boroCTF 2026

ECHOClub | Open Division | Solo Competitor

June 13–15, 2026

41	5,000	276th	205th
Challenges Solved	Total Points	Overall Rank	Open Division

out of 831 teams total | 653 in Open Division | competing solo

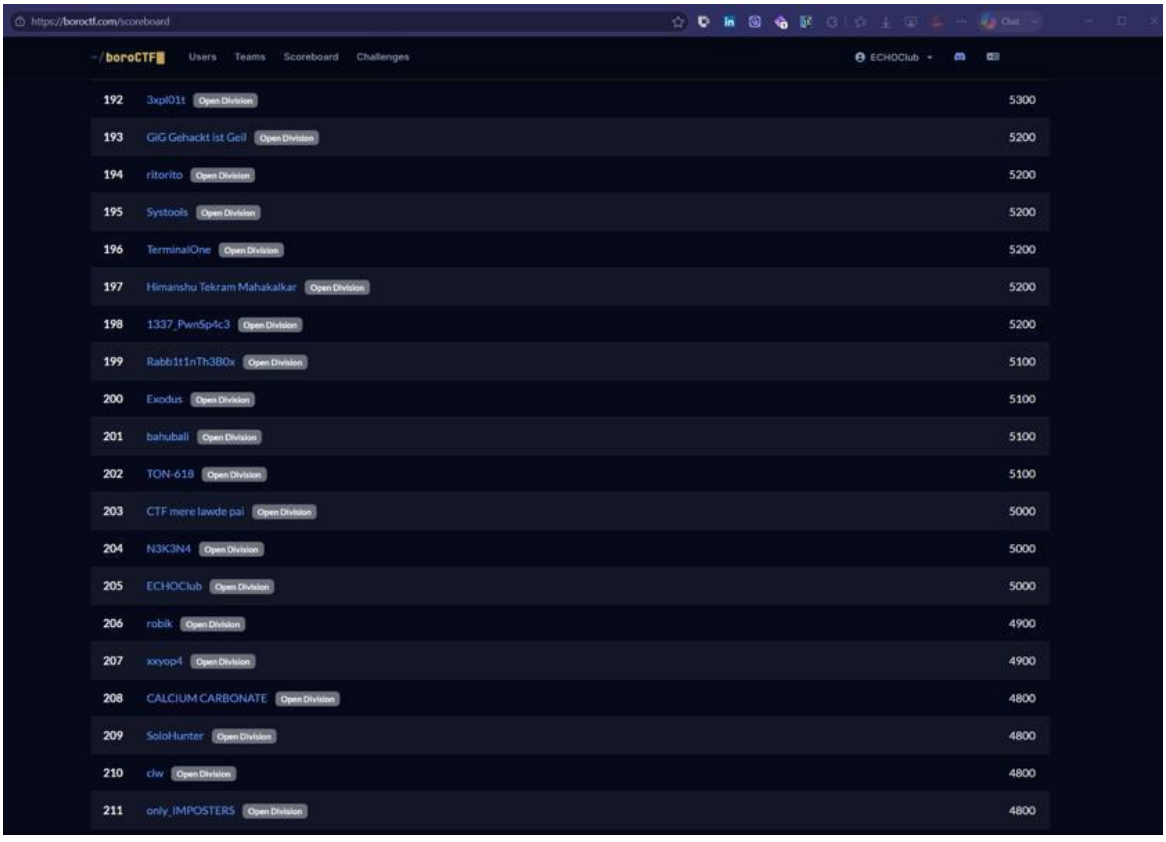
1. About This Report

This report documents ECHOClub's participation in boroCTF 2026, a Capture the Flag cybersecurity competition hosted by Freehold Borough and open to high school and open division competitors worldwide. The competition ran from June 13–16, 2026.

