sales@candelatech.com
support@candelatech.com
+1 (360) 380-1618 [PST, GMT -8]

Ath10k Candela Technologies CT 10.1 Firmware

The CT 10.1 firmware is a modified version of the official firmware from Qualcom-Atheros based on the 10.1.467 release. It should support all features available in the upstream 10.1.467 firmware as well as additional features.

Want to help fund new ath10k CT firmware features with modest contributions? See the ath10k kickstarter page.

This is 'wave-1' firmware, and is known to support at least these NICS. Various OpenWRT platforms are also supported, and other OEM NICs such as generic 9887 chipsets:

- WLE900VX 3x3 dual-band a/b/g/n/AC
  Stable and works in wide variety of boards.
- WLE600VX 2x2 dual-band a/b/g/n/AC
  Stable and works in wide variety of boards.
- DR900VX dual-band a/b/g/n/AC
  This uses the same chipset as the WLE900VX, seems to work well, advertises a higher tx power than WLE900VX. Early versions had problems when device was about 2 feet away (signal was too hot I guess), but newer versions may fix this.

To use this firwmare, download one of the firmware images and rename it firmware-2.bin. If there are any firmware-X.bin files where X is greater than 2, remove or rename them so that the driver will load the CT firmware-2.bin firmware instead of the others with higher numbers. The commands below should work on most systems:

```
mkdir -p /lib/firmware/ath10k/QCA988X/hw2.0/orig
mv /lib/firmware/ath10k/QCA988X/hw2.0/firmware-[3456].bin /lib/firmware/ath10k/QCA988X/hw2.0/orig/
cp firmware-2-ct-full-community.bin /lib/firmware/ath10k/QCA988X/hw2.0/firmware-2.bin
```

Get the **board.bin** file from the official firmware site. Then, reboot or reload the ath10k_pci driver to start using the new firmware. Look in the kernel logs (or dmesg) to make sure the firmware version contains '-ct', such as: `10.1-ct-8x-_xtH-019-ddf2a35`

For more advanced configuration options, see the 10.4 advanced config section. The fwcfg file logic works for at least 10.1 and 10.4 CT firmware.

There are two types of CT firmware: **The community version supports all features EXCEPT connecting multipe vifs to the same AP when using encryption.** The community version may be used for any purpose allowed by the official firmware from Qualcom-Atheros, including commercial applications.
firmware-2-ct-full-community.bin (latest) | 9887

The non-commercial firmware from Candela Technologies does support multiple station vifs connecting to a single AP (really, it supports rx-software-crypt, which is the enabling feature). The non-commercial firmware is NOT freely available. It is restricted to non-commerical use unless you arrange a commercial-use license with Candela Technologies. Contact sales@candelatech.com for additional information on this topic.

Any and all bug reports involving this firmware (and the modified kernels from Candela Technologies) should be sent to support@candelatech.com. Qualcom-Atheros is not responsible for the changes made to the modified firmware and should not be bothered with bug reports relating to it. Reports of success are welcome as well!

To submit a useful bug report, please include kernel logs, especially any firmware crash logs. These crash logs are often chunks of ascii hex. Candela has tools that can usually decode these, but due to NDA issues, these tools may not be shared with the general public. Candela engineers will attempt to decode any reported crashes and provide help as possible. Note that unless you have a contract with Candela that provides otherwise, any help with bugs may be slow or even not much actual help at all. Please also report the kernel version and any other details about how the problem was triggered.

Candela offers paid support options, please contact sales@candelatech.com if you have interest.

See the bottom of this page for some common crash signatures.

CT Firmware Differences from Official QCA Firmware

The ath10k firmware from Candela is based on the 10.1.467 firmware from QCA, but has quite a few added features and fixes. Some notable differences are listed below. Most of these require the kernel modifications in the 3.17 and higher Candela Linux kernels, but the firmware images will work on un-modified kernels for the standard features.

- Supports rx-software-crypt (non-commercial version only, unless you purchase commercial license.). This enables having multiple station VIFs connect to the same AP. Decrypt is done on CPU, so it is relatively slow, especially on slower CPUs.
- Supports up to 64 station VIFS.

