Лабораторная работа №6

Исследование дампа машины Tesla

Выполнили:

Ким Анастасия

Завьялова Вероника

Казачкова Олеся

Лабораторная работа выполнена с учетом статей 272 и 273 УК РФ.

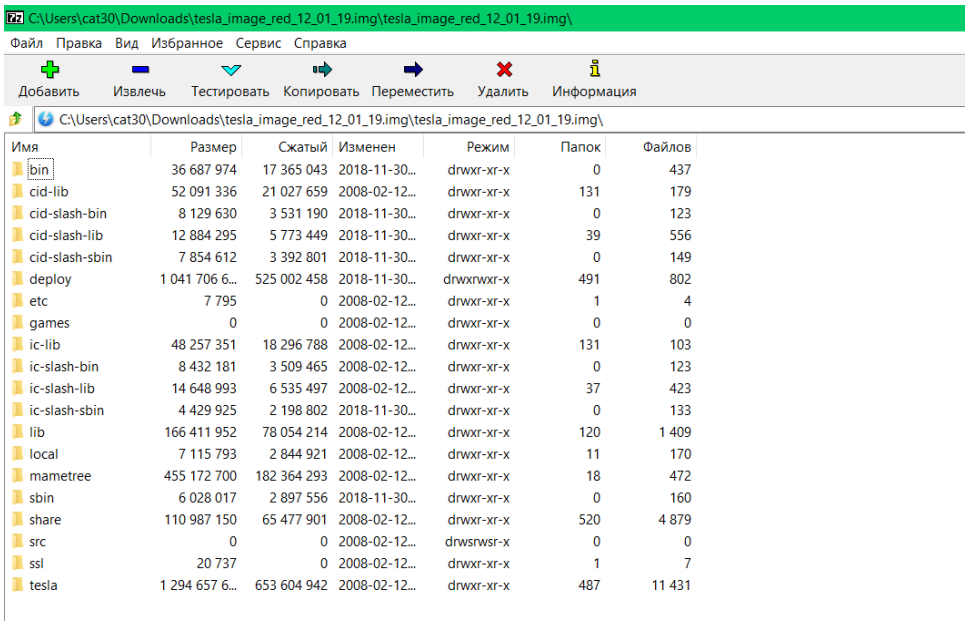
Постановка задачи: скачать образ виртуальной машины

Техническое задание:

Необходимо провести анализ дампа операционной системы машины Tesla (да, той самой, 19го года). Необходимо построить схему работы приложений внутри, большая часть из которых являются веб приложениями. Внутри существует множество папок и файлов, содержащие различные веб приложения, документацию, бортовые системы и т.д. Образ 19го года, поэтому данные приложения являются уязвимыми. Необходимо найти как минимум 2 уязвимости, либо руководствуясь исходниками, которые есть в образе, либо можно запустить сервисы и найти их вручную и эксплуатировать. Результатом работы будет карта образа, в любом удобном для вас виде, mindmap, дерево папок с описанием и т.д., где должны быть описаны ключевые сервисы, присутствующие в дампе. Второй частью задания найти уязвимости в данном дампе. С образом разрешено производить все виды манипуляций. Лабораторная работа выполняется в группе от 2-х до 5 человек.

