OSU CTF

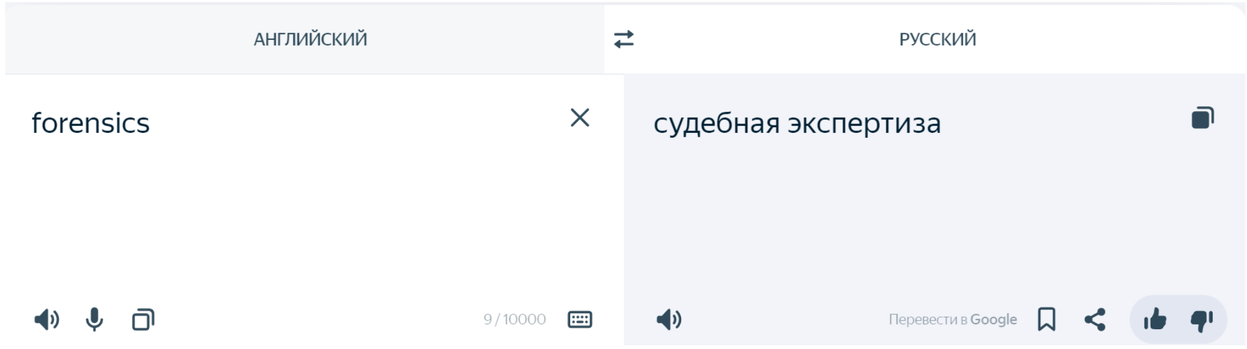
Forensics

SIGAN

ОРЕНБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Forensics

В контексте CTF задачи «криминалистики» могут включать анализ форматов файла, стеганографию, дампа памяти, образа диска или дампа сетевых пакетов

