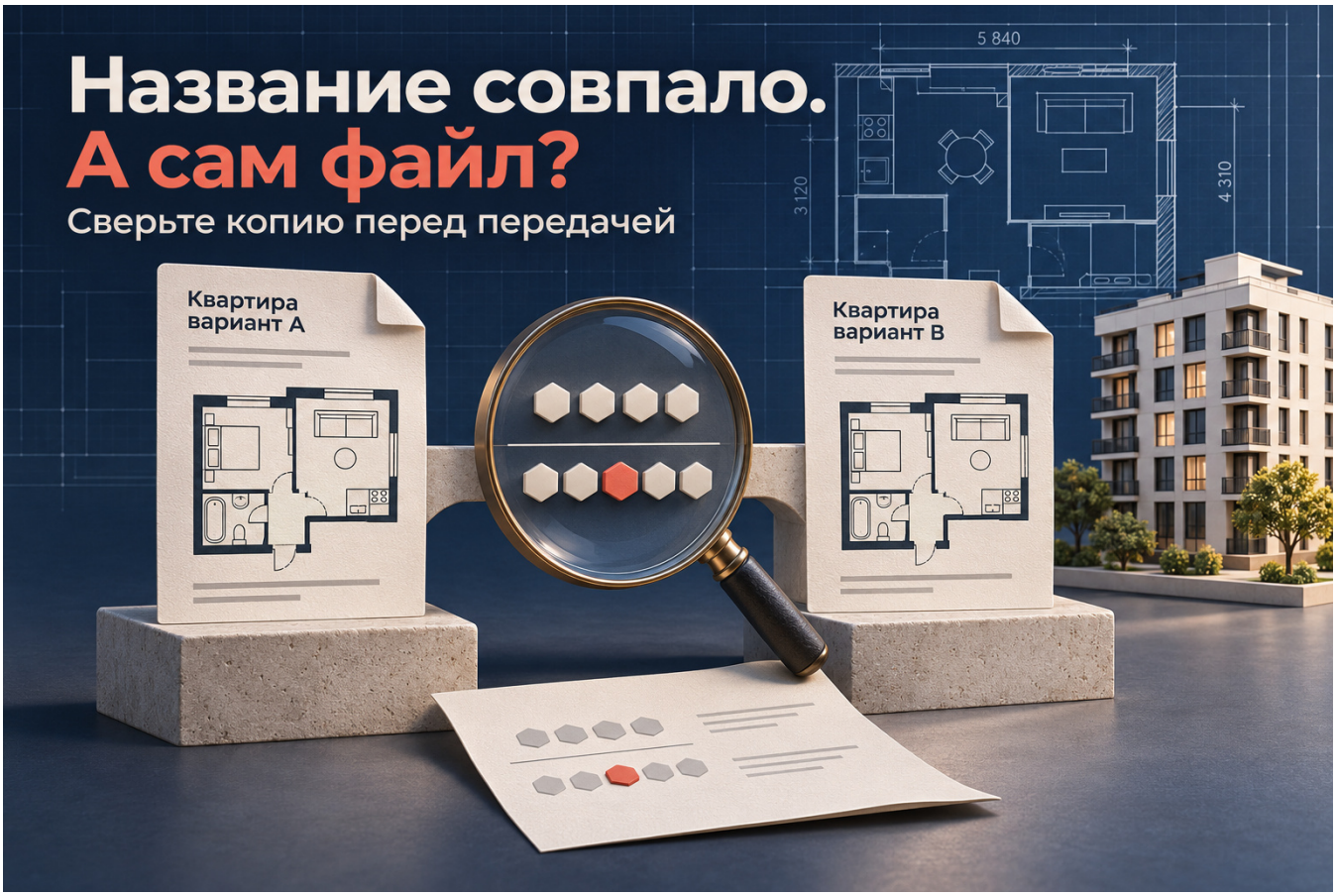
Тот ли файл отправлен: журнал SHA256 и проверка копии К147

Локальная проверка SHA256, опыт на трёх файлах, журнал эталонов и разбор несовпадения.



Практический гайд с заполненным учебным примером и чистыми рабочими листами. Подготовлено редакцией Нейросистемы риелтора.

Учебные цифры не являются данными о текущем рынке. Обложка представляет концептуальную иллюстрацию.

