تقرير التحليل الجنائي لذاكرة النظام

اسم الطالب: محمد حيدر المعمري

---

1. مقدمة

يُعد تحليل الذاكرة العشوائية (Memory Forensics) أحد الأساليب المهمة في التحقيقات الجنائية الرقمية؛ إذ يتيح فحص البيانات التي كانت موجودة في ذاكرة الحاسوب وقت التقاط صورة الذاكرة.

تحتوي الذاكرة على معلومات مفيدة للتحقيق، مثل العمليات قيد التشغيل، والعلاقات بين العمليات، ومسارات الملفات التنفيذية، وبعض الآثار المرتبطة بالأنشطة الضارة.

في هذه التجربة، جرى التركيز على فحص صورة ذاكرة باسم `infected.vmem` باستخدام أداة Volatility 3، بهدف تحديد العملية المشبوهة، وتتبع علاقتها بالعمليات الأخرى، ومعرفة مسار تشغيل الملف الضار، والتعرف على مؤشرات الإصابة ببرمجية الفدية WannaCry.

1.1 أهداف التحقيق

1. تحديد العملية التي تظهر عليها مؤشرات النشاط المشبوه.
2. معرفة رقم العملية الأب (PPID) للعملية المشبوهة.
3. تحليل شجرة العمليات لتتبع العلاقات بين العمليات.
4. البحث عن عملية يُشتبه في ارتباطها بحذف ملفات الضحية.
5. تحديد المسار الذي شُغِّل منه الملف التنفيذي المشبوه.
6. تحديد عائلة برمجية الفدية المحتملة.
7. البحث عن ملف المفتاح ذي الامتداد `eky.`.

1.2 بيئة التحليل

- نظام التشغيل المستهدف: Windows.
- نوع الدليل الرقمي: صورة ذاكرة.
- ملف الإدخال: `infected.vmem`.

- أداة التحليل: Volatility 3.
- مجلد حفظ النتائج: `Mohammed_MemoryLab\Analysis`.

> ملاحظة منهجية: يجب تسجيل إصدار Volatility الفعلي وبيئة التشغيل المستخدمة عند تنفيذ الأوامر. ولا ينبغي اعتبار الأوامر المنفذة أو النتائج المذكورة في هذا التقرير دليلاً على إعادة تنفيذ التحليل ما لم تكن مدعومة بمخرجات فعلية أو لقطات شاشة.

```
C:\MemoryLab>sc query winpmem

SERVICE_NAME: winpmem
        TYPE               : 1  KERNEL_DRIVER
        STATE              : 4  RUNNING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

```
C:\MemoryLab>mkdir D:\Mohammed_MemoryLab\Analysis

C:\MemoryLab>mkdir D:\Mohammed_MemoryLab\Report
```

2. السؤال الأول: ما اسم العملية المشبوهة؟

الأمر المستخدم

```
python vol.py -f infected.vmem windows.pslist.PsList
```

شرح الأداة

تُستخدم إضافة `PsList` لعرض العمليات التي يمكن العثور عليها في قائمة عمليات Windows الموجودة في صورة الذاكرة.

تتضمن النتائج عادةً اسم العملية، ومعرّف العملية (PID)، ومعرّف العملية الأب (PPID)، إضافة إلى معلومات أخرى تساعد المحقق على فهم العمليات الموجودة في النظام.

النتائج والتحليل

أثناء مراجعة قائمة العمليات، ظهرت عملية باسم:

`or4qtckT.exe`

وكانت معلوماتها كما يلي:

- **PID:** `2732`
- **PPID:** `1456`

يبدو اسم العملية غير مألوف مقارنةً بأسماء العديد من عمليات Windows المعروفة، ولذلك استدعى مزيدًا من الفحص.

ومع ذلك، فإن غرابة الاسم وحدها لا تثبت أن الملف ضار؛ بل يجب ربط هذه الملاحظة بمعلومات أخرى، مثل علاقة العملية بعمليات الفدية ومسار الملف التنفيذي.

الاستنتاج

تم تحديد العملية `or4qtckT.exe` بوصفها عملية مشبوهة تستحق التحليل الإضافي.

الإجابة: `or4qtckT.exe`

مكان إدراج الصورة: ضع لقطة شاشة تظهر اسم العملية وحقلي PID وPPID من نتائج `PsList` .

