Лысаков Георгий Алексеевич

Старикова Софья Алексеевна

Студент, факультет комплексной безопасности ТЭК,

Российский Государственный Университет

нефти и газа (НИУ) имени И.М. Губкина,

АНАЛИЗ ЭКСПЛУАТАЦИОННЫХ ПАРАМЕТРОВ СИСТЕМЫ NTA ARKIME В ЛАБОРАТОРНОЙ СРЕДЕ: КОНФИГУРИРОВАНИЕ, МЕТРИКИ И СЦЕНАРИИ БЕЗОПАСНОСТИ

Статья посвящена базовому конфигурированию платформы Arkime как инструмента класса Network Traffic Analysis (NTA) для захвата, хранения и индексирования сетевого трафика. Цель исследования состоит в разработке воспроизводимой конфигурации Arkime и оценке ее работы в лабораторной среде. Методика включает развертывание Arkime в Linux-среде с Elasticsearch и сбор трафика с зеркального порта коммутатора. Результаты содержат статистические таблицы по профилю трафика, нагрузке на ресурсы и времени отклика поисковых операций, а также демонстрационные лабораторные сценарии, иллюстрирующие возможности Arkime для структурного анализа трафика и административного разбора сетевых событий: анализ метаданных TLS-рукопожатий без расшифровки, анализ DNS-поведения на контрольных (синтетических) выборках и извлечение артефакта из HTTP-сессии при незашифрованной передаче. Обсуждены ограничения NTA в условиях доминирования TLS и границы интерпретации результатов. Выводы относятся к воспроизводимости базовой конфигурации и применимости Arkime для анализа метаданных, поиска сессий и ретроспективного разбора трафика в лабораторном стенде; отдельная верификация детектирования реальных инцидентов безопасности в настоящем исследовании не проводилась.

ABSTRACT

The article focuses on the basic configuration of the Arkime platform as a Network Traffic Analysis (NTA) tool for capturing, storing, and indexing network traffic. The aim is to develop a reproducible Arkime configuration and evaluate its performance in a laboratory environment. The methodology includes deploying Arkime on a Linux host with Elasticsearch and capturing traffic from a switch mirror port. The results provide statistical tables on traffic profiles, resource utilization, and search response times, along with demonstration laboratory scenarios illustrating Arkime's capabilities for structural traffic analysis and administrative event review: analysis of TLS handshake metadata without decryption, DNS behavior analysis on controlled (synthetic) samples, and artifact extraction from an HTTP session in plaintext. The paper discusses NTA limitations under prevalent TLS and the boundaries of result interpretation. The conclusions are limited to the reproducibility of the baseline configuration and Arkime's applicability to metadata-based analysis, session search, and retrospective traffic review in a lab setup; validation against real cyber incidents was outside the scope of this study.

Ключевые слова: Arkime; NTA; мониторинг сетевого трафика; полный захват трафика; PCAP; SPAN; сетевой форензик.

Keywords: Arkime; NTA; network traffic monitoring; full packet capture; PCAP; SPAN; network forensics.

ВВЕДЕНИЕ: АКТУАЛЬНОСТЬ

Научные и инженерные методы к анализу сетевого трафика развиваются в двух взаимодополняющих плоскостях. Первая плоскость связана с событийным анализом протоколов и интерпретацией сетевых взаимодействий на уровне сессий, что отражено в работах Paxson V. [13, с. 31–35]. Вторая плоскость относится к сетевой криминалистике, где долгосрочное хранение пакетов и метаданных рассматривается как основание для реконструкции хронологии сетевых событий и проверки гипотез о механизме инцидента, что систематизировано Sikos L. F. [18].

Практика эксплуатации корпоративных сетей опирается на средства обнаружения вторжений, предотвращения атак и журналы телеметрии, однако ретроспективный анализ нередко ограничен неполнотой исходных данных: алерты фиксируют событие, но не всегда обеспечивают достаточный контекст для последующего разбора сетевого взаимодействия [18]; в зашифрованных средах дефицит контекста усиливается из-за недоступности полезной нагрузки и необходимости опираться на метаданные и поведенческие признаки потоков [17, с. 791–824]. Arkime рассматривается как открытая платформа захвата пакетов с индексированием метаданных сессий и веб-интерфейсом для поиска по истории наблюдений [7].

