Hacking an NFC Toy with the ChameleonMini

Fabian Peters
Federico Cerutti

Fabian Peters
Federico Cerutti

Fabian Peters
Federico Cerutti

```
fptrs@vm:~$ python3 ~/git/ChameleonMiniCeres/Software/chamlog.py -f log

Note: If parityBit check failed, '!' is appended to the decoded data and raw data with parity bit is displayed.

17200 ms <+17200 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17447 ms <  +247 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17693 ms <  +246 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17696 ms <    +3 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17943 ms <  +247 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17969 ms <   +26 ms>:CODEC RX                    (5   bytes) [260100f60a          ]
17982 ms <   +13 ms>:CODEC RX                    (10  bytes) [02b304040480a291d62a]
18009 ms <   +27 ms>:CODEC RX                    (5   bytes) [260100f60a          ]
18033 ms <   +24 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e0006150]
18062 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e001e841]
18092 ms <   +30 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e0027373]
18121 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e003fa62]
18150 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e0044516]
18180 ms <   +30 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e005cc07]
18209 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e0065735]
18238 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e007de24]
18268 ms <   +30 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
18298 ms <   +30 ms>:CODEC RX                    (17  bytes) [22ba04523a9610500304e07698d0892806]
18543 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
18788 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
19033 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
19279 ms <  +246 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
19524 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
19769 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
20014 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
20259 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
```

```
fptrs@vm:~$ python3 ~/git/ChameleonMiniCeres/Software/chamlog.py -f log

Note: If parityBit check failed, '!' is appended to the decoded data and raw data with parity bit is displayed.

17200 ms <+17200 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17447 ms <  +247 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17693 ms <  +246 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17696 ms <    +3 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17943 ms <  +247 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17969 ms <   +26 ms>:CODEC RX                    (5   bytes) [260100f60a          ]
17982 ms <   +13 ms>:CODEC RX                    (10  bytes) [02b3040404480a291d62a]
18009 ms <   +27 ms>:CODEC RX                    (5   bytes) [260100f60a          ]
18033 ms <   +24 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e0006150]
18062 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e001e841]
18092 ms <   +30 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e0027373]
18121 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e003fa62]
18150 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e0044516]
18180 ms <   +30 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e005cc07]
18209 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e0065735]
18238 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e007de24]
18268 ms <   +30 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
18298 ms <   +30 ms>:CODEC RX                    (17  bytes) [22ba04523a9610500304e07698d0892806]
18543 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
18788 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
19033 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
19279 ms <  +246 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
19524 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
19769 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
20014 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
20259 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
```

```
fptrs@vm:~$ python3 ~/git/ChameleonMiniCeres/Software/chamlog.py -f log

Note: If parityBit check failed, '!' is appended to the decoded data and raw data with parity bit is displayed.

17200 ms <+17200 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17447 ms <  +247 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17693 ms <  +246 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17696 ms <    +3 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17943 ms <  +247 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17969 ms <   +26 ms>:CODEC RX                    (5   bytes) [260100f60a          ]
17982 ms <   +13 ms>:CODEC RX                    (10  bytes) [02b304040480a291d62a]
18009 ms <   +27 ms>:CODEC RX                    (5   bytes) [260100f60a          ]
18033 ms <   +24 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e0006150]
18062 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e001e841]
18092 ms <   +30 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e0027373]
18121 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e003fa62]
18150 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e0044516]
18180 ms <   +30 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e005cc07]
18209 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e0065735]
18238 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e007de24]
18268 ms <   +30 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
18298 ms <   +30 ms>:CODEC RX                    (17  bytes) [22ba04523a9610500304e07698d0892806]
18543 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
18788 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
19033 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
19279 ms <  +246 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
19524 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
19769 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
20014 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
20259 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
```

```
fptrs@vm:~$ python3 ~/git/ChameleonMiniCeres/Software/chamlog.py -f log

Note: If parityBit check failed, '!' is appended to the decoded data and raw data with parity bit is displayed.

17200 ms <+17200 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17447 ms <  +247 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17693 ms <  +246 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17696 ms <    +3 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17943 ms <  +247 ms>:CODEC RX                    (5   bytes) [02b2048e3c          ]
17969 ms <   +26 ms>:CODEC RX                    (5   bytes) [260100f60a          ]
17982 ms <   +13 ms>:CODEC RX                    (10  bytes) [02b304040480a291d62a]
18009 ms <   +27 ms>:CODEC RX                    (5   bytes) [260100f60a          ]
18033 ms <   +24 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e0006150]
18062 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e001e841]
18092 ms <   +30 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e0027373]
18121 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e003fa62]
18150 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e0044516]
18180 ms <   +30 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e005cc07]
18209 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e0065735]
18238 ms <   +29 ms>:CODEC RX                    (13  bytes) [2220523a9610500304e007de24]
18268 ms <   +30 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
18298 ms <   +30 ms>:CODEC RX                    (17  bytes) [22ba04523a9610500304e07698d0892806]
18543 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
18788 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
19033 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
19279 ms <  +246 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
19524 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
19769 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
20014 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
20259 ms <  +245 ms>:CODEC RX                    (13  bytes) [22b204523a9610500304e089a6]
```