- Optimized tx-credits handling. Host driver can configure maximum tx-credits and firmware will return credits immediately so less flush-mgmt hacks are needed on host.
- Work around tx-credits hang due to WMI/CE lockup in firmware (Rls 13+)
- Support IBSS (ADHOC) mode (Rls 13+). IBSS-RSN added in Rls 14, fixed in Rls 19
- Supports reporting tx-rate to the sending stack.
- Optimized firmware memory usage to be more stable in strange configurations.
- Supports configuring the firmware tx-buffer count below 1024.
- Support sending RAW frames, but only non-encrypted frames are currently supported. Also requires out-of-tree patch.
- Lots of bug fixes and hardening related to memory usage issues.
- Firmware returns proper tx-status codes (stock 10.1.467 did not)
- Fix 802.11r (fast roaming) in station mode.

Known CT Firmware/Kernel Bugs

- CE transport failure assert. See the **CT Firmware Crash Signatures** section below.
  Not specific to CT firmware or kernels, very easy to reproduce in some environments. Seems at least mostly fixed these days.
- WMI keepalive failure, probably due to inability to send mgt frames in bad RF environment.
  Not often seen in recent firmware, possibly it is fixed.
- See the ath10k bugs page to view or report bugs.

To take advantage of all of the CT firmware features, please consider using one of the kernels found at: https://github.com/greearb.

The CT firmware has a separate release number appended to the end of the version string. A large number of fixes have been added to the stock 10.1.467. The highlights of those are above. A more detailed changelog is kept for release 14 and above.

BETA (-22)

- No significant changes yet.

See BETA release notes for details.

firmware-2-ct-full-community.bin 988X | 9887

No CT-HTT-MGT feature, no supported upstream features compiled out (no diet). Available for commercial and non-commercial use at no charge.

firmware-2-ct-non-commercial-full.bin 988X | 9887

No CT-HTT-MGT feature, no upstream features compiled out (no diet). Supports rx-sw-crypt (commercial use not allowed unless you have a license from Candela Technologies.

These htt-mgt firmwares require driver patches (use ath10k-ct driver or CT kernel). See release notes.

firmware-2-ct-htt-mgt-community.bin 988X | 9887

If unsure, this is the suggested firmware to use.
Has CT-HTT-MGT feature, un-needed features compiled out of the firmware to allow more stations/vdevs/etc.
Available for commercial and non-commercial use at no charge.

firmware-2-ct-full-nrcc-community.bin 988X | 9887

No CT-HTT-MGT feature, no supported upstream features compiled out (no diet), Rate-ctrl host-caching (swap) is compiled out. This may help on systems with weak CPU or minimal host RAM. Available for commercial and non-commercial use at no charge. See fwcfg notes to use this firmware.

firmware-2-ct-full-htt-mgt-community.bin 988X | 9887

Has CT-HTT-MGT feature, no upstream features compiled out (no diet). Available for commercial and non-commercial use at no charge.

firmware-2-ct-nrcc-community.bin 988X | 9887

No CT-HTT-MGT feature, swbmiss, beacon filtering, roaming code, descriptor-mgt compiled out. Rate-ctrl host-caching (swap) is compiled out. This may help on systems with weak CPU or minimal host RAM. Available for commercial and non-commercial use at no charge. See fwcfg notes to use this firmware.

firmware-2-ct-htt-mgt-nrcc-community.bin 988X | 9887

Has CT-HTT-MGT feature, but swbmiss, beacon filtering, roaming code, descriptor-mgt compiled out. Rate-ctrl host-caching (swap) is compiled out. This may help on systems with weak CPU or minimal host RAM. Available for commercial and non-commercial use at no charge. See fwcfg notes to use this firmware.

firmware-2-ct-non-commercial-full-htt-mgt.bin 988X | 9887

Has CT-HTT-MGT feature, no upstream features compiled out (no diet). Supports rx-sw-crypt

(commercial use not allowed unless you have a license from Candela Technologies.