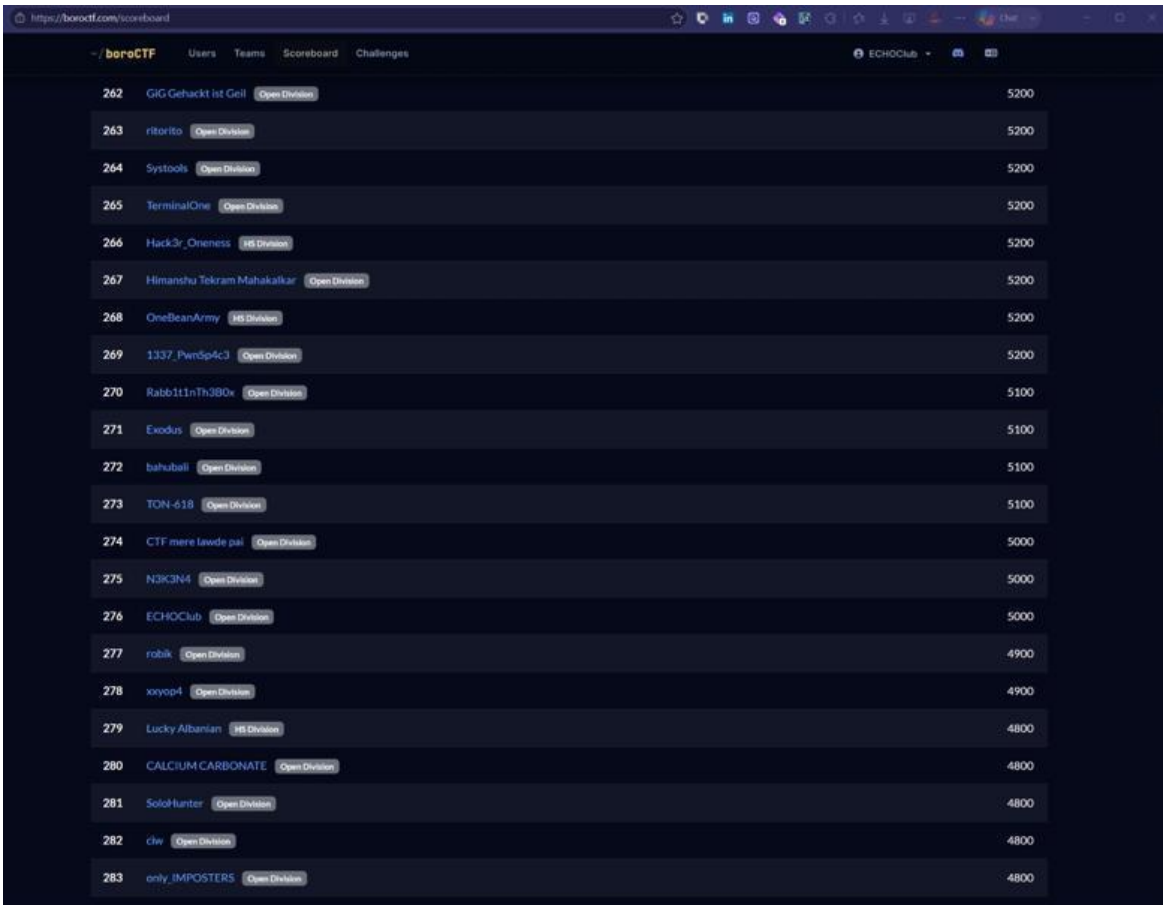
ECHOClub competed in the Open Division as a solo entry — one competitor, three days, 41 challenges solved across six categories. This report serves as both a personal record and an educational resource for the ECHOClub community, demonstrating real-world cybersecurity techniques through the lens of competitive CTF play.

2. Competition Results

2.1 Final Standings



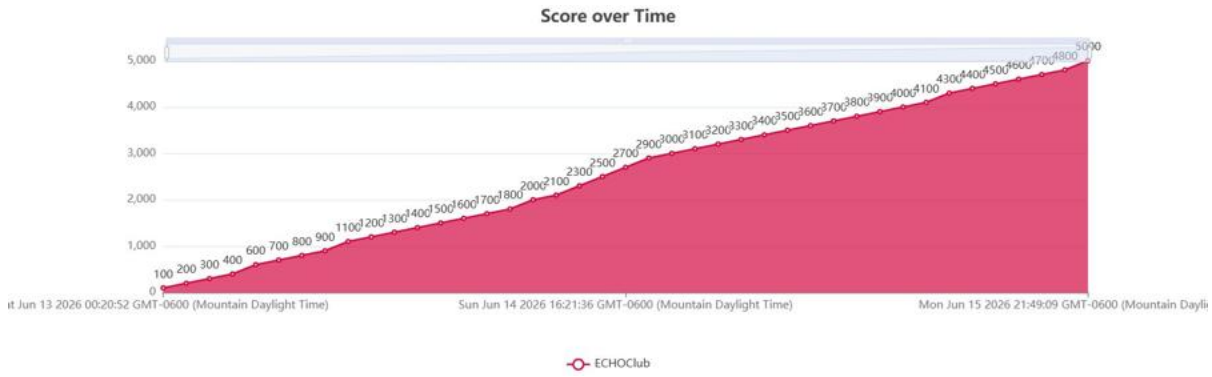
ECHOClub — 205th place, Open Division (5,000 pts)



