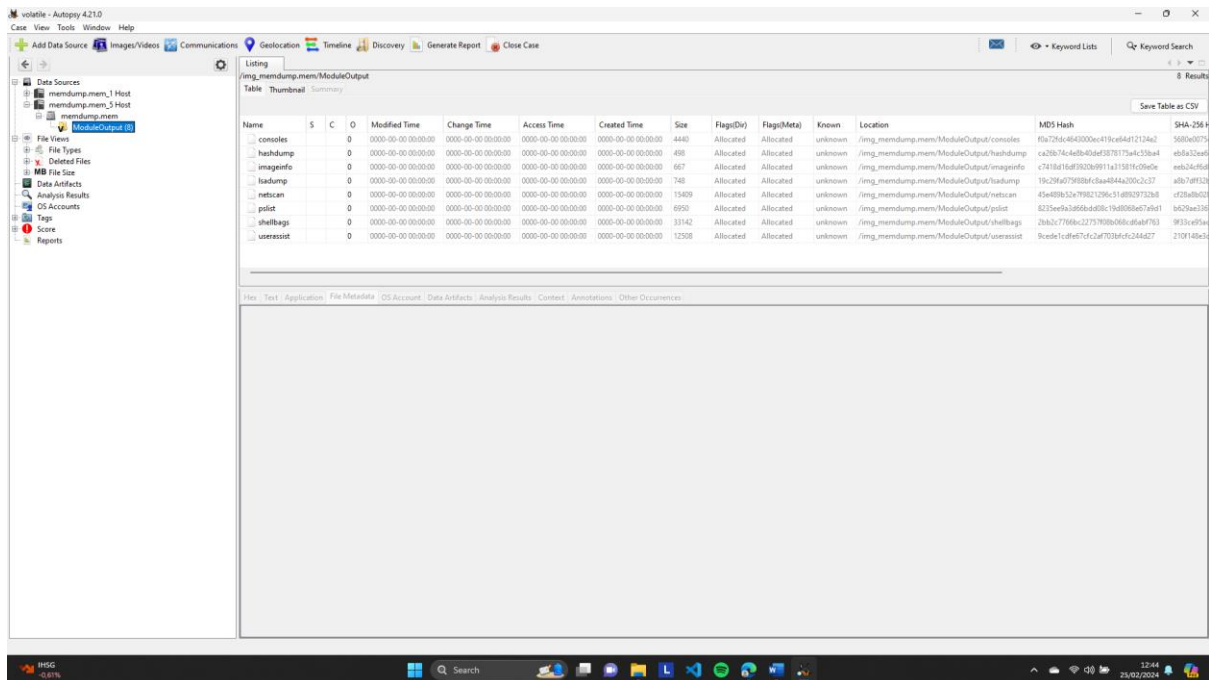


Klik next, lalu browse tempat dimana teman-teman menyimpan file memdump.mem tadi yang sudah di extract. Lalu pada plugin. Cukup ceklis beberapa plugin dibawah ini:

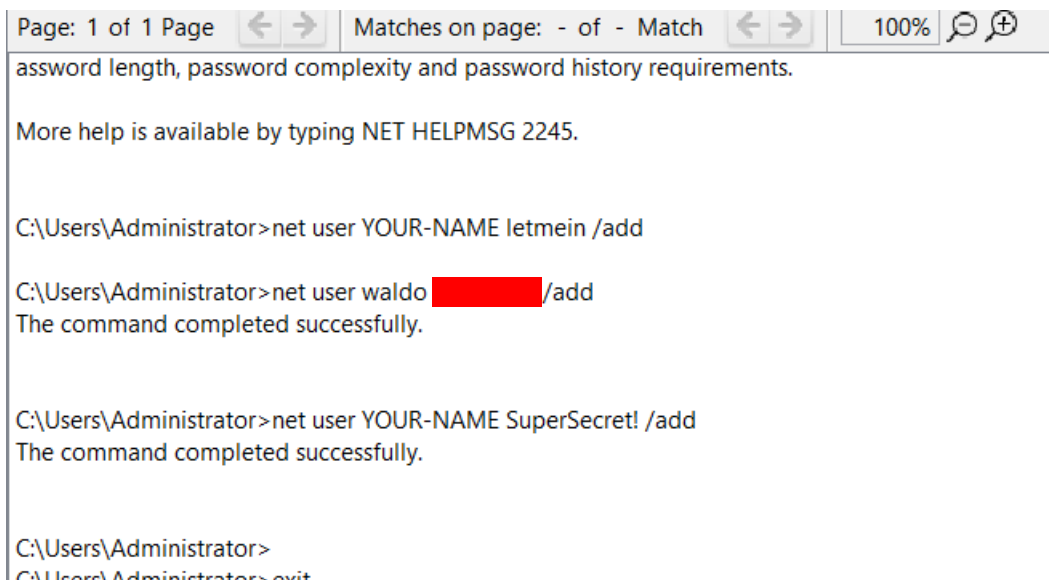
- Consoles (untuk mengekstrak informasi konsol yang berjalan)
- Hashdump (untuk mengekstrak nilai hash dari password pengguna)
- Isadump (untuk mengekstrak informasi ruang alamat ISA)
- Netscan (untuk pemindaian jaringan pada memori sistem)
- Pslist (untuk mengekstrak daftar proses yang berjalan pada sistem)
- Shellbags (untuk mengekstrak informasi tentang shellbags dalam sistem)
- Userassist (untuk mengekstrak informasi tentang penggunaan aplikasi)

Setelah itu tinggal next dan finish.

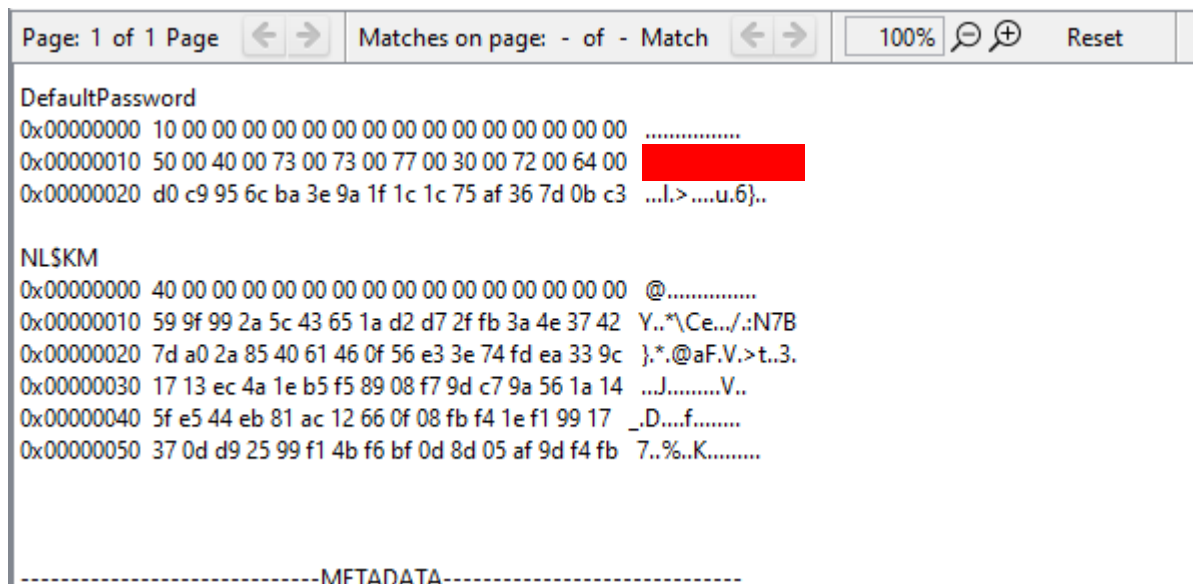
Berikut adalah tampilan awal dari autopsy jika teman-teman sudah melakukannya dengan benar.



- Buka Consoles dan carilah “waldo’s password” yang tertutup pada gambar dibawah.



- Buka isadump dan carilah password default, yang tertutup pada gambar dibawah.



- Buka netscan dan carilah executable listening di port 8080, yang tertutup pada gambar dibawah.

