



# «ТУЛЗЫ» ДЛЯ FORENSIC'U

ОСНОВНЫЕ ИНСТРУМЕНТЫ КРИМИНАЛИСТИЧЕСКОГО АНАЛИЗА

## *Понятия:*

*Форензика (компьютерная криминалистика) — прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств.*

*Дамп памяти (англ. memory dump; в Unix — core dump) — содержимое рабочей памяти одного процесса, ядра или всей операционной системы.*

*Анализатор трафика, или сниффер (от англ. to sniff — нюхать) — программа или устройство для перехвата и анализа сетевого трафика (своего и/или чужого).*

## *Основные инструменты:*

- 1) Volatility — инструмент для анализа дампа оперативной памяти и образов системы.  
Широкий спектр поддерживаемых форматов (\*.mem, \*.img и тд.)*
- 2) Wireshark — программа-анализатор трафика для компьютерных  
сетей Ethernet и некоторых других.*
- 3) R-studio — группа полнофункциональных утилит для восстановления данных.*

## Volatility

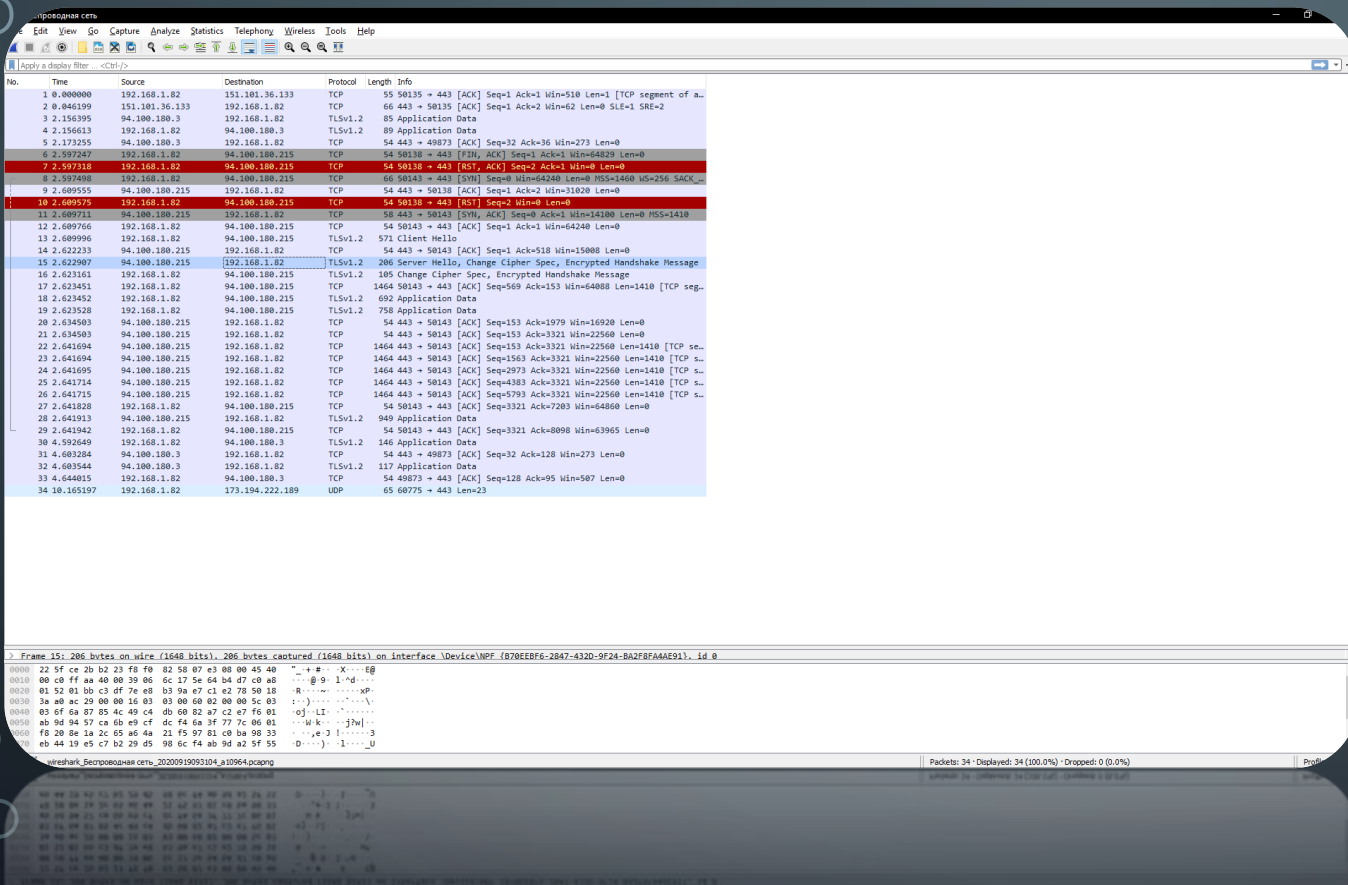
Предоставляет основную информацию о дампе оперативной памяти. Дает возможность просмотреть список процессов, открытых сокетов, учетные записи компьютера.

```
sonq@sonq: ~/Документы/Tasks/Forensica1
Cmd #36 @ 0x1600c4: ?????
Cmd #37 @ 0x18cf70: ???
sonq@sonq:~/Документы/Tasks/Forensica1$ volatility -f 20200908_1.mem --profile=Win7SP1x86_23418 pstree
Volatility Foundation Volatility Framework 2.6
Name                               Pid  PPid  Thds  Hnds  Time
-----
0x8541f030:csrss.exe                392   376    9    502  2020-09-08 16:25:33 UTC+0000
0x85428d40:wininit.exe              428   376    3     73  2020-09-08 16:25:33 UTC+0000
. 0x8545d1e0:lsass.exe               528   428    7    713  2020-09-08 16:25:33 UTC+0000
. 0x85456380:lsm.exe                 536   428   10   145  2020-09-08 16:25:33 UTC+0000
. 0x85450500:services.exe           520   428   11   212  2020-09-08 16:25:33 UTC+0000
.. 0x854cc690:svchost.exe            640   520   10   351  2020-09-08 16:25:34 UTC+0000
... 0x840cbd40:dllhost.exe          2976   640    6     82  2020-09-08 17:49:09 UTC+0000
... 0x83ff9c70:dllhost.exe          2936   640    6     79  2020-09-08 17:49:09 UTC+0000
.. 0x83ee9aa0:svchost.exe            3200   520   10   315  2020-09-08 17:27:40 UTC+0000
.. 0x83f77190:wmipnetwk.exe          2336   520   16   457  2020-09-08 17:27:25 UTC+0000
.. 0x855046d0:taskhost.exe           1696   520    9    175  2020-09-08 17:27:17 UTC+0000