1. Установка образа виртуальной машины

Ссылка: https://disk.yandex.ru/d/4J_tc2sAFwtiDg



Имя	Размер	Сжатый	Изменен	Режим	Папок	Файлов
bin	36 687 974	17 365 043	2018-11-30...	drwxr-xr-x	0	437
cid-lib	52 091 336	21 027 659	2008-02-12...	drwxr-xr-x	131	179
cid-slash-bin	8 129 630	3 531 190	2018-11-30...	drwxr-xr-x	0	123
cid-slash-lib	12 884 295	5 773 449	2018-11-30...	drwxr-xr-x	39	556
cid-slash-sbin	7 854 612	3 392 801	2018-11-30...	drwxr-xr-x	0	149
deploy	1 041 706 6...	525 002 458	2018-11-30...	drwxrwxr-x	491	802
etc	7 795	0	2008-02-12...	drwxr-xr-x	1	4
games	0	0	2008-02-12...	drwxr-xr-x	0	0
ic-lib	48 257 351	18 296 788	2008-02-12...	drwxr-xr-x	131	103
ic-slash-bin	8 432 181	3 509 465	2008-02-12...	drwxr-xr-x	0	123
ic-slash-lib	14 648 993	6 535 497	2008-02-12...	drwxr-xr-x	37	423
ic-slash-sbin	4 429 925	2 198 802	2018-11-30...	drwxr-xr-x	0	133
lib	166 411 952	78 054 214	2008-02-12...	drwxr-xr-x	120	1 409
local	7 115 793	2 844 921	2008-02-12...	drwxr-xr-x	11	170
mametree	455 172 700	182 364 293	2008-02-12...	drwxr-xr-x	18	472
sbin	6 028 017	2 897 556	2018-11-30...	drwxr-xr-x	0	160
share	110 987 150	65 477 901	2008-02-12...	drwxr-xr-x	520	4 879
src	0	0	2008-02-12...	drwsrwsr-x	0	0
ssl	20 737	0	2008-02-12...	drwxr-xr-x	1	7
tesla	1 294 657 6...	653 604 942	2008-02-12...	drwxr-xr-x	487	11 431

2. Поиск уязвимостей

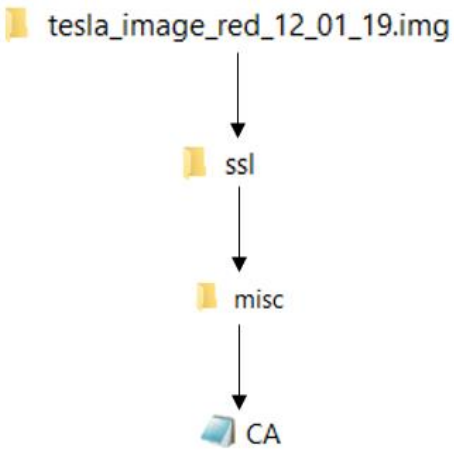
Перед рассмотрением папок внимательно изучим количество содержащихся в них файлов.

Сразу исключаем две пустые папки: games и src.

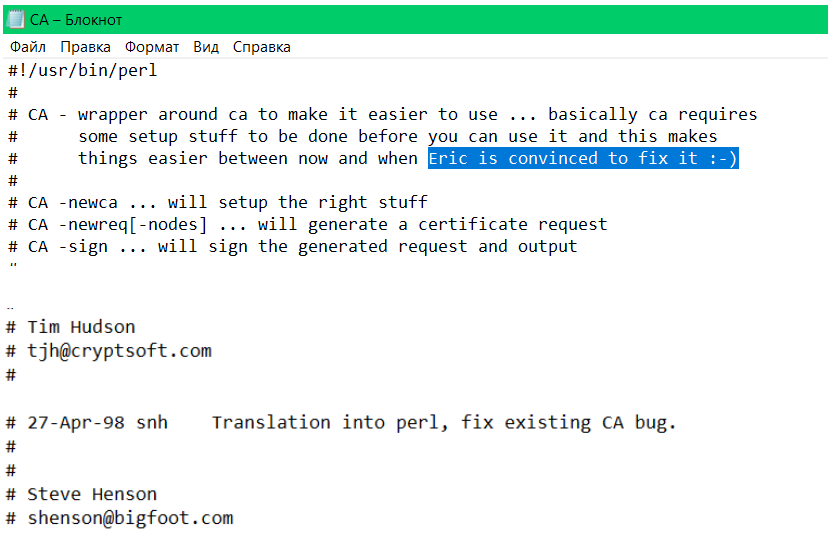
Далее, переходим к рассмотрению папок ssl и etc, поскольку в них содержится наименьшее количество файлов и их изучение не займет много времени.