10.1.467-ct-22

- December 12 2018: Remove assert in tx-abort handling when peer cannot be found.
- Feb 14, 2019: Remove logic that causes assert when swba logic is not initialized. This was seen when trying to bring up 6 VAP vdevs. A similar fix went into wave-2 firmware some time ago.
- Feb 27, 2019: Support up to 32 vAP vdevs, fix stack corruption when driver requests too many vAP.
- Feb 28, 2019: Support beacon-tx-wmi callback message. This lets driver properly clean up beacon buffers so we don't crash (somethings the entire OS/system) due to DMA errors.
- March 12, 2019: Add btcoex feature flag for 2.4Ghz only adapters, backported from upstream 10.2 firmware.
- March 12, 2019: Support offloading decrypt of PMF blockack frames to the host. This lets us do blockack with PMF and rx-sw-crypt. Normal hwcrypt scenarios would not need this.
- March 28, 2019: Fix sometimes using bad TID for management frames in htt-mgt mode. (Backported from wave2, looks like bug would be the same though.)
- April 2, 2019: Support some get/set API for eeprom rate power tables. Mostly backported from 10.2
- April 2, 2019: Support adaptive-CCA, backported from 10.2 (later disabled)
- April 3, 2019: Support adding eeprom configAddr pairs via the set-special API. These configAddrs can be used to change the default register settings for up to 12 registers. Values are read from the board.bin and used by default, or users may directly input them from debugfs.
- May 3, 2019: Fix tx-power settings for 2x2, 3x3 rates. Original logic I put in back in 2016 set 2x2 and 3x3 lower than the needed to be when using most NICs (very high powered NICs would not have been affected I think, not sure any of those exist though.) This improves throughput for 2x2 and 3x3 devices, especially when the signal is weaker.
- May 9, 2019: Tweak rate-ctrl: Ramp PER up faster, down slower. This helps throughput in rate-vs-range test, especially with nss1.
- May 20, 2019: Disable adaptive-CCA. I am not sure it helps, and it may make it slower to detect noise that should tell the system to stop transmitting. If someone has means to test this properly, I'd be happy to work with them.
- June 24, 2019: Try allocating low-priority WMI msgs if high-prio are not available.
- June 24, 2019: Init rate-ctrl to start at lowest rate instead of in the middle. Hoping this helps DHCP when station connects from a long distance.
- October 5, 2019: Fix too-short msg caused by invalid use of PayloadLen in receive path. This appears to resolve the issue of getting (and ignoring) too-short commands when we detect loss of CE interrupts and go into polling mode.
- October 12, 2019: Fix regression in IBSS mode that caused SWBA overrun issues. Related to regression added during the ct-station logic, specifically TSF allocation. Thanks for Ahmed Zaki @ Mage-Networks for helping to diagnose and test.
- October 15, 2019: Only send beacon tx completion events if we can detect CT driver is being used (based on CT_STATS_OK flag being set). This should help CT firmware work better on stock driver.
- November 29, 2019: Fix IBSS merge issue, related to TSF id leakage bug in firmware code. Thanks for Ahmed Zaki @ Mage-Networks for helping to diagnose and test.
- January 22, 2020: Report actual per-chain noise-floor stats, similar to what I did for wave-2.
- February 28, 2020: Fix custom-tx path when sending in 0x0 for rate-code. Have tries == 0 mean one try but NO-ACK (similar to how wave-2 does it).
- March 19, 2020: Fix problem where power-save was not enabled when going off-channel to scan. The problem was a boolean logic inversion in the chmgr code, a regression I introduced a long time ago.
- March 19, 2020: When scanning only on current working channel, do not bother with disable/enable powersave. This should make an on-channel scan less obtrusive than it was previously.
- March 23, 2020: Fix channel-mgr use-after-free problem that caused crashes in some cases. The crash was exacerbated by recent power-save changes.
- March 23, 2020: Fix station-mode power-save related crash: backported the fix from 10.2 QCA firmware.
- March 23, 2020: Attempt to better clean up power-save objects and state, especially in station mode.
- April 13, 2020: Fix scan-on-channel bug introduced recently, and increase WMI buffers available to scan logic so that it works more often, especially when scanning on channel.
- Fall 2021: Optimize compiler options for memory usage and performance.
- Jan 17 2021: Enable peer fixed rate feature (S.G)

See Release notes for details.

firmware-2-ct-full-community-22.bin 988X | 9887

No CT-HTT-MGT feature, no supported upstream features compiled out (no diet). Available for commercial and non-commercial use at no charge.

firmware-2-ct-non-commercial-22.bin 988X | 9887

No CT-HTT-MGT feature, swbmiss, beacon filtering, roaming code, descriptor-mgt compiled out. Supports rx-sw-crypt (commercial use not allowed unless you have a license from Candela Technologies.

firmware-2-ct-non-commercial-full-22.bin 988X | 9887

No CT-HTT-MGT feature, no upstream features compiled out (no diet). Supports rx-sw-crypt (commercial use not allowed unless you have a license from Candela Technologies.

