МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»

ИМКТ

Департамент информационной безопасности

Тананов Алексей Александрович
Жуков Владимир Владимирович

M9120-09.04.02ибкфс

ЛР № 6

«Исследование дампа машины Tesla»

г. Владивосток

2022

Постановка задачи:

Необходимо провести анализ дампа операционной системы машины Tesla. 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.

Был рассмотрен образ системы tesla_image_red_12_01_19.img

Построено дерево папок с указанием их содержимого.

/bin - содержит стандартные утилиты

/cid-lib - библиотеки для управления процессором, дисплеем и медиасистемами (cid - Center Display)

    /cid-lib/...

/cid-slash-bin

/cid-slash-lib

    /cid-slash-lib/...

/cid-slash-sbin

/deploy - ПО для развёртывания системы

    /deploy/...

/etc - содержит конфигурационные файлы

    /etc/openvpn - содержит конфиги и скрипт для openvpn

/games - пустой каталог

/ic-lib - библиотека для управления процессором, дисплеем и медиасистемами (ic - Instrument Cluster)

    /ic-lib/...

/ic-slash-bin

/ic-slash-lib

    /ic-slash-lib/...

/ic-slash-sbin

/lib - библиотеки и модули ядра

    /lib/...

/local - содержит пользовательские файлы

    /local/bin - утилиты, используемые интерфейсом

    /local/etc - пустой

    /local/games - пустой

    /local/include - пустой

    /local/lib - пустой

    /local/sbin - пустой

    /local/share - пустой

    /local/src - пустой

/mametree - эмулятор

    /mametree/lib - библиотеки эмулятора

    /mametree/opt - каталог для установленных программ эмулятора

        /mametree/opt/mame

            /mametree/opt/mame/rom

/mametree/usr - содержит пользовательские файлы эмулятора, в т.ч. файлы мультимедийного фреймворка gstreamer

/mametree/usr/...

/sbin - набор утилит для системного администрирования

/share - содержит общие файлы, документы, пакеты

/share/...

/src - пустой каталог

/ssl - содержит конфиг ssl

/ssl/misk - содержит скрипты для ssl

/tesla - каталог tesla

/tesla/UI - интерфейс

/tesla/UI/apps - приложения

/tesla/UI/apps/AudioTest

/tesla/UI/apps/Browser - браузер

/tesla/UI/apps/DiagnosticTools - приложение для диагностики автомобиля

/tesla/UI/apps/DiagnosticTools/assets

/tesla/UI/apps/DiagnosticTools/assets/thermalscreen - интерфейс

/tesla/UI/apps/ImageViewer

/tesla/UI/apps/MapUpdate

/tesla/UI/apps/NavTest

/tesla/UI/apps/NVH

/tesla/UI/apps/Sketchpad

/tesla/UI/apps/Sketchpad2

/tesla/UI/apps/TestAtari

/tesla/UI/apps/WifiTest

/tesla/UI/assets - файлы дизайна, приложений интерфейса, озвучка и тп.

/tesla/UI/assets/...

/tesla/UI/bin - утилиты, вызываемые из интерфейса

/tesla/UI/bin/...

/tesla/UI/lib - библиотеки интерфейса

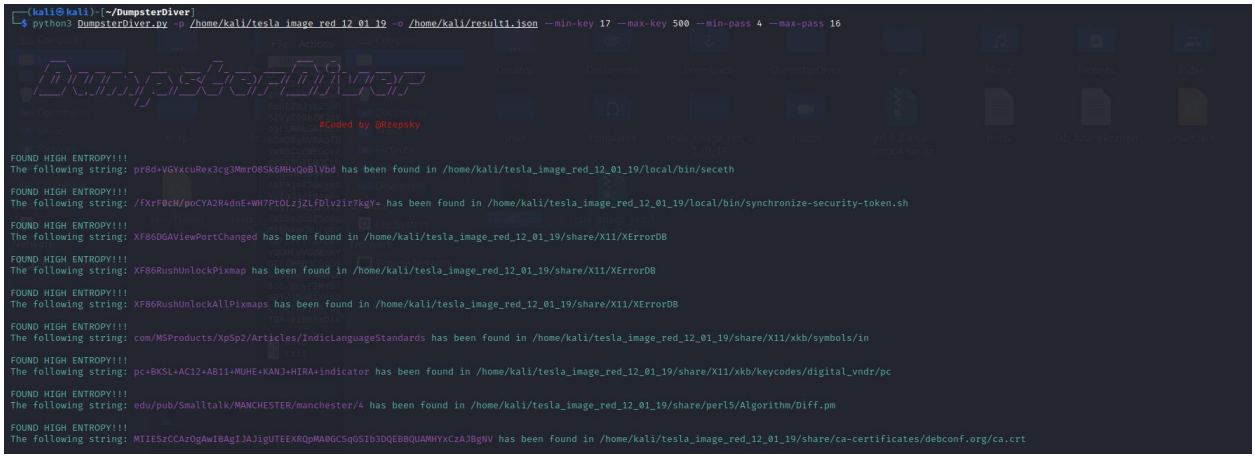
/tesla/UI/lib/...