```
2732    1456    or4qtckT.exe    0x83ed4350      8       79      1       False   2021-01-31 18:02:16.000000      N/A     Disable
d
```

---

3. السؤال الثاني: ما قيمة PPID للعملية المشبوهة؟

الأمر المستخدم

```
python vol.py -f infected.vmem windows.pslist.PsList
```

شرح الأداة

يمثل الحقل `PID` معرّف العملية نفسها، بينما يمثل الحقل `PPID` معرّف العملية الأب التي ارتبط إنشاء العملية بها.

تساعد هذه القيم على بناء تصور عن تسلسل تشغيل العمليات، لكنها لا تثبت بمفردها أن العملية الأب هي التي أنشأت العملية فعليًا في جميع الظروف؛ لذا تُراجع النتائج مع شجرة العمليات وأدلة الذاكرة الأخرى.

النتائج والتحليل

أظهرت نتائج العملية المشبوهة المعلومات التالية:

الحقل	القيمة
اسم العملية	`or4qtckT.exe`
PID	`2732`
PPID	`1456`

تشير البيانات إلى أن معرّف العملية الأب للعملية المشبوهة هو `1456`.

وبحسب تحليل شجرة العمليات الوارد في نتائج هذه العينة، يرتبط هذا المعرّف بالعملية `explorer.exe`.

الاستنتاج

قيمة PPID المسجلة للعملية المشبوهة هي `1456`.

الإجابة: `1456`

مكان إدراج الصورة: ضع لقطة شاشة لنتائج `PsList` التي تعرض العملية ومعرّفاتها.

---

4. السؤال الثالث: ما الملف التنفيذي الضار الذي أنشأ العملية المرتبطة ببرمجية الفدية؟

الأمر المستخدم

```
python vol.py -f infected.vmem windows.pstree.PsTree
```

شرح الأداة

تُستخدم إضافة `PsTree` لعرض العمليات في صورة هرمية توضح علاقات الأبوة بين العمليات.

يساعد هذا العرض في تتبع تسلسل العمليات وفهم كيفية ارتباط عملية مشبوهة بعمليات أخرى، بما فيها العمليات التي قد تكون مرتبطة بنشاط ضار.

النتائج والتحليل

وفقًا لشجرة العمليات التي جرى وصفها في نتائج العينة، ظهر التسلسل التالي:

```
                                        explorer.exe
                                              |
                                    or4qtckT.exe --+
                                              |
                                  WanaDecryptor@ --+
```

وتتضمن العلاقات المسجلة:

- `explorer.exe` — PID `1456`
- `or4qtckT.exe` — PID `2732`
- `@WanaDecryptor` — PID `3968`

يشير هذا التسلسل إلى ارتباط العملية `or4qtckT.exe` بعملية تحمل اسمًا مرتبطًا ببرمجية الفدية.

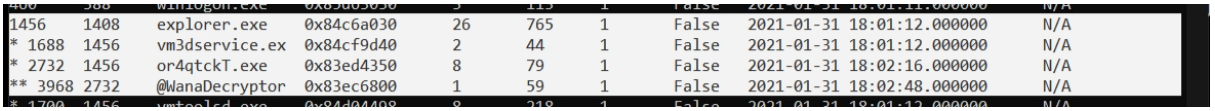
ومن المهم التمييز بين العملية التي أنشأت عملية أخرى والملف الذي بدأ الهجوم في الأصل؛ فقد يكون الملف التنفيذي المشبوه جزءًا من سلسلة تنفيذ أوسع. لذلك تُصاغ النتيجة هنا بناءً على علاقة العمليات الظاهرة في العينة، وليس على افتراض أن شجرة العمليات وحدها تثبت جميع مراحل الإصابة.

الاستنتاج

تدعم شجرة العمليات الاشتباه في أن `or4qtckT.exe` هو الملف التنفيذي المرتبط بإنشاء عملية الفدية الظاهرة في العينة.

الإجابة: `or4qtckT.exe`

مكان إدراج الصورة: أدرج لقطة شاشة من `PsTree` توضح العمليات الثلاث والعلاقات بينها.



1456	1408	explorer.exe	0x84c6a030	26	765	1	False	2021-01-31 18:01:12.000000	N/A
* 1688	1456	vm3dservice.ex	0x84cf9d40	2	44	1	False	2021-01-31 18:01:12.000000	N/A
* 2732	1456	or4qtckT.exe	0x83ed4350	8	79	1	False	2021-01-31 18:02:16.000000	N/A
** 3968	2732	@WanaDecryptor	0x83ec6800	1	59	1	False	2021-01-31 18:02:48.000000	N/A

5. السؤال الرابع: ما العملية المرتبطة بحذف ملفات الضحية؟

الأمر المستخدم