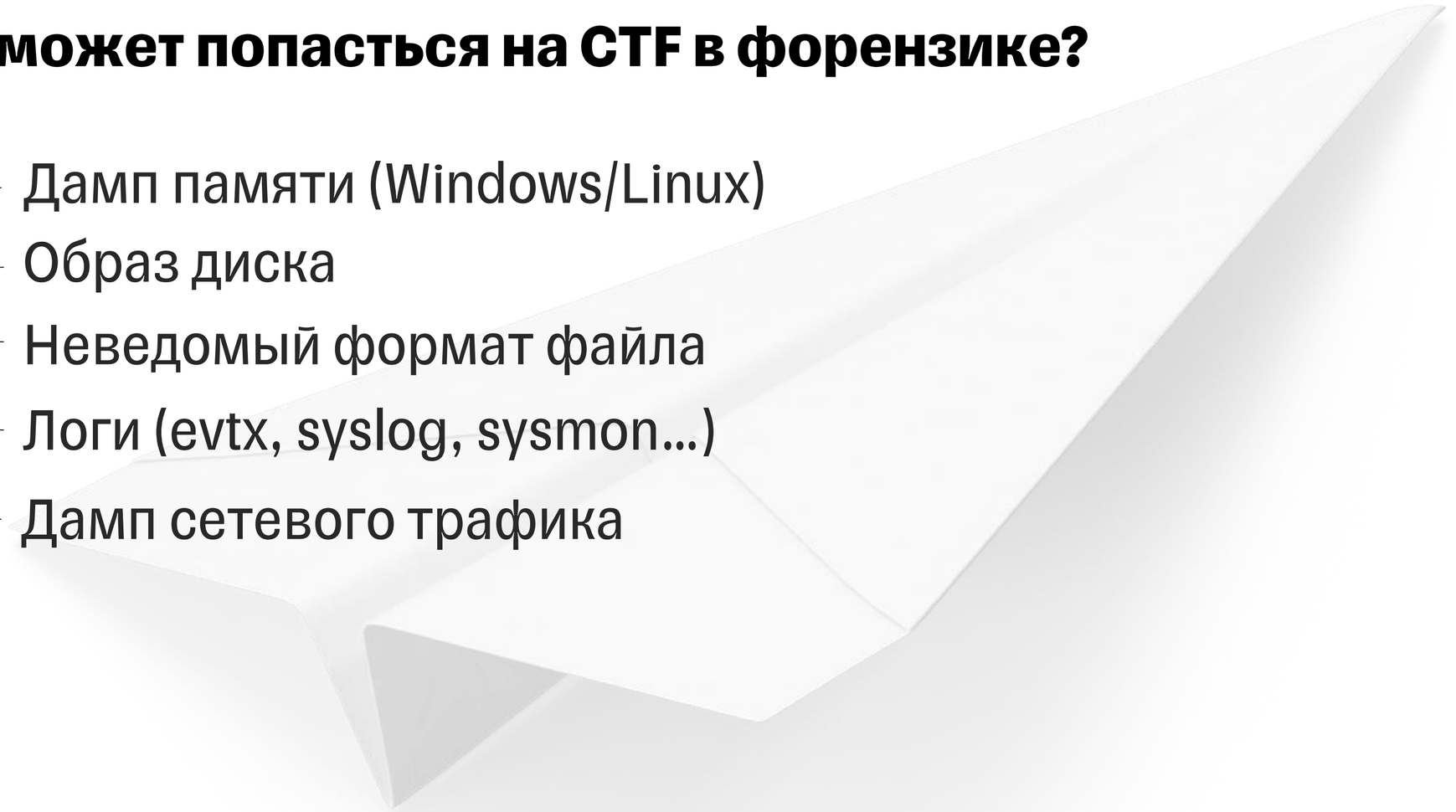


Навыки:

- Знание скриптового языка (например, Python)
- Знание того, как манипулировать двоичными данными (манипуляции на уровне байтов) на этом языке
- Распознавание форматов, протоколов, структур и кодировок

Что может попасться на CTF в форензике?

- Дамп памяти (Windows/Linux)
- Образ диска
- Неведомый формат файла
- Логи (evtx, syslog, sysmon...)
- Дамп сетевого трафика



Memory Dump

По слепку ОЗУ можно определить, какие приложения запускались **во время работы** компьютера, данные процессов и файлов, другую полезную информацию.

Все это можно сделать пока пользователь не выключил или не перезагрузил ПК.

Для получения снимка:

- Windows: DumpIt, Гибернация (hiberfil.sys)
- Linux: Linux Memory Extractor (LiME)
- VM: vda, vmem

Volatility 2 (python 2)

Одна из лучших утилит для анализа дампа памяти – **Volatility**:

- volatility -f %имя_образа% **imageinfo** – определить профиль
- volatility -f %имя_образа% --profile=Win7SP1 **clipboard** - буфер
- volatility -f %имя_образа% --profile=Win7SP1 **pslist** / **pstree** - процессы
- volatility -f %имя_образа% --profile=Win7SP1 **netscan** – анализ сети
- volatility -f %имя_образа% --profile=Win7SP1 **cmdline** / **console** – cmd команды / дамп powershell
- volatility -f %имя_образа% --profile=Win7SP1 **filescan** – список файлов
- volatility -f %имя_образа% --profile=Win7SP1 **dumpfiles -Q** <адрес>

--dump-dir <директория вывода> – достать файлы (можно -p <PID>)

Volatility 3 (python 3)

Свежая версия **Volatility**:

- `vol.py -f </path/to/file> windows.info / linux.info`
- `vol.py -f </path/to/file> windows.pslist / pstree - процессы`
- `vol.py -f </path/to/file> -o </path/to/dir> windows.dumpfiles --pid <PID>`
  `- достать файлы`
- `vol.py -f </path/to/file> windows.netscan / netstat - анализ сети`
- `vol.py -f </path/to/file> windows.cmdline - cmd команды`
- `vol.py -f </path/to/file> windows.filescan - список файлов`
- `vol.py -f </path/to/file> windows.hashdump`

Useful links

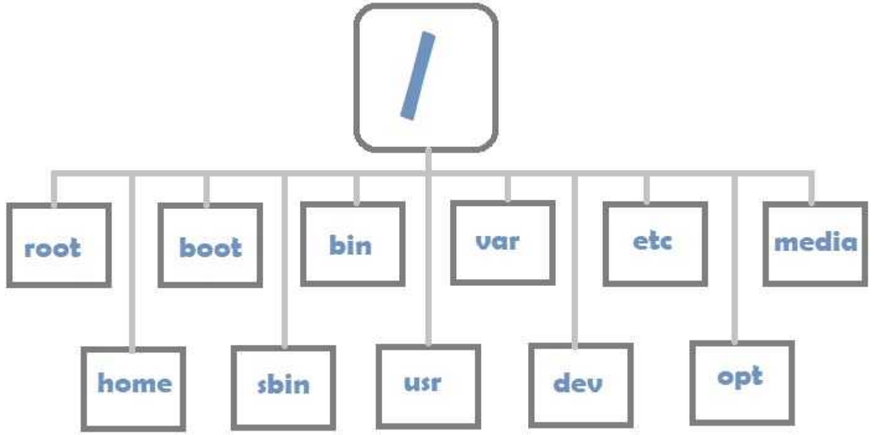
Volatility **cheatsheet**

Volatility **GUI**

Диски

Оперативная память — это простое и быстрое хранилище данных, однако некоторую информацию хотелось бы сохранять не только до момента выключения компьютера. Для этого существуют жёсткие диски, твердотельные и флеш-накопители.

