Digital Forensics Investigation of the Tesla Autopilot File System

SECURWARE 2022

Kevin Gomez Buquerin[1,2] and Hans-Joachim Hof[1]

[1]Technische Hochschule Ingolstadt, CARISSMA Institute of Electric, Connected, and Secure Mobility (C-ECOS)
[2]Friedrich Alexander University Erlangen Nürnberg

CARISSMA
Automotive Safety Research

IARIA

Who am I?

Kevin Gomez Buquerin

I am a PhD student at the Technical University Ingolstadt and Friedrich Alexander University Erlangen Nürnberg in Germany. My main research area is automotive digital forensics. I focus on the implementation of new methods for extraction and analysis of digital evidence in modern and future automotive systems.

CARISSMA
Automotive Safety Research

IARIA

Tesla

Figure 1: Tesla Model S [Tesla Website, 2022]

CARISSMA
Automotive Safety Research

IARIA

Accidents involving the autopilot

Figure 2: Tesla Model S [Scott J. Engle, 2021]

CARISSMA
Automotive Safety Research

IARIA

Digital evidence in modern vehicles

- Infotainment system,

Digital evidence in modern vehicles

- Infotainment system,
- Vehicle-to-vehicle systems,

Digital evidence in modern vehicles

- Infotainment system,
- Vehicle-to-vehicle systems,
- Airbag control unit,

Digital evidence in modern vehicles

- Infotainment system,
- Vehicle-to-vehicle systems,
- Airbag control unit,
- Telematic control system,

CARISSMA
Automotive Safety Research

IARIA

Digital evidence in modern vehicles

- Infotainment system,
- Vehicle-to-vehicle systems,
- Airbag control unit,
- Telematic control system,
- End-point devices,

CARISSMA
Automotive Safety Research

IARIA

Digital evidence in modern vehicles

- Infotainment system,
- Vehicle-to-vehicle systems,
- Airbag control unit,
- Telematic control system,
- End-point devices,
- and many more.

CARISSMA
Automotive Safety Research

IARIA

Automotive digital forensics

In automotive digital forensics investigations, different involved components must be **understood** to generate an **overall picuture of the digital events** that have taken place.

Automotive digital forensics

In automotive digital forensics investigations, different involved components must be **understood** to generate an **overall picuture of the digital events** that have taken place.

This includes an understanding of the **autopilot.**

CARISSMA
Automotive Safety Research

IARIA

Digital forensics questions [Gom2021]

- **Who** performed or is responsible for a digital event?

Digital forensics questions [Gom2021]

- **Who** performed or is responsible for a digital event?
- **What** digital event was performed?

Digital forensics questions [Gom2021]

- **Who** performed or is responsible for a digital event?
- **What** digital event was performed?
- **When** did the digital event take place?

Digital forensics questions [Gom2021]

- **Who** performed or is responsible for a digital event?
- **What** digital event was performed?
- **When** did the digital event take place?
- **Where** did the digital event take place?

Digital forensics questions [Gom2021]

- **Who** performed or is responsible for a digital event?
- **What** digital event was performed?
- **When** did the digital event take place?
- **Where** did the digital event take place?
- **How** did the digital event take place?

Digital forensics questions [Gom2021]

- **Who** performed or is responsible for a digital event?
- **What** digital event was performed?
- **When** did the digital event take place?
- **Where** did the digital event take place?
- **How** did the digital event take place?
- **Why** did the digital event take place?

CARISSMA
Automotive Safety Research

IARIA

What is metadata?

Metadata is **data that describes data**. It is **directly linked** to the describing object [Car2005].

Examples are timestamps, object size, file types, directory structures, and many more.

Why is metadata important?

Metadata changes when the object is modified, deleted, or other wise changed [Car2005].

Metadata can **answer forensic questions** [Buc2004].

Research question and hypothesis

Research question

What are DF- and ADF-specific characteristics that can be captured in the file system of a modern vehicle?

CARISSMA
Automotive Safety Research

IARIA

Research question and hypothesis

Research question

What are DF- and ADF-specific characteristics that can be captured in the file system of a modern vehicle?

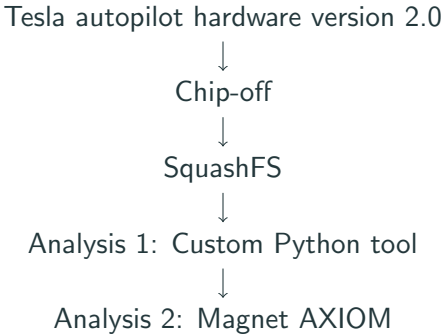
Hypothesis

The file system of the Tesla autopilot contains metadata relevant to answer forensic questions in ADF investigations.

