«Волшебный источник»: новые методы поиска и применения данных из RAM для целей криминалистической экспертизы

Чиликов А.А., к.ф.-м.н., доцент кафедры «Информационная безопасность», МГТУ им.Баумана, Passware Inc.

22 марта 2017 г.

Актуальность

Сценарий	DMG	TrueCrypt (обычный)	TrueCrypt (скрытый)	VeraCrypt (обычный)	VeraCrypt (скрытый)
Контейнер: + Образ памяти: -	+	+	+	+	+
Контейнер: + Образ памяти: + (в момент, когда контейнер смонтирован)	?	+	?	+	?
Контейнер: + Образ памяти: + (в момент, когда контейнер размонтирован)	-	-	?	-	?

Расшифрование Apple DMG образов

Сценарий	DMG	TrueCrypt (обычный)	TrueCrypt (скрытый)	VeraCrypt (обычный)	VeraCrypt (скрытый)
Контейнер: + Образ памяти: -	+	+	+	+	+
Контейнер: + Образ памяти: + (в момент, когда контейнер смонтирован)	?	+	?	+	?
Контейнер: + Образ памяти: + (в момент, когда контейнер размонтирован)	-	-	?	-	?

Образы Apple DMG

- Стандарт для образов дисков для macOS
- Множество поддерживаемых форматов (UDRW, UDRO, UDCO и т.д.)
- Обладает рядом особенностей, затрудняющих классическую RAM-атаку:
  - Помимо шифрования, образ также может быть сжат (затруднение отбраковки ложных кандидатов в ключи)
  - Для шифрования используется пара ключей - *encKey*, *ivKey* - обычно располагающихся на разных страницах образа RAM (требуется проверить корректность пары ключей)

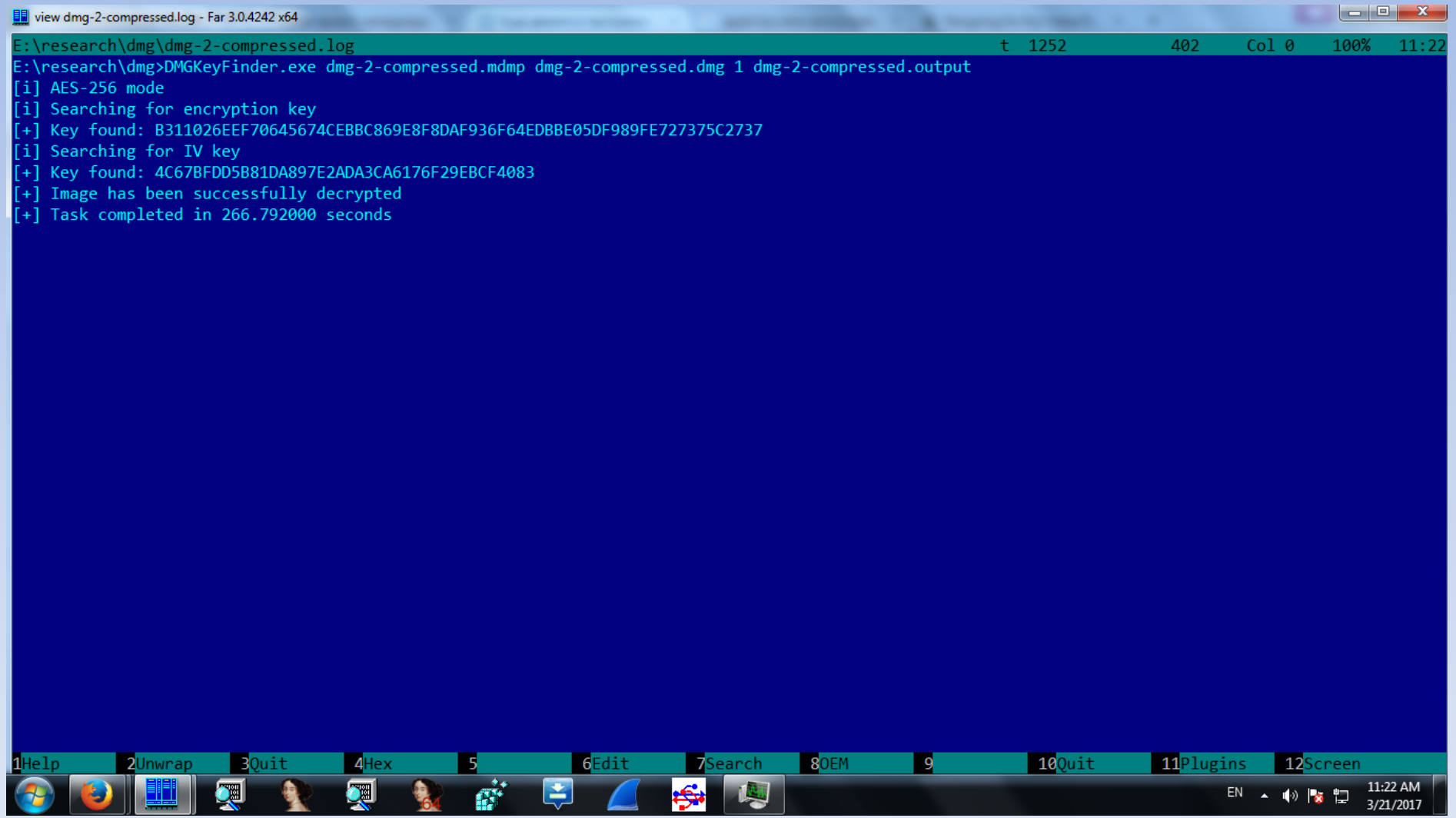
Оптимизация RAM-атаки (1)

