«ТУЛЗЫ» ДЛЯ FORENSIC'И

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.

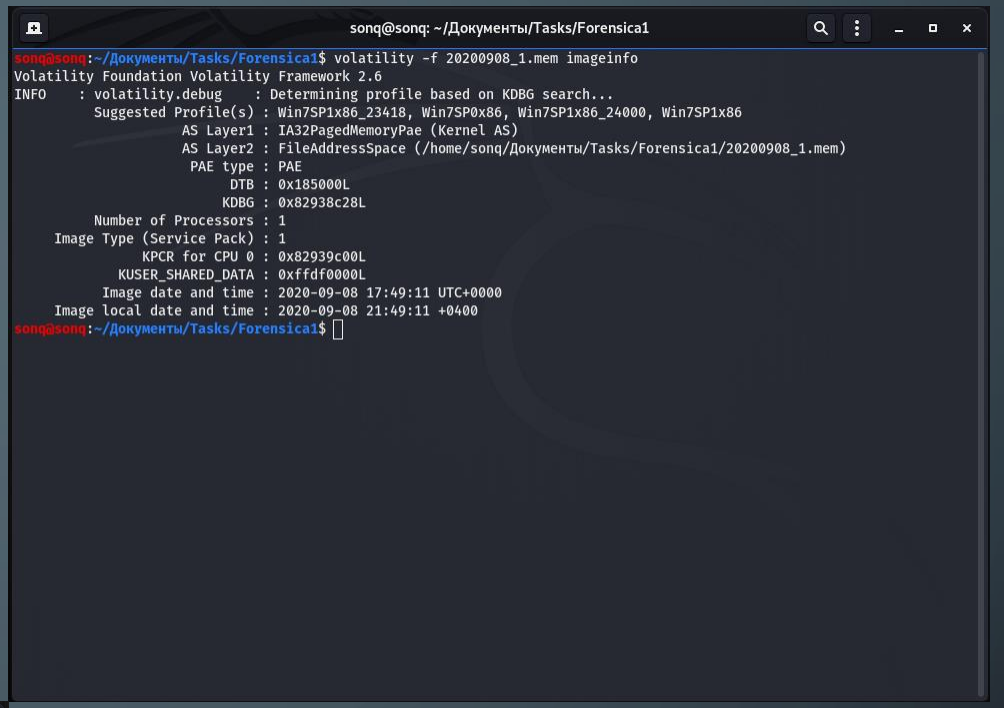
Анализатор трафика, или сниффер (от англ. to sniff — нюхать) — программа или устройство для перехвата и анализа сетевого трафика (своего и/или чужого).

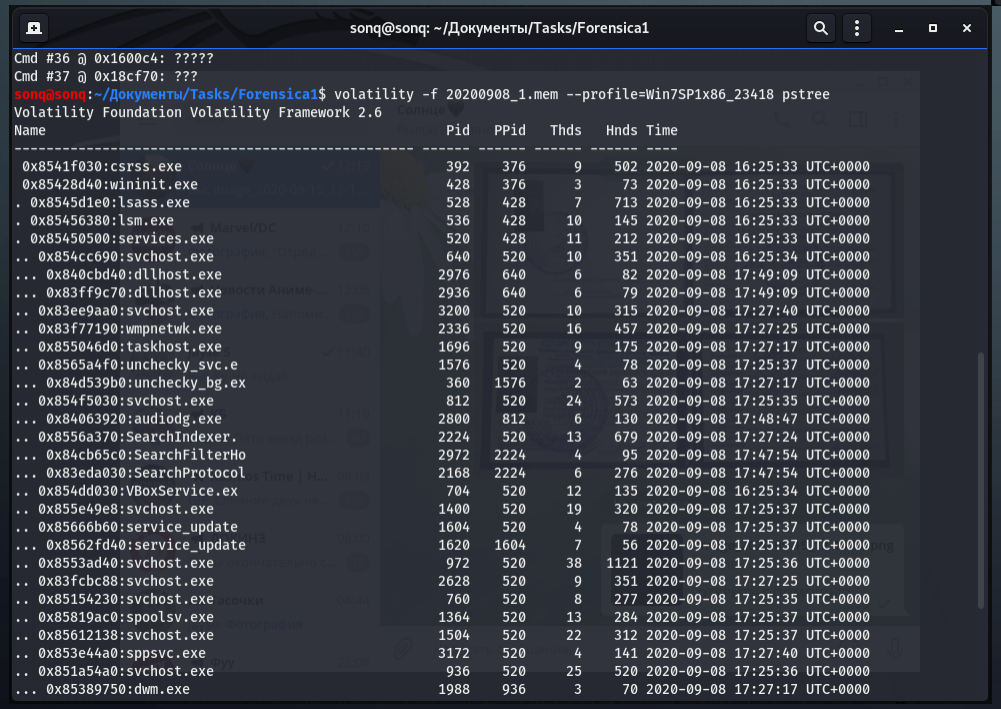
Основные инструменты:

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

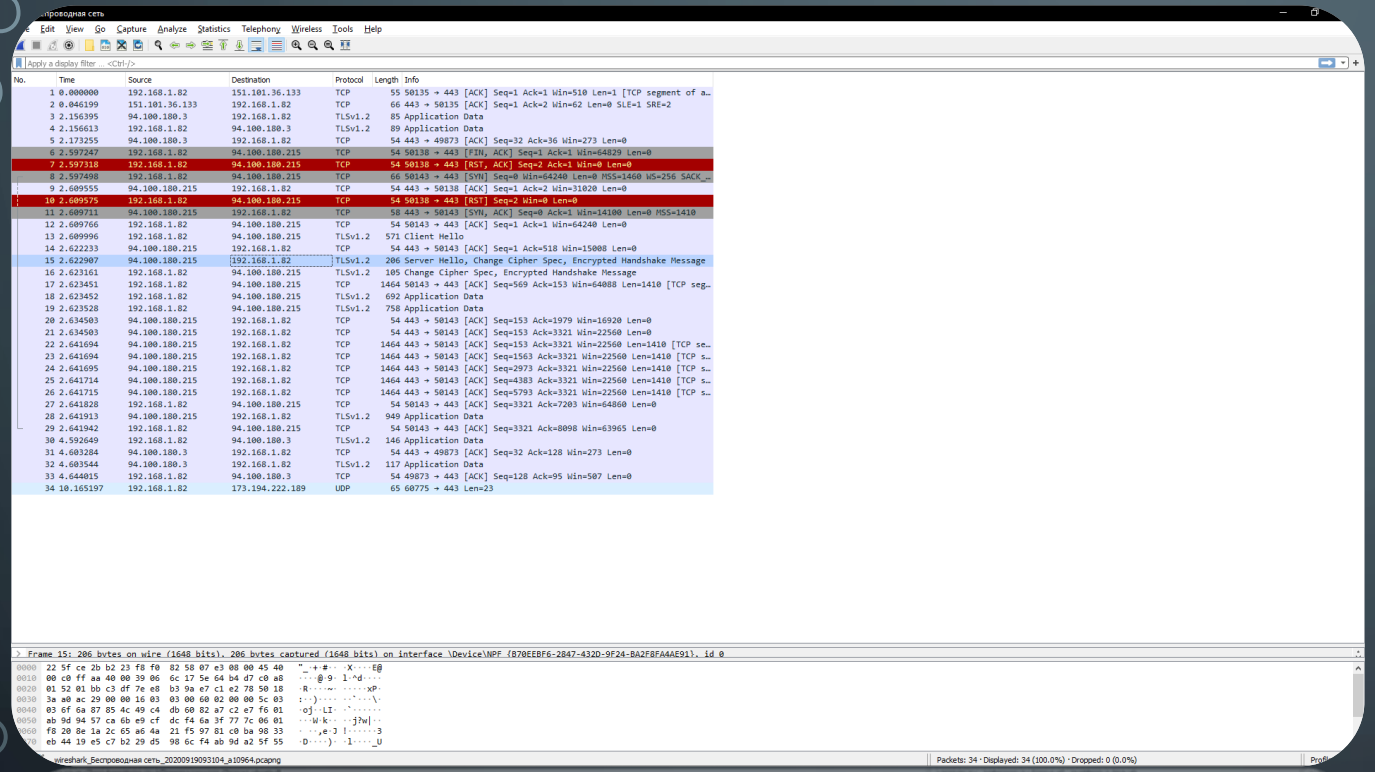
Предоставляет основную информацию о дампе оперативной памяти. Дает возможность просмотреть список процессов, открытых сокетов, учетные записи компьютера.