.. 0x8565a4f0:unchecky_svc.e         1576   520    4     78  2020-09-08 17:25:37 UTC+0000
... 0x84d539b0:unchecky_bg.ex        360   1576    2     63  2020-09-08 17:27:17 UTC+0000
.. 0x854f5030:svchost.exe            812   520   24   573  2020-09-08 17:25:35 UTC+0000
... 0x84063920:audiodg.exe          2800   812    6    130  2020-09-08 17:48:47 UTC+0000
... 0x8556a370:SearchIndexer.       2224   520   13    679  2020-09-08 17:27:24 UTC+0000
... 0x84cb65c0:SearchFilterHo       2972  2224    4     95  2020-09-08 17:47:54 UTC+0000
... 0x83eda030:SearchProtocol       2168  2224    6    276  2020-09-08 17:47:54 UTC+0000
.. 0x854dd030:VBoxService.ex        704   520   12   135  2020-09-08 16:25:34 UTC+0000
.. 0x855e49e8:svchost.exe            1400   520   19   320  2020-09-08 17:25:37 UTC+0000
.. 0x8566b60:service_update         1604   520    4     78  2020-09-08 17:25:37 UTC+0000
.. 0x8562fd40:service_update        1620  1604    7     56  2020-09-08 17:25:37 UTC+0000
.. 0x8553ad40:svchost.exe            972   520   38  1121  2020-09-08 17:25:36 UTC+0000
.. 0x83fcbc88:svchost.exe           2628   520    9   351  2020-09-08 17:27:25 UTC+0000
.. 0x85154230:svchost.exe            760   520    8    277  2020-09-08 17:25:35 UTC+0000
.. 0x85819ac0:spoolsv.exe            1364   520   13   284  2020-09-08 17:25:37 UTC+0000
.. 0x85612138:svchost.exe            1504   520   22   312  2020-09-08 17:25:37 UTC+0000
.. 0x853e44a0:sppsvc.exe             3172   520    4    141  2020-09-08 17:27:40 UTC+0000
.. 0x851a54a0:svchost.exe            936   520   25   520  2020-09-08 17:25:36 UTC+0000
... 0x85389750:dwm.exe              1988   936    3     70  2020-09-08 17:27:17 UTC+0000
```

```
sonq@sonq: ~/Документы/Tasks/Forensica1
sonq@sonq:~/Документы/Tasks/Forensica1$ volatility -f 20200908_1.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
      AS Layer1 : IA32PagedMemoryPae (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/sonq/Документы/Tasks/Forensica1/20200908_1.mem)
      PAE type : PAE
      DTB : 0x185000L
      KDBG : 0x82938c28L
      Number of Processors : 1
      Image Type (Service Pack) : 1
      KPCR for CPU 0 : 0x82939c00L
      KUSER_SHARED_DATA : 0xfffff0000L
      Image date and time : 2020-09-08 17:49:11 UTC+0000
      Image local date and time : 2020-09-08 21:49:11 +0400
sonq@sonq:~/Документы/Tasks/Forensica1$
```