- Сжатые образы (UDCO, UDZO и другие) помимо запакованных данных содержат метаданные в формате XML (размер – порядка 0x2000 байт)
- Шифрование производится посекторно (секторы не зависят друг от друга, размер сектора – 0x200 байт)
- Вместо полного расшифрования образа и декомпрессии, достаточно проверить корректность сектора(ов), содержащих метаданных

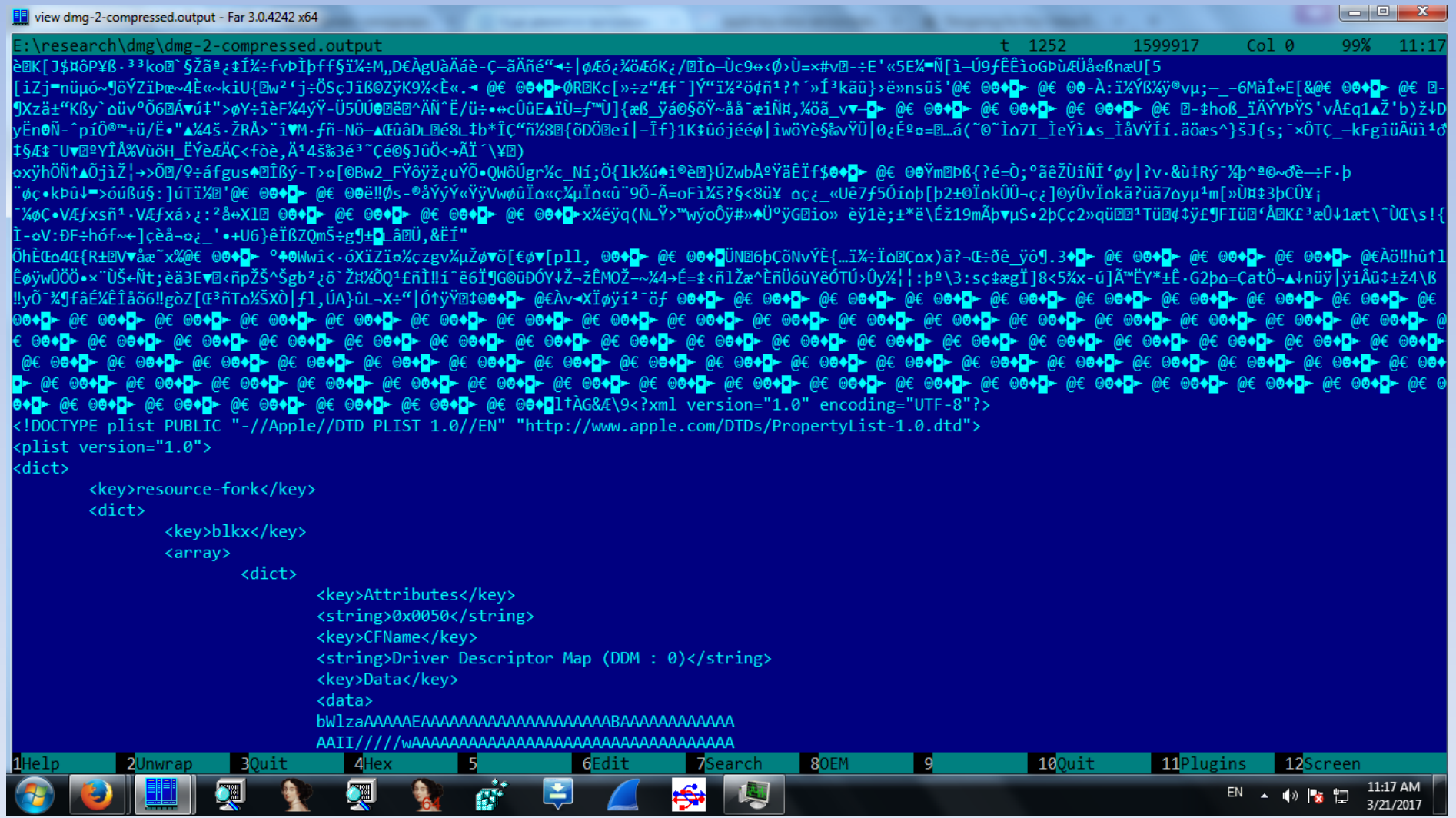
Оптимизация RAM-атаки (2)