ECHOClub — 276th place overall out of 831 teams

2.2 Score Progression

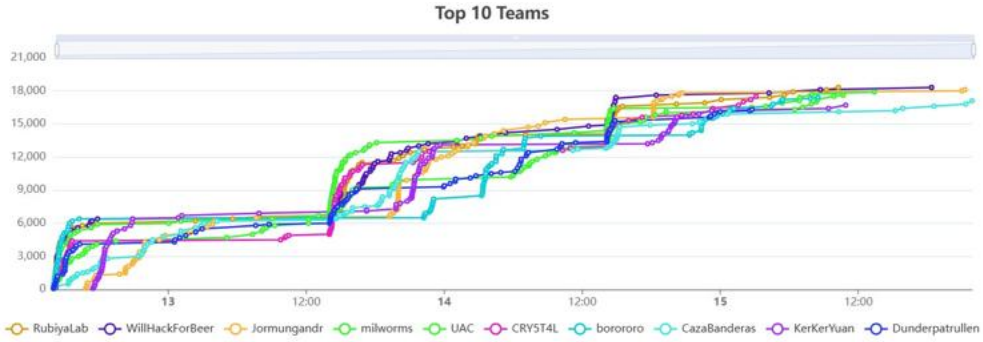
The following chart shows ECHOClub's score over the competition period. The consistent upward slope reflects steady solo solving across all three days — no large team bursts, just methodical work.



ECHOClub Score over Time — June 13 to June 15, 2026

2.3 Top 10 Teams

For context, the top 10 teams reached 18,000+ points — reflecting large multi-person teams solving in parallel. ECHOClub's solo 5,000 point performance is competitive within that field.



Top 10 Teams Score Progression — boroCTF 2026

3. Solves by Category

41 challenges were solved across six categories over the competition period:

Category	Challenges Solved	Points Earned	% of Total
Forensics	13	1,800 pts	36%
OSINT	11	1,300 pts	26%
Crypto	7	700 pts	14%
Web	6	700 pts	14%
Misc	4	500 pts	10%
TOTAL	41	5,000 pts	100%

Forensics was the strongest category, accounting for 36% of total points. OSINT and Cryptography were also strong performers. Web exploitation challenges were solved cleanly across all 6 available.

4. Full Solve List

Challenge	Category	Points	Time
Boro Hero	OSINT	100	Jun 13, 12:20 AM
Nature's Takeover	OSINT	100	Jun 13, 12:23 AM
The Squad	OSINT	100	Jun 13, 12:36 AM
Satoshi Hunt	OSINT	100	Jun 13, 11:01 AM
Satoshi's Secret	OSINT	200	Jun 13, 11:54 AM
Physical Access >>	OSINT	100	Jun 13, 2:33 PM
Oops...	OSINT	100	Jun 13, 2:34 PM
Fireman	OSINT	100	Jun 13, 2:57 PM
Where there's smoke, there's fire	OSINT	200	Jun 13, 4:47 PM
kitty kitty meow meow	Forensics	100	Jun 13, 10:03 PM
Grep'n it	Forensics	100	Jun 13, 9:42 PM
Billie Eilish	Forensics	100	Jun 13, 10:30 PM
The Shattered Needle	Forensics	100	Jun 13, 11:09 PM
File Me to the Moon	Forensics	100	Jun 13, 11:10 PM
Silent Sentinel	Forensics	100	Jun 13, 11:14 PM
Satoshi: A Memory of The Past	Forensics	100	Jun 13, 11:20 PM
A basic start	Crypto	100	Jun 14, 12:09 PM
Looking through Windows	Forensics	200	Jun 14, 12:16 PM
Retinal Burn	Forensics	200	Jun 14, 11:55 AM
File-et Mignon	Forensics	200	Jun 14, 3:59 PM

Chronos	Forensics	200	Jun 14, 4:21 PM
Blackwall Protocol	Forensics	200	Jun 14, 4:54 PM
Mark Zuckerburg	Forensics	100	Jun 14, 5:31 PM
Boro Coin 1	Crypto	100	Jun 14, 5:49 PM
Et Tu, Brute	Crypto	100	Jun 14, 6:03 PM
Not the Flag	Crypto	100	Jun 14, 6:05 PM
Flipper's Dilemma	Crypto	100	Jun 14, 6:07 PM
So Many Layers	Crypto	100	Jun 14, 6:17 PM
Flight	Crypto	100	Jun 14, 6:46 PM
Hidden Meaning	OSINT	100	Jun 14, 7:09 PM
Go Knicks!	OSINT	100	Jun 14, 7:11 PM
Nature's Delight	Misc	100	Jun 14, 7:22 PM
Distortion	Misc	100	Jun 14, 7:22 PM
Its a Simple Challenge Really	Misc	100	Jun 14, 7:32 PM
64 is life	Misc	200	Jun 14, 11:02 PM
Beyond the Homepage	Web	100	Jun 15, 12:09 AM
Cracking the Vault	Web	100	Jun 15, 12:15 AM
boro-senpai 1	Web	100	Jun 15, 12:22 AM
dotdotslashflagtxt	Web	100	Jun 15, 12:55 AM
Drone Dash	Web	100	Jun 15, 12:56 AM
Jay W. Tee	Web	200	Jun 15, 9:49 PM