2.1 Изучение папки ssl.

Путь к папке: C:\tesla_image_red_12_01_19.img\ssl\misc\CA.pl



Файлы, полученные при изучении папки:


CA – Блокнот

Файл Правка Формат Вид Справка

```
#!/usr/bin/perl
#
# CA - wrapper around ca to make it easier to use ... basically ca requires
#      some setup stuff to be done before you can use it and this makes
#      things easier between now and when Eric is convinced to fix it :-)
#
# CA -newca ... will setup the right stuff
# CA -newreq[-nodes] ... will generate a certificate request
# CA -sign ... will sign the generated request and output
"

..
# Tim Hudson
# tjh@cryptsoft.com
#

# 27-Apr-98 snh    Translation into perl, fix existing CA bug.
#
#
# Steve Henson
# shenson@bigfoot.com
```

Результатом исследования стали полученны упоминания Tim Hudson и Steve Hunson, которые были использованы для упоминания автора используемой библиотеки и создателя программного обеспечения. По итогу данная информация не принесла пользы.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

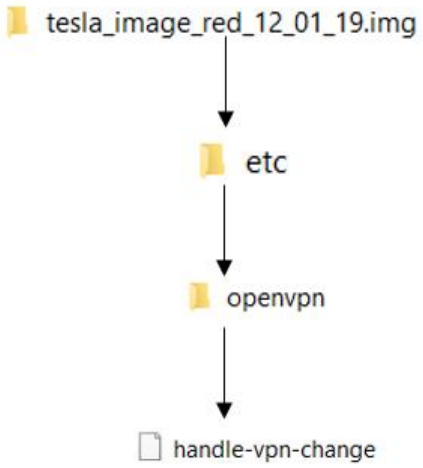
Telif Hakkı(C) 1995-1998 Eric Young (eay@cryptsoft.com) Her hakkı saklıdır.

Bu paket Eric Young tarafından yazılmış olan bir SSL uyarlamasıdır(eay@cryptsoft.com). Uyarlama Netscapes SSL ile uyumlu çalışmak üzere yazılmıştır.

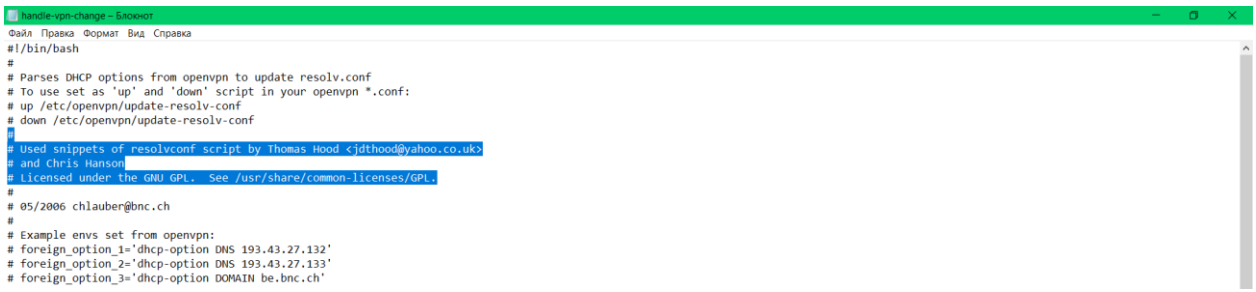
This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