Fabian Peters
Federico Cerutti

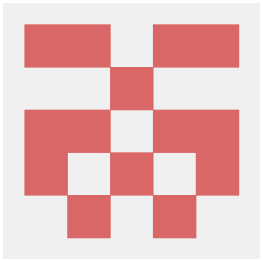
Fabian Peters
Federico Cerutti

```
fptrs@vm:~$ python3 ~/git/ChameleonMiniCeres/Software/chamlog.py -f log

Note: If parityBit check failed, '!' is appended to the decoded data and raw data with parity bit is displayed.

37513 ms <+37513 ms>:CONFIG SET                    (9   bytes) [ICODE_SLI          ]
51253 ms <+13740 ms>:UID SET                       (8   bytes) [e004035010963a52    ]
56018 ms < +4765 ms>:CODEC RX                      (5   bytes) [02b2048e3c          ]
56018 ms <    +0 ms>:CODEC TX                      (5   bytes) [000000ccc6          ]
56045 ms <   +27 ms>:CODEC RX                      (5   bytes) [260100f60a          ]
56058 ms <   +13 ms>:CODEC RX                      (10  bytes) [02b304045b6efd7fcc0a]
56058 ms <    +0 ms>:CODEC TX                      (3   bytes) [0078f0              ]
56077 ms <   +19 ms>:CODEC RX                      (5   bytes) [260100f60a          ]
56077 ms <    +0 ms>:CODEC TX                      (12  bytes) [0000523a9610500304e03738]
56103 ms <   +26 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e0006150]
56103 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56132 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e001e841]
56132 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56161 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e0027373]
56162 ms <    +1 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56191 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e003fa62]
56191 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56220 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e0044516]
56220 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56249 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e005cc07]
56250 ms <    +1 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56279 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e0065735]
56279 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56308 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e007de24]
56308 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
```

```
fptrs@vm:~$ python3 ~/git/ChameleonMiniCeres/Software/chamlog.py -f log

Note: If parityBit check failed, '!' is appended to the decoded data and raw data with parity bit is displayed.

37513 ms <+37513 ms>:CONFIG SET                    (9   bytes) [ICODE_SLI          ]
51253 ms <+13740 ms>:UID SET                       (8   bytes) [e004035010963a52    ]
56018 ms < +4765 ms>:CODEC RX                      (5   bytes) [02b2048e3c          ]
56018 ms <    +0 ms>:CODEC TX                      (5   bytes) [000000ccc6          ]
56045 ms <   +27 ms>:CODEC RX                      (5   bytes) [260100f60a          ]
56058 ms <   +13 ms>:CODEC RX                      (10  bytes) [02b304045b6efd7fcc0a]
56058 ms <    +0 ms>:CODEC TX                      (3   bytes) [0078f0              ]
56077 ms <   +19 ms>:CODEC RX                      (5   bytes) [260100f60a          ]
56077 ms <    +0 ms>:CODEC TX                      (12  bytes) [0000523a9610500304e03738]
56103 ms <   +26 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e0006150]
56103 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56132 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e001e841]
56132 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56161 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e0027373]
56162 ms <    +1 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56191 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e003fa62]
56191 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56220 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e0044516]
56220 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56249 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e005cc07]
56250 ms <    +1 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56279 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e0065735]
56279 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56308 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e007de24]
56308 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
```

```
fptrs@vm:~$ python3 ~/git/ChameleonMiniCeres/Software/chamlog.py -f log

Note: If parityBit check failed, '!' is appended to the decoded data and raw data with parity bit is displayed.

37513 ms <+37513 ms>:CONFIG SET                    (9   bytes) [ICODE_SLI          ]
51253 ms <+13740 ms>:UID SET                       (8   bytes) [e004035010963a52    ]
56018 ms < +4765 ms>:CODEC RX                      (5   bytes) [02b2048e3c          ]
56018 ms <    +0 ms>:CODEC TX                      (5   bytes) [000000ccc6          ]
56045 ms <   +27 ms>:CODEC RX                      (5   bytes) [260100f60a          ]
56058 ms <   +13 ms>:CODEC RX                      (10  bytes) [02b30404[redacted]c0a]
56058 ms <    +0 ms>:CODEC TX                      (3   bytes) [0078f0              ]
56077 ms <   +19 ms>:CODEC RX                      (5   bytes) [260100f60a          ]
56077 ms <    +0 ms>:CODEC TX                      (12  bytes) [0000523a9610500304e03738]
56103 ms <   +26 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e0006150]
56103 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56132 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e001e841]
56132 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56161 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e0027373]
56162 ms <    +1 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56191 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e003fa62]
56191 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56220 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e0044516]
56220 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56249 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e005cc07]
56250 ms <    +1 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56279 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e0065735]
56279 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
56308 ms <   +29 ms>:CODEC RX                      (13  bytes) [2220523a9610500304e007de24]
56308 ms <    +0 ms>:CODEC TX                      (7   bytes) [000000000077cf      ]
```

Fabian Peters
Federico Cerutti



Fabian Peters – fptrs

Federico Cerutti – ceres-c

KASPER OSWALD
Ingenieure für innovative Sicherheitslösungen

https://github.com/emsec/ChameleonMini/

Want a Chameleon?
Look for this man

Fabian Peters
Federico Cerutti