Rachel Gully

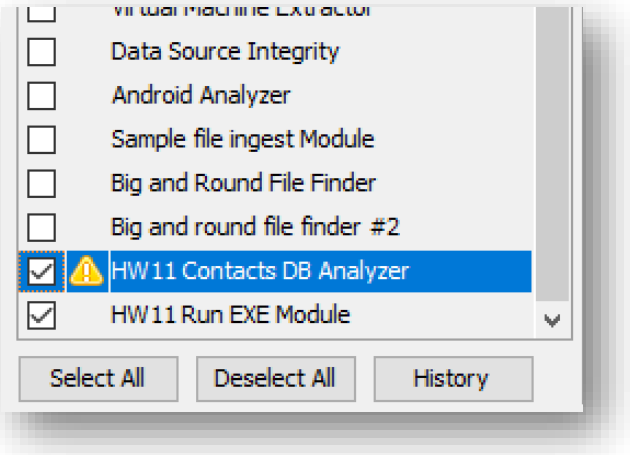
CFRS 772 – Homework 11

April 15th, 2019

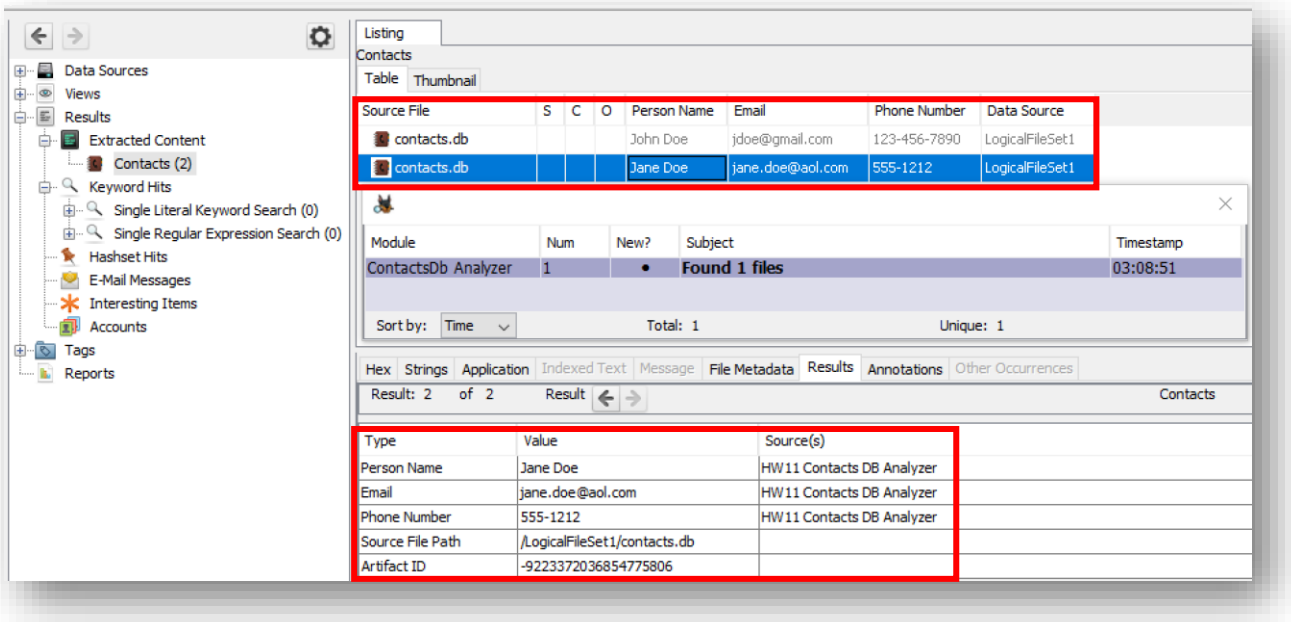
1. Result of running the Volatility “MyPlugin” against vm.vmem.

```
E:\Tools\Volatility>vol_2.6_x64.exe --plugins="E:\GMU DFCA\CFRS 772\Projects\Homework 11\PLUGINS" -f "E:\GMU DFCA\CF
RS 772\Projects\Homework 11\vm.vmem" --profile=WinXPSP2x86 myplugin
Volatility Foundation Volatility Framework 2.6
PID  Created                  Image
   4 1970-01-01 00:00:00 UTC+0000 System
 548 2014-09-04 15:41:28 UTC+0000 smss.exe
 620 2014-09-04 15:41:31 UTC+0000 csrss.exe
 644 2014-09-04 15:41:32 UTC+0000 winlogon.exe
 688 2014-09-04 15:41:32 UTC+0000 services.exe
 700 2014-09-04 15:41:32 UTC+0000 lsass.exe
 800 2014-09-04 15:41:32 UTC+0000 vmacthlp.exe
 884 2014-09-04 15:41:33 UTC+0000 svchost.exe
 980 2014-09-04 15:41:33 UTC+0000 svchost.exe
1084 2014-09-04 15:41:33 UTC+0000 svchost.exe
1160 2014-09-04 15:41:34 UTC+0000 svchost.exe
1272 2014-09-04 15:41:34 UTC+0000 svchost.exe
1532 2014-09-04 15:41:35 UTC+0000 explorer.exe
1600 2014-09-04 15:41:35 UTC+0000 spoolsv.exe
1716 2014-09-04 15:41:35 UTC+0000 vmtoolsd.exe
2020 2014-09-04 15:41:52 UTC+0000 vmtoolsd.exe
 500 2014-09-04 15:42:00 UTC+0000 wscntfy.exe
1288 2014-09-04 15:42:02 UTC+0000 alg.exe
1052 2014-09-04 15:42:45 UTC+0000 wuauclt.exe
1328 2014-09-04 15:42:59 UTC+0000 wuauclt.exe
1252 2014-09-04 15:43:23 UTC+0000 cmd.exe
1136 2014-09-10 16:46:07 UTC+0000 wmiprvse.exe
1676 2014-09-10 16:46:55 UTC+0000 cmd.exe
1364 2014-09-10 16:46:55 UTC+0000 ipconfig.exe
```

2. Listing of current Autopsy ingest modules, highlighting the “HW11” additions.



3. Result of running the Autopsy “HW11 Data Source Module” against contacts.db.



4. Result of running the Autopsy “Run Exe” Ingest Module against “control.dd” from https://www.cfreds.nist.gov/Controlv1_0/DCFL_Control_Standard_V1_0.html.