1. Что именно проверяем

К147 помогает сверить переданную копию с конкретным эталоном. Он не устанавливает правильность текста, актуальность версии или автора документа. Сначала назначьте проверенный эталон, затем сравнивайте с ним копию.

Подходящая задача	Отдельная задача
Совпадает ли скачанная копия с эталоном?	Правильно ли рассчитана цена?
Не изменились ли байты при передаче?	Кто действительно согласовал условия?
Тот ли архив получен?	Какие именно пункты изменились?

Опыт и его границы
Три учебных TXT-файла созданы без клиентских данных. SHA256 вычислена через Python и установленную команду shasum; результаты совпали. PowerShell в этом опыте не запускался, его синтаксис проверен по официальной документации.

Предмет сверки	Выбранный эталон	Кто отвечает

2. Паспорт эталона

Поле	Учебное заполнение
Рабочий код	Объект А, демонстрация К147
Файл	original.txt
Назначение	Несекретный пример сверки
Алгоритм	SHA256
Размер	43 байта
Принцип выбора	Создан как исходник упражнения
Источник значения	Локальное вычисление, два средства

В реальной работе эталон выбирают после согласования нужной версии. Имя «финал» само по себе не является основанием. После изменения передаваемого файла старую сумму не переносите автоматически.

Код / файл	Дата / основание выбора	Алгоритм / где хранится сумма

3. Windows: команда и чтение результата

Откройте PowerShell и укажите существующий файл. Пример ниже относится к учебной папке; замените путь своим.

Get-FileHash -LiteralPath 'C:\Kit147\original.txt' -Algorithm SHA256

Поле результата	Что проверить
Algorithm	Использован именно SHA256
Hash	Скопирована полная строка
Path	Обработан нужный файл

Ситуация	Действие
Путь не найден	Исправить путь, результата сверки ещё нет
Файл недоступен	Проверить разрешённый доступ
Обработан соседний файл	Выбрать правильный, вычислить заново

Команда читает указанный локальный файл. Не добавляйте к ней непонятные действия из чужих инструкций. Необходимость внешней загрузки для такого вычисления отсутствует.

Ваш путь	Алгоритм / дата	Результат или ошибка

4. Mac: локальная проверка

В установленной среде для этого опыта использована команда shasum. Явно указаны SHA256 и двоичное чтение. Пример пути замените существующим файлом.

shasum -a 256 -b "/полный/путь/файл.pdf"

Вывод содержит контрольную сумму и имя файла. Проверьте оба значения. Если копируете длинную строку вручную, не теряйте символы. Для реального сравнения используйте полные значения одного алгоритма.

До запуска	После запуска
Известен путь выбранного файла	Путь в результате соответствует выбору
Файл сохранён окончательно	Сумма относится к этой версии
Нет необходимости загружать данные наружу	Вычисление сделано локально

Файл	Полное значение хранится в	Что сравниваю

5. Три файла одного размера

K147. Одинаковый размер не означает одинаковый файл

original.txt 43 байта, исходник	**H1**
renamed.txt 43 байта, копия с другим именем	**H1**
changed.txt 43 байта, изменено 100 на 101	**H2**

H1 и H2: метки схемы. Для сверки используйте полные SHA256.

H1 и H2 являются короткими метками схемы, не настоящими контрольными суммами.

Файл	Размер	Что сделано
original.txt	43 байта	Условная запись с числом 100
renamed.txt	43 байта	Побайтовая копия под другим именем
changed.txt	43 байта	Число 100 изменено на 101

У первых двух одинаковый хеш, у третьего другой. H1 и H2 на рисунке нужны для чтения схемы, не являются значениями SHA256. Полные результаты на следующей странице.

Файл	Что изменилось	Какой результат ожидаю проверить

6. Полные результаты опыта

original.txt и renamed.txt, SHA256:

5f3ee21105b4088a35ba014914a9be05
e161bb813dfb68c011aee05a377a622d

changed.txt, SHA256:

30d926a25d7aaeeb630e7ea537720113
472cd05bddefbc4f766a2acfc74bcda4

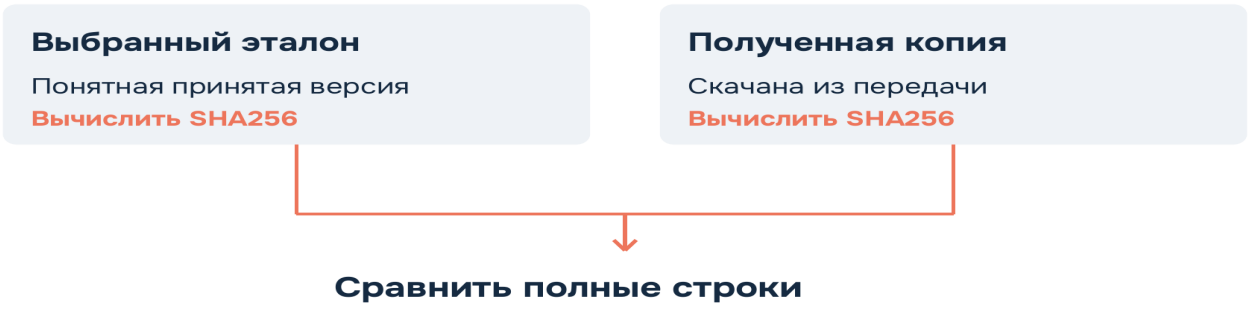
Строки разбиты на две части только для печати. При сравнении соедините их без пробелов и переносов. В каждом значении 64 шестнадцатеричных символа.

Проверка опыта	Результат
original.txt против renamed.txt	Совпало
original.txt против changed.txt	Не совпало
Python против shasum для всех трёх	3 совпадения из 3
Файлы одинакового размера	3 из 3 по 43 байта

Что не исследовано
Это маленький воспроизводимый опыт на TXT, не тест всех PDF и не проверка настоящей передачи клиенту. Полная строка относится только к сохранённым байтам примера.

7. Маршрут сверки полученной копии

K147. Два файла, один алгоритм, полные значения



Совпало: запись о копии. Различается: выяснить причину.

H1 и H2 являются короткими метками схемы, не настоящими контрольными суммами.

Контрольный вопрос	Почему важен
Выбран именно скачанный файл?	Иначе можно дважды проверить эталон
Эталон нужной версии?	Совпадение со старым не делает его актуальным
Одинаковый алгоритм?	Разные алгоритмы не сравнивают как одну сумму
Полные строки?	Короткий префикс недостаточен

Эталон	Полученная копия	Результат / дата

8. Если значения различаются

Возможная причина	Что выяснить
Выбрано старое вложение	Где находится нужная согласованная версия
После согласования выполнено сжатие	Кто создал новый файл и принят ли он
Файл пересохранён	Что изменилось, какой экземпляр передавать
Ошибка чтения	Есть ли вообще корректно вычисленный результат
Причина неизвестна	Сохранить обе версии и запросить уточнение

Заполненный пример
После согласования подборку сжали. Скачанная версия отличается от эталона. Следующий шаг: проверить новый файл, подтвердить его назначение, затем осознанно назначить новый эталон. Не менять эталон только ради совпадения.

Несовпадение	Причина / подтверждение	Решение / повторная проверка

9. Границы доверия

Утверждение	Почему его нельзя делать по одной сумме
Документ точно составил собственник	Хеш сам по себе не подтверждает автора
Все условия верны	Смысл документа не проверялся
Никто ничего не менял	Нужно знать происхождение эталона
Подпись проверена	Для подписи нужны отдельные механизмы
Копия не совпала, значит обман	Изменение может иметь обычную техническую причину

Эталонную сумму берут из доверенной записи или согласованного канала. Сверка файла и приложенной к нему неизвестной строки не устанавливает источник, если происхождение обоих неясно.

Что действительно проверено	Что не проверялось	Кому уточнить

10. Журнал одной передачи

Код / эталон	Копия / дата получения	Алгоритм / результат

Полные значения храните в связанной записи. После исправления снова проверьте конкретную копию, затем запишите результат и ответственного. Не ставьте отметку совпадения по внешнему виду страницы.

Первая практика
Начните с несекретного учебного файла. Отделите исходник от копии, выполните обе проверки и убедитесь, что понимаете источник каждого результата.

Диагностическая карта Нейросистемы риелтора помогает оценить общий путь материалов и обращений. К147 закрывает конкретную задачу: сверить переданный файл с выбранной версией.

Источники и проверка

Microsoft: Get-FileHash

NIST: хеш-функция

NIST: цифровая подпись