5. Challenge Highlights

The following challenges are highlighted for their technical depth and educational value. Full writeups for all 41 challenges will be published on the ECHOClub website and Instagram page.

Jay W. Tee — JWT Token Forging (Web, 200 pts)

The challenge name itself was the hint — Jay W. Tee = JWT (JSON Web Token). The site accepted any login credentials and returned a signed JWT with role: guest. Using the alg:none vulnerability, we forged a new token with role: admin and an empty signature, bypassing authentication entirely.

- Decoded the JWT to reveal: {"username":"admin","role":"guest"}
- Forged new header: {"alg":"none","typ":"JWT"} encoded via Base64URL in CyberChef
- Forged new payload: {"username":"admin","role":"admin"} encoded via Base64URL
- Replaced cookie in Dev Tools — navigated to /admin — flag retrieved

Flag: boroCTF{n0_s1gn4tur3_n0_pr0bl3m^^}

Key lesson: Never trust the alg field from the token itself. Servers must enforce algorithm server-side.

File-et Mignon — Sparse File Analysis (Forensics, 200 pts)

The challenge file appeared to be 10 terabytes in size — but only 32KB of real data existed. This is a Linux sparse file where large gaps of zeros are not stored on disk.

- Used du -sh to confirm only 32KB of actual data
- Used Python os.lseek() with SEEK_DATA/SEEK_HOLE flags to find 8 real data regions
- Each region sat at exact 1TB intervals (1TB, 2TB, 3TB... 8TB), each 4096 bytes
- Read each chunk, assembled 5-character flag fragments

Flag: boroCTF{y0u_c4rv3d_th3_v01d_l1k3_4_ch3f}

Key lesson: File size on disk vs apparent size — always check actual disk usage with du before assuming file contents.

Chronos & Blackwall Protocol — Timing Steganography (Forensics, 200 pts each)

Both challenges hid binary data inside network packet timing — not in the packet contents, but in the microsecond gaps between packets.

- Chronos: packet intervals of exactly 0.25s (bit 0) and 0.75s (bit 1)
- Blackwall Protocol: timing differences of ~150us (bit 0) and ~650us (bit 1)
- Both required brute-forcing bit alignment offset (0-7) to find readable output
- Offset 7 decoded to the flag in both cases

Flags: boroCTF{c0mbobulat3_sp@gh3tti_nep0t1$m} | boroCTF{s4nd3v1st4n_gh0st_1n_th3_m4ch1n3_8f92a}

Key lesson: Steganography isn't just images — data can be hidden in timing, metadata, whitespace, and protocol behavior.

Looking Through Windows — NTFS File Recovery (Forensics, 200 pts)

A corrupted VHD disk image appeared empty but contained deleted files in the NTFS recycle bin recoverable with forensic tools.

- Mounted NTFS partition with correct offset: mount -t ntfs-3g -o ro,offset=65536
- Used ntfsundelete to find and recover deleted file $RIFYI8L.zip
- Cracked zip password with fcrackzip + rockyou.txt — password: forget92936281
- Extracted flag.txt from recovered zip

Flag: boroCTF{f!l3_f0r3nsics_FTW!!}

Key lesson: Deleted files are not gone — NTFS maintains metadata about deleted files until the space is overwritten.

6. About ECHOClub

ECHOClub is a cybersecurity club dedicated to making security education accessible, hands-on, and engaging for all skill levels. Through live challenge walkthroughs, tool demonstrations, and competition participation, ECHOClub bridges the gap between classroom theory and real-world security skills.

- Instagram walkthroughs: instagram.com/truth_addicts/
- Planned live demos: JWT token forging, packet timing steganography, NTFS forensics
- Focus areas: OSINT, Digital Forensics, Web Exploitation, Cryptography

boroCTF 2026 represents exactly the kind of real-world challenge ECHOClub trains for. Full writeups for all 41 solved challenges will be published as educational content for the community.