**Отчёт по цифровой форензике**

Кейс: [Название кейса]  
Автор: [Ваше имя] | Дата: [YYYY-MM-DD]

**1. Введение / Цель**

Кратко опишите цель исследования: что дано (образ диска, дамп памяти, PCAP и т.д.) и какую задачу требуется решить.

**2. Объекты исследования**

Перечислите файлы/образы, с которыми будете работать (имя файла, источник, время получения).

**3. Chain of Custody (цепочка хранения доказательств)**

Опишите, кто и когда получил объект, какие действия применялись. Включите все копии и их хэши.

**4. Инструменты и окружение**

Укажите версии инструментов и ОС. Пример:  
- Autopsy v4.x  
- Volatility 3 (commit XXXXX)  
- Wireshark 4.x  
- CAINE Linux (live)  
Убедитесь, что указали, что работа велась с копиями, а не с оригиналами.

**5. Методология**

Кратко опишите последовательность действий (сбор, сохранение, анализ, верификация).

**6. Ход исследования (пошагово)**

Приводите команды, скриншоты и краткие пояснения. Пример команд:  
- md5sum image.dd  
- sha256sum image.dd  
- strings -n 8 suspect.bin | less  
- volatility3 -f memory.raw windows.pslist  
  
(Включайте скриншоты как файлы в папке и ссылки на них в отчёте.)

**7. Находки**

Подробно опишите обнаруженные артефакты: имя файла, путь, размер, хэши, краткое пояснение почему это важно.

**8. Выводы и рекомендации**

Краткие и понятные выводы: что было обнаружено, как это может повлиять, какие дальнейшие шаги предлагаете.

**9. Приложения**

Скрипты, экспортированные логи, хэши, дампы фрагментов, ссылки на репозитории с кодом или write-up'ы.

Таблица доказательств (пример)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Имя файла | Источник | Размер | MD5 / SHA256 | Примечания |
| image.dd | Получено: HTB challenge / 2025-08-01 | 2.1 GB | MD5: a3dcb4d229de6fde0db5686dee47145d SHA256: 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b | Копия №1, использована для анализа |

Примеры команд и их назначение:

**Создать копию образа (только чтение):**dd if=/dev/sdX of=image.dd bs=4M conv=sync,noerror

**Посчитать хешы:**md5sum image.dd  
sha256sum image.dd

**Посмотреть список разделов:**mmls image.dd

**Поиск строк в бинарнике:**strings -n 8 suspect.bin | less

**Анализ памяти (Volatility3):**volatility3 -f memory.raw windows.pslist

**Анализ PCAP (Wireshark):**wireshark capture.pcap

Советы по оформлению:

- Всегда указывайте точные версии инструментов и даты.  
- Включайте снимки экрана ключевых шагов (результаты команд, экспортированные объекты).  
- Объясняйте, почему вы сделали тот или иной шаг — это демонстрирует понимание.