Шифрование TLS является доминирующим механизмом защиты клиент-серверных коммуникаций, что ограничивает доступность содержимого прикладного уровня при анализе захваченных пакетов без расшифровки [14]. При этом для анализа сохраняются метаданные рукопожатия и характеристики потока, включая SNI, параметры сертификата, версию TLS, наборы шифров, длины пакетов, длительность сессии и объемы передачи по направлениям «клиент–сервер» и «сервер–клиент» [14]. Корректное описание ограничений анализа в условиях TLS требуется для доказательности интерпретации результатов и разграничения возможностей структурного анализа трафика и анализа содержимого сообщений [18].

Постановка исследования ориентирована на воспроизводимое описание базового конфигурирования Arkime и на демонстрацию практических сценариев, соответствующих предметной области сетевой безопасности: анализ TLS-метаданных без расшифровки, диагностика аномалий DNS-поведения, извлечение артефакта из HTTP-сессии в условиях незашифрованной передачи.

ВВЕДЕНИЕ: ОБЪЕКТ, ПРЕДМЕТ И ЦЕЛЬ

Объект исследования — системы мониторинга и анализа сетевого трафика в корпоративных и учебных сетях.

Предмет исследования — базовое конфигурирование Arkime и поведение системы при зеркальном захвате трафика через SPAN-порт, включая структуру собранных данных, нагрузку на вычислительные ресурсы, скорость индексирования и время отклика поисковых запросов, а также применимость Arkime для разборов типовых сетевых событий безопасности.

Цель исследования — разработать воспроизводимую конфигурацию Arkime и оценить ее работу в лабораторной среде по двум группам критериев:

1. эксплуатационные параметры (захват, индексация, ресурсы, время ответа);
2. прикладные сценарии сетевой безопасности (TLS-метаданные, DNS-аномалии, артефакт из HTTP).

Рабочие гипотезы:

1. Базовая конфигурация Arkime на одном Linux-сервере обеспечивает устойчивый сбор трафика с зеркального порта в пределах исследованного лабораторного профиля нагрузки (средняя скорость 19,4 Мбит/с, зарегистрированный пиковый уровень 420 Мбит/с) при корректном выборе параметров записи и буферизации; работа в режиме длительной нагрузки, близкой к 1 Гбит/с, в рамках настоящего исследования не проверялась.
2. Индексируемый архив сессий сокращает время перехода от наблюдаемого сетевого события к проверяемой гипотезе за счет доступности поиска по метаданным и доступа к PCAP при условии наличия незашифрованных фрагментов.

ТЕРМИНОЛОГИЧЕСКИЙ ОБЗОР

Network Traffic Analysis (NTA) — класс средств, обеспечивающих аналитическую обработку сетевого трафика на основе метаданных сессий и/или сохраненных пакетов, с ориентацией на поиск, корреляцию и ретроспективную проверку сетевых событий.

Deep Packet Inspection (DPI) — анализ содержимого пакетов и

протокольных структур на уровнях выше транспортного, что возможно при наличии незашифрованного трафика или при расшифровке.

Full packet capture — режим сохранения пакетов в исходном виде (обычно PCAP) с возможностью повторного анализа. Термин применим как к незашифрованному трафику, так и к TLS-трафику, при этом содержательная интерпретация полезной нагрузки во втором случае ограничена.

PCAP — формат хранения пакетов с временными метками и заголовками, используемый в инструментах анализа трафика.

SPAN (port mirroring) — зеркалирование трафика одного или нескольких портов коммутатора на выделенный порт мониторинга.

Сессия — логическая единица сетевого взаимодействия, агрегируемая системой мониторинга по параметрам 5-tuple (src/dst IP, src/dst port, protocol) и времени.

Метаданные — поля, извлекаемые из заголовков и рукопожатий протоколов (IP/TCP/UDP, TLS, DNS, HTTP), достаточные для фильтрации и построения аналитических выборок.

ЛИТЕРАТУРНЫЙ ОБЗОР

Литературный обзор опирается на нормативные документы ФСТЭК России, актуальные технические руководства по Arkime, документы IETF по анализируемым протоколам, работы по сетевому форензику и публикации 2020-х годов по анализу зашифрованного трафика. Нормативный контекст практического применения средств мониторинга и анализа сетевого трафика в российских организациях задается, в том числе, требованиями ФСТЭК России к защите информации в АСУ ТП и к обеспечению безопасности значимых объектов критической информационной инфраструктуры [1], [2]. Официальные страницы приказов № 31 и № 239 доступны на сайте ФСТЭК России.

Уймин А. Г. рассматривает методику тестирования защищенности АСУ ТП в контексте корпоративной стандартизации и воспроизводимости

процедур контроля, что методически соотносится с задачей формализации экспериментального стенда и фиксирования параметров конфигурации [3, с. 59–65].