/tesla/UI/libexec - хранятся файлы webkit (движок для отображения веб-страниц)

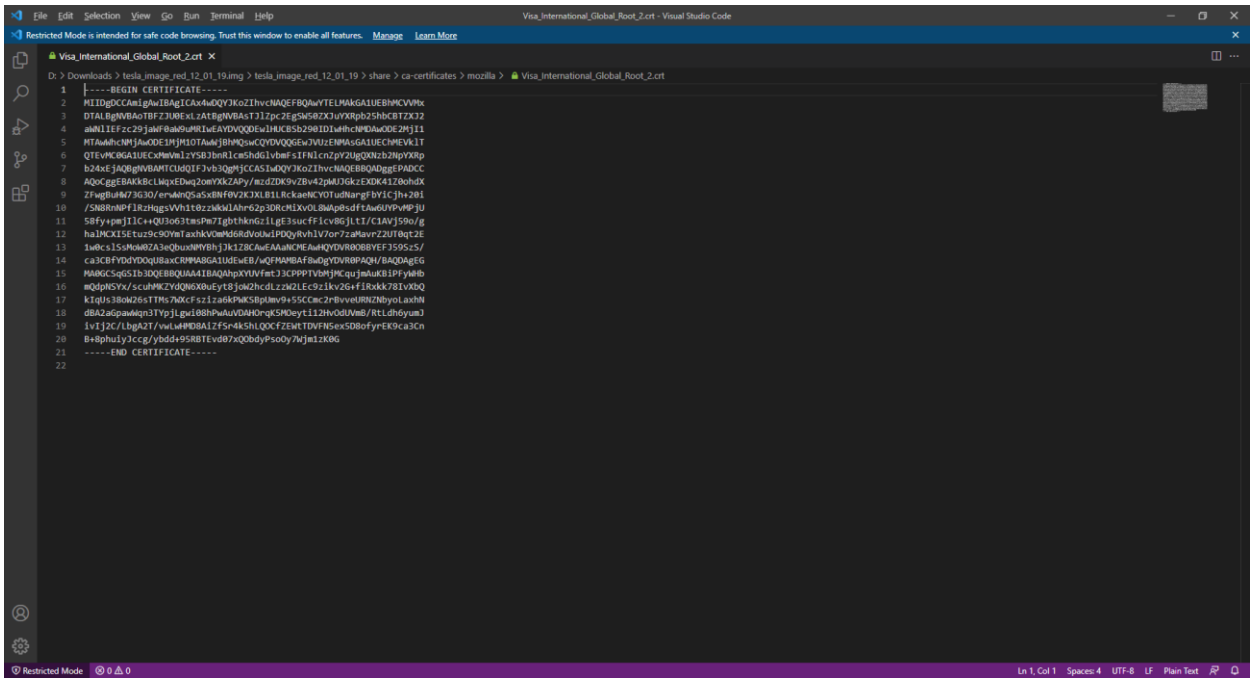
/tesla/UI/navigon - сервис навигации

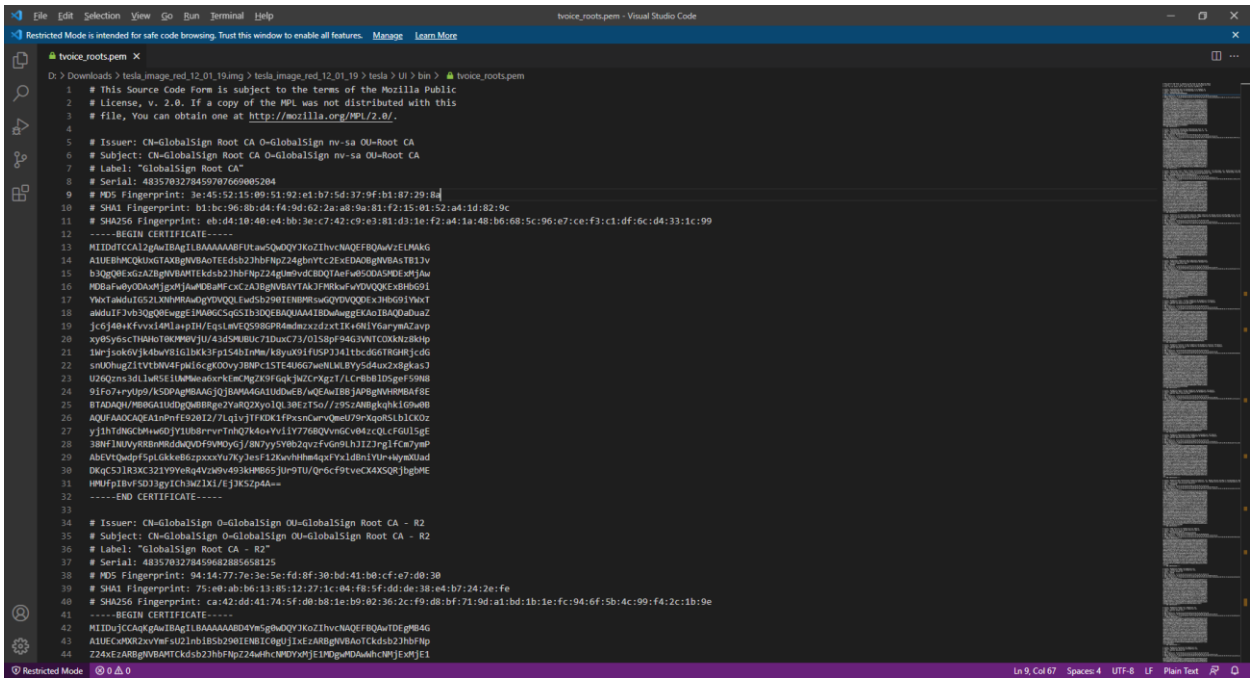
/tesla/UI/navigon/...

