# Forensics-11-1

## Криптомайнер в контейнерах

### Условие задачи

На хостинге Pinecraft была замечена подозрительная активность: вместо игровых серверов в Docker‑контейнерах запускались криптомайнеры. Администратор успел экспортировать подозрительные Docker‑образы (docker\_images.tar), сохранить логи контейнеров (docker\_logs.json) и метрики нагрузки CPU (system\_metrics.log). Нужно выявить вредоносный образ, определить адрес кошелька и вычислить суммарное использование CPU майнерами.

### Что требуется найти

Флаг №1 — первые 12 символов SHA256‑хеша вредоносного Docker‑образа. Флаг №2 — адрес криптокошелька для майнинга. Флаг №3 — суммарный CPU usage всех майнеров (в процентах, округлённый до целого).

### Используемые инструменты

tar, docker, grep, jq, awk, sed, john.

### Анализ и решение

Получаем из задания зашифрованный архив. Используем zip2john, чтобы получить хеш для перебора.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Используем john и стандартный wordlist – rockyou.txt.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

С данным паролем можно успешно расшифровать zip архив.

После распаковки docker\_images.tar читаем manifest.json и ищем образы, относящиеся к проекту Pinecraft. Один из них содержит бинарник xmrig, что указывает на майнер. SHA256‑хеш этого образа начинается с a3f5c8d9e2b1…. Из этого значения берём первые 12 символов — a3f5c8d9e2b1 — первый флаг.

Адрес кошелька для майнинга обычно хранится в конфигурации майнера. Ищем строку --wallet в распакованных слоях: grep -r "wallet" .. В найденном конфигурационном файле значение --wallet=47BEukN83whUBb4QKJJM1B4Pe5qGSTiCBH — это адрес злоумышленника и второй флаг.

Файл system\_metrics.log содержит метрики CPU для каждого майнера. Отбираем строки, связанные с процессом xmrig, извлекаем процент использования (sed 's/.\*CPU: \([0-9.]\*\)%.\*//') и складываем значения с помощью awk. Полученная сумма 57269,4 округляется до 57269 — это третий флаг.

### Итог

| Флаг | Значение |
| --- | --- |
| №1 | a3f5c8d9e2b1 |
| №2 | 47BEukN83whUBb4QKJJM1B4Pe5qGSTiCBH |
| №3 | 57269 |