2.2 Изучение папки etc

Путь к папке: C: \tesla_image_red_12_01_19.img\etc\openvpn\handle-vpn-change



Файлы, полученные при изучении папки:


handle-vpn-change – Блокнот

Файл Правка Формат Вид Справка

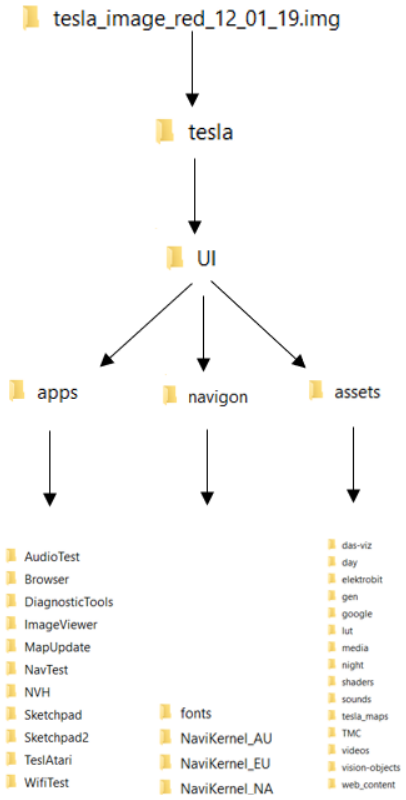
```
#!/bin/bash
#
# Parses DHCP options from openvpn to update resolv.conf
# To use set as 'up' and 'down' script in your openvpn *.conf:
# up /etc/openvpn/update-resolv-conf
# down /etc/openvpn/update-resolv-conf
#
# Used snippets of resolvconf script by Thomas Hood <jdthood@yahoo.co.uk>
# and Chris Hanson
# Licensed under the GNU GPL.  See /usr/share/common-licenses/GPL.
#
# 05/2006 chlauber@bnc.ch
#
# Example envs set from openvpn:
# foreign_option_1='dhcp-option DNS 193.43.27.132'
# foreign_option_2='dhcp-option DNS 193.43.27.133'
# foreign_option_3='dhcp-option DOMAIN be.bnc.ch'
```

Результатами исследований стали упоминания авторов скриптов, которые также не принесли полезной информации для работы.

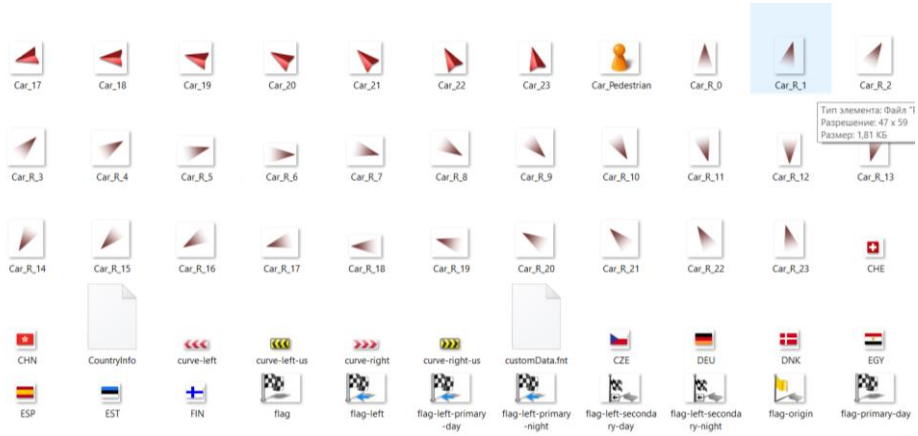
2.3 Изучение папки tesla

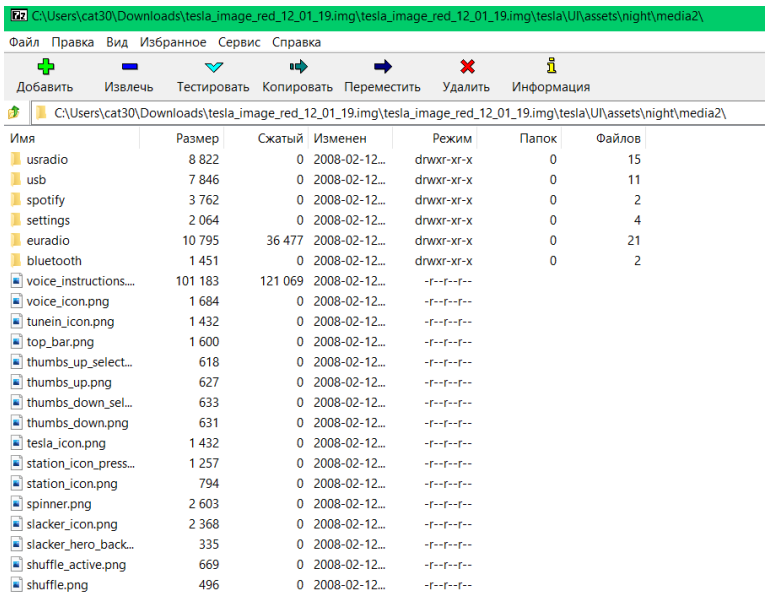
Путь к папкам:

C:\tesla_image_red_12_01_19.img\tesla\

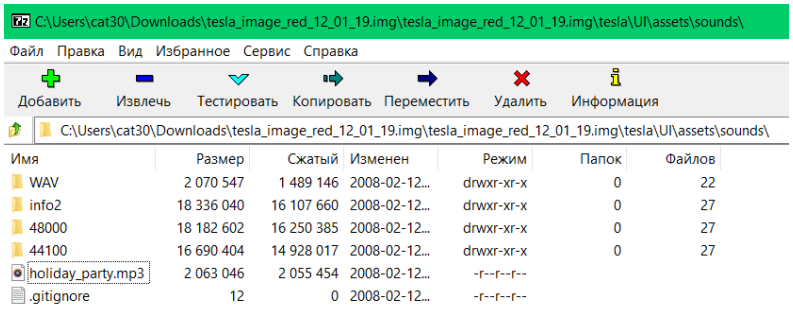


Файлы, полченные при изучении папки:

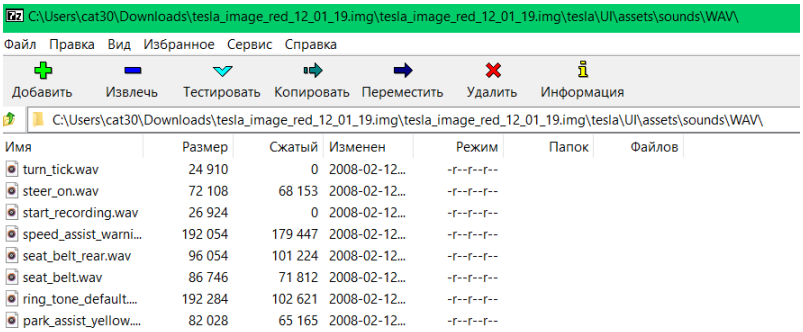




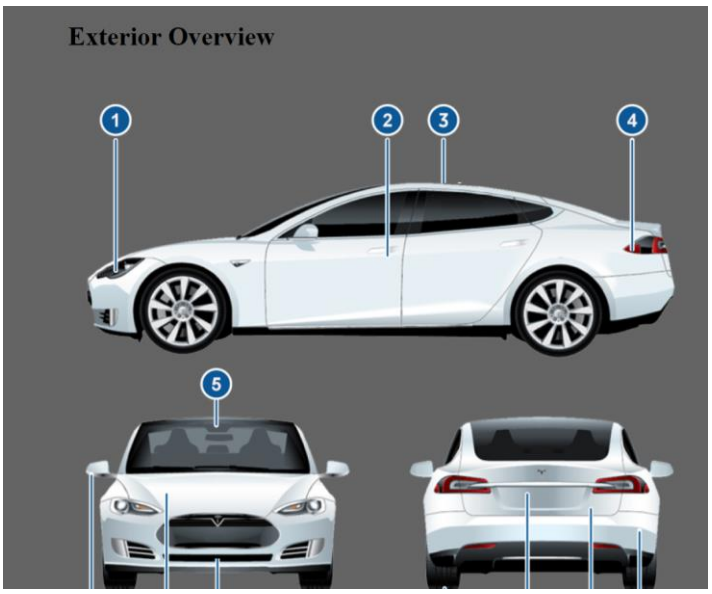
Имя	Размер	Сжатый	Изменен	Режим	Папок	Файлов
usradio	8 822	0	2008-02-12...	drwxr-xr-x	0	15
usb	7 846	0	2008-02-12...	drwxr-xr-x	0	11
spotify	3 762	0	2008-02-12...	drwxr-xr-x	0	2
settings	2 064	0	2008-02-12...	drwxr-xr-x	0	4
euradio	10 795	36 477	2008-02-12...	drwxr-xr-x	0	21
bluetooth	1 451	0	2008-02-12...	drwxr-xr-x	0	2
voice_instructions....	101 183	121 069	2008-02-12...	-r--r--r--		
voice_icon.png	1 684	0	2008-02-12...	-r--r--r--		
tunein_icon.png	1 432	0	2008-02-12...	-r--r--r--		
top_bar.png	1 600	0	2008-02-12...	-r--r--r--		
thumbs_up_select...	618	0	2008-02-12...	-r--r--r--		
thumbs_up.png	627	0	2008-02-12...	-r--r--r--		
thumbs_down_sel...	633	0	2008-02-12...	-r--r--r--		
thumbs_down.png	631	0	2008-02-12...	-r--r--r--		
tesla_icon.png	1 432	0	2008-02-12...	-r--r--r--		
station_icon_press...	1 257	0	2008-02-12...	-r--r--r--		
station_icon.png	794	0	2008-02-12...	-r--r--r--		
spinner.png	2 603	0	2008-02-12...	-r--r--r--		
slacker_icon.png	2 368	0	2008-02-12...	-r--r--r--		
slacker_hero_back...	335	0	2008-02-12...	-r--r--r--		
shuffle_active.png	669	0	2008-02-12...	-r--r--r--		
shuffle.png	496	0	2008-02-12...	-r--r--r--		



Имя	Размер	Сжатый	Изменен	Режим	Папок	Файлов
WAV	2 070 547	1 489 146	2008-02-12...	drwxr-xr-x	0	22
info2	18 336 040	16 107 660	2008-02-12...	drwxr-xr-x	0	27