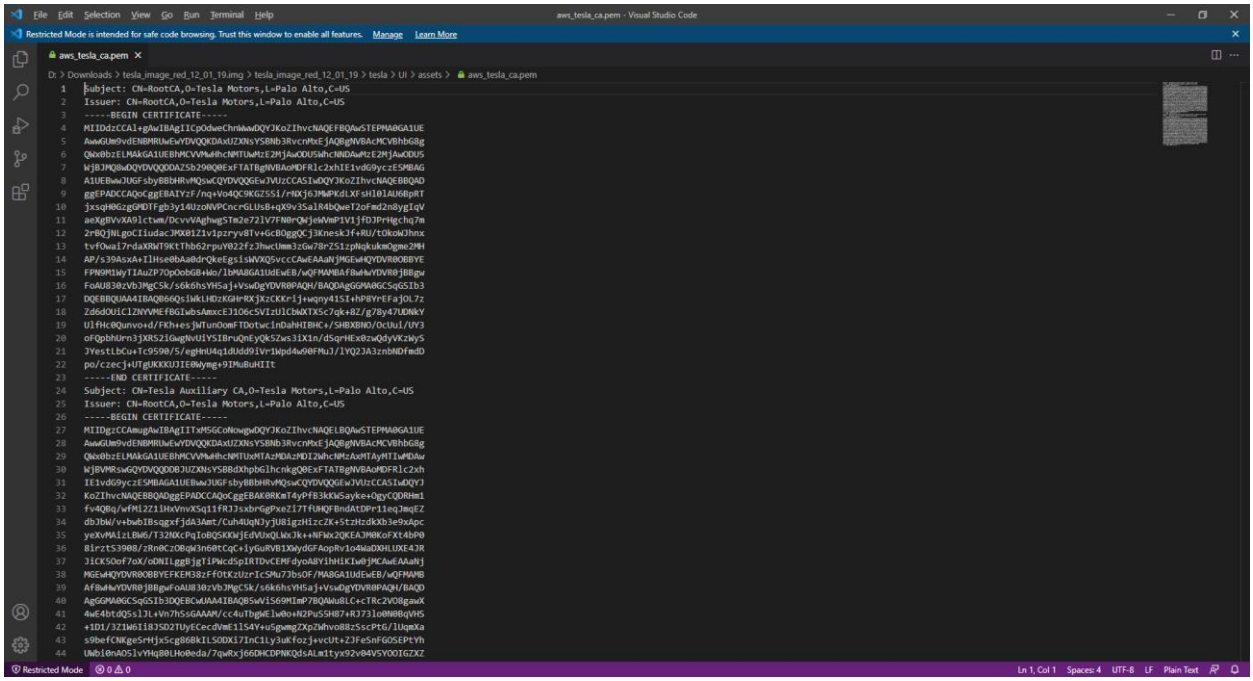
Также была использована утилита DumpsterDiver– Инструмент для поиска чувствительных данных (паролей, хешей, API ключей, ключей ассиметричного шифрования) в файлах различного типа.

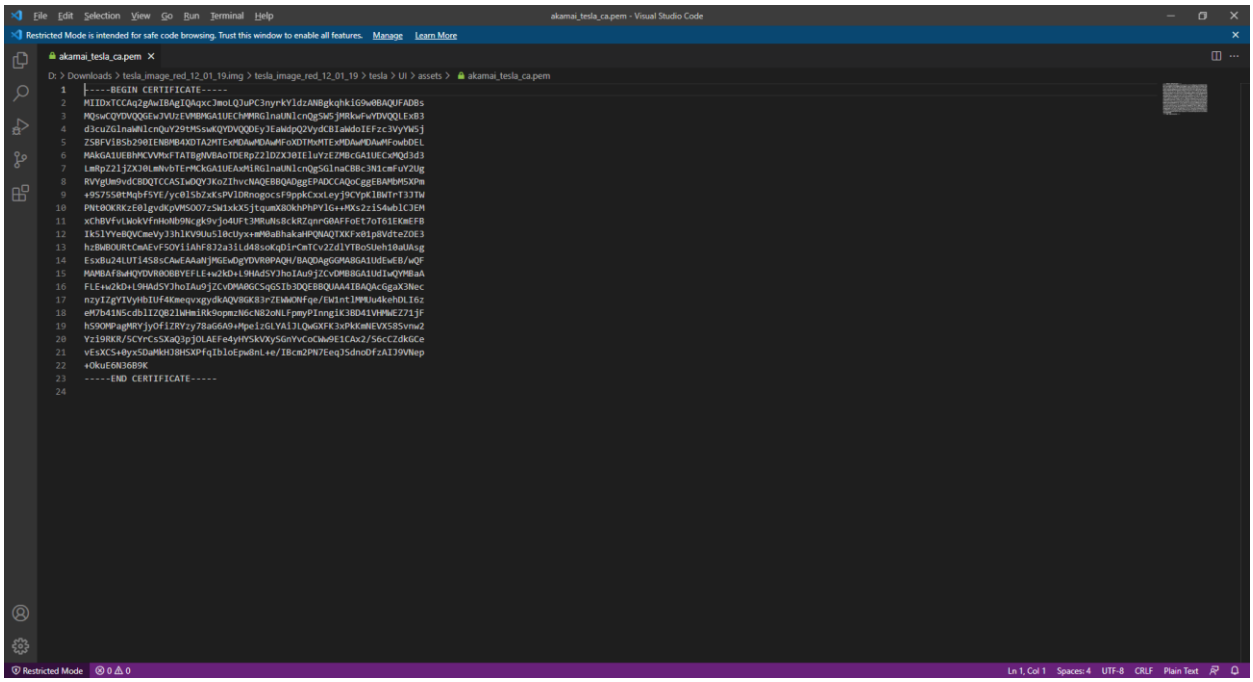


Были найдены сертификаты:

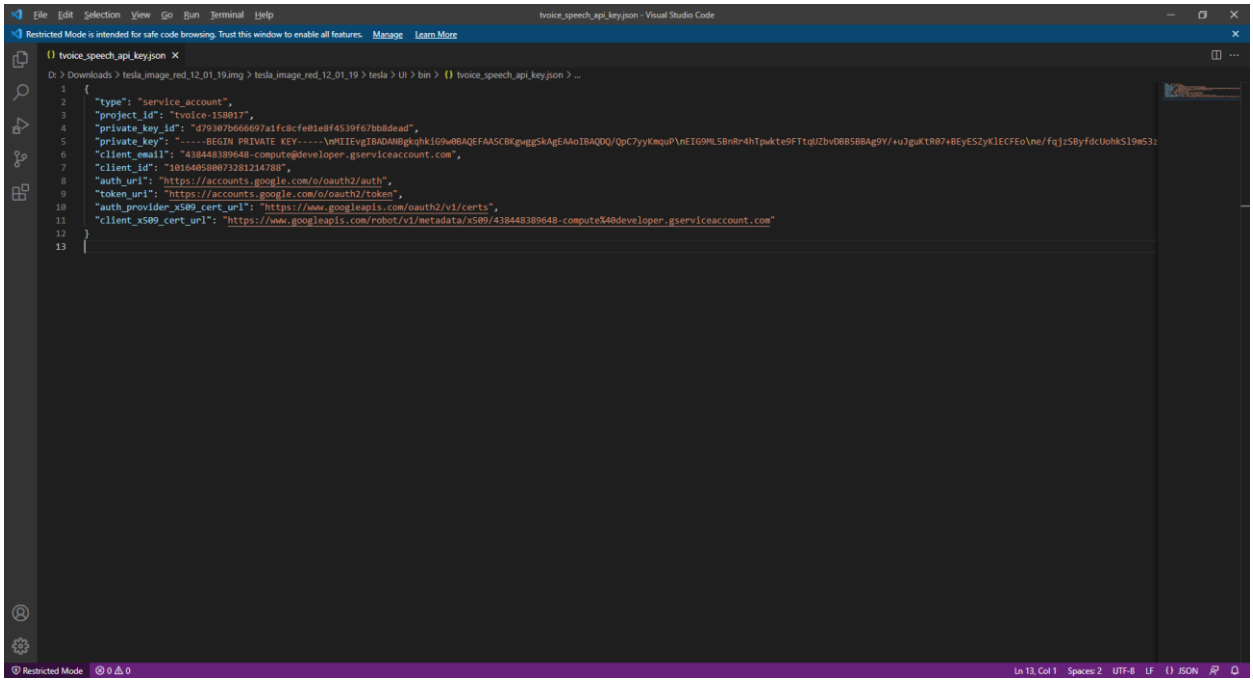



File Edit Selection View Go Run Terminal Help
tvoice_roots.pem - Visual Studio Code
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
tvoice_roots.pem
D: > Downloads > tesla_image_red_12_01_19.img > tesla_image_red_12_01_19 > tesla > UI > bin > tvoice_roots.pem
This Source Code Form is subject to the terms of the Mozilla Public
License, v. 2.0. If a copy of the MPL was not distributed with this
file, You can obtain one at http://mozilla.org/MPL/2.0/.
Issuer: CN=GlobalSign Root CA O=GlobalSign nv-sa OU=Root CA
Subject: CN=GlobalSign Root CA O=GlobalSign nv-sa OU=Root CA
Label: "GlobalSign Root CA"
Serial: 4835703278459707669005204
MD5 Fingerprint: 3e:45:52:15:09:51:92:e1:b7:5d:37:9f:b1:87:29:8a
SHA1 Fingerprint: b1:bc:96:8b:d4:f4:9d:62:2a:a8:9a:81:f2:15:01:52:a4:1d:82:9c
SHA256 Fingerprint: eb:d4:10:40:e4:bb:3e:c7:42:c9:e3:81:d3:1e:f2:a4:1a:48:b6:68:5c:96:e7:ce:f3:c1:df:6c:d4:33:1c:99
-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgILBAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEGdsb2JhbFNpZ24gbnYtc2Exa0AQBgNVBAsTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw05ODA5MDExMjAw
MDBaFw0yODA5MjgxMjAwMDBaMFcxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9i
YWxTaWduIG52LXNhMRAwDgYDVQQLEwdSb290IENBMRswGQYDVQQDExJHbG9iYWxT
aWduIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaDuaZ
jc6j40+Kfvvxi4Mla+pIH/EqsLmVEQS98GPR4mdmzxzdzxtIK+6NiY6arymAZavp
xy0Sy6scTHAHoT0KMM0VjU/43dSMUBUc71DuxC73/OlS8pF94G3VNTCOXkNz8kHp
1Wrjsok6Vjk4bwY8iGlbKk3Fp1S4bInMm/k8yuX9ifUSPJJ4ltbcdG6TRGHRjcdG
snUOhugZitVtbNV4FpWi6cgKOOvyJBNPc1STE4U6G7weNlWLBYy5d4ux2x8gkasJ
U26Qzns3dLlwR5EiUWMWea6xrkEmCMgZK9FGqkjWZCrXgzT/LCr8bB1DSgeF59N8
9iFo7+ryUp9/kSDPAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8E
BTADAQH/MB0GA1UdDgQWBBRge2YaRQ2XyolQL30EzTSo//z9SzANBgkqhkiG9w0B
AQUFAAOCAQEA1nPnfE920I2/7LqivjTFKDK1fPxsnCwrvQmeU79rXqoRSLblCKOz
yj1hTdNGCbM+w6DjY1Ub8rrvrTnhQ7k4o+YviiY776BQVvnGCv04zcQLcFGUl5gE
38NflNUVyRRBnMRddWQVDf9VMOyGj/8N7yy5Y0b2qvzfvGn9LhJIZJrglfCm7ymP
AbEVtQwdpf5pLGkkeB6zpxxxYu7kyJesFi2KwvhNhm4qxFYxldBnlYUr+WymXUad
DKqC5JlR3XC321Y9YeRq4Vzk0v493kMB65jUr9TU/Qn6cf9tveCX4XSQRjbgbME
HMUfpIBvfSDJkyICh3kZ1Xi/EjJKSZp4A==
-----END CERTIFICATE-----
Issuer: CN=GlobalSign O=GlobalSign OU=GlobalSign Root CA - R2
Subject: CN=GlobalSign O=GlobalSign OU=GlobalSign Root CA - R2
Label: "GlobalSign Root CA - R2"
Serial: 4835703278459682885658125
MD5 Fingerprint: 94:14:77:7e:3e:5e:fd:8f:30:bd:41:b0:cf:e7:d0:30
SHA1 Fingerprint: 75:e0:ab:b6:13:85:12:27:1c:04:f8:5f:dd:de:38:e4:b7:24:2e:fe
SHA256 Fingerprint: ca:42:dd:41:74:5f:d0:b8:1e:b9:02:36:2c:f9:d8:bf:71:9d:a1:bd:1b:1e:fc:94:6f:5b:4c:99:f4:2c:1b:9e
-----BEGIN CERTIFICATE-----
MIIDujCCAqKgAwIBAgILBAAAAABD4Ym5g0wDQYJKoZIhvcNAQEFBQAwTDEgMB4G
A1UECxMXR2xvYmFsU2lnbiBSb290IENBIC0gUjIxEzARBgNVBAoTCkdsb2JhbFNp
Z24xEzARBgNVBAMTCkdsb2JhbFNpZ24wHhcNMDYxMjE1MDgwMDA wWhcNMjExMjE1