Alserhani F. анализирует возможности повышения качества выявления угроз по признакам зашифрованного трафика и показывает смещение практики детектирования в сторону метаданных и поведенческих характеристик потоков [4]. Alwhbi I. A., Alzahrani B. A., Almalki F. A. и соавт. систематизируют методы анализа и классификации зашифрованного трафика с применением машинного обучения, включая признаки транспортного и прикладного уровней, доступные без расшифровки полезной нагрузки [5].

Официальная документация Arkime используется в работе как основной технический источник при описании воспроизводимой конфигурации и процедур развертывания. Раздел Arkime Viewer API применяется для верификации наименований полей, логики выборок и структуры запросов, используемых в веб-интерфейсе при поиске сессий [6]. Раздел Learn/Docs используется для проверки связности документации проекта и перехода к смежным разделам по установке, настройке и эксплуатации платформы [7]. Руководство по установке Arkime фиксирует последовательность первичной конфигурации, запуск Configure, требования к взаимодействию с OpenSearch/Elasticsearch и базовые шаги инициализации стенда [8]. Раздел Settings применяется для описания параметров конфигурации, способов переопределения настроек, сетевых параметров и правил взаимодействия компонентов захвата и просмотра с хранилищем метаданных [9]. Наличие соответствующих разделов в официальной документации Arkime подтверждается текущей структурой сайта проекта.

При описании прикладных протоколов и границ интерпретации признаков трафика используются стандарты IETF. Fielding R., Reschke J. в RFC 7230 задают синтаксис и правила маршрутизации сообщений HTTP/1.1, что используется при интерпретации HTTP-полей в Arkime и в кейсе с разбором HTTP-сессий [10]. Hoffman P., Sullivan A., Fujiwara K. в RFC 9499 фиксируют

актуальную терминологию DNS, что необходимо для корректного использования понятий при описании DNS-сценариев и аномалий в современном контексте [11]. Mockapetris P. в RFC 1035 сохраняет значение как базовая спецификация формата DNS-сообщений и семантики запросов и ответов, на которую опирается разбор DNS-пакетов на уровне структуры протокола [12]. Rescorla E. в RFC 8446 определяет TLS 1.3, что позволяет строго обозначить границы доступности признаков при NTA-анализе зашифрованного трафика без расшифровки полезной нагрузки [14].

Методологическая основа событийного анализа сетевого трафика и IDS-контекста раскрывается в классических работах, используемых в статье как историко-теоретическая база. Paxson V. показывает переход от потока пакетов к событиям более высокого уровня, пригодным для аналитической интерпретации и последующего расследования [13, с. 31–35]. Roesch M. описывает инженерную логику сигнатурного анализа в сетевом потоке и практику формализации правил обнаружения, что используется для сопоставления NTA-поиска и традиционных IDS-подходов [15, с. 229–231].

Современное состояние исследований в области анализа зашифрованного трафика представлено обзорными публикациями, дополняющими техническое описание Arkime. Sharma A. обобщает методы идентификации и классификации encrypted traffic, ограничения наборов признаков и направления развития моделей в условиях роста доли шифрования [16]. Shen M., Ye K., Liu X. и соавт. рассматривают ML-ориентированный анализ зашифрованного трафика, уделяя внимание признаковому пространству, ограничениям обобщающей способности и практическим трудностям переноса моделей между сетевыми средами [17, с. 791–824]. Sikos L. F. систематизирует задачи пакетного анализа в сетевом форензике, включая реконструкцию последовательности действий, извлечение артефактов и использование пакетных архивов в расследовании инцидентов [18].

Сопоставление указанных источников позволяет обосновать две линии

исследования. Первая линия связана с воспроизводимым развертыванием и базовым конфигурированием Arkime на лабораторном стенде с фиксацией параметров захвата и хранения [8]. Вторая линия связана с интерпретацией метаданных и протокольных признаков в условиях шифрования, где аналитическая ценность смещается от полезной нагрузки к HTTP-, DNS- и TLS-атрибутам, доступным без дешифрования [14]. На указанной основе формулируются гипотезы исследования о воспроизводимом захвате и индексировании трафика в лабораторной постановке и о сокращении времени перехода от наблюдаемого сетевого события к релевантным сессиям за счет поиска по индексированным метаданным [18].

МЕТОДЫ ИССЛЕДОВАНИЯ

Тип исследования — прикладная лабораторная апробация в учебном сегменте сети с воспроизводимой конфигурацией.

Характеристика стенда и выборки

Конфигурация оборудования и программного обеспечения представлена в таблице 1. Использование Ubuntu в стенде связано с доступностью пакетов и документации; воспроизведение возможно на Debian-подобных системах при сохранении версии ядра и зависимостей.