These htt-mgt firmwares require driver patches (use ath10k-ct driver or CT kernel). See release notes.

firmware-2-ct-htt-mgt-community-22.bin 988X | 9887

If unsure, this is the suggested firmware to use.
Has CT-HTT-MGT feature, un-needed features compiled out of the firmware to allow more stations/vdevs/etc.
Available for commercial and non-commercial use at no charge.

firmware-2-ct-full-nrcc-community-22.bin 988X | 9887

No CT-HTT-MGT feature, no supported upstream features compiled out (no diet), Rate-ctrl host-caching (swap) is compiled out. This may help on systems with weak CPU or minimal host RAM. Available for commercial and non-commercial use at no charge. See fwcfg notes to use this firmware.

firmware-2-ct-full-htt-mgt-community-22.bin 988X | 9887

Has CT-HTT-MGT feature, no upstream features compiled out (no diet). Available for commercial and non-commercial use at no charge.

firmware-2-ct-nrcc-community-22.bin 988X | 9887

No CT-HTT-MGT feature, swbmiss, beacon filtering, roaming code, descriptor-mgt compiled out. Rate-ctrl host-caching (swap) is compiled out. This may help on systems with weak CPU or minimal host RAM. Available for commercial and non-commercial use at no charge. See fwcfg notes to use this firmware.

firmware-2-ct-non-commercial-htt-mgt-22.bin 988X | 9887

Has CT-HTT-MGT feature, swbmiss, beacon filtering, roaming code, descriptor-mgt compiled out. Supports rx-sw-crypt (commercial use not allowed unless you have a license from Candela Technologies.

firmware-2-ct-non-commercial-htt-mgt-nrcc-22.bin 988X | 9887

Has CT-HTT-MGT feature, swbmiss, beacon filtering, roaming code, descriptor-mgt compiled out. Rate-ctrl host-caching (swap) is compiled out. This may help on systems with weak CPU or minimal host RAM. Supports rx-sw-crypt (commercial use not allowed unless you have a license from Candela Technologies. See fwcfg notes to use this firmware.

firmware-2-ct-non-commercial-full-htt-mgt-22.bin 988X | 9887

Has CT-HTT-MGT feature, no upstream features compiled out (no diet). Supports rx-sw-crypt (commercial use not allowed unless you have a license from Candela Technologies.

firmware-2-ct-full-htt-mgt-nrcc-community-22.bin 988X | 9887

Has CT-HTT-MGT feature, no upstream features compiled out (no diet). Rate-ctrl host-caching (swap) is compiled out. This may help on systems with weak CPU or minimal host RAM. Supports rx-sw-crypt (commercial use not allowed unless you have a license from Candela Technologies. See fwcfg notes to use this firmware.

10.1.467-ct-21

- Save about 6k of RAM by consolidating some rate-ctrl storage. Backported from wave-2 ath10k-ct firmware. And provide a new way to report tx rate status that helps us better differentiate a non-report from 48Mbps (which has rate-code and flags of 0x0). This last bit requires a new driver tweak as well, but driver and firmware should be forwards and backwards compatible.
- The driver can set the software retry for agg and non-agg TIDs, but the ath10k driver doesn't ever actually do this currently. Change defaults in the firmware to do zero non-agg retries (hardware will still retry 4 times it seems), and default agg-retries to 4 instead of 16. I'm not sure if the firmware actually handles the agg-retries or not, possibly that is handled by upper layers anyway.
- Don't do software retry for non-local frames (ie, frame sent from the driver). This means that instead of seeing around 60 null-data probes on air when peer dies, we will instead only see 4. Similar to logic I did in wave-2 firmware recently.
- Fix crash when monitor dev became the only active vdev. Backported fix from my wave-2 firmware.
- Backport 'survey' logic from 10.2 to 10.1. And while doing so, fix some issues with how 10.2 tried (and failed) to clear the cycle counters when asking for pdev survey info.