- Для шифрования применяется AES-128/AES-256 в режиме CBC
- *encKey* – можно опробовать независимо от *ivKey* путем расшифрования второго и последующих блоков
- *ivKey* – опробуется при известном *encKey* (значительный размер метаданных позволяет отбраковывать ложных кандидатов)

Пример (1)


view dmg-2-compressed.log - Far 3.0.4242 x64
E:\research\dmg\dmg-2-compressed.log t 1252 402 Col 0 100% 11:22
E:\research\dmg>DMGKeyFinder.exe dmg-2-compressed.mdmp dmg-2-compressed.dmg 1 dmg-2-compressed.output
[i] AES-256 mode
[i] Searching for encryption key
[+] Key found: B311026EEF70645674CEBBC869E8F8DAF936F64EDBBE05DF989FE727375C2737
[i] Searching for IV key
[+] Key found: 4C67BFDD5B81DA897E2ADA3CA6176F29EBCF4083
[+] Image has been successfully decrypted
[+] Task completed in 266.792000 seconds
1Help 2Unwrap 3Quit 4Hex 5 6Edit 7Search 8OEM 9 10Quit 11Plugins 12Screen
EN
11:22 AM
3/21/2017

Пример (2)


view dmg-2-compressed.output - Far 3.0.4242 x64
E:\research\dmg\dmg-2-compressed.output
t 1252 1599917 Col 0 99% 11:17
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>resource-fork</key>
<dict>
<key>blkx</key>
<array>
<dict>
<key>Attributes</key>
<string>0x0050</string>
<key>CFName</key>
<string>Driver Descriptor Map (DDM : 0)</string>
<key>Data</key>
<data>
bWlzaAAAAAEAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAA
AAII/////wAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
1Help 2Unwrap 3Quit 4Hex 5 6Edit 7Search 8OEM 9 10Quit 11Plugins 12Screen
EN
11:17 AM
3/21/2017