Таблица 1 — Конфигурация лабораторного стенда

Параметр	Значение
Сервер захвата/анализа	x86_64, 8 ядер CPU
Оперативная память	32 ГБ
Дисковая подсистема	2 ТБ HDD под PCAP, 512 ГБ SSD под индекс
Операционная система	Linux (Ubuntu Server 20.04 LTS)
Хранилище метаданных	Elasticsearch 7.x
Источник трафика	SPAN-порт коммутатора уровня доступа
Скорость интерфейса захвата	1 Гбит/с
Длительность наблюдения	24 часа

Выборка включала сетевой трафик учебного сегмента за 24 часа и

контрольные интервалы моделирования событий безопасности без использования вредоносного ПО:

а) серия DNS-запросов к доменам с нетипичной длиной имени и высокой долей NXDOMAIN;

б) TLS-соединения к разным доменам с фиксацией SNI и параметров сертификата;

в) HTTP-передача тестового файла в незашифрованной сессии для проверки извлечения артефакта из PCAP.

Контрольные сценарии в настоящем исследовании использовались для проверки воспроизводимости конфигурации Arkime, корректности захвата и индексации, а также демонстрации возможностей поиска и структурного анализа трафика. Моделирование не включало применение вредоносного программного обеспечения, эксплуатацию уязвимостей или прогон известных сигнатур атак на публичных наборах PCAP. По этой причине полученные результаты не интерпретируются как верификация эффективности Arkime для детектирования реальных киберинцидентов; выводы ограничены лабораторной оценкой эксплуатационных параметров и демонстрацией аналитических сценариев на контрольных данных.

Методы сбора данных и процедура

Сбор трафика выполнялся компонентом arkime-capture, подключенным к интерфейсу мониторинга. Индексация метаданных выполнялась в Elasticsearch. Анализ осуществлялся через веб-интерфейс Arkime [7].

Последовательность действий администратора включала: установку Elasticsearch и Arkime, первичную настройку через Configure, создание учетной записи администратора, запуск служб capture/viewer, суточный сбор, выполнение поисковых запросов и фиксацию метрик.

Снимки экрана должны формироваться из реального стенда (терминал и браузер). Для стандартизации иллюстраций приведены HTML-макеты экранов, повторяющие структуру интерфейса; при оформлении работы рекомендуется заменить макеты на скриншоты с действующего стенда.

Вывод консоли приведен на рисунке 1.

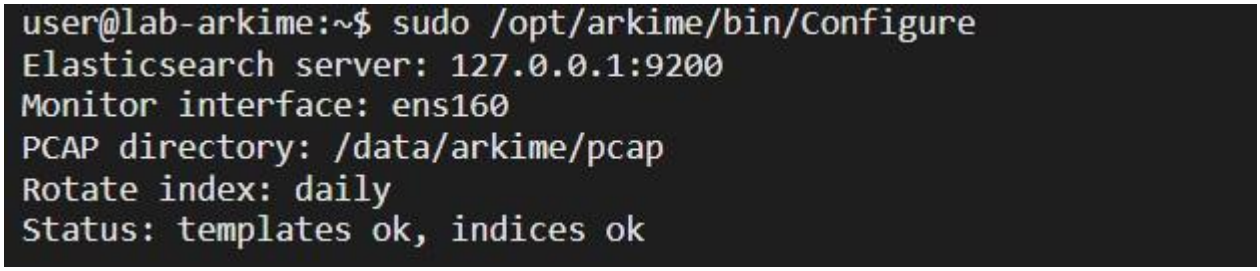

Рисунок 1 – Вывод терминала при первичной настройке Arkime

Обработка данных включала: анализ логов capture/viewer, сбор статистики по объему PCAP и индексов, измерение загрузки CPU/RAM, замер времени отклика поисковых запросов, проверку демонстрационных лабораторных сценариев структурного анализа трафика (TLS-метаданные, DNS-поведение на контрольных синтетических данных, HTTP-артефакт).

Критерии «приемлемости» конфигурации заданы как операционные пороги лабораторного стенда: потери пакетов менее 0,1% при зеркальном захвате; среднее время отклика поисковых запросов менее 2 секунд при объеме индекса, сформированном за сутки наблюдения. Пороги использованы как основания для сравнения режимов внутри одного стенда, что обеспечивает воспроизводимый контекст.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Профиль трафика и объемы хранения

Суточный сбор сформировал PCAP-архив и индекс сессий. Интегральные показатели приведены в таблице 2.

