BE-CSI: Unlocking 320 MHz CSI on Commodity Wi-Fi 7 Devices

Stefano Fontana*
University of Brescia/CNIT
Brescia, Italy
stefano.fontana@unibs.it

Jakob Link
TU Darmstadt
Darmstadt, Germany
jlink@seemoo.tu-darmstadt.de

Francesca Meneghello
Northeastern University
Boston, USA
fr.meneghello@northeastern.edu

Matthias Hollick
TU Darmstadt
Darmstadt, Germany
IMDEA Networks Institute
Madrid, Spain
mhollick@seemoo.tu-darmstadt.de

Francesco Restuccia
Northeastern University
Boston, USA
f.restuccia@northeastern.edu

Francesco Gringoli*
University of Brescia/CNIT
Brescia, Italy
francesco.gringoli@unibs.it

Abstract

Channel state information (CSI) is a fundamental measurement primitive for Wi-Fi channel characterization, MIMO analysis, localization, and integrated sensing and communication (ISAC). However, CSI access on commercial Wi-Fi devices remains limited, particularly for the new IEEE 802.11be generation (Wi-Fi 7). This paper presents BE-CSI, a firmware-based CSI extraction tool for commercial Broadcom Wi-Fi 7 access points. BE-CSI extends the NexmonCSI extraction approach to a variety of devices and adapts it to the architectural changes introduced by the extremely high throughput (EHT) PHY. The development of BE-CSI was supported by an AI-assisted reverse-engineering workflow that accelerates firmware porting. We have prototyped BE-CSI on commodity ASUS Wi-Fi 7 platforms and evaluated its ability to extract CSI from 320 MHz EHT channels and 4×4 MIMO transmissions in the 6 GHz band. Experimental results show that BE-CSI exposes consistent wide-band CSI across different channel widths, supports Wi-Fi 7-specific features, and can reach 1.6 million extracted subcarriers per second. We further demonstrate that the dual-radio architecture of the target platform can be exploited to obtain an aggregate CSI observation bandwidth of approximately 480 MHz.

*Also with CNIT, National Inter-University Consortium for Telecommunications.



This work is licensed under a Creative Commons Attribution 4.0 International License.

WiNTECH '26, Austin, TX, USA

© 2026 Copyright held by the owner/author(s).

ACM ISBN 979-8-4007-2879-2/26/10
https://doi.org/10.1145/3831662.3844167

CCS Concepts

• **Hardware → Wireless devices**; • **Networks → Wireless local area networks**.

Keywords

Channel State Information, Reverse Engineering, IEEE 802.11be, IEEE 802.11bf, Wi-Fi, Wireless Sensing.

ACM Reference Format:
Stefano Fontana, Jakob Link, Francesca Meneghello, Matthias Hollick, Francesco Restuccia, and Francesco Gringoli. 2026. BE-CSI: Unlocking 320 MHz CSI on Commodity Wi-Fi 7 Devices. In *20th ACM Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization (WiNTECH '26), October 26–30, 2026, Austin, TX, USA.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3831662.3844167

1 Introduction

Channel state information (CSI) is a widely used measurement primitive in Wi-Fi research. By exposing the frequency response between transmitter and receiver antennas, CSI gives researchers access to fine-grained properties of the wireless channel. This paves the way to several device-free sensing applications such as channel characterization, localization, gesture recognition, beamforming analysis, and integrated sensing and communications (ISAC) [18, 3, 27, 26, 23]. These applications are based on the observation that changes in the surrounding environments are reflected into variations in CSI values, which, in turn, can be used as a proxy for the surroundings [25, 5, 19].

The role of sensing in telecommunication systems has become increasingly important as wireless systems move toward tighter integration between communication and environmental awareness. Unlike earlier approaches that treated

sensing as an opportunistic byproduct of communication signals, modern ISAC frameworks aim to make environmental awareness part of the wireless stack itself [23, 1]. Wi-Fi is a natural candidate for this transition because access points (APs) are already widely deployed in homes, offices, and public spaces. The establishment of IEEE 802.11bf [13] for Wi-Fi sensing reflects this broader shift toward wireless devices that can support both communication and sensing functions [19]. For this reason, access to accurate CSI from commercial Wi-Fi devices is not a mere measurement problem; it is a prerequisite for ISAC research to evaluate how sensing and communication can coexist on deployed infrastructures and prototype new applications.

Despite its potential, CSI remains difficult to obtain from commercial hardware. Commodity chipsets rarely expose CSI through documented interfaces like IEEE 802.11bf standardizes [4], and 802.11bf-compliant devices are not yet available on the market.

The introduction of IEEE 802.11be (Wi-Fi 7) makes current approaches insufficient, since Wi-Fi 7 increases the maximum channel bandwidth from 160 MHz to 320 MHz and introduces extremely high throughput (EHT) features such as wider orthogonal frequency-division multiple access (OFDMA) configurations and preamble puncturing [12, 9]. The wider bandwidth provides qualitative improvement for CSI-based applications. In the frequency domain, a wider channel exposes a larger portion of its response and provides more subcarrier observations. In the delay domain, bandwidth determines the ability to separate multipath components: doubling the bandwidth from 160 MHz to 320 MHz reduces the nominal delay resolution from about 6.25 ns to about 3.125 ns. This strongly impacts ISAC, since many applications depend on distinguishing small changes in the multipath profile caused by body motion, object displacement or changes in the indoor environment [23, 24].