48000	18 182 602	16 250 385	2008-02-12...	drwxr-xr-x	0	27
44100	16 690 404	14 928 017	2008-02-12...	drwxr-xr-x	0	27
holiday_party.mp3	2 063 046	2 055 454	2008-02-12...	-r--r--r--		
.gitignore	12	0	2008-02-12...	-r--r--r--		



Имя	Размер	Сжатый	Изменен	Режим	Папок	Файлов
turn_tick.wav	24 910	0	2008-02-12...	-r--r--r--		
steer_on.wav	72 108	68 153	2008-02-12...	-r--r--r--		
start_recording.wav	26 924	0	2008-02-12...	-r--r--r--		
speed_assist_warni...	192 054	179 447	2008-02-12...	-r--r--r--		
seat_belt_rear.wav	96 054	101 224	2008-02-12...	-r--r--r--		
seat_belt.wav	86 746	71 812	2008-02-12...	-r--r--r--		
ring_tone_default....	192 284	102 621	2008-02-12...	-r--r--r--		
park_assist_yellow....	82 028	65 165	2008-02-12...	-r--r--r--		
park_assist_red_re...	47 096	0	2008-02-12...	-r--r--r--		
park_assist_red.wav	76 844	101 896	2008-02-12...	-r--r--r--		
park_assist_green....	192 044	109 451	2008-02-12...	-r--r--r--		
lock_chime.wav	68 176	0	2008-02-12...	-r--r--r--		
lane_departure_w...	50 958	92 386	2008-02-12...	-r--r--r--		
hands_on_now.wav	53 512	0	2008-02-12...	-r--r--r--		
forward_collision_...	68 876	104 166	2008-02-12...	-r--r--r--		
convert.sh	643	0	2008-02-12...	-r-xr-xr-x		
autopilot_unavaila...	72 506	68 233	2008-02-12...	-r--r--r--		
alert_chime.wav	192 044	78 801	2008-02-12...	-r--r--r--		
acc_steer_on.wav	86 840	77 823	2008-02-12...	-r--r--r--		
acc_steer_off.wav	200 964	123 023	2008-02-12...	-r--r--r--		
acc_on.wav	114 762	80 942	2008-02-12...	-r--r--r--		
acc_off.wav	72 174	64 003	2008-02-12...	-r--r--r--		



