Расшифровка WIFI трафика в примерах

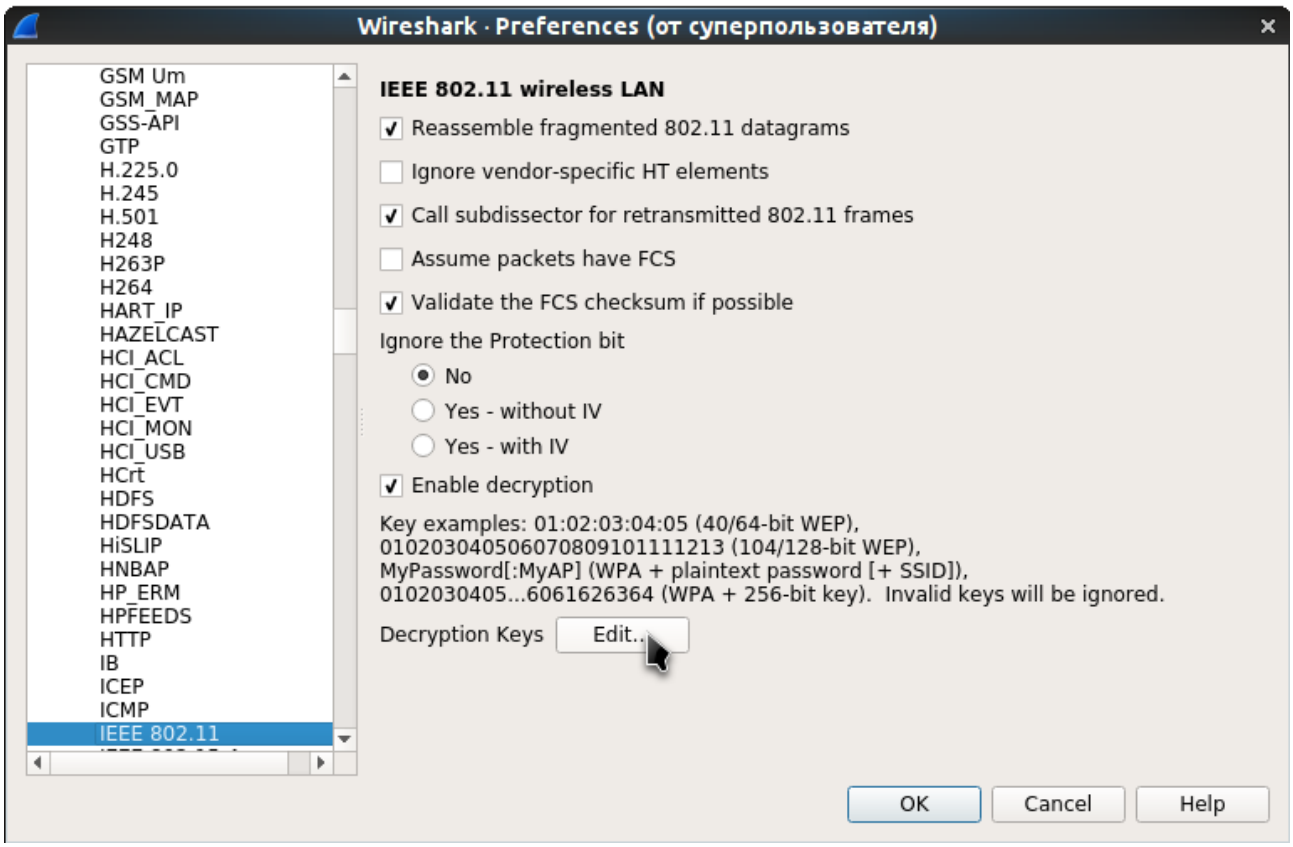
В общей логике аудита WIFI сетей заказчика, неизбежен диалог позиции защиты и вектора дальнейшего развития общей защиты WIFI сетей заказчика.

В 60% случаев заказчика не пугает возможность использования его сетей сторонними лицами. Рекомендуется провести анализ и демонстрацию полной расшифровки WIFI трафика в сети заказчика.

Общедоступные методы расшифровки WIFI трафика, программа **Wireshark** и **airdecap-ng**.

Wireshark

Для понимания полноты действия настроек, обратитесь к документации разработчика (https://wiki.wireshark.org/HowToDecrypt802.11).



Общие правила описания ключей в программе:

- **wep** The key is parsed as a WEP key.