This paper addresses the gap between newer Wi-Fi technology and available extraction platforms by introducing BE-CSI, a CSI extraction system for commercial Wi-Fi 7 devices. BE-CSI targets current Broadcom IEEE 802.11be hardware and recovers the physical (PHY) metadata needed to extract CSI from EHT frames and export it to host-side analysis tools. This enables ISAC experiments with commodity Wi-Fi 7 devices and supports configurations that were not available through previous commercial off-the-shelf (COTS) CSI tools, including bandwidths up to 320 MHz and 4×4 multiple-input multiple-output (MIMO) configurations. BE-CSI will be included as part of Nexmon CSI, retaining open source[1] access to the code. The initial BE-CSI release will focus on the Asus GT-BE98 device family. Later development will extend the support to other EHT chipsets.

[1]https://github.com/seemoo-lab/nexmon_csi/tree/be-csi

2 Related Work

The landscape of CSI extraction has diversified significantly, providing researchers with a spectrum of choices ranging from modified COTS hardware to highly specialized software-defined radio (SDR) instrumentation.

Legacy COTS Extraction Platforms. Historically, the sensing research community has primarily relied on the Intel 5300 network interface card (NIC) and the Linux 802.11n CSI Tool [10]. Despite its pioneering role, the platform is limited by its 802.11n protocol constraints and a low spectral resolution that reports only 30 orthogonal frequency-division multiplexing (OFDM) subcarrier groups rather than individual OFDM tones [9]. Later, Qualcomm-based solutions like the Atheros CSI Tool for the AR9300 series, improved upon this by providing uncompressed CSI for up to 114 subcarriers in 40 MHz channels [17]. More recently, the Nexmon CSI Extractor bridged the gap for 802.11ac hardware, enabling full-CSI 4×4 MIMO extraction from 80 MHz very high throughput (VHT) frames on several Broadcom and Cypress chipsets [22]. AX-CSI [9] further extended this to the 802.11ax standard, enabling the extraction of 2048 subcarriers 160 MHz CSI from Broadcom 43684 hardware, even though limited to a very specific AP model, which is no longer manufactured by Asus. All of these systems rely on firmware patches or undocumented driver features to extract PHY-layer information after the frame has been received and processed by the hardware. As this processing is performed by closed-source hardware components, the resulting CSI measurements may not represent genuine, unaltered channel observations, but rather data that have been implicitly filtered, calibrated, or otherwise transformed by the device. Consequently, dedicated normalization procedures are often required to compensate for such hardware-dependent effects.

High-End SDR and USRP-based Systems. For applications requiring high definition, specialized systems like the universal software radio peripheral (USRP) X300 or X400 series are preferred [7]. These platforms support massive channel bandwidth and link speeds and provide high clock rates necessary to analyze 320 MHz 802.11be-compliant waveforms [2].

These systems provide the highest accuracy in terms of resolution and flexibility, as they give access to raw signal samples that can be processed, typically in MATLAB, to recover genuine, unfiltered CSI data. However, they are extremely costly, often up to two orders of magnitude higher than commodity AP [14]. In addition, they require computationally intensive post-processing to extract CSI data, making them significantly slower than hardware-based baseband (BB) processing, resulting in limited real-time packet processing rates.

SDR-Based Middleware – Openwifi. Openwifi represents a full-stack, open-source IEEE 802.11 implementation on field-programmable gate array (FPGA) system on chip (SoC) architectures [15]. Its primary strength lies in its low-latency medium access control (MAC) timing, allowing it to be "as fast as possible" in terms of protocol interaction and flexibility. The downside of this system is its bandwidth, which is limited to 20 MHz in the open-source version due to the SoC maximum sampling rate and constraints [6, 15]. The subscription-based Openwifi software includes support for 802.11ax and, in turn, should enable CSI extraction for larger bandwidths, up to 160 MHz.

PicoScenes. This is a versatile middleware platform supporting concurrent CSI measurement from multiple NICs and SDR devices [14]. Its primary strength is a unified API implementation that supports 802.11ax and earlier standard amendments on COTS hardware, and 802.11be on USRP platforms. COTS support for the latest amendments is currently limited to the Intel AX210, which provides OFDMA monitoring capabilities [14, 8] but lacks the deep firmware-level control available on Broadcom-based Nexmon platforms.

Embedded and Specialized Platforms. On the ultra-low-cost end of the solutions, the ESP-CSI platform for Espressif ESP32 chipsets allows for distributed sensing in both the 2.4 GHz and 5 GHz bands up to Wi-Fi 6. While highly accessible, it suffers from very limited resolution, providing only 108 subcarriers at 40 MHz [16], and lower CSI quality due to significant hardware noise and clock drift. Finally, FeitCSI [11] is an open-source 802.11 CSI measurement and injection tool designed for modern Intel Wi-Fi that also provides fine time measurement (FTM) functionalities. The system utilizes already existing extraction features in the NIC with a modified kernel-space driver, instead of relying on firmware modifications like Nexmon [22]. At the time of writing, FeitCSI only supports Intel AX series.