File Edit Selection View Go Run Terminal Help
aws_tesla_ca.pem - Visual Studio Code
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
aws_tesla_ca.pem
D: > Downloads > tesla_image_red_12_01_19.img > tesla_image_red_12_01_19 > tesla > UI > assets > aws_tesla_ca.pem
Subject: CN=RootCA,O=Tesla Motors,L=Palo Alto,C=US
Issuer: CN=RootCA,O=Tesla Motors,L=Palo Alto,C=US
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIICpOdweChnWkwDQYJKoZIhvcNAQEFBQAwSTEPMA0GA1UE
AwwGUm9vdENBMRUwEwYDVQQKDAxUZXNsYSBNb3RvcnMxEjAQBgNVBAcMCVBhbGlv
QWx0bzELMAkGA1UEBhMCVVMwHhcNMTUwMzE2MjAwODU5WhcNNDAwMzE2MjAwODU5
WjBJMQ8wDQYDVQQDDAZSb290QOExFTATBgNVBAoMDFRlc2xhIE1vdG9yczESMBAG
A1UEBwwJUGFsbyBBbHRvMQswCQYDVQQGEwJVUzCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAIYzF/nq+Vo4QC9KGZSSi/rNXj6JMwPKdLXFsH10lAU6BpRT
jxsqH0GzgGHDTFgb3y14UzoNVPCncrGLUsB+qX9v3SalR4bQweT2oFmd2n8ygIqV
aeXgBVvXA9ictwm/DcvVAghwgSTm2e72lV7FN0rQWjeWVmP1VijfDJPrHgchq7m
2rBQjBWLgpCIiudacJM901Z1vipzryv8Tv+GcBOggQCjJKneskJfrRU/tOKcWJhnx
tvfOwaI7rdaXRNT9KtThb62rpuY022fzJhwcUmm3zGw78rZ51zpNqkukmOgmo2MH
AP/s39AsxA+IlHse0bAa0drQkeEgsiSWVXQ5vccCAwEAAaNjMGEwHQYDVR0OBBYE
FPN9M1WyTIAuZP7OpOobGB+Wo/lbMA8GA1UdEwEB/wQFMAMBAf8wHwYDVR0jBBgw
FoAU830zVbJMgC5k/s6k6hsYH5ajVswDgYDVR0PAQH/BAQDAgGGMA0GCSqGSIb3
DQEBBQUAA4IBAQB66Qs1WkLHDzKGHrRXjXzCKKrij+wqny41SI+hP8YrEFajOL7z
Zd6dOUiClZNYVMEfBGIwbsAmxcE3lO6cSVIzUlCbWXTXSc7qk+8Z/g78y47UDNkY
UlfHc0Qunvo+d/FKh+esjWTunOomFTDotwcinDahHIBHC+/SHBXBNO/OcUui/UY3
oFQpbhUrn3jXRS2iGwgNvUiYSIBruQnEyQk5Zws3iX1n/dSqrHEx0zwQdyVKzWyS
JYestLbCu+Tc9590/5/egHnU4q1dUdd9iVr1Wpd4w90FMuJ/lYQ2JA3znbNDfmdD
po/czecj+UTgUKKKUJIE0Wymg+9IMuBuHIIt
-----END CERTIFICATE-----
Subject: CN=Tesla Auxiliary CA,O=Tesla Motors,L=Palo Alto,C=US
Issuer: CN=RootCA,O=Tesla Motors,L=Palo Alto,C=US
-----BEGIN CERTIFICATE-----
MIIDgzCCAmugAwIBAgITYxMSGCoNowgwDQYJKoZIhvcNAQELBQAwSTEPMA0GA1UE
AwwGUm9vdENBMRUwEwYDVQQKDAxUZXNsYSBNb3RvcnMxEjAQBgNVBAcMCVBhbGlv
QWx0bzELMAkGA1UEBhMCVVMwHhcNMTUwMTAzMDAzMDI2WhcNMTAyMTIwMDAw
WjBVMRswGQYDVQQDDBJUZXNsYSBBdGhpbGlhcnkgQ0ExFTATBgNVBAoMDFRlc2xh
IE1vdG9yczESMBAGA1UEBwwJUGFsbyBBbHRvMQswCQYDVQQGEwJVUzCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAK0RKmT4yPfB3kKWSayke+OgyCQDRHm1
fv4QBq/wfMi2Z1iHxVnvXSq11fRJJsxbrGgPxeZi7TfUHQFBndAtDPr11eqJmqEZ
dbJbW/v+bwbIBsqgxfjdA3Amt/Cuh4UqNJyjU8igzHizcZK+5tzHzdkXb3e9xApc
yeXvMAizLBW6/T32NXcPqIoBQSKKWjEdVUxQLWxJk++NFWx2QKEAJM0KoFXt4bP0
8irztS3908/zRn0CzOBqW3n60tCqC+iyGuRVB1XWydGFAopRv1o4WaDXHLUXE4JR
JiCK5OoF7oX/oDNILggBjgTiPWcdSpIRTDvCEMFdyoA8Y1hHiKIw0jMCAwEAAaNj
MGEwHQYDVR0OBBYEFKEM38zFfOtKzUzrIcSMu7JbsOF/MA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBgwFoAU830zVbJMgC5k/s6k6hsYH5ajVswDgYDVR0PAQH/BAQD
AgGGMA0GCSqGSIb3DQEBCwUAA4IBAQB5wViS69MImP7BQAWu8LC+cTRc2VO8gawX
4wE4btdQSsslJL+Vn7hSsGAAAM/cc4uTbgWElw0o+N2PuSSH87+RJ73lo0N0BqVHS
+1D1/3Z1W6I18JSD2TUyECecdVmE1lS4Y+u5gwmgZXpZWhvo88zSscPtG/lUqmXa
s9befCNKgeSrHJxScg868kIL5ODXi7InC1Ly3uKfozj+vcUt+Z3Fe5nFGO5EPtYh
UWbi0nAO5lvYHqB0LHo0eda/7qwRxJ66DHCDPNKQdsALm1tyx92v04VSYOOIGZXZ