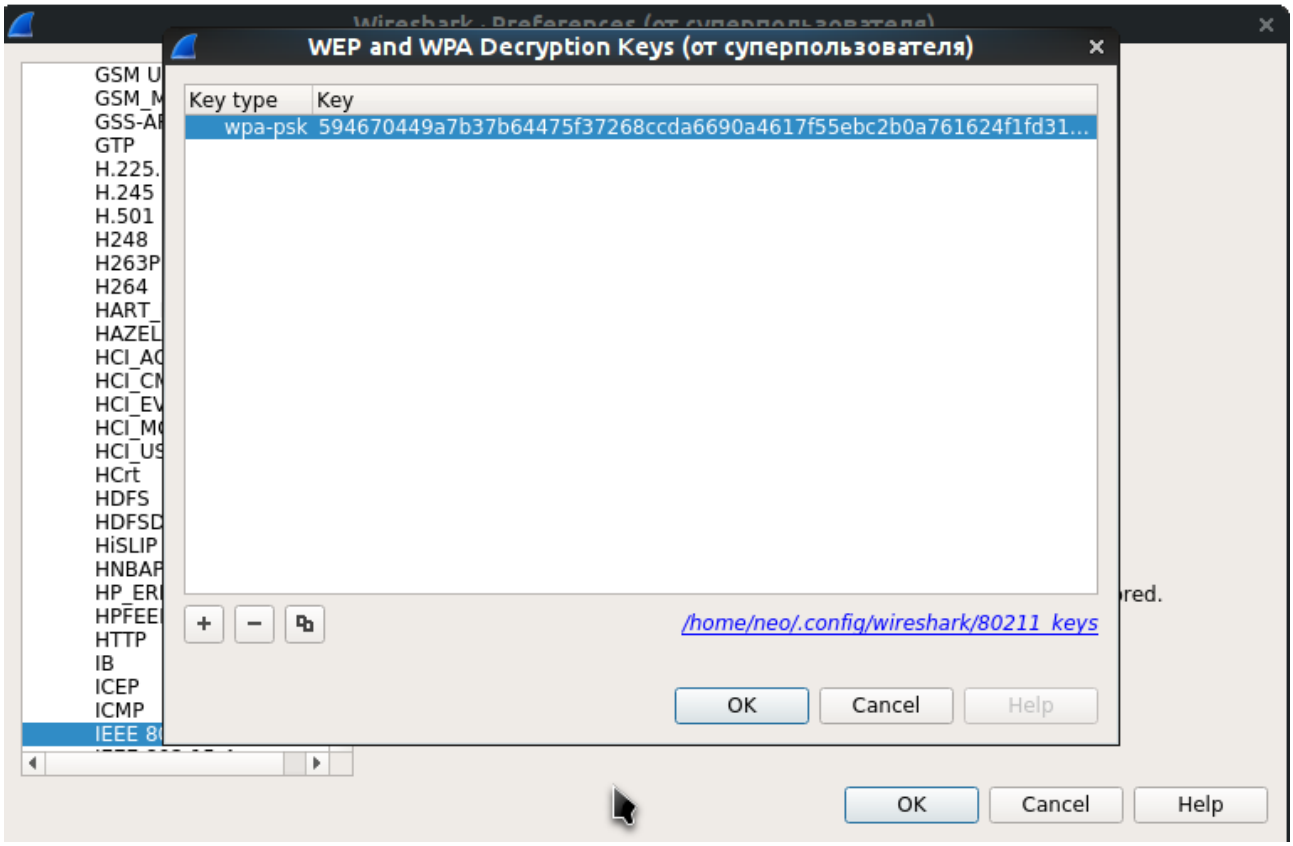
```
wep:a1:b2:c3:d4:e5
```

- **wpa-pwd** The password and SSID are used to create a raw pre-shared key.

```
wpa-pwd:MyPassword:MySSID
```

- **wpa-psk** The key is parsed as a raw pre-shared key.

```
Wpa-psk:010203040506070809101l...6061626364
```



Захваченный файл должен иметь четыре корректных **handshake**. Для этой цели файл имеющий (пакеты 2 и 3) или (пакеты 3 и 4) будет работать правильно.

Онлайн генераторы ключей для **Wireshark…**

https://www.wireshark.org/tools/wpa-psk.html

Airdecap-ng

Он создает новый файл с расширением ”-dec.cap”, который является расшифрованной версией входящего файла.

Использование

airdecap-ng [параметры]

Параметр	Значение	Описание
-l		Не удалять 802.11 заголовки
-b	bssid	Точка доступа, фильтрация по MAC-адресам
-k	pmk	WPA/WPA2 парный мастер-ключ в шестнадцатеричном виде
-e	essid	Целевая сеть по ascii идентификатору
-p	pass	Целевая сеть WPA/WPA2 парольная фраза
-w	key	Целевая сеть WEP-ключ в шестнадцатеричном виде

Примеры использования

Следующая команда удалит заголовки из открытой сети (без **WEP**) захвата:

airdecap-ng -b 00:09:5B:10:BC:5A open-network.cap

Следующая команда расшифровывает **WEP-**шифрование захваченное с использованием шестнадцатеричного **WEP**-ключа:

airdecap-ng -w 11A3E229084349BC25D97E2939 wep.cap

Следующая команда расшифровывает зашифрованный **WPA/WPA2** захваченный пакет с использованием парольной фразы:

airdecap-ng -e ‘the ssid’ -p passphrase tkip.cap

Захваченный файл должен иметь четыре корректных **handshake**. Для этой цели файл имеющий (пакеты 2 и 3) или (пакеты 3 и 4) будет работать правильно.

Вывод отладки скрипта...

IT-Karro WiFi Scripts

Total number of packets read 602243

Total number of WEP data packets 0

Total number of WPA data packets 135891

Number of plaintext data packets 0

Number of decrypted WEP packets 0

Number of corrupted WEP packets 0

Number of decrypted WPA packets 105190

Done…

Используйте **Wireshark** для анализа декодированных пакетов.

Методы и программы для перехвата WIFI трафика не рассматриваются.

http://crimea-karro.ru/dev_karro/b_scripts.html
http://crimea-karro.ru/download/WiFi_scripts.tar.bz2