Strings		Extracted Text		Translation	
Page: 1 of 1 Page		Matches on page: - of - Match		100% Reset	
0x1e5e96e8	TCPv4	127.0.0.1:53	0.0.0.0:0	LISTENING	1480 dns.exe
0x1e5e9ad0	TCPv4	192.168.119.191:53	0.0.0.0:0	LISTENING	1480 dns.exe
0x1e5ec3d0	TCPv4	0.0.0.0:1028	0.0.0.0:0	LISTENING	1480 dns.exe
0x1e5ec3d0	TCPv6	:::1028	:::0	LISTENING	1480 dns.exe
0x1e5f7ca8	TCPv4	0.0.0.0:21	0.0.0.0:0	LISTENING	1508 ftpbasicsvr.exe
0x1e5f92c0	TCPv4	0.0.0.0:8080	0.0.0.0:0	LISTENING	1508 [REDACTED]
0x1e966e10	TCPv4	0.0.0.0:1030	0.0.0.0:0	LISTENING	616 lsass.exe
0x1e966e10	TCPv6	:::1030	:::0	LISTENING	616 lsass.exe
0x1e966f60	TCPv4	0.0.0.0:1030	0.0.0.0:0	LISTENING	616 lsass.exe
0x1e9c7598	TCPv4	0.0.0.0:1026	0.0.0.0:0	LISTENING	884 svchost.exe
0x1e9f9300	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	848 svchost.exe
0x1e9f9300	TCPv6	:::135	:::0	LISTENING	848 svchost.exe
0x1e9faf60	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	848 svchost.exe
0x1e9ff148	TCPv4	0.0.0.0:1025	0.0.0.0:0	LISTENING	524 wininit.exe
0x1e9ff148	TCPv6	:::1025	:::0	LISTENING	524 wininit.exe
0x1e143e10	TCPv4	54.213.58.70:80	54.213.58.70:80	CLOSED	1888 iexplore.exe

- Pada bagian shellbags carilah shared folder yang terhubung dengan mesin ini, yang tertutup pada gambar dibawah.

```

1 0 Control Panel 8e908fc9-becc-40fb-913b-14ca0e/0d05d Network and Sharing Center EXPLORER, MY_GAMES
0 1 Control Panel 7007acc7-3202-11d1-aad2-00805fc1270e Unknown GUID EXPLORER, MY_GAMES
*****

Registry: \Device\HarddiskVolume1\Users\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\0
Last updated: 2013-06-01 15:44:19 UTC+0000
Value Mru File Name Modified Date Create Date Access Date File Attr Path
-----
0 0 [REDACTED] 2013-05-29 17:31:36 UTC+0000 2013-03-29 20:19:20 UTC+0000 2013-06-01 15:30:14 UTC+0000 DIR \vmware-host\Shared Folders\[REDACTED]
*****

Registry: \Device\HarddiskVolume1\Users\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\0\0
Last updated: 2013-06-01 15:44:49 UTC+0000

```

- Pada bagian userassist, carilah nama dangerous executable yang berjalan pada 13-09-2013 pukul 23:12:30, yang tertutup pada gambar dibawah.

```

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annota
Strings Extracted Text Translation
Page: 1 of 1 Page < > Matches on page: - of - Match < > 100% [REDACTED] [REDACTED] Reset
REG_BINARY UEME_RUNPATH=C:\Users\Administrator\Downloads\PI2.3.2\[REDACTED]
ID: 3
Count: 1
Last updated: 2013-09-12 23:07:27 UTC+0000
Raw Data:
0x00000000 03 00 00 00 06 00 00 00 a0 1d 4f d9 0c b0 ce 01 .....O.....

REG_BINARY UEME_RUNPATH=C:\Users\Administrator\Downloads\PI2.3.2\[REDACTED] :
ID: 3
Count: 6
Last updated: 2013-09-13 23:12:30 UTC+0000
Raw Data:
0x00000000 03 00 00 00 0b 00 00 00 00 d8 8a b8 d6 b0 ce 01 .....

REG_BINARY UEME_RUNPATH=C:\Users\Administrator\Downloads\PI2.3.2\evil2.exe :
ID: 3
Count: 2

```

- Carilah password dari akun probe di bagian hashdump. Setelah ketemu, cobalah untuk melakukan decrypt pada hash code tersebut.