3 AI-Assisted Reverse Engineering

The BE-CSI reverse-engineering workflow combines conventional firmware analysis with large language model (LLM)-assisted interpretation. The LLM does not replace binary-analysis tools or manual validation; instead, it integrates and interprets the partial evidence they produce. We primarily used GPT-5 model [21] and Ghidra reverse engineering software [20]. Fig. 1 summarizes the workflow.

The process starts with binary diffing between a previously reverse-engineered AX-CSI Broadcom firmware image and the target IEEE 802.11be `BCM6726b0` firmware. This stage is performed independently of the LLM and produces candidate function matches together with their similarity scores

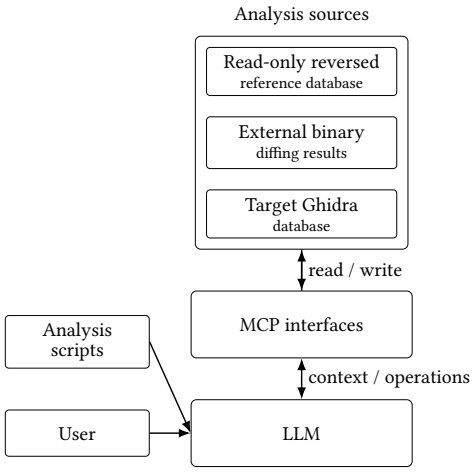


Figure 1: AI-assisted firmware reverse-engineering workflow and its evidence sources. Validated hypotheses are written back to the target database as recovered names, comments, and structure fields.

and match types. The corresponding AX-CSI Ghidra database is also retained as a read-only reference for confrontation.

Through model context protocol (MCP) interfaces, these artifacts and both Ghidra analysis contexts are exposed to the LLM. The model can retrieve decompiled functions, call sites, and cross-references, compare target functions with reference candidates, and correlate these observations with the diffing results. Analysis scripts and direct prompts then use this context to formulate hypotheses, for example by identifying relocated structure fields from equivalent control and data flows.

Model outputs are treated strictly as hypotheses. Recovered function names, inferred roles, and structure offsets are manually verified in Ghidra, while changes affecting BE-CSI are additionally validated at runtime on the device under test (DUT). Only validated results are incorporated into the target database as names, comments, structure definitions, and annotations.

As the database becomes progressively richer, the same interface also serves as an interactive analysis layer for inspecting functions, call chains, reference matches, and structure-field uses. In this mode, the LLM acts as a front end to the accumulated analysis state rather than an autonomous reverse-engineering agent. Database modifications remain explicitly user-directed and subject to manual inspection.

This workflow enabled the first working BE-CSI port to be completed within one week. In particular, model-assisted retrieval, comparison, and targeted analysis scripting accelerated the identification of code relationships and structure-field semantics while retaining human control over every accepted result.

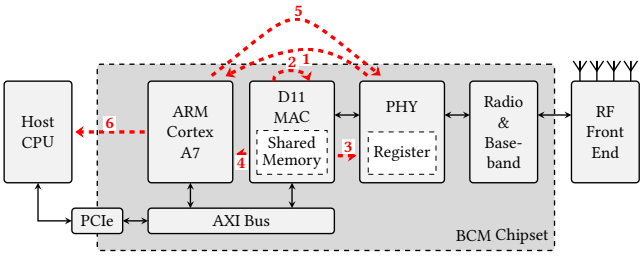


Figure 2: CSI extraction process implemented in the new port of the extractor: Upon frame reception, the PHY status information is sent to the dongle (1). Meanwhile, the D11 core performs filtering operation on the MAC layer of the received frame (2) and places the PHY in deaf mode if matching (3). Then the D11 core triggers the reception path of the dongle (4), which will start the extraction process. Upon finishing, it places the PHY back into reception mode (5) and sends the extracted data as network packets to the host (6).

4 BE-yond AX-CSI

The implementation of this new CSI extraction tool builds on our previous work on 802.11ax [9]. More specifically, we adapted the tool developed for the Broadcom `BCM43684` 802.11ax chipset to the Broadcom `BCM6726` 802.11be chipset. The reference platform is the Asus GT-BE96 Pro, running Nexmon modified firmware [22], which represents the Wi-Fi 7 successor of the 802.11ax platform considered in [9]. Although the overall FullMAC architecture remains similar across the two generations, supporting CSI extraction on the BCM6726 required substantial rework in some areas, mainly due to changes in how PHY status information is delivered to the dongle firmware.