Полный перечень команд:

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

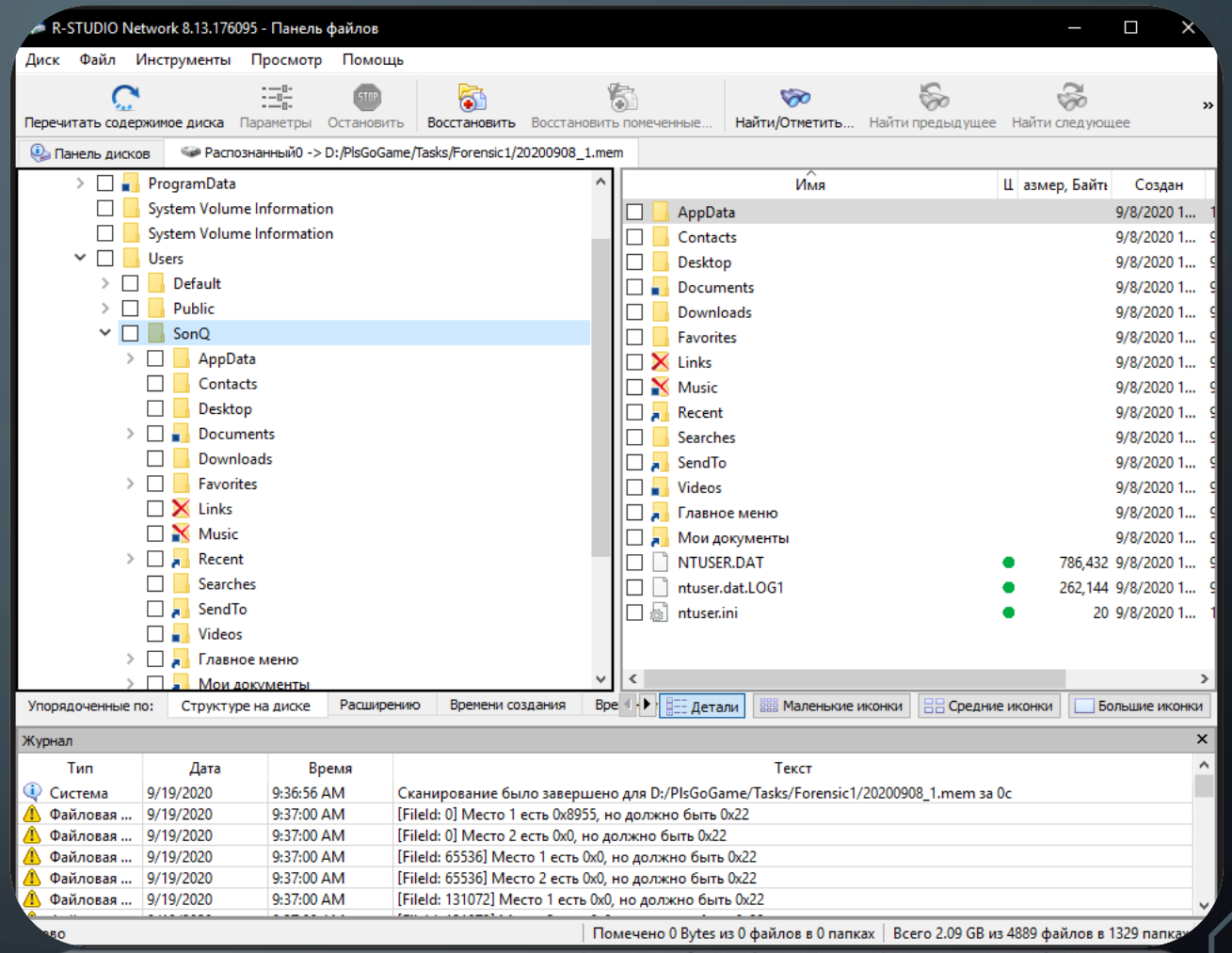


Wireshark
Программа для перехвата и анализа трафика. Дает возможность автоматически собирать пакеты из одного потока (Follow), экспортировать передаваемые объекты (Export objects)

R-studio

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

Отображает файловую систему, удаленные и поврежденные файлы.



Спасибо за внимание!