- Owner's Manual
  - Overview
    - Interior Overview
    - Exterior Overview
    - Touchscreen Overview
  - Opening and Closing
    - Keys
    - Doors
    - Doors
    - Windows
    - Rear Trunk
    - Front Trunk
    - Interior Storage and Electronics
    - Sunroof
    - Sun Visors
  - Seating and Safety Restraints
    - Front and Rear Seats
    - Seat Belts
    - Child Safety Seats
    - Tesla Built-In Rear Facing Child Seats
    - Airbags
  - Driving
    - Driver Profiles
    - Steering Wheel
    - Mirrors
    - Starting and Powering Off
    - Gears
    - Lights
    - Lights
    - Car Status
    - Instrument Panel
    - Wipers and Washers
    - Brakes
    - Traction Control
    - Cruise Control
    - Park Assist
    - Vehicle Hold
    - Hill Start Assist

Authenticated Phone

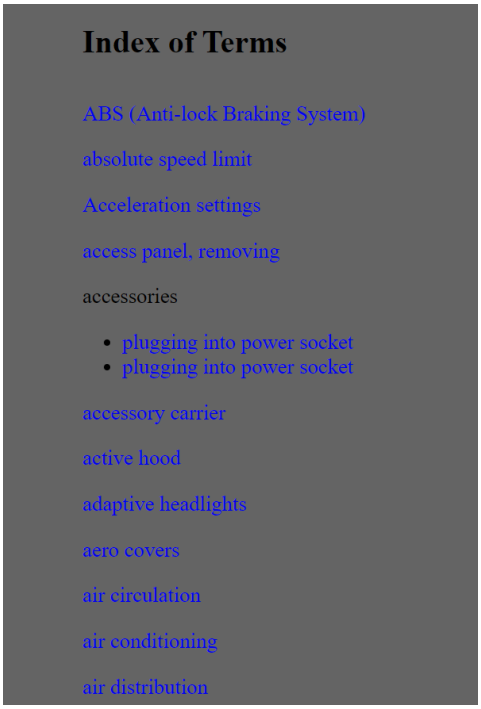
Using your phone is the most convenient way to access your Model 3. As you approach, your phone's Bluetooth signal is detected and doors unlock when you press a door handle. Likewise, when you exit and walk away with the phone, doors automatically lock (provided the **Walk-Away Door Lock** feature is turned on, as described in Walk-Away Door Lock).

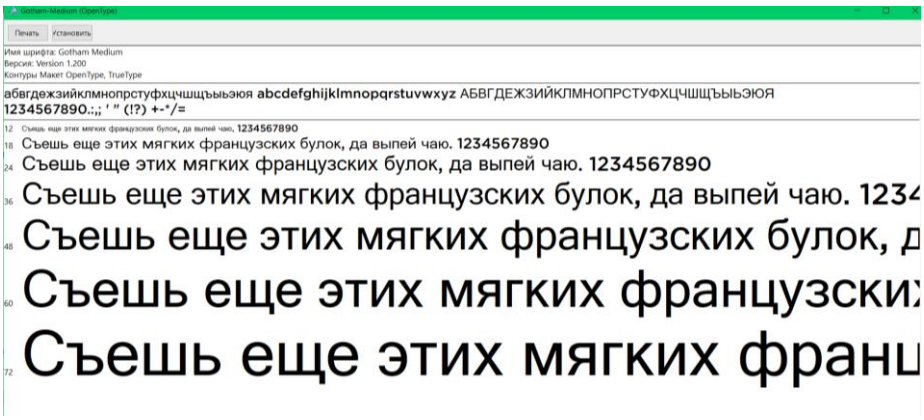
Before you can use a phone to access Model 3, follow these steps to authenticate it:

1. Download the Tesla mobile app to your phone.
2. Log into the Tesla mobile app using your Tesla Account user name and password.