Кроме того, найден приватный ключ:



Утилита gitleaks также нашла данный ключ:

```
└─$ gitleaks --repo-url=https://github.com/Alalexys27/123 -v                    1 ✕
INFO[0000] cloning ... https://github.com/Alalexys27/123
Enumerating objects: 18015, done.

Total 18015 (delta 0), reused 0 (delta 0), pack-reused 18015
{
        "line": "  \"type\": \"service_account\",",
        "lineNumber": 2,
        "offender": "\"type\": \"service_account\"",
        "offenderEntropy": -1,
        "commit": "0b9b34008477d97589b347f0b80f1aa41e67f10b",
        "repo": "123",
        "repoURL": "https://github.com/Alalexys27/123",
        "leakURL": "https://github.com/Alalexys27/123/blob/0b9b34008477d97589b347f0b80
f1aa41e67f10b/tesla/UI/bin/tvoice_speech_api_key.json#L2",
        "rule": "Google (GCP) Service Account",
        "commitMessage": "first commit\n",
        "author": "Alalexys27",
        "email": "alalexan777@gmail.com",
        "file": "tesla/UI/bin/tvoice_speech_api_key.json",
        "date": "2022-01-22T15:12:25+10:00",
        "tags": "key, Google"
}
{
        "line": "  \"private_key\": \"-----BEGIN PRIVATE KEY-----\\nMIIEvgIBADANBgkqhk
iG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQ/QpC7yyKmquP\\nEIG9ML5BnRr4hTpwkte9FTtqUZbvDBB5BBAg9
Y/+uJguKtR07+BEyESZyKlECFEo\\ne/fqjzSByfdcUohkSl9m53zY4Lnv0Zt2fH2DuJYuvgYF6wkuHEaQdkaW
1seY0WQa\\nYMpXK7WTLlJsikziaQ4jWFErVl1sQDdNtGUyTXP1EgF5rNrnfZuhCXflwedUcQQ1\\npLpJuCeS
xht/0xk0MeisDooTaMGdXuow3EjkwFTt9W82+VznxxGkL+pRYX07CkF8\\nW27N/7c4oTwaC4nzTQufmZhcCSj
fr40PVU+QCuOsZdqbXXD5vr2okpXp8AVxhJdZ\\ntCs+Hkl9AgMBAAECggEAZjC1SdGF6CiFZyldJ1OkVJUr0Q
Xkc5N6Jp0xNmW69hzi\\nGSqhcFxjEtzUnQ6YYK3C7h83XDNAgWHHvZIQwgNQW36Uk/JPeyrax4i+BZatlNTb\
\nve5VuYkS9rw4WcB59rAg2RbcoXlYlCMfXb6ickmPOe7Wovhla/iOzz2qQxSyDfHd\\nV8fVxs6vykivoFoMo
BZVOz50Qvc/JL23ygbnD1xv75hKYczEzevPJ4gRMBwAEVL4\\npsAWgcfLZ9xj/8O9H5poWBKp4UXOM//e1fCm
OdS/Psl2MkijFC4ydNj3CUj7jV+x\\nW0mNN5DG4arI/cvof4bWRjFvWPZ4RuDtdYcssrCGgQKBgQD+q2jrqXG
pzErPCk7J\\nyqS1VkwVpIWYsFLIufrYVQ7zCVwt2jN6zOwu9wp1H68/SpXH7pZUNxIvoNmYd6RB\\nJG9mqJV
iSarAvQPYbUDE9VhzCL0otko1T/z1coH7RSq/XAYWjc0Nj+Moyslgce4q\\n/g2EJ+ZsSer/bkv7j3Yaqb2nrQ
KBgQDSFImEYLyMwHXToo9522XOdSU03mO81bQ0\\nW/3ZZ+hFrgwcgcMI9vcDkv23nOFGRWeUCJcb60kIl93t0
SYg/ihcPoHlKSgAbZ20\\nyqmj/q/aeIRRSWcEfZjLAweCfE6MW3xami100Isu94S2zleoLrpt0bXZLXMkrX6m
\\nL/qn5i+jEQKBgQDwlE8mqUimBkb5dZxeht+4KtDvdR970b4yv3aX3SqlL0d0TXhq\\nXqIT7+5iHM958+Sx
HdPHtMqqUcKdhRCXNWtDyKhuVHdJYoX6c6NHLRskeLHxftt1\\np52o5Uajb4Dli3J45fY7BJ2skH1Sbe53kM6
F9Qd5bw7fxHtlJu6EW6u9dQKBgC1z\\negkk8MY3AYcHPalsmUsgtysIDmYVikZlvLcjrvIcZMxqGqs+21Rvoe
ruyyJr86vo\\na+EDd6qfSMmiHXC37D2A3JOa4uesz5kE28z6VkubFW2MxvgGwF7zydUmVcwyIuZr\\nQvhqAi
LoNFNkszxU18rYu1JAbg/6ZVNJQB7BQ38xAoGBAJDQjndCk2sTfB+HXqqh\\n12eeCUWpB1l9WUU8rY17c2MXN
iUZVNM/KTiDyKSSqXyFDfAgA7KZJe5Ld1Gkdkt6\\nHwTUGDA8jGdTvw0NjNIeELm5Rl8FAxdy5n6U2Lm5aVNy
SXNo4GM9qQUhZPmJjCdz\\nlNYSgsDMkz8PQQO4lUa6RWKS\\n-----END PRIVATE KEY-----\\n\",",
        "lineNumber": 5,
        "offender": "-----BEGIN PRIVATE KEY-----",
        "offenderEntropy": -1,
        "commit": "0b9b34008477d97589b347f0b80f1aa41e67f10b",
        "repo": "123",
        "repoURL": "https://github.com/Alalexys27/123",
        "leakURL": "https://github.com/Alalexys27/123/blob/0b9b34008477d97589b347f0b80
f1aa41e67f10b/tesla/UI/bin/tvoice_speech_api_key.json#L5",
```