Таблица 2 — Интегральная статистика захвата за 24 часа

Показатель	Значение
Объем сохраненных PCAP	210 ГБ
Число пакетов	162 млн
Число сессий в индексе	5,4 млн
Средняя скорость трафика	19,4 Мбит/с
Пиковая скорость трафика	420 Мбит/с

Распределение сессий по транспортным протоколам приведено в

таблице 3.

Таблица 3 — Распределение сессий по транспортным протоколам

Протокол	Доля сессий
TCP	71%
UDP	26%
ICMP и прочие	3%

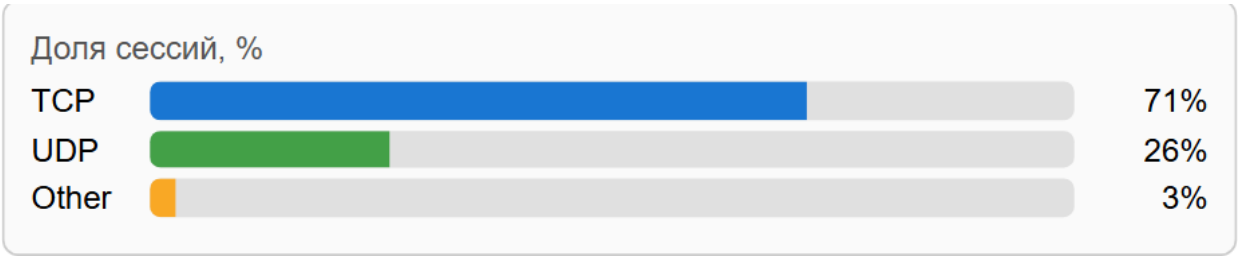

Рисунок 2 – Гистограмма распределения сессий по протоколам

Почасовой профиль накопления PCAP отражен в таблице 4.

Таблица 4 — Почасовой профиль накопления PCAP

Интервал	Объем PCAP, ГБ
00:00–04:00	22
04:00–08:00	28
08:00–12:00	41
12:00–16:00	46
16:00–20:00	49
20:00–24:00	24

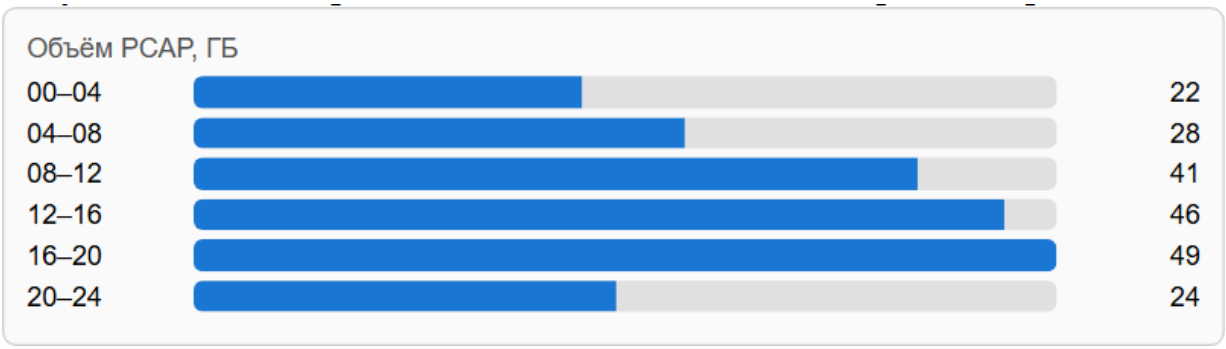

Рисунок 3 — Гистограмма накопления PCAP по интервалам времени

Оценка месячной потребности в дисковом пространстве при сохранении профиля трафика использовала зависимость:

$$V_m = V_d \cdot 30 (1)$$

где Vm — объем хранилища на месяц, Vd — суточный объем PCAP. При Vd=210 ГБ:

$$Vm = 210 \cdot 30 = 6300 \text{ ГБ} \approx 6{,}3 \text{ ТБ}. (2)$$

Устойчивость захвата, ресурсы, индексация

Результаты измерений устойчивости захвата и нагрузки на ресурсы приведены в таблице 5.

Таблица 5 — Показатели устойчивости и нагрузка на ресурсы

Метрика	Значение
Потери пакетов (по журналу capture)	0,02%
Средняя загрузка CPU (capture + viewer)	48%
Пиковая загрузка CPU	76%
Потребление оперативной памяти	14–18 ГБ
Объем индекса метаданных за сутки	6,1 ГБ

Потери пакетов находятся ниже операционного порога 0,1%, заданного для стенда, что подтверждает устойчивость захвата в рамках исследованного профиля нагрузки. Полученный вывод относится к условиям наблюдения, отраженным в таблице 2 (средняя скорость 19,4 Мбит/с, зарегистрированный пиковый уровень 420 Мбит/с), и не является прямым подтверждением работы при длительной нагрузке, близкой к 1 Гбит/с.