Полный перечень команд:

<https://tools.kali.org/forensics/volatility>



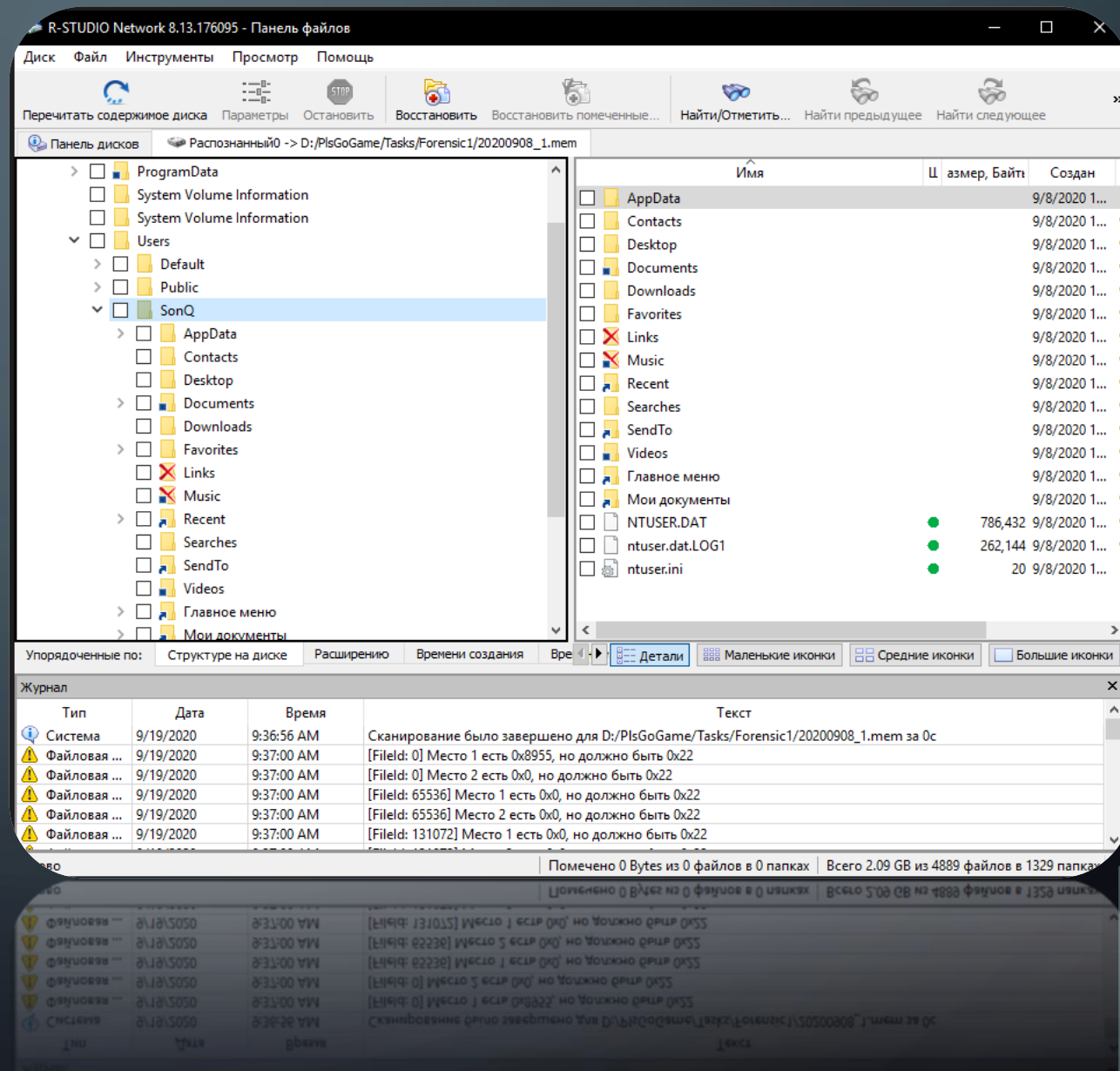
*Wireshark*  
Программа для перехвата и анализа трафика. Дает возможность автоматически собирать пакеты из одного потока (Follow), экспортировать передаваемые объекты (Export objects)



## R-studio

Дает возможность восстанавливать файлы с образа HDD, \*.image и оперативной памяти.

Отображает файловую систему, удаленные и поврежденные файлы.



The image features a dark blue gradient background. In the corners, there are decorative white line art elements resembling circuit boards or neural network connections, with small circles at the end of the lines.

*Спасибо за внимание!*