- Fix peer stats problem introduced way back in 2016, and also a more recent bug introduced when I did the survey patch.
- Don't generate self-peer peer-stats. They do not seem worth showing.
- Don't crash if retries is set to greater than 2. The rate-ctrl related logic hit an assert due to code that assumes there cannot be more than 2 retries. Stock drivers cannot set retry count, so this bug would not normally be seen in the wild (though it was at least once before based on an old bug report, perhaps due to rts/cts or something like that?)
- Support limited vdev stats, return tsf64 value as requested by a user.
- Support CT-STA mode. This is similar to proxy-sta logic, but allows hw-crypt when we have multiple station vdevs connected to the same AP. This feature is only useful for wifi testing scenarios, and is only in the non-commercial (without a license from Candela Technologies) builds. A likely limitation is that stations on a radio cannot connect to more than 2 different APs. And, this needs lots of testing.
- Backport PMF support from 10.2, especially for block-ack. This has been tested in hw-crypt mode with htt-mgt. Block-ack does not work in sw-rx-crypt mode with 802.11w/PMF.

10.1.467-ct-20

- Improve ability to send frames on mgt devices
- Stability fixes
- Work-around for -40 deg C startup issue.
- Per-chain mgt-frame RSSI reporting.
- Fix stuck scan machine issue (hopefully?).
- Fix PTK rekey problem when using EAP-PEAP (at least).

10.1.467-ct-19

- Fix IBSS + RSN
- Fix TS-SBTC when NSS is set to 1
- Fix unitialized variable that broke block-ack sometimes.
- Fix channel reservation logic.
- Support reading temp through WMI. Requires modified ath10k driver to utilize this.
- Add set-special command to disable certain bandwidths to help with regulatory testing.

10.1.467-ct-18

Big backport of 10.2 features, including ability to build 9887 firmware.
Fix 802.1q VLANs.
Fix issue where radio went deaf to scanning due to inverted boolean statement.
Fix rate-ctrl issue where stations (at least) could get stuck in a low rate.

10.1.467-ct-17

Fix HTT-Mgt TX on 4.5 and higher kernels. Properly configure RX mask on startup to work around problem reported by Mr. Kazior. Allow configuring and disabling firmware station kickout messages.

10.1.467-ct-16

Auto-calculate base MAC addr, allow disabling 20,40,80Mhz bandwidths for TX, fix beacon-miss crash, backport iqcal baseband hang fix, disable congestion bin logic, allocate more stateless tids to stop rare crash, re-work rate-ctrl cache to deal better with many peers, backport AXI/CE fix from 10.2, fix scan requests for many ssids.

10.1.467-ct-15

Support management over HTT, fix 802.11r, lots of rate-ctrl changes, monitor-mode receives assoc-request and other frames it was previously dropping, allow configuring some CCA related values to better pass regulatory tests, off-channel fixes

10.1.467-ct-14

IBSS improvements, increase tx power for NSS < 3 rates, support setting mgmt tx-rate, return proper tx-status, bug-fixes in rate-ctrl, etc.

10.1.467-ct-013

Add IBSS/AHDOC support.
Work-around tx-credits hang due to WMI/CE lockup in firmware (requires ath10k driver patches)
Attempt to fix a few asserts reported by users (scan code, rate-ctrl, resource-mgr, etc)

10.1.467-ct-012

Pay better attention to max-nss in rate-control logic.
Allow to request no channel reservation when starting vdev (improves connect time, especially with multiple vdevs)
Fix crash when using raw-tx mode.

10.1.467-ct-011

Stop using feature flag that is now used by upstream 10.2.x firmware. This lets CT firmware work with latest ath10k driver.

10.1.467-ct-010

Fix bug introduced in version 009 (related to moving some structures to IRAM).
Support the assert-on-purpose ath10k driver patch recently applied to upstream.
Slight optimization to use about 1k less IRAM.

10.1.467-ct-009

Improve RAM usage: Re-organized, trimmed, and otherwise made better use of RAM. Allow compiling out swbmiss, beacon filtering, roaming code. Images with 'full' in their name do NOT have the previously mentioned features compiled out. Over-all, freed up about 80k of extra RAM, which can be used for more vdevs, peers, buffers, etc.
Supports 64 vdevs (one should be reserved for monitor interface, so effectively 63 vdevs for current kernels.)

10.1.467-ct-008

Fix crash related to AP configured with IBSS_RSN, reported and tested by Emanuel Taube.
Improve memory usage by packing structs and moving some stuff to IRAM. Can now support 44 vdevs.
Remove some un-needed MEMSET operations, might help performance a very small bit (this was not hot-path items as far as I can tell.).

10.1.467-ct-007

Save some RAM by more tightly packing structures. Enables an additional vdev, so can now support 37.