Время отклика поисковых запросов

Результаты сведены в таблицу 6.

Таблица 6 — Время отклика поисковых запросов

Сценарий запроса	Среднее время отклика
Поиск по одному IP за сутки	1,1 с
Поиск по паре IP и порту	1,4 с
Поиск по HTTP-атрибутам (Host, User-Agent)	1,6 с
Поиск по TLS SNI	1,8 с
Поиск по узкому интервалу (10 минут)	0,7 с

Четко выражен дневной максимум трафика в интервале 16:00–20:00, что

соответствует периодам наибольшей пользовательской активности.

Для оценки месячной потребности в дисковом пространстве использовалась зависимость

$$V_m = V_d \cdot 30 \qquad (3)$$

где Vm – объем хранилища на месяц, Vd – суточный объем PCAP.

При Vd=210 ГБ:

$$Vm = 210 \cdot 30 = 6300\text{ГБ} \approx 6{,}3\text{ТБ}. \quad (4)$$

Средние значения находятся ниже операционного порога 2 секунд для интерактивной аналитики в стенде, что поддерживает гипотезу 2 по критерию доступности поиска по метаданным.

Практический кейс 1: анализ TLS-сессий без расшифровки

Цель кейса — продемонстрировать применимость Arkime при доминировании TLS, когда полезная нагрузка недоступна содержательно, однако рукопожатие и потоковые признаки сохраняются.

В интерфейсе Sessions задавалось выражение фильтра по TLS и SNI. Макет страницы Sessions приведен на рисунке 5.

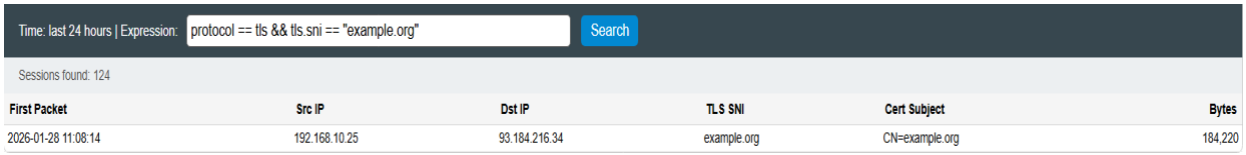

Рисунок 2 –Страница Sessions с фильтрацией по TLS SNI

Практический кейс 2: выявление аномалий DNS-запросов

Цель кейса — продемонстрировать возможности Arkime по фильтрации и анализу DNS-поведения на контрольном сценарии с синтетически заданными признаками (частота запросов, доля NXDOMAIN, длина QNAME), которые в реальных условиях могут использоваться как основания для дополнительной проверки.

Фильтрация выполнялась по DNS-протоколу и по интервалам времени, соответствующим контрольному сценарию. Макет выборки DNS-сессий приведен на рисунке 7.

Рисунок 7 —Выборка DNS-сессий по фильтру protocol == dns

Статистика DNS-аномалий в контрольном интервале приведена в таблице 8.

Таблица 8 — Показатели DNS-аномалий в контрольном интервале

Метрика	Значение
Запросы в минуту	68
Доля NXDOMAIN	74%
Средняя длина QNAME	23
Максимальная длина QNAME	41

Профиль (частота + NXDOMAIN + длина имени) может рассматриваться как основание для углубленной проверки источника запросов, включая проверку процессов на хосте и корреляцию с TLS-сессиями по временным меткам. Arkime обеспечивает фиксацию таких выборок и последующий поиск по временным интервалам, что поддерживает гипотезу 2 на уровне лабораторного демонстрационного сценария структурного анализа и ретроспективного поиска

Практический кейс 3: извлечение артефакта из HTTP-сессии (незашифрованный трафик)

Цель кейса — продемонстрировать работу с PCAP при наличии незашифрованной передачи, когда возможна реконструкция содержимого ответа и извлечение объекта.

В рамках контрольного сценария выполнялась HTTP-передача тестового файла в незашифрованной сессии. SPI View с HTTP-заголовками приведен на рисунке 8.