Fig. 2 shows the FullMAC architecture adopted by the target Broadcom platform. Most 802.11-specific functions are handled internally by the chipset. On the host side, the Linux operating system mainly configures the radio and exchanges data with the wireless device through the direct memory access (DMA) interface, where packets are exposed as Ethernet-like traffic. Inside the wireless chipset, operations are split between the D11 core and the embedded ARM CPU, hereafter referred to as the dongle. The dongle mainly manages non-time-critical operations, whereas the D11 core handles time-sensitive tasks such as channel access, frame acknowledgment, and other real-time MAC procedures.

Similar to our prior work on 802.11ax, CSI extraction is coordinated between the D11 core and the dongle. The D11 core firmware is patched to identify target frames and mark them accordingly. When a target frame is received, the D11 core disables the receiver to freeze the PHY state associated with the frame. The dongle then extracts the CSI information, delivers it to the host, and finally resumes normal radio operation.

The main architectural difference between the `BCM6726` and the `BCM43684` concerns the handling of PHY status information. On the BCM43684, the PHY status and the corresponding frame data could be processed along a receive path that makes their association available to the firmware in a relatively direct way. On the BCM6726, instead, PHY status information is delivered through a different mechanism. The chipset uses a separate queue for PHY status events, and the firmware processes frame data and PHY status through two independent interrupt request (IRQ) chains. As a result, the frame payload and its associated PHY status are not naturally available within the same receive-processing function, and the PHY status information is always cleared after the related code has operated on it, introducing possible timing problems if unnoticed.

This separation prevents a direct port of the 802.11ax extraction logic. We therefore modify the receive path to enable PHY status storage and to introduce the flow-control mechanisms required to make the correct PHY status available when the corresponding frame-data interrupt is handled. In practice, the firmware stores PHY status entries as they arrive through their dedicated path and later associates them with the target frame when the frame data becomes available.

The PHY status delivery path differs depending on the type of received traffic. For management frames, PHY status information is attached to the frame through the management queue. Instead, for data frames, PHY status is delivered through the alternate PHY-status queue. The modified firmware handles both cases. When a management or control frame is targeted, the corresponding PHY status can be recovered from the management receive path. When a data frame is targeted, the firmware retrieves the PHY status previously stored from the alternate queue and synchronizes it with the frame-data interrupt.

The resulting CSI extraction proceeds as indicated in red in Fig. 2 and is detailed next. Upon frame reception, the relevant PHY state information is sent to the dongle through its dedicated channel. In the meantime, the D11 core performs parsing operations, where our patched code marks packets that match the configured filtering rules against the MAC-layer information. Once a frame has been matched, the D11 disables the radio receiver, placing the device in deaf mode to preserve the PHY state. Then, the frame data is delivered to the dongle through the appropriate receive paths. Depending on the frame type, the firmware either obtains the PHY status from the management queue or retrieves it from the storage populated by the patched alternate PHY-status queue. Once the target frame and its PHY status are both available, the dongle extracts the CSI data from the PHY, encapsulates

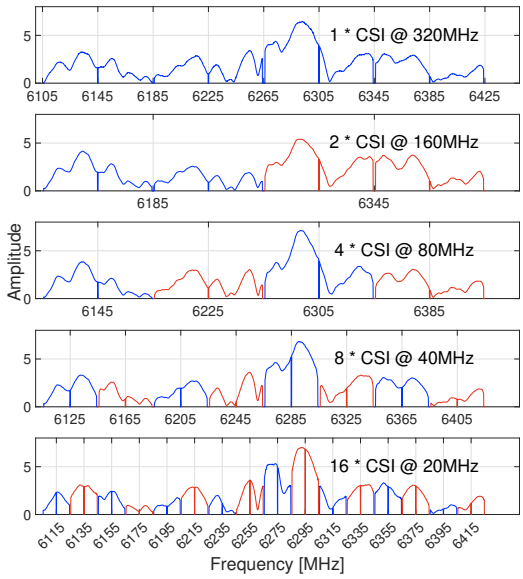


Figure 3: The same link captured at 320 MHz and as aggregated narrower channels.

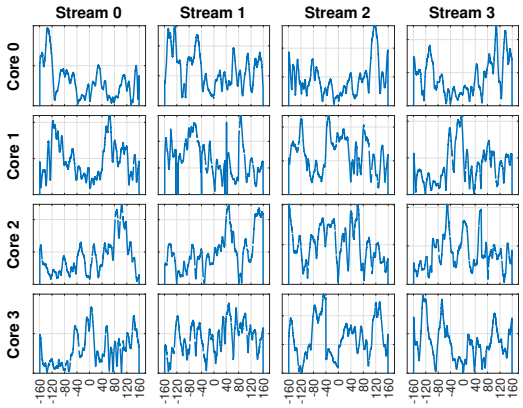


Figure 4: CSI for all sixteen links of a 320 MHz 4×4 MIMO transmission.

the measurements into datagrams, and forwards them to the host through the DMA interface. A userspace application running on the host receives these datagrams and stores the CSI samples into a packet. Once all CSI data associated with the target frame have been transferred to the host, the dongle re-enables the receiver and normal Wi-Fi operation resumes. Note that as we also verified in the 802.11ax implementation, performing CSI extraction in the dongle rather than entirely inside the D11 core introduces additional latency and limits the maximum CSI extraction rate. Nevertheless, the proposed modifications preserve the same high-level extraction architecture while enabling CSI collection on 802.11be hardware.

