# Forensics-9-2

## Читерский клиент

### Условие задачи

Игрок с ником xX\_ProGamer\_Xx был забанен античитом за использование запрещённых модификаций. Он утверждает, что его аккаунт был взломан. Администрация сервера сделала дамп памяти игрового клиента в момент обнаружения читов: файл pinecraft\_memory.dmp (~100 МБ). Требуется определить версию используемого клиента, идентификатор активного модуля и UUID токена сессии.

### Что требуется найти

Флаг №1 — версия чит‑клиента. Флаг №2 — ID активного в момент бана чит‑модуля. Флаг №3 — UUID токен сессии игрока.

### Используемые инструменты

strings, grep, xxd (опционально).

### Анализ и решение

Чит‑клиенты часто оставляют в памяти строки с названием и версией. Извлекаем печатаемые строки из дампа памяти командой strings pinecraft\_memory.dmp и выполняем поиск по известным названиям клиентов. В результате grep -i wurstclient находим строку WurstClient v7.35 loaded. Из неё берём только номер версии — 7.35 — это первый флаг.

Для поиска активного модуля ищем в дампе структурированные записи. Поиск по ключевому слову module\_id (strings pinecraft\_memory.dmp | grep module\_id) выявляет запись {"module\_id":"godmode\_001","enabled":true}. Флаг enabled:true означает, что модуль был активен. Значение godmode\_001 является вторым флагом.

UUID токена сессии имеет стандартный формат xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx. Можно искать по регулярному выражению (grep -E "[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}") или воспользоваться ключевыми словами (grep -i -E "uuid|session"). В дампе появляется строка "session\_uuid":"a1b2c3d4-e5f6-7890-abcd-ef1234567890". Это значение передаётся как третий флаг.

### Итог

| Флаг | Значение |
| --- | --- |
| №1 | 7.35 |
| №2 | godmode\_001 |
| №3 | a1b2c3d4-e5f6-7890-abcd-ef1234567890 |