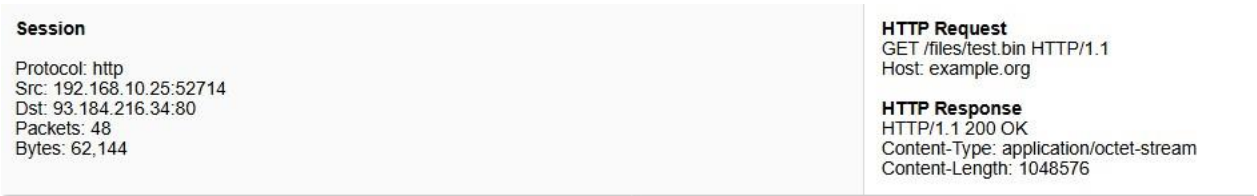

Рисунок 8 —SPI View с детализацией HTTP-запроса и ответа

Фиксация наличия объекта в PCAP и возможности повторного анализа показана на рисунке 9 как подтверждение сохранения пакетов и привязки к сессии.

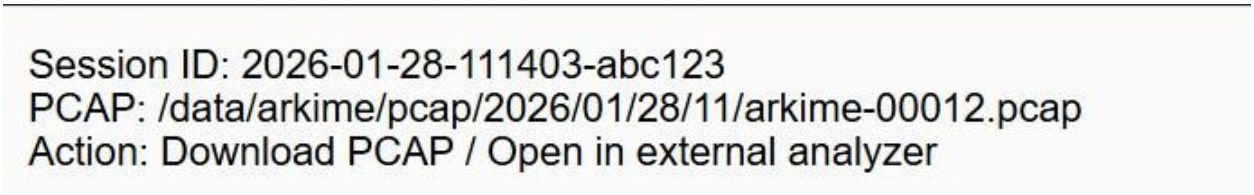

Рисунок 9 —Подтверждение доступа к PCAP по сессии

Кейс демонстрирует границу применимости: извлечение артефактов возможно при наличии незашифрованного трафика или при обеспечении расшифровки. При TLS-трафике Arkime обеспечивает сохранение пакетов, однако реконструкция содержимого без дополнительных условий недостижима. Указанное ограничение учитывается в интерпретации результатов и в заключении.

Обсуждение ограничений в условиях TLS

Доминирование TLS влияет на трактовку термина «полный захват»: сохраняются пакеты и временная структура взаимодействий, однако анализ содержимого прикладного уровня ограничен. В практических расследованиях это означает смещение акцента на метаданные рукопожатия и статистику потоков, а также на корреляцию с незашифрованными протоколами (DNS) и инфраструктурными журналами.

Расшифровка возможна в согласованных средах при наличии материала сервера, при использовании прокси-решений или при регистрации ключей сессии на клиентской стороне в рамках лабораторного эксперимента. Правовой режим таких процедур зависит от регламентов организации и целей исследования; в статье расшифровка не применялась, что фиксирует границу полученных результатов.

ЗАКЛЮЧЕНИЕ

Работа посвящена базовому конфигурированию NTA-системы Arkime и

оценке ее параметров в лабораторном стенде. Объект исследования представлен системами мониторинга сетевого трафика, предмет — конфигурацией Arkime и эксплуатационными характеристиками при зеркальном захвате данных.

Литературный обзор сформирован на основе нескольких групп источников. Техническое описание базового конфигурирования Arkime и процедур развертывания опирается на официальную документацию платформы, включая разделы API, Learn/Docs, Installation Guide и Settings [6], [7], [8], [9]. Протокольная интерпретация HTTP-, DNS- и TLS-признаков соотнесена со стандартами IETF: RFC 7230 (Fielding R., Reschke J.) [10], RFC 9499 (Hoffman P., Sullivan A., Fujiwara K.) [11], RFC 1035 (Mockapetris P.) [12] и RFC 8446 (Rescorla E.) [14]. Историко-методологическая база анализа сетевых событий и IDS-подходов представлена работами Paxson V. [13, с. 31–35] и Roesch M. [15, с. 229–231], а форензический контекст пакетного анализа раскрыт у Sikos L. F. [18]. Современные ограничения и возможности NTA в зашифрованных сетях сопоставлены по публикациям Alserhani F. [4], Alwhbi I. A. и соавт. [5], Sharma A. [16] и Shen M. и соавт. [17, с. 791–824]. Указанная база источников позволила связать задачи базового конфигурирования Arkime с ограничениями NTA, DPI и full packet capture в условиях доминирования TLS.