10.1.467-ct-006

Disable the scan-on-operating-channel-only optimization. This was not working right. Will fix and re-enable this sometime later.

10.1.467-ct-005

Fix inverted scan rx-filter logic. Improves scan all around, and fixes completely broken scan on DFS channels.

10.1.467-ct-004

Add support for flushing all tids for all peers for all vdevs. Hopefully this will help ath10k driver flush itself faster.
Changed order of some patches, but over-all code should not be modified.

10.1.467-ct-003

Hit two more asserts in overnight testing of -002:
Attempt to work around assert related to scanning while deleting vdev.
Attempt to work around assert in rate-control logic.

10.1.467-ct-002

Attempt to work around crash related to scanning while deleting vdev.
Attempt to work around crash in rate-control logic.

10.1.467-ct-001

Implemented community v/s non-commercial-only builds.
Added numeric versioning for easier bug reporting.

CT Firmware Crash Signatures

There is at least one persistent firmware crash that I have not been able to fix (and do not have a lot of ideas on how to attempt to fix it). This section gathers details on such known crashes so that users can attempt to understand if they are seeing a known crash. Please report it anyway, but I am especially interested in crashes not listed here. Since the crash-decode tool cannot be made public, you have to make do with searching for specific hex.

Firmware CE Engine assert

There is a known bug, seen on x86, Gateworks Ventana boards and probably everywhere else. It is seen with WLE900VX as well as Doodle-Labs ACE-DB-3, and probably others. It is seen with upstream firmware-5.bin and stock kernels, so this is not something specific to CT firmware or kernels. This bug is seen in both AP and Station mode.

The bug is that the CE engine in the firmware reports a fatal error and then asserts. It is very easy to trigger this problem if you try to transmit high-speed UDP traffic while the RF network is very busy. A 99.9% constant-transmit source to act as a blocking signal will reproduce this bug within seconds.

A more general test case is typically something like: Set up AP with 8+ stations associated, use wget (or similar) to download 1MB web pages over and over to simulate streaming media, and firmware will typically crash in less than 10 hours.

At least with a recent version 14 firmware (community-build), the crash site is at address: **0x009b5a8d**. Likely any crash very near that address on version 14 firmware is the same bug. If you are running a CT 3.17 or higher kernel, or at least with those patches applied, you will often also see a 0x9110aaa1 signature (this is a firmware debuglog message that prints before the assert hits). The stock driver may not print out the firmware debuglog info.

For instance, here is a hex-dump of the binary crash log captured from /debug/ieee80211/phy1/ath10k/fw_crash_dump after a firmware crash that shows this signature:

```
hexdump ~/tmp/crashphy1.dump.2.4ghz |more

0000000 5441 3148 4b30 462d 2d57 5544 504d 0000
0000010 ab00 0000 0001 0000 07b3 9ec8 3f6f 4e6d
0000020 2e97 3201 00b1 d4c1 02ff 0432 0000 0000
0000030 016c 4100 0041 0000 01d3 0000 0000 0000
0000040 0000 0000 0003 0000 003f 0000 003f 0000
0000050 085b 0000 01b2 3380 0003 0000 3031 312e
0000060 342e 3736 632d 2d74 6f63 2d6d 7566 6c6c
0000070 302d 3431 342d 3431 3862 0061 7906 5537
0000080 0000 0000 b8e3 1b4a 0000 0000 0e05 0003
0000090 2e33 3431 352e 5320 504d 6d20 646f 755f
00000a0 6c6e 616f 2064 5241 764d 2037 3270 3876
00000b0 0020 0000 0000 0000 0000 0000 0000 0000
00000c0 0000 0000 0000 0000 0000 0000 0000 0000
00000d0 9fa4 0040 16a0 0040 0c00 0040 d4f0 0040
00000e0 0000 0000 0000 0000 0000 0000 0000 0000
*
0000150 0000 0000 00f0 0000 016c 4100 15b3 0000
0000160 5a8d 009b 5b31 0095 5a8d 009b 0530 0006
.....
00006b0 aaa1 9110
....
```

Note the 5a8d 009b in line 0x160..that is the signature for this crash. Farther down in the file you may also see the aaa1 9110 signature from the dbglog entry.