Меры, позволяющие затруднить RAM-атаку

- Ключи шифрования располагаются на различных страницах образа памяти
- Режим шифрования не позволяет независимо опробовать ключи (например, XTS)
- К образу в открытом применен алгоритм сжатия
- В расшифрованном образе отсутствуют участки, позволяющие эффективно опробовать кандидатов в ключи

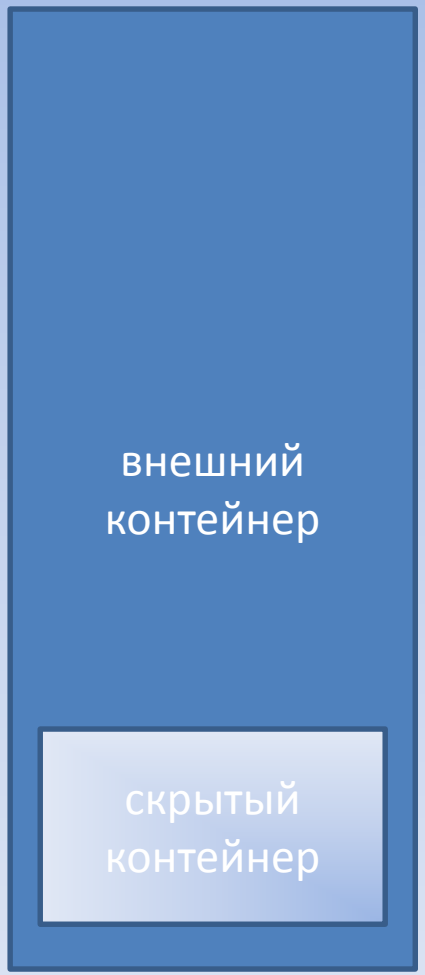
Расшифрование скрытых контейнеров TrueCrypt/VeraCrypt

Сценарий	DMG	TrueCrypt (обычный)	TrueCrypt (скрытый)	VeraCrypt (обычный)	VeraCrypt (скрытый)
Контейнер: + Образ памяти: -	+	+	+	+	+
Контейнер: + Образ памяти: + (в момент, когда контейнер смонтирован)	+	+	?	+	?
Контейнер: + Образ памяти: + (в момент, когда контейнер размонтирован)	-	-	?	-	?

Скрытые контейнеры TrueCrypt/VeraCrypt

- Скрытые контейнеры располагаются внутри обычных TC/VC контейнеров

- В открытой литературе **мало изучены методы, позволяющих определить наличие/отсутствие скрытого контейнера** (даже при наличии ключа шифрования внешнего контейнера)