5 Results

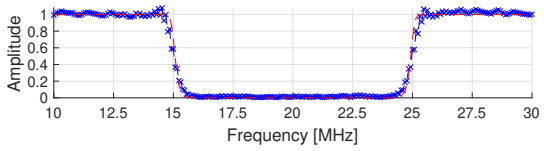
We evaluated BE-CSI on COTS Broadcom BCM6726 802.11be hardware. We chose to focus on newly introduced features, like 320 MHz EHT 4×4 MIMO and preamble puncturing. In addition, we enhanced our evaluation by measuring extraction latency and comparing it with the AX-CSI latency [9]. Finally, we considered dual-radio operation beyond the nominal 320 MHz bandwidth.

5.1 CSI Extraction Performance

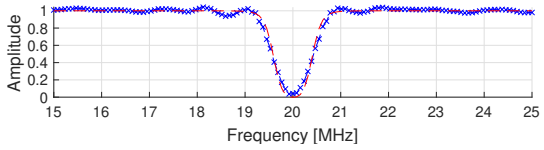
Fig. 3 shows the CSI amplitude extracted from frames transmitted over different subchannel bandwidths mapped onto the main 320 MHz channel. The plot highlights how the 320 MHz EHT channel is described with marginal deviation as the composition of smaller spectral portions. This confirms that BE-CSI correctly reconstructs the wideband CSI representation exposed by the chipset, rather than reporting only a partial or narrowband view of the received frame. The overlap between the CSI traces obtained from different bandwidth configurations also provides an experimental consistency check as the same spectral region is observed through different channel configurations. Assuming an empty room and a static environment, the extracted amplitudes follow the same channel response, up to the expected differences caused by calibration, filtering, and receiver-chain effects. Note that the CSI amplitudes have been normalized to maintain the area under them constant for display purposes.

The experimental results in Fig. 4 show the CSI evaluated on four different spatial streams in a MIMO transmission. Two identical GT-BE98-Pro devices featuring 4 spatial streams each were used for this evaluation. Each subplot depicts the CSI amplitude of the 320 MHz transmission for one transmit–receive antenna pair, giving a total of sixteen stream-specific CSI. For each received frame, the platform exposes a wideband CSI vector for every MIMO link, yielding a large amount of complex-valued channel information. This is a substantial increase over previous commodity CSI platforms, including AX-CSI, which supported up to 160 MHz and 4×4 MIMO on IEEE 802.11ax hardware [9]. The distinct responses across the sixteen MIMO links reflect the independent channels observed by each antenna pair, which provide spatial diversity for sensing, MIMO characterization, beamforming, and ISAC experiments.

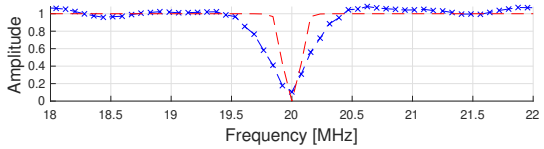
To further assess the frequency-domain resolution of BE-CSI, we performed a controlled experiment in which a known spectral modification was introduced before transmission and then observed in the CSI extracted at the receiver. The experiment used a USRP X310 connected by coaxial cable and suitable attenuation to one 5 GHz radio, yielding almost flat CSI at the receiver. The generated signal is a 160 MHz



(a) 10 MHz notch filter.



(b) 1 MHz notch filter.



(c) 200 kHz notch filter.

Figure 5: Measured normalized CSI (blue) and expected notch response (red).

Table 1: BE-CSI extraction throughput across EHT-PHY configurations.

BW [MHz]	80	160	160	320	320	320
MIMO config.	1×1	1×1	4×4	1×1	1×4	4×4
# subcarriers	1024	2048	32768	4096	16384	65536
Frames per second	982	566	47	339	95	25
Subcarriers per second	1M	1.16M	1.55M	1.4M	1.55M	1.6M

wide 802.11be frame with a high order digital notch filter applied before transmission. Fig. 5 shows the normalized CSI when varying the notch bandwidth. The `BCM6726` reported CSI correctly follows the filtered signal behavior, especially with larger notch bandwidths such as in Fig. 5a. The presence of ripple, especially in Fig. 5b, may indicate that the receiver is performing a still-unknown interpolation process to the raw data.

5.2 Extraction Timing Analysis

As mentioned in Sect. 4, CSI extraction temporarily interrupts normal reception while the platform preserves PHY state, reads CSI tables, and exports data to the host. During this interval, the system does not process or collect incoming frames; therefore, both the frames themselves and the corresponding CSI measurements are lost. As in AX-CSI [9], this limits the rate of IEEE 802.11 frames that can be successfully received and used for CSI extraction. Tab. 1 reports BE-CSI performance for different channel-width and MIMO configurations. The measurements were obtained by configuring a GT-BE98-PRO as transmitter and saturating the channel using the packet injector already available in the system, which is based on Broadcom's PKTENG utility and is part of the original firmware. This tool bypasses the standard channel-access procedure and allows frames to be transmitted with a constant inter-frame gap.