В UNIX существует только один корневой каталог, а все остальные файлы и каталоги вложены в него. Windows – C:\ D:\ ...



Disk Image

Дамп диска — содержимое рабочей памяти одного процесса, ядра или всей операционной системы.

Иногда криминалистическая задача CTF состоит из полного образа диска, и игрок должен иметь стратегию для поиска флага в этом стоге данных.

- Монтирование образа в Linux – **mount**
- **kpartx** - Для монтирования диска (разделение файловых систем)
- **dd** – копирование двоичных данных (в т.ч. разделов)
- **OSFmount, FTKimager**
- **quemu-nbd** – монтирование виртуальных образов (vdi, vmdk…)

Логи

Логи – это записи событий и сообщений, создаваемые программой или системой во время ее работы.

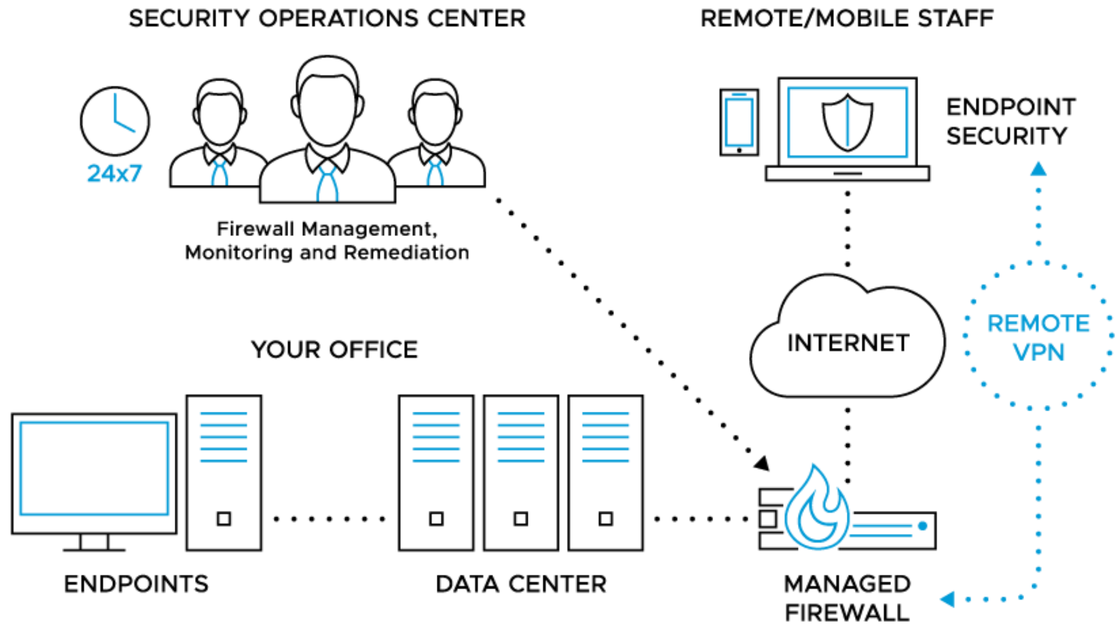
В каждой операционной системе предусмотрено логирование работы, в том числе для обеспечения безопасности.

Анализ логов в форензике – зачастую просмотр записей в настроенных системах безопасности, например:

- Sysmon, evtx для Windows (C:\Windows\System32\winevt\Logs\)
- Содержимое /var/log/ для Linux
- Записи SIEM или IDS в качестве отфильтрованных сборок логов с нескольких машин

Security Operations Center (SOC)

Специалисты SOC собирают и анализируют данные с различных объектов инфраструктуры организации и при обнаружении подозрительной активности принимают меры для предотвращения атаки.



Security Operations Center, SOC

Security Operations Center, SOC

- Аналитик 1 уровня (**L 1**). Его задача заключается в первичной обработке инцидента

- Аналитик 2 уровня (**L 2**). Это опытный ИБ-специалист, который может разобраться в сложной ситуации и принять «креативное» решение.

- Специалист по реверсу. Имеет знания которые в ситуациях, незнакомых ни аналитику L2, ни вспомогательным системам (**TI**).

- Эксперт по **форензике**. Инциденты нужно расследовать: оценить нанесенный ущерб, описать поведение вредоноса, отследить путь хакеров до точки входа в инфраструктуру. Всем этим занимается форензик-эксперт или же специалист по компьютерной криминалистике.