Вручную нашли также:

Информацию о сервисных центрах:

service_contact_info.json – Блокнот

Файл Правка Формат Вид Справка


```
{
    "service_contact_info" : [
        {
            "countryCode" : "US",
            "phoneNumber" : "18777983752",
            "formattedPhoneNumber" : "1-877-79TESLA",
                "email": "ServiceHelpNA@teslamotors.com"
        },
        {
            "countryCode" : "CA",
            "phoneNumber" : "18777983752",
            "formattedPhoneNumber" : "1-877-79TESLA",
            "email": "ServiceHelpNA@teslamotors.com"
        },
        {
            "countryCode" : "MX",
            "phoneNumber" : "018002288145",
            "formattedPhoneNumber" : "01 800 228 8145",
            "email": "ServiceHelpNA@teslamotors.com"
        },
        {
            "countryCode" : "DE",
            "phoneNumber" : "08005893542",
            "formattedPhoneNumber" : "0800 589 3542",
            "email": "ServiceHelpEU@teslamotors.com"
        },
        {
            "countryCode" : "FR",
            "phoneNumber" : "0800941029",
            "formattedPhoneNumber" : "0800 94 1029",
            "email": "ServiceHelpEU@teslamotors.com"
        },
        {
            "countryCode" : "IT",
            "phoneNumber" : "800596815",
            "formattedPhoneNumber" : "800 596 815",
            "email": "ServiceHelpEU@teslamotors.com"
        },
        {
            "countryCode" : "NL",
            "phoneNumber" : "08000200160",
            "formattedPhoneNumber" : "0800 020 0160",
            "email": "ServiceHelpEU@teslamotors.com"
        },
        {
            "countryCode" : "AT",
            "phoneNumber" : "0800880992",
            "formattedPhoneNumber" : "0800 88 0992",
            "email": "ServiceHelpEU@teslamotors.com"
        },
        {
            "countryCode" : "BE",
            "formattedPhoneNumber" : "0800 29 027",
```

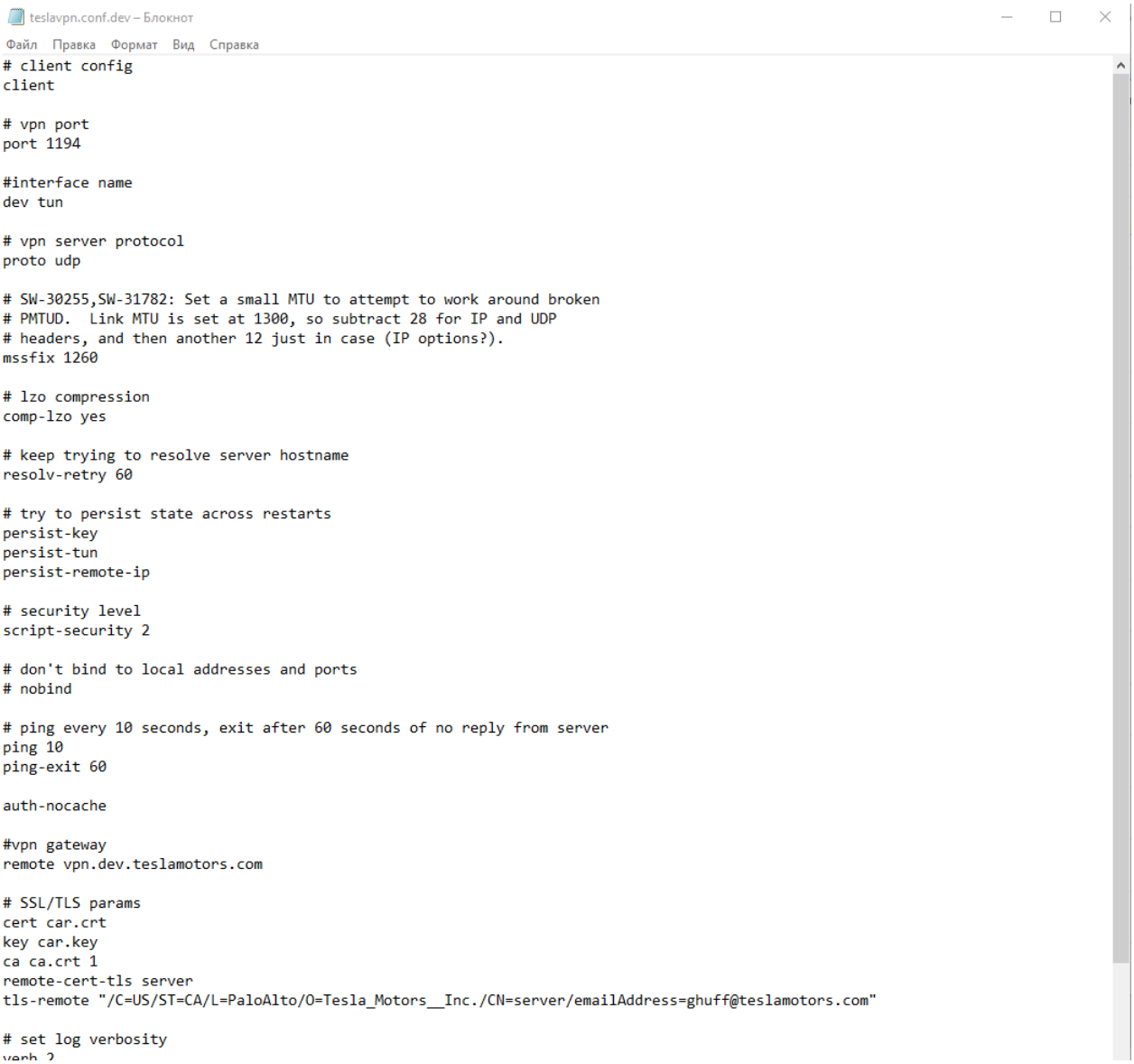
Valhalla – механизм маршрутизации. Конфигурация:

valhalla.json – Блокнот

Файл Правка Формат Вид Справка

```
{
  "mjolnir": {
    "max_cache_size": 200000000,
    "global_synchronized_cache": true,
    "connectivity_map": false,
    "tile_dir": "/data/valhalla",
    "admin": "/data/valhalla/admin.sqlite",
    "timezone": "/data/valhalla/tz_world.sqlite",
    "transit_dir": "/data/valhalla/transit",
    "logging": {
      "type": "std_out",
      "color": true
    },
    "override_file": "/home/tesla/.Tesla/data/map_override.pbf.gz",
    "override_key": "dev"
  },
  "additional_data": {
    "elevation": "/data/valhalla/elevation/"
  },
  "loki": {
    "actions":
["locate","route","one_to_many","many_to_one","many_to_many","sources_to_targets","optimized_route","isochrone",
"trace_route","trace_attributes","probable_path","match_openlr", "health", "reload"],
    "use_connectivity": "false",
    "service_defaults": {
      "radius": 0,
      "minimum_reachability": 50
    },
    "logging": {
      "type": "std_out",
      "color": true,
      "long_request": 86400.0
    },
    "service": {
      "proxy": "ipc:///tmp/loki"
    }
  },
  "skadi": {
    "actions":["height"],
    "logging": {
      "type": "std_out",
      "color": true,
      "long_request": 86400.0
    },
    "service": {
      "proxy": "ipc:///tmp/skadi"
    }
  },
  "thor": {
    "logging": {
      "type": "std_out",
      "color": true,
      "long_request": 86400.0
```

Конфиг впн:



teslavpn.conf.dev – Блокнот

Файл Правка Формат Вид Справка

```
# client config
client

# vpn port
port 1194

#interface name
dev tun

# vpn server protocol
proto udp

# SW-30255,SW-31782: Set a small MTU to attempt to work around broken
# PMTUD.  Link MTU is set at 1300, so subtract 28 for IP and UDP
# headers, and then another 12 just in case (IP options?).
mssfix 1260

# lzo compression
comp-lzo yes

# keep trying to resolve server hostname
resolv-retry 60

# try to persist state across restarts
persist-key
persist-tun
persist-remote-ip

# security level
script-security 2

# don't bind to local addresses and ports
# nobind

# ping every 10 seconds, exit after 60 seconds of no reply from server
ping 10
ping-exit 60

auth-nocache

#vpn gateway
remote vpn.dev.teslamotors.com

# SSL/TLS params
cert car.crt
key car.key
ca ca.crt 1
remote-cert-tls server
tls-remote "/C=US/ST=CA/L=PaloAlto/O=Tesla_Motors__Inc./CN=server/emailAddress=ghuff@teslamotors.com"

# set log verbosity
verb 2
```

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'

NAMESERVERS_FILE="/var/run/nameservers.openvpn"

LOG="logger -t handle-vpn-change"

post_certinfo() {
    install-new-cert --post-cert-info # this will wait for dnsmasq to restart & reconfigure
}

echo "$script_type $script_context $*" | $LOG

connected=0
case $script_type in

route-up)
        # Update the file that tells dnsmasq which servers to use to resolve certain names over the VPN
        for optionname in ${!foreign_option_*} ; do
                option="${!optionname}"
                $LOG "$optionname $option"
                declare -a NS
                if [[ $option =~ dhcp-option\ DNS\ ([^\ ]*) ]] ; then
                        NS+=(${BASH_REMATCH[1]})
                fi
        done
        echo ${NS[*]} > $NAMESERVERS_FILE
        # Restart dnsmasq to get it to use the new file
        restart dnsmasq

        # On restart events, ask netmanager to check network health
        if [ $script_context = "restart" ] ; then
            $LOG "Notify netmanager that VPN has restarted"
            curl 'http://localhost:4060/NetManager/checkHealth?reason=VPN%20restarted'
        fi

        # So we'll notify netmanager of the correct change
        connected=1

        # Post the VPN certificate serial number and expiration date to mothership.
        # openvpn is not happy when this script takes too long, so spawn this work
        # into the background.
        post_certinfo &
        ;;

down)
        # Update dnsmasq to no longer try to resolve certain names over the VPN
        if [ $script_context != "restart" ] ; then
            rm -f $NAMESERVERS_FILE
            restart dnsmasq
        fi
        ;;
esac

# notify netmanager of vpn connection change
curl "http://localhost:4060/NetManager/notifyVpnConnected?connected=$connected"
```

Возможные векторы атак:

- Подключение с применением поддельной точки доступа Wi-Fi

- CVE-2019-9977 (Процесс рендеринга в развлекательной системе автомобилей неправильно обрабатывает компиляцию JIT, что позволяет злоумышленникам инициировать выполнение кода прошивки и отображать созданное сообщение для пассажиров автомобиля.)

- CVE-2019-13581 (Через модуль Parrot Faurecia Automotive FC6050W. Переполнение буфера позволяет удаленным злоумышленникам вызвать отказ в обслуживании или выполнить произвольный код с помощью искаженных пакетов Wi-Fi.)