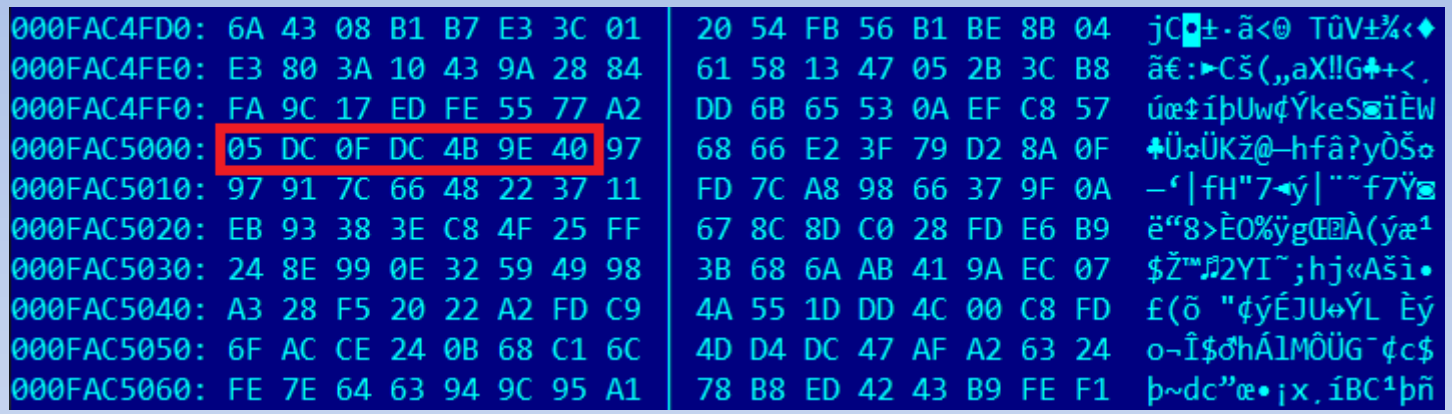


Расшифрование скрытых контейнеров TrueCrypt/VeraCrypt

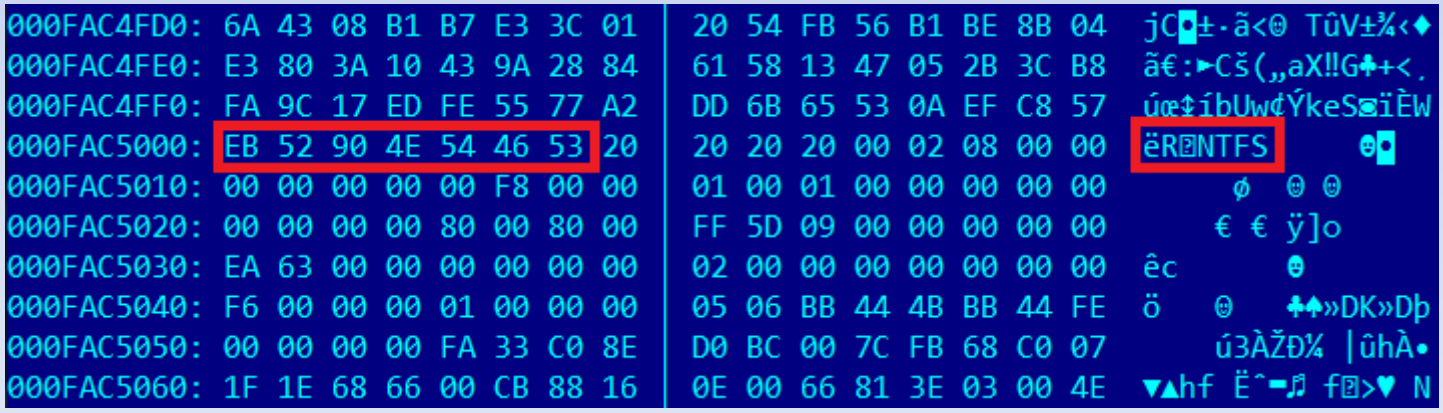
- Ключи шифрования в образе оперативной памяти определяются аналогично ключам обычных контейнеров
- **Начало области зашифрованных данных не зафиксировано**, необходимо опробовать все возможные варианты
- В качестве критерия корректности определения ключа предлагается анализировать первые несколько расшифрованных секторов (сигнатуры, псевдослучайность)

Расшифрование скрытых контейнеров TrueCrypt/VeraCrypt

Зашифрованный скрытый контейнер:



Расшифрованный скрытый контейнер:



Детектирование скрытых контейнеров TrueCrypt/VeraCrypt

Сценарий	DMG	TrueCrypt (обычный)	TrueCrypt (скрытый)	VeraCrypt (обычный)	VeraCrypt (скрытый)
Контейнер: + Образ памяти: -	+	+	+	+	+
Контейнер: + Образ памяти: + (в момент, когда контейнер смонтирован)	+	+	+	+	+
Контейнер: + Образ памяти: + (в момент, когда контейнер размонтирован)	-	-	?	-	?