   Note: You must remain logged in to your Tesla Account to use your phone to access Model 3.
3. Ensure that your phone's Bluetooth setting is turned on.

   Note: Model 3 communicates with your phone using Bluetooth. To authenticate your phone or use it as a key, the phone must be powered on and Bluetooth must be enabled. Keep in mind that your phone must have enough battery power to run Bluetooth and that many phones disable Bluetooth when the battery is low.





Было обнаружено большое количество иконок и различных логотипов в формате png, также различные заставки видео, стили и шрифты, mp3 файлы, используемые в приложении, инструкция по применению включающая в себя обзор автомобиля, инструкцию по открытию и закрытию, управление средствами безопасности, глоссарий терминов и т.п

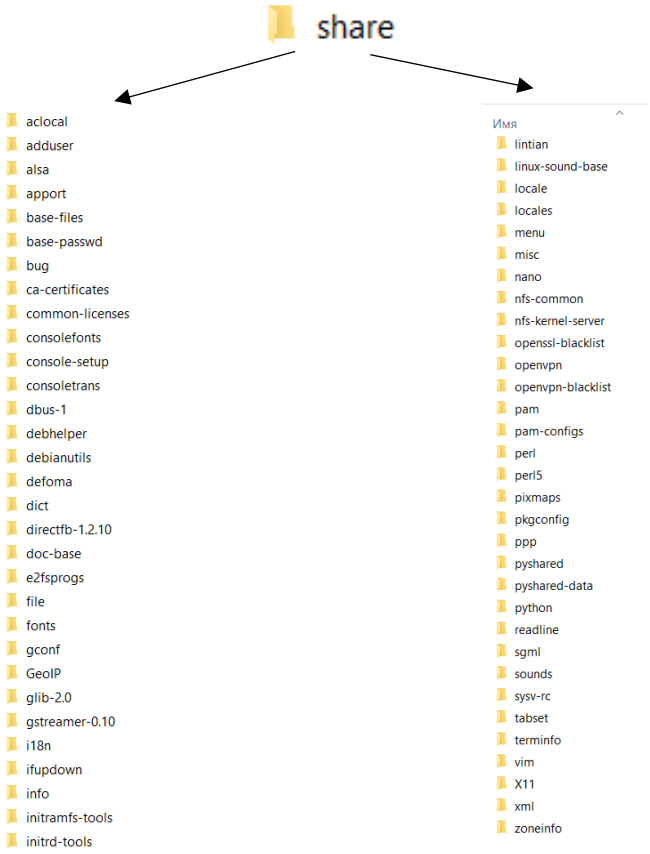
Таким образом, папка tesla не содержит в себе полезных данных.

2.4 Изучение папок share, sbin

Путь к папкам:

C:\tesla_image_red_12_01_19\sbin

C:\tesla_image_red_12_01_19\share



В результате не было обнаружено необходимой информации, поскольку указанные папки содержали в себе системные файлы, информацию об обновлениях и т.п.

Вывод

Таким образом, в ходе исследования дампа машины Tesla не было получено полезной для взлома информации.

Однако были получены:

- знания об использовании машины Tesla
- знания о механическом строении машины Tesla
- знания о системном наполнении машины Tesla
- знания о используемом шрифте в навигации Tesla
- знания терминологии машины Tesla
- красивые видеозаставки
- mp3 дорожки