Two main observations can be drawn from the results. First, the number of processed frames per second decreases as the configuration complexity increases, as expected due to the larger amount of CSI data that must be retrieved and exported for wider channels and higher MIMO orders. Second, and less intuitively, the number of extracted subcarriers per second is not constant across configurations: it increases for heavier configurations, remains relatively stable among them, and reaches its maximum in the 320 MHz 4×4 case. Conversely, for lighter configurations, such as the single-channel 80 MHz case, the number of extracted subcarriers per second can decrease by up to approximately 50%. This behavior can be explained by the fixed overhead associated with each CSI extraction operation: after a frame is received, the platform must notify the dongle-side code, trigger the routine that accesses the PHY tables, process their content, and export the resulting data. For lightweight configurations, this per-frame overhead dominates the overall extraction time, reducing the effective subcarrier extraction rate.

Finally, we note that AX-CSI [9] reported a processing rate of 37 frames/s for the 160 MHz AX 4×4 configuration, which is equivalent to the 160 MHz BE 4×4 configuration in terms of the number of extracted subcarriers. In contrast, BE-CSI achieves 47 frames/s under the same channel-width and MIMO configuration, corresponding to an improvement of approximately 30%. This gain can be attributed to the increased processing capabilities of the newer chipset generation, which is expected to provide higher computational resources to support the additional features introduced by the EHT standard.

5.3 IEEE 802.11be-Specific Features

Beyond wider channels, IEEE 802.11be introduces mechanisms that directly affect the structure of the received spectrum. One of the most relevant is preamble puncturing, which allows a transmitter to avoid selected portions of an otherwise wide channel. This feature improves coexistence and spectrum utilization, but it also changes the CSI representation because some frequency regions are intentionally not occupied by the transmitted signal. Although puncturing was already introduced in IEEE 802.11ax, its applicability was limited to specific High Efficiency (HE) multi user configurations and to a restricted set of puncturing patterns. IEEE 802.11be

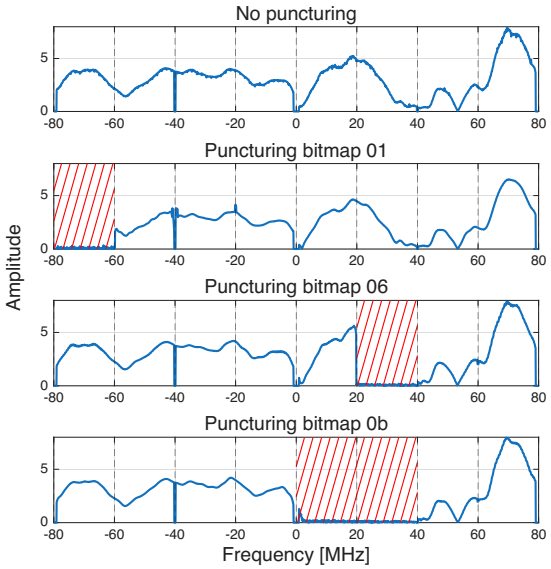


Figure 6: USRP X420 CSI without puncturing and with bitmaps 0x01, 0x06, and 0x0b.

generalizes this concept by supporting more flexible puncturing configurations, making the technology a more prominent feature in the interpretation and processing of wideband CSI.

Fig. 6 shows CSI amplitude traces extracted for different puncturing configurations that were specifically obtained by encoding 160 MHz 802.11be frames with Matlab and transmitting them with an USRP X420. The unpunctured case exhibits CSI over the full occupied channel, whereas the punctured configurations show clear 20 or 40 MHz spectral gaps corresponding to the puncturing bitmap.

5.4 Extending BE-CSI Dual Radio Support

The GT-BE98-Pro device that we used for developing BE-CSI contains two separate 6 GHz radios, one covering the lower part of the 6 GHz spectrum and one covering the higher part. We modified the available channel list of both radios to operate close to their analog filter limits. This makes it possible to transmit and receive frames outside the nominal center of each radio's preferred operating range and to observe how the analog front-end attenuates the received CSI near the band edges.

Fig. 7 shows the combined CSI derived by merging the CSI obtained in the two channels into a single 480 MHz CSI. The first radio provides usable CSI over the lower portion of the considered spectrum (blue), after which the measured amplitude decreases as the analog filter suppresses the signal. The same happens with the second radio (red), as it provides usable CSI over the higher portion of the spectrum, with attenuation visible near its lower transition band. When the two

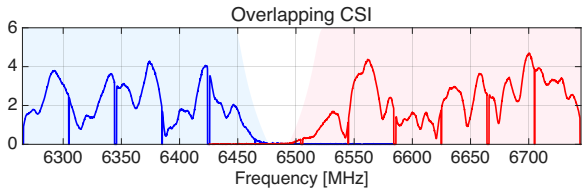


Figure 7: Composite 480 MHz CSI reconstructed by merging the measurements of the lower (blue) and upper (red) 6 GHz radio, each operating near the edge of its analog bandwidth.

measurements are combined in frequency, they provide an aggregate CSI observation spanning approximately 480 MHz.