```
python vol.py -f infected.vmem windows.psscan.PsScan
```

شرح الأداة

تقوم إضافة `PsScan` بالبحث في الذاكرة عن هياكل العمليات، وقد تكشف عن عمليات لا تظهر في قائمة `PsList`، بما فيها بعض العمليات المنتهية أو غير المدرجة في القائمة المعتادة.

تُعد مقارنة نتائج `PsList` و`PsScan` مفيدة في التحقيق؛ لأنها قد تساعد على اكتشاف عمليات إضافية تحتاج إلى الفحص.

النتائج والتحليل

وفقًا للنتائج الواردة في العينة، ظهرت عملية باسم:

`taskdl.exe`

بالمعلومات التالية:

- **PID:** `4060`
- **PPID:** `2732`

يرتبط معرّف العملية الأب `2732` بالعملية المشبوهة `or4qtckT.exe`.

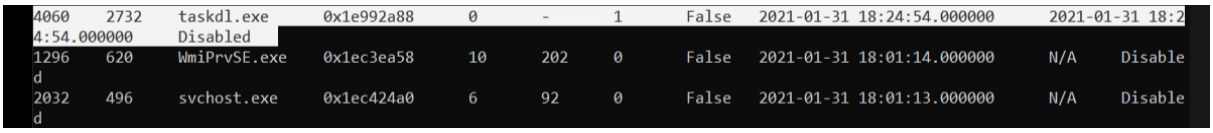
ويُشتبه في ارتباط `taskdl.exe` بنشاط حذف الملفات ضمن سلسلة الإصابة. لكن ينبغي الانتباه إلى أن اسم العملية وعلاقة الأبوة وحدهما لا يثبتان تنفيذ عملية حذف فعلية؛ ويُفضّل تأكيد ذلك من خلال أدلة إضافية، مثل آثار الملفات، أو سجلات النظام، أو نتائج تحليل سلوك البرمجية.

الاستنتاج

تم تحديد `taskdl.exe` باعتبارها العملية المرتبطة بنشاط حذف الملفات وفقًا لتفسير نتائج العينة.

الإجابة: `taskdl.exe`

مكان إدراج الصورة: أدرج لقطة شاشة من `PsScan` توضح اسم العملية وPID وPPID.



---

6. السؤال الخامس: من أي مسار شُغّل الملف التنفيذي المشبوه؟

الأمر المستخدم

```
python vol.py -f infected.vmem windows.cmdline.CmdLine
```

شرح الأداة

تُستخدم إضافة `CmdLine` لاستخراج معلومات سطر الأوامر المرتبطة بالعمليات التي يمكن تحليلها من صورة الذاكرة.

قد تتضمن النتائج مسار الملف التنفيذي والمعاملات التي استُخدمت عند تشغيل العملية، مما يساعد المحقق على تحديد موقع الملف الذي ارتبط بالنشاط المشبوه.

النتائج والتحليل

وفقًا للنتيجة المذكورة في العينة، ظهر السجل التالي:

```
"or4qtckT.exe    "C:\Users\hacker\Desktop\or4qtckT.exe    2732
```

يشير هذا السجل إلى المسار التالي:

```
C:\Users\hacker\Desktop\or4qtckT.exe
```

أما المجلد الذي يحتوي على الملف فهو:

```
\C:\Users\hacker\Desktop
```

يساعد تحديد هذا المسار في توجيه التحقيق إلى الملف المرتبط بالعملية، والبحث عن آثار إضافية تخصه. لكنه لا يعني أن الملف ما زال موجودًا على القرص؛ إذ إن بيانات المسار المستخرجة من الذاكرة قد تبقى حتى إذا تغير وضع الملف لاحقًا.

الاستنتاج

يشير سجل سطر الأوامر إلى أن الملف التنفيذي المشبوه شُغّل من مجلد سطح المكتب الخاص بالمستخدم `hacker`.

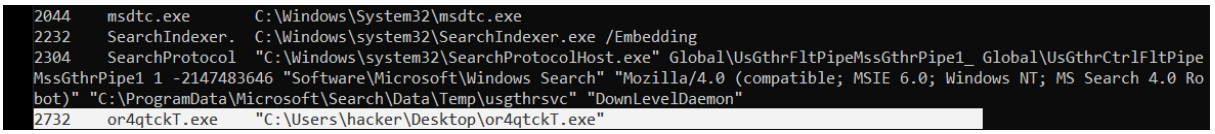
الإجابة الكاملة:

`C:\Users\hacker\Desktop\or4qtckT.exe`

الإجابة المختصرة (المجلد):

`C:\Users\hacker\Desktop\`

مكان إدراج الصورة: أدرج لقطة شاشة من `CmdLine` تُظهر المسار الكامل للعملية.



---

7. السؤال السادس: ما عائلة برمجية الفدية التي تشير إليها آثار الذاكرة؟

الأوامر المستخدمة

لفحص قائمة العمليات:

```
python vol.py -f infected.vmem windows.pslist.PsList
```

ولفحص العلاقات بين العمليات:

```
python vol.py -f infected.vmem windows.pstree.PsTree
```

شرح التحليل

يمكن أن تساعد أسماء العمليات المرتبطة ببرمجيات معروفة في تحديد عائلة البرمجية الضارة المحتملة.

لكن التعرف الدقيق على عائلة برمجية الفدية ينبغي أن يستند إلى مجموعة من المؤشرات، مثل أسماء الملفات والعمليات، وآثار التشفير، والملفات المرتبطة بالهجوم، ورسائل الفدية أو مؤشرات أخرى خاصة بالعائلة.

النتائج والتحليل

ظهرت عملية باسم:

`@WanaDecryptor`

بالمعلومات التالية:

- **PID:** `3968`
- **PPID:** `2732`

وترتبط هذه العملية، وفقًا لشجرة العمليات الموصوفة في العينة، بالعملية `or4qtckT.exe`.

يُعد الاسم `WanaDecryptor@` مؤشرًا يتوافق مع آثار مرتبطة ببرمجية WannaCry، ولذلك يدعم الاشتباه في أن العينة تتعلق بإصابة من هذه العائلة.

الاستنتاج

تدعم الآثار المذكورة تحديد عائلة برمجية الفدية باسم WannaCry، على أن يُستحسن تأكيد هذا الاستنتاج من مؤشرات إضافية داخل العينة.

الإجابة: `WannaCry Ransomware`

مكان إدراج الصورة: ضع لقطة شاشة تُظهر العملية `WanaDecryptor@` وعلاقتها بالعملية المشبوهة.

```
2976   404    conhost.exe      0x85dc25f8  1   33   1   False  2021-01-31 18:02:20.000000  N/A  Disable
d
3968   2732   @WanaDecryptor   0x83ec6800  1   59   1   False  2021-01-31 18:02:48.000000  N/A  Disable
d
2204   496    svchost.exe      0x85ed91c8  11  143  0   False  2021-01-31 18:03:14.000000  N/A  Disable
d
```

---

8. السؤال السابع: ما اسم ملف المفتاح ذي الامتداد EKY؟

الأمر المستخدم

لحفظ نتائج فحص الملفات في ملف نصي:

```
python vol.py -f infected.vmem windows.filescan.FileScan > filescan.txt
```

للبحث عن الملفات التي يظهر في مسارها الامتداد `eky.`:

```
findstr /i ".eky" filescan.txt
```

شرح الأداة

تُستخدم إضافة `FileScan` للبحث في الذاكرة عن هياكل ملفات يمكن التعرف عليها.

قد تساعد هذه العملية في العثور على آثار لملفات مرتبطة بالبرمجيات الضارة، حتى عندما لا يكون من الممكن الوصول إلى الملف مباشرةً على القرص.

جرى توجيه المخرجات إلى ملف نصي باسم `filescan.txt` لتسهيل مراجعتها والبحث داخلها، بدلًا من التعامل يدويًا مع كامل النتائج المعروضة في الطرفية.

النتائج والتحليل

بحسب نتائج العينة المذكورة، ظهر المسار التالي:

```
Users\hacker\Desktop\00000000.eky\
```

اسم الملف هو:

`00000000.eky`

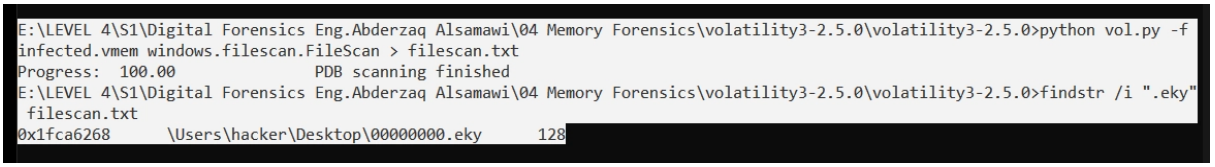
يمثل الامتداد `eky.` مؤشرًا مرتبطًا بملفات مفاتيح التشفير في سياق هذه العينة. ومع ذلك، لا يكفي الامتداد وحده لتحديد وظيفة الملف أو إثبات أنه يحتوي على مفتاح بعينه؛ ويجب تفسيره في ضوء بقية آثار برمجية الفدية.

الاستنتاج

تم تحديد ملف باسم `eky.00000000` ضمن آثار الملفات المستخرجة من الذاكرة.

الإجابة: `eky.00000000`

مكان إدراج الصورة: أدرج لقطة شاشة تُظهر نتيجة البحث عن `eky.` في ملف `filescan.txt`.



9. ملخص النتائج

رقم السؤال	النتيجة
1	العملية المشبوهة: `or4qtckT.exe`
2	PPID للعملية المشبوهة: `1456`
3	الملف التنفيذي المرتبط بعملية الفدية: `or4qtckT.exe`
4	العملية المرتبطة بحذف الملفات: `taskdl.exe`
5	مسار الملف المشبوه: `C:\Users\hacker\Desktop\or4qtckT.exe`
6	عائلة برمجية الفدية المحتملة: WannaCry
7	اسم ملف المفتاح: `eky.00000000`

10. توصيات أمنية

بناءً على مؤشرات الإصابة المذكورة، يمكن اقتراح الإجراءات التالية:

1. عزل الجهاز المصاب عن الشبكة عند الاشتباه في استمرار نشاط برمجية الفدية.
2. الحفاظ على الأدلة الرقمية قبل إجراء تغييرات غير ضرورية على النظام.
3. فحص الملف التنفيذي المشبوه داخل بيئة تحليل معزولة، وعدم تشغيله على جهاز العمل.
4. مراجعة سجلات النظام وآثار الملفات لتحديد نطاق الضرر.
5. التحقق من وجود ملفات مشفرة أو رسائل فدية تدعم تحديد العائلة.
6. الاحتفاظ بنسخ احتياطية منفصلة عن الأجهزة المتأثرة، واختبار إمكانية استعادتها.
7. تحديث أنظمة التشغيل والبرامج، وتقييد الصلاحيات، وتعزيز وسائل الحماية من البرمجيات الضارة.

11. الخاتمة

أوضح هذا التطبيق كيف يمكن استخدام تحليل الذاكرة لدعم التحقيق في حادثة يُشتبه في ارتباطها ببرمجية فدية. فمن خلال مراجعة العمليات وعلاقاتها، وفحص معلومات سطر الأوامر، والبحث عن آثار الملفات، أمكن تحديد مجموعة من المؤشرات التي تتوافق مع نشاط مرتبط بعائلة WannaCry في العينة المدروسة.

تؤكد التجربة أهمية ربط النتائج المستخرجة من الأدوات بالسياق العام للحادثة، مع توثيق الأدلة والتمييز بين الحقائق المباشرة والتفسيرات. كما توضح أن تحليل الذاكرة يمثل مصدرًا مهمًا

للمعلومات، لكنه يكون أكثر فاعلية عند دمجه مع مصادر أدلة أخرى.