Firmware CE watchdog assert

CT firmware has a WMI message watchdog feature that can be enabled when using the CT patched drivers/kernels. The driver will send no-operation (NOP) message every second to the firmware. After the firmware receives one of these messages, if it ever does NOT receive the message for 5 seconds in a row after that, it will assert and crash. This allows the host to take recovery actions instead of just having the system effectively hang forever.

The signature for this type of crash is to see 0x91103345 in the debug-log contents when firmware crashes, for instance:

```
[   36.914223] ath10k_pci 0000:05:00.0: firmware crashed! (uuid fdbe13ae-630d-4079-8ec3-86f69887fe98)
[   36.914251] ath10k_pci 0000:05:00.0: qca988x hw2.0 (0x4100016c, 0x043202ff) fw 10.1.467-ct-com-full-014-ff596b
[   36.914272] ath10k_pci 0000:05:00.0: debug 0 debugfs 1 tracing 0 dfs 0 testmode 1
[   36.919384] ath10k_pci 0000:05:00.0: firmware register dump:
[   36.919408] ath10k_pci 0000:05:00.0: [00]: 0x4100016C 0x000015B3 0x009A90B7 0x00955B31
[   36.919428] ath10k_pci 0000:05:00.0: [04]: 0x009A90B7 0x00060130 0x00000005 0x00000032
[   36.919446] ath10k_pci 0000:05:00.0: [08]: 0x0040ECB0 0x00411030 0x00400000 0x00000005
[   36.919465] ath10k_pci 0000:05:00.0: [12]: 0x00000009 0x00000000 0x00958360 0x0095836B
[   36.919482] ath10k_pci 0000:05:00.0: [16]: 0x00958080 0x0094085D 0x00000000 0x00000000
[   36.919501] ath10k_pci 0000:05:00.0: [20]: 0x409A90B7 0x0040AE44 0x00009198 0x00400000
[   36.919519] ath10k_pci 0000:05:00.0: [24]: 0x80944C31 0x0040AEA4 0x00411294 0xC09A90B7
[   36.919537] ath10k_pci 0000:05:00.0: [28]: 0x80942BE7 0x0040AED4 0x00411294 0x00000000
[   36.919555] ath10k_pci 0000:05:00.0: [32]: 0x80942EB3 0x0040AEF4 0x004090A0 0x00409110
[   36.919572] ath10k_pci 0000:05:00.0: [36]: 0x80940F18 0x0040AF14 0x00000008 0x00403A20
[   36.919590] ath10k_pci 0000:05:00.0: [40]: 0x80940EEA 0x0040AF44 0x00400000 0x00000000
[   36.919607] ath10k_pci 0000:05:00.0: [44]: 0x80940F31 0x0040AF64 0x00401C10 0x00400600
[   36.919624] ath10k_pci 0000:05:00.0: [48]: 0x40940024 0x0040AF84 0x004068E8 0x004068E8
[   36.919642] ath10k_pci 0000:05:00.0: [52]: 0x00000000 0x0040AFA4 0x009BB001 0x00040020
[   36.919658] ath10k_pci 0000:05:00.0: [56]: 0x00403BEC 0x00000000 0x00000001 0x00400600
[   36.924724] ath10k_pci 0000:05:00.0: state: 1 debug log header, dbuf: 0x412548  dropped: 0
[   36.927300] ath10k_pci 0000:05:00.0: state: 1 [0] next: 0x412560 buf: 0x4103ac sz: 1500 len: 216 count: 8 free
[   36.929840] ATH10K_DBG_BUFFER:
[   36.929860] ath10k: [0000]: 00009198 17FC0432 00000000 00000704 00000005 00000000 00000000 00009198
[   36.929876] ath10k: [0008]: 17FC0432 00000000 00000000 00000000 00000000 00000000 00009198 17FC0432
[   36.929892] ath10k: [0016]: 00000001 00000000 00000000 00000000 00000000 00009198 17FC0432 00000002
[   36.929926] ath10k: [0024]: 00000000 00000000 00000000 00000000 00009199 17FC0432 00000003 00000000
[   36.929951] ath10k: [0032]: 00000000 00000000 00000000 00009199 17FC0432 00000004 00000000 00000000
[   36.929977] ath10k: [0040]: 00000000 00000000 00009199 0FFC0432 91103345 00006F07 00009198 00009199
[   36.930003] ath10k: [0048]: 17FC0001 000015B3 000015B3 0040AD34 4100016C 00000000
[   36.930016] ATH10K_END
```