Детектирование скрытых контейнеров TrueCrypt/VeraCrypt

- На ОС Windows 7 (x86/x64) **после размонтирования** контейнера в образе RAM **остаются служебные структуры** (размер внешнего и скрытого контейнера, имя файла)
- Детектирование скрытых контейнеров основано на полях с размером (строго меньше размера внешнего контейнера)
- Актуально для файлов гибернации

Детектирование скрытых контейнеров TrueCrypt/VeraCrypt

- **Вход:** образ RAM, предполагаемый внешний контейнер, конфигурация системы (x86/x64, TC/VC, номер версии)
- **Выход:** путь до контейнера на файловой системе, тип (обычный/скрытый), размер скрытого контейнера

Детектирование скрытых контейнеров TrueCrypt/VeraCrypt

```
[!] Invalid bytes_per_sector value : 00000000
[i] Candidate found at offset 000000003F0B9210
[!] disk_size is too large
[i] Candidate found at offset 000000003F0B9218
[!] Invalid bytes_per_sector value : 1B2D3777
[i] Candidate found at offset 000000003F0B9248
[!] disk_size is too large
[i] Candidate found at offset 000000003F0B9250
[!] Invalid bytes_per_sector value : 00000000
[i] Candidate found at offset 000000003F15F030
[!] Invalid bytes_per_sector value : 85F5F04C
[i] Candidate found at offset 000000003F15F120
[!] Invalid bytes_per_sector value : 0010E400
[i] Candidate found at offset 000000003FA54210
[!] disk_size is too large
[i] Candidate found at offset 000000003FA54218
[!] Invalid bytes_per_sector value : 1B2D3777
[i] Candidate found at offset 000000003FA54248
[!] disk_size is too large
[i] Candidate found at offset 000000003FA54250
[!] Invalid bytes_per_sector value : 00000000
[i] Candidate found at offset 000000003FD00B58
[i] Shortened struct found at offset 000000003FD00CD0
[i] Shortened struct found at offset 000000003FF68CD8
[i] Processing offset : 0000000040000000
---
  [i] It is a HIDDEN container

  [i] Host size            = 0000000001400000
  [i] Disk size            = 00000000009E0000
  [i] Volume name          = \??\C:\tmp\ruscrypto17\tc-1
```

Детектирование скрытых контейнеров TrueCrypt/VeraCrypt

```
[!] disk_size is too large
[i] Candidate found at offset 000000003F0B80C0
[!] Invalid bytes_per_sector value : F8759439
[i] Candidate found at offset 000000003F0B80F0
[!] disk_size is too large
[i] Candidate found at offset 000000003F0B80F8
[!] Invalid bytes_per_sector value : 00000000
[i] Candidate found at offset 000000003F286970
[!] Invalid bytes_per_sector value : 00500000
[i] Candidate found at offset 000000003F2869D0
[!] Invalid bytes_per_sector value : 00500000
[i] Candidate found at offset 000000003FA77160
[i] Candidate found at offset 000000003FA772E0
[!] disk_size is too large
[i] Candidate found at offset 000000003FC7CAC0
[!] disk_size == 0
[i] Candidate found at offset 000000003FD5A0B8
[!] disk_size is too large
[i] Candidate found at offset 000000003FD5A0C0
[!] Invalid bytes_per_sector value : F8759439
[i] Candidate found at offset 000000003FD5A0F0
[!] disk_size is too large
[i] Candidate found at offset 000000003FD5A0F8
[!] Invalid bytes_per_sector value : 00000000
[i] Processing offset : 0000000040000000
---
  [i] It is a normal container

  [i] Host size           = 0000000000B00000
  [i] Disk size           = 0000000000AC0000
  [i] Volume name         = \??\C:\tmp\ruscrypto17\vc-2
```

Детектирование скрытых контейнеров TrueCrypt/VeraCrypt

- Проведено экспериментов - 15
- Вероятность ошибки **I-го рода : 0**
- Вероятность ошибки **II-го рода : 0.2** (в 3 случаях из 15 контейнер не обнаружен)
- На ОС Windows 8 и выше служебные структуры не обнаруживались ни в одном эксперименте

Результаты работы

- Предложен метод **расшифрования** Apple DMG образов при наличии образа памяти (в момент, когда образ **смонтирован**)
- Предложен метод **расшифрования** скрытых контейнеров TrueCrypt/VeraCrypt при наличии образа памяти (в момент, когда контейнер **смонтирован**)
- Предложен метод **детектирования** скрытых контейнеров TrueCrypt/VeraCrypt при наличии образа памяти (в момент, когда контейнер **размонтирован**)

Спасибо за внимание!