CARISSMA
Automotive Safety Research

IARIA

Our approach



CARISSMA
Automotive Safety Research

IARIA

Extensions

Ext.	Cnt.	Ext.	Cnt.	Ext.	Cnt.
.so	356	.sh	28	.5	11
.0	221	.txt	26	.10	9
.crt	140	.map	26	.wav	9
.pem	133	.hlp	25	.pdf	8
.conf	103	.bin	24	.3	7
.mo	100	.4	19	.profile	7
.sl	46	.rules	18	.00	7
.1	41	.56	15	.13	6
.2	33	.hwdb	14	.16	6
.img	32	.6	14		

Table 1: Number of file extensions within a Tesla autopilot

CARISSMA
Automotive Safety Research

IARIA

Timestamps

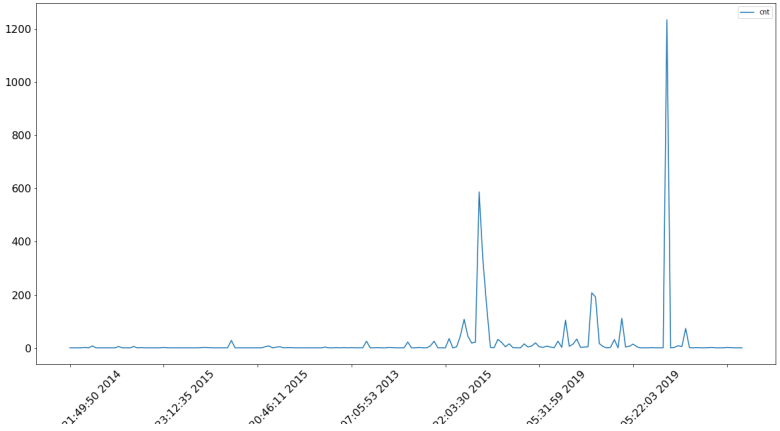


Figure 3: Timestamps of the files within the Tesla autopilot

CARISSMA
Automotive Safety Research

IARIA

Additional metadata

User accounts:

- root
- daemon
- temperature_monitor
- visualizer
- legacyvehicle
- drivermonitor
- gps
- etc.

Additional metadata

Other:

- 1 .csv file
- 8 .pdf files
- 26 .txt files (READMEs)
- 32 .img files (firmware images)
- Buildroot configuration file with an unique identifier
- etc.

CARISSMA
Automotive Safety Research

IARIA

Can we trust the collected data?

Forensic soundness

Degree of correctness, atomicity, and integrity in memory acquisitions [Voe2012][Ott2022]

Can we trust the collected data?

Forensic soundness

Degree of correctness, atomicity, and integrity in memory acquisitions [Voe2012][Ott2022]

Due to the usage of a chip-off, **we are forensically-sound** with our acquisition.

CARISSMA
Automotive Safety Research

IARIA

How helpful is the metadata?

Forensic questions	Corresponding identified metadata
Who	User accounts and cron-jobs
Where	Files and folders structure
When	Timestamps of the files and log-files
What	Log files within the *etc* folder
How	Configuration files
Why	Can not be answered

Table 2: Results of the analysis in relation to the forensic questions

CARISSMA
Automotive Safety Research

IARIA

To summarize

Research question

What are DF- and ADF-specific characteristics that can be captured in the file system of a modern vehicle?

CARISSMA
Automotive Safety Research

IARIA

To summarize

Research question

What are DF- and ADF-specific characteristics that can be captured in the file system of a modern vehicle?

→ **We identified general and automotive-specific characteristics.**

CARISSMA
Automotive Safety Research

IARIA

To summarize

Research question

What are DF- and ADF-specific characteristics that can be captured in the file system of a modern vehicle?

→ **We identified general and automotive-specific characteristics.**

Hypothesis

The file system of the Tesla autopilot contains metadata relevant to answer forensic questions in ADF investigations.

CARISSMA
Automotive Safety Research

IARIA

To summarize

Research question

What are DF- and ADF-specific characteristics that can be captured in the file system of a modern vehicle?

→ **We identified general and automotive-specific characteristics.**

Hypothesis

The file system of the Tesla autopilot contains metadata relevant to answer forensic questions in ADF investigations.

→ **We can answer all forensic questions except “why”.**

CARISSMA
Automotive Safety Research

IARIA

References

[Gom2021] K. Gomez Buquerin, C. Corbett, and H.-J. Hof, "*A generalized approach to automotive forensics*," Forensic Science International: Digital Investigation, Vol. 36, p. 301111, 2021

[Car2005] B. D. Carrier, "*File System Forensic Analysis*," Addison-Wesley, 2005

[Buc2004] F. Buchholz and E. Spafford, "*On the role of file system metadata in digital forensics*," Digital Investigation, Vol. 1, No. 4, Elsevier BV, pp. 298-309, 2004

[Voe2012] S. Vömel and F. Freiling, "*Correctness, atomicity, and integrity: Defining criteria for forensically-sound memory acquisitions*," Digital Investigation, Vol. 9, No. 2, Elsevier BV, pp. 125-137, 2012

[Ott2022] J. Ottmann, F. Breitinger, and F. Freiling, "*Defining Atomicity (and Integrity) for Snapshots of Storage in Forensic Computing*," Proceedings of the Digital Forensics Research Conference Europe (DFRWS EU), 2022

CARISSMA
Automotive Safety Research

IARIA