This approach extends the sensing bandwidth available to the platform beyond a single 320 MHz EHT channel. In principle, the wider frequency aperture can improve delay-domain resolution and provide richer multipath information for sensing and channel characterization. However, the combined CSI is affected by the analog filtering of the two radios. In particular, the transition regions introduce a hole in the middle of the reconstructed spectrum, where neither radio provides a strong and reliable measurement.

6 Nexmon CSI Platforms

Tab. 2 lists the targeted Broadcom revisions and dual- or tri-band platforms across Wi-Fi 6, 6E, and 7; additional revisions remain under development.

Table 2: Targeted Nexmon CSI platforms.

Chip	Platforms	Wi-Fi
BCM43684	RT-AX86U, RT-AX82U, XT8	6
BCM6715B0†	RT-AX86U Pro, RT-AX82U v2	6
BCM43684C0	GT-AXE11000	6E
BCM4389C1†	Google Pixel 7	6E
BCM4383A3†	Google Pixel 10	6E
BCM6726B0	GT-BE98, GT-BE98 Pro	7
BCM6717A0†	RT-BE96U	7
BCM4398D0†	Google Pixel 8	7
BCM4390B1†	Google Pixel 9	7

†Currently under development, future release planned.

7 Conclusion

BE-CSI brings firmware-based CSI extraction to commodity Broadcom Wi-Fi 7 by adapting Nexmon to the BCM6726 receive path. It supports 320 MHz channels and 4×4 MIMO in the 6 GHz band, provides consistent measurements across channel widths and all sixteen MIMO links, follows controlled spectral modifications, and shows the gaps created by

preamble puncturing. Its two-radio capture spans roughly 480 MHz. Although export pauses reception, BE-CSI reaches 1.6 million subcarriers/s in its most demanding configuration.

Access on deployed-class hardware lowers the barrier to Wi-Fi 7 channel characterization, ISAC, MIMO analysis, and privacy-aware sensing. We plan to use the AI-assisted workflow to support further Broadcom devices, investigate receiver-side processing of exported CSI, and release an open-source Nexmon patch for reproduction and extension.

8 Acknowledgement

This work was partially supported at CNIT by project 6G-INTENSE (Intent-driven NaTive AI architecturE supporting Compute-Network abstraction and Sensing at the Deep Edge), Horizon Europe SNS JU Grant Agreement N. 101139266; and by project PAISES-6G (Pioneering AI-enhanced SEcure 6G Services framework), Horizon Europe SNS JU Grant Agreement N. 101292896. At Northeastern University by the National Science Foundation under Grant ECCS-2229472, in part by the Air Force Office of Scientific Research under Grant FA9550-23-1-0261, in part by the Office of Naval Research under Grant N00014-23-1-2221 and in part by the ARO under Grant W911NF261A165.

References

[1] Giovanni Angelo Alghisi, Giovanni Perin, Francesca Meneghello, and Francesco Gringoli. 2025. Let It Beam: Enabling Selective and Secure CSI-based Sensing via Beamforming. In *Proc. ACM WiNTECH*, 9–16. doi:10.1145/3737895.3768295.

[2] Joana Angjo, Elena Tonini, Falko Dressler, and Renato Lo Cigno. 2025. Poster: mmWave CSI-based Sensing: a Feasibility Study. In *Proc. ACM MobiCom*, 1353–1355. doi:10.1145/3680207.3765684.

[3] Roshan Ayyalasomayajula, Aditya Arun, Chenfeng Wu, Shrivatsan Rajagopalan, Shreya Ganesaraman, Aravind Seetharaman, Ish Kumar Jain, and Dinesh Bharadia. 2020. LocAP: Autonomous Millimeter Accurate Mapping of WiFi Infrastructure. In *Proc. USENIX NSDI*, 1115–1129.

[4] Cheng Chen, Hao Song, Qinghua Li, Francesca Meneghello, Francesco Restuccia, and Carlos Cordeiro. 2022. Wi-Fi sensing based on IEEE 802.11bf. *IEEE Commun. Mag.*, 61, 1, 121–127.

[5] Zhenghua Chen, Le Zhang, Chaoyang Jiang, Zhiguang Cao, and Wei Cui. 2019. WiFi CSI Based Passive Human Activity Recognition Using Attention Based BLSTM. *IEEE Trans. Mobile Comput.*, 18, 11, 2714–2724. doi:10.1109/TMC.2018.2878233.

[6] Marco Cominelli, Felix Kosterhon, Francesco Gringoli, Renato Lo Cigno, and Arash Asadi. 2021. IEEE 802.11 CSI randomization to preserve location privacy: An empirical evaluation in different scenarios. *Computer Networks*, 191, 107970.

[7] [SW] Ettus Research, USRP Hardware Driver (UHD) Software version 4.10.0.0, 2026. URL: https://github.com/EttusResearch/uhd.