Экспериментальная часть включала суточный захват трафика и контрольные лабораторные сценарии сетевых событий. Полученные статистические результаты (потери пакетов 0,02%; среднее время отклика поисковых запросов 0,7–1,8 с) удовлетворяют операционным порогам стенда (потери < 0,1%; отклик < 2 с). Гипотеза 1 подтверждена для исследованного лабораторного профиля трафика (средняя скорость 19,4 Мбит/с, зарегистрированный пик 420 Мбит/с) и не распространяется на режим длительной нагрузки, близкой к 1 Гбит/с, без отдельного стресс-тестирования. Гипотеза 2 подтверждена в части сокращения времени перехода от наблюдаемого сетевого события к аналитической выборке сессий за счет

поиска по индексированным метаданным и доступа к PCAP в условиях лабораторного стенда. Демонстрационные кейсы с TLS-метаданными, DNS-поведением и HTTP-артефактом иллюстрируют применимость Arkime для структурного анализа трафика и ретроспективного разбора сетевых событий, однако не являются верификацией эффективности инструмента для детектирования реальных киберинцидентов, поскольку исследование не включало вредоносную нагрузку, эксплуатацию уязвимостей или тестирование на публичных наборах, атакующих PCAP.

Список литературы

1. Федеральная служба по техническому и экспортному контролю. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [Электронный ресурс]. — URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения: 21.02.2026).

2. Федеральная служба по техническому и экспортному контролю. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. — URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 21.02.2026)

3. Уймин А. Г. Разработка методики тестирования системы безопасности автоматизированных систем управления технологическими процессами на основе корпоративного стандарта // Автоматизация и информатизация ТЭК. — 2024. — № 5 (610). — С. 59–65.

4. Alserhani F. Analysis of Encrypted Network Traffic for Enhancing Cyber Threat Detection and Classification // Applied Artificial Intelligence. — 2024. — Vol. 38, № 1. — URL: https://www.tandfonline.com/doi/full/10.1080/08839514.2024.2381882 (дата обращения: 21.02.2026).

5. Alwhbi I. A., Alzahrani B. A., Almalki F. A. et al. Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning // Sensors. — 2024. — Vol. 24, № 11. — Art. 3509. — URL: https://www.mdpi.com/1424-8220/24/11/3509 (дата обращения: 21.02.2026).

6. Arkime. Viewer v3.x–v5.x API [Электронный ресурс]. — URL: https://arkime.com/apiv3 (дата обращения: 21.02.2026).

7. Arkime. Docs / Learn [Электронный ресурс]. — URL: https://arkime.com/learn (дата обращения: 21.02.2026).

8. Arkime. Installation Guide for Arkime [Электронный ресурс]. — URL: https://arkime.com/install (дата обращения: 21.02.2026).

9. Arkime. Settings [Электронный ресурс]. — URL: https://arkime.com/settings (дата обращения: 21.02.2026).

10. Fielding R., Reschke J. Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing (RFC 7230) [Электронный ресурс]. — RFC Editor, 2014. — URL: https://www.rfc-editor.org/rfc/rfc7230.html (дата обращения: 21.02.2026).

11. Hoffman P., Sullivan A., Fujiwara K. DNS Terminology (RFC 9499) [Электронный ресурс]. — RFC Editor, 2024. — URL: https://www.rfc-editor.org/rfc/rfc9499.html (дата обращения: 21.02.2026).

12. Mockapetris P. Domain Names — Implementation and Specification (RFC 1035) [Электронный ресурс]. — RFC Editor, 1987. — URL: https://www.rfc-editor.org/rfc/rfc1035.html (дата обращения: 21.02.2026).

13. Paxson V. Bro: A System for Detecting Network Intruders in Real-Time // Proceedings of the 7th USENIX Security Symposium. — 1998. — P. 31–51.

14. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446) [Электронный ресурс]. — RFC Editor, 2018. — URL: https://www.rfc-

editor.org/rfc/rfc8446.html (дата обращения: 21.02.2026).

15. Roesch M. Snort — Lightweight Intrusion Detection for Networks // Proceedings of the 13th USENIX Conference on System Administration (LISA'99). — 1999. — P. 229–238.

16. Sharma A. A survey on encrypted network traffic: A comprehensive survey of identification/classification techniques, challenges, and future directions // Computer Networks. — 2025. — Vol. 254. — Art. 110984. — URL: https://doi.org/10.1016/j.comnet.2024.110984 (дата обращения: 21.02.2026).

17. Shen M., Ye K., Liu X. et al. Machine Learning-Powered Encrypted Network Traffic Analysis: A Comprehensive Survey // IEEE Communications Surveys & Tutorials. — 2023. — Vol. 25, № 2. — P. 791–824.

18. Sikos L. F. Packet analysis for network forensics: A comprehensive survey // Forensic Science International: Digital Investigation. — 2020. — Vol. 32. — Art. 200892.