[8] Stefano Fontana, Francesca Meneghello, Jakob Link, Francesco Restuccia, Matthias Hollick, and Francesco Gringoli. 2025. Breaking the Barrier to Downlink Packet Capture in OFDMA Wi-Fi Networks. In *Proc. ACM WiNTECH*, 49–56. doi:10.1145/3737895.3768300.

[9] Francesco Gringoli, Marco Cominelli, Alejandro Blanco, and Joerg Widmer. 2021. AX-CSI: Enabling CSI Extraction on Commercial 802.11ax Wi-Fi Platforms. In *Proc. ACM WiNTECH*, 46–53. doi:10.1145/3477086.3480833.

[10] Daniel Halperin, Wenjun Hu, Anmol Sheth, and David Wetherall. 2011. Tool release: gathering 802.11n traces with channel state information. *SIGCOMM Comput. Commun. Rev.*, 41, 1, 53. doi:10.1145/1925861.1925870.

[11] Miroslav Hutar, Peter Brida, and Juraj Machaj. 2023. FeitCSI, the 802.11 CSI tool. https://feitcsi.kuskosoft.com.

[12] IEEE. 2025. IEEE Standard for Information Technology–Telecommunications and Information Exchange Between Systems–Local and Metropolitan Area Networks–Specific Requirements–Part 11: Wireless LAN MAC and PHY Specifications–Amendment 2: Enhancements for Extremely High Throughput (EHT). *IEEE Std 802.11be-2024*, 1–1020. doi:10.1109/IEEESTD.2024.11090080.

[13] IEEE. 2025. IEEE Standard for Information Technology–Telecommunications and Information Exchange Between Systems–Local and Metropolitan Area Networks–Specific Requirements–Part 11: Wireless LAN MAC and PHY Specifications–Amendment 4: Enhancements for Wireless LAN Sensing. *IEEE Std 802.11bf-2025*, 1–228. doi:10.1109/IEEESTD.2025.11184214.

[14] Zhiping Jiang et al. 2021. Eliminating the barriers: Demystifying Wi-Fi baseband design and introducing the PicoScenes Wi-Fi sensing platform. *IEEE Internet Things J.*, 9, 6, 4476–4496.

[15] Xianjun Jiao, Wei Liu, Michael Mehari, Muhammad Aslam, and Ingrid Moerman. 2020. openwifi: a free and open-source IEEE 802.11 SDR implementation on SoC. In *Proc. IEEE VTC-Spring*, 1–2.

[16] Han Li, Qinghua Yang, Changfa Wang, Zhipeng Yuan, and Xiaolei Wang. 2025. A Deep Learning-Enhanced CSI-Based System for High-Precision Indoor Positioning. *IEEE Trans. Instrum. Meas.*, 74, 1–14.

[17] Linux Wireless Documentation Project. 2024. ath10k spectral scan. (2024). Retrieved July 9, 2026 from https://wireless.docs.kernel.org/en/latest/en/users/drivers/ath10k/spectral.html.

[18] Yongsen Ma, Gang Zhou, and Shuangquan Wang. 2019. WiFi sensing with channel state information: A survey. *ACM Comput. Surv.*, 52, 3, 1–36.

[19] Francesca Meneghello, Nicolò Dal Fabbro, Domenico Garlisi, Ilenia Tinnirello, and Michele Rossi. 2023. A CSI dataset for wireless human sensing on 80 MHz Wi-Fi channels. *IEEE Commun. Mag.*, 61, 9, 146–152.

[20] [SW] National Security Agency, Ghidra Software Reverse Engineering Framework 2019. URL: https://github.com/NationalSecurityAgency/ghidra.

[21] OpenAI. 2025. GPT-5. (2025). https://openai.com/index/introducing-gpt-5/.

[22] Matthias Schulz, Daniel Wegemer, and Matthias Hollick. 2017. Nexmon: the c-based firmware patching framework. https://nexmon.org.

[23] Elena Tonini and Renato Lo Cigno. 2026. Leveraging Mutual Information in Stochastic CSI Analysis for Wi-Fi Sensing. In *Proc. WONS*, 97–104. doi:10.23919/WONS68803.2026.11501829.

[24] Elena Tonini, Francesco Gringoli, Renato Lo Cigno, and Marco Cominelli. 2025. Towards a Quantitative Analysis of CSI for AI/ML Based Sensing. In *Proc. IEEE WCNC*, 1–6. doi:10.1109/WCNC61545.2025.10978183.

[25] Xuyu Wang, Chao Yang, and Shiwen Mao. 2020. On CSI-based vital sign monitoring using commodity WiFi. *ACM Trans. Comput. Healthcare*, 1, 3, 1–27.

[26] Yue Zheng, Yi Zhang, Kun Qian, Guidong Zhang, Yunhao Liu, Chenshu Wu, and Zheng Yang. 2019. Zero-effort cross-domain gesture recognition with Wi-Fi. In *Proc. ACM MobiSys*, 313–325.

[27] Rui Zhou, Meng Hao, Xiang Lu, Mingjie Tang, and Yang Fu. 2018. Device-free localization based on CSI fingerprints and deep neural networks. In *Proc. IEEE SECON*, 1–9.