

## „Kuźnia Custom Firmware”

Jak bardzo chciałbyś CFW (Custom Firmware) na PlayStation Vita? A co jeśli ci powiem, że już dziś jest to możliwe? Zgadza się, taiHEN (zapewniający patchowanie systemu) + Ensō (zapewniający bootowanie konsoli z HENkaku) + wtyczki (zapewniające dodatkowe funkcje) z powodzeniem można nazwać CFW. Naturalnie, że nie taki jak na PS3 (wszak nie można go zainstalować w taki sam sposób jak oryginalne oprogramowanie), ale dla użytkownika końcowego zupełnie niczym się nie różni. Na PSV i PSTV to ty jesteś tym, który ten CFW zbuduje, adekwatnie do potrzeb, dogrywając stosowne wtyczki i instalując dodatkowe programy.

Niniejszy poradnik nie prowadzi krok po kroku, a jedynie wskazuje na konkretne czynności, jakie należy wykonać po kolei. Opisy są lakoniczne, skierowane do umysłów, które potrafią czytać ze zrozumieniem, znają podstawy języka angielskiego (np. aby rozumieć treść readme.md projektów na githubie – terazniejszej mekce otwartego oprogramowania), i osób które potrafią posługiwać się managerem plików (co w dobie „pokolenia smartfonów” powoli staje się co najmniej nieoczywiste).



## Przygotuj żelazo

Podstawą każdego miecza jest dobry stop. :) A więc upewnij się, że masz wersję fw 3.60, ponieważ na żadnej innej nie zadziała. Jeśli masz nowszą to niestety ale będziesz musiał poczekać aż ktoś znajdzie nowe exploity. Jeśli starszą to zaktualizuj **za pomocą USB** lub specjalnej strony (ponieważ z witryny Sony starsze fw są zdejmowane, po prostu ustaw DNS w konsoli na 212.47.229.76 i aktualizuj tak jak oficjalny fw (**ale tylko jeśli wyświetli się: Firmware 3.60 (変革 Compatible)**)). Następnie odwiedź stronę **HENkaku** i cierpliwie czekaj, aż konsola rozgrzeje się do białości – to jest, aż przeglądarka zostanie zamknięta.

I to jest podstawa, tzw. „przeróbka” która działa aż do wyłączenia konsoli. Można teraz instalować i uruchamiać niepożądaną przez Sony programy.

## Ostrzenie oręża

Przed sobą masz teraz trzy drogi:

1. Albo za każdym razem exploitować konsolę poprzez odwiedzenie strony internetowej z HENkaku (uciążliwe i uzależniające od serwera hostującego pliki).
2. Albo przygotowanie wersji offline, która zagnieździ się w mailu na partycji użytkownika (PSTV) lub karcie pamięci (PSV).
3. Albo modyfikacja MBR pamięci wewnętrznej konsoli i skryptu startowego (czyli Ensō, bezobsługowe, a więc nie tak jak w przypadku maila, ale za to inwazyjne i teoretycznie ryzykowne).

Jeśli zdecydowałeś się na wariant **drugi**, to po prostu uruchom MolecularShell (manager plików) i wgraj **HENkaku Offline Installer**. Uruchom go z dostępem do internetu i cierpliwie czekaj. Po tym zabiegu po każdym uruchomieniu konsoli będziesz musiał otwierać specjalnie spreparowany list aplikacją systemową i liczyć na to, że akurat exploit znajdzie punkt do zahaczenia się w pamięci (na v10 prawie zawsze kończy się sukcesem). Szczegółowy opis znajdziesz w **poradniku** opisującym cały proces.

Jeśli zdecydowałeś się na wariant **trzeci**, to po prostu uruchom MolecularShell (manager plików) i wgraj **HENkaku Ensō Installer** (czyli pobierz plik **\*.vpk** i go zainstaluj). Uruchom instalator i postępuj zgodnie z wyświetlanymi poleceniami, czyli wciśnij kółko potwierdzając świadomość ryzyka i chęć uwolnienia konsoli, ;) a następnie iks aby dokonać stosownych modyfikacji środowiska uruchomieniowego. Po pomyślnej instalacji, pozostaje już tylko wcisnąć dowolny przycisk by zresetować konsolę. Od teraz Vita powinna za każdym razem uruchamiać się z od razu aktywnym HENkaku.

```
Built On: 2017-07-29T05:13:01Z
This software will make PERMANENT modifications to your Vita. If anything goes wrong,
there is NO RECOVERY (not even with a hardware flasher). The creators provide this
tool "as is", without warranty of any kind, express or implied and cannot be held
liable for any damage done.
Press CIRCLE to accept these terms or any other key to not accept.
Options:
CROSS      Install/reinstall the hack.
TRIANGLE  Uninstall the hack.
SQUARE     Fix boot configuration (use this if taiHEN isn't loading on boot).
CIRCLE     Exit without doing anything.
Looking system...
Checking MBR... ok!
Checking os0... ok!
Checking for previous installer...
Writing config... ok!
Writing blocks... ok!
Writing MBR... ok!
The installation was completed successfully.
Success.
Press any key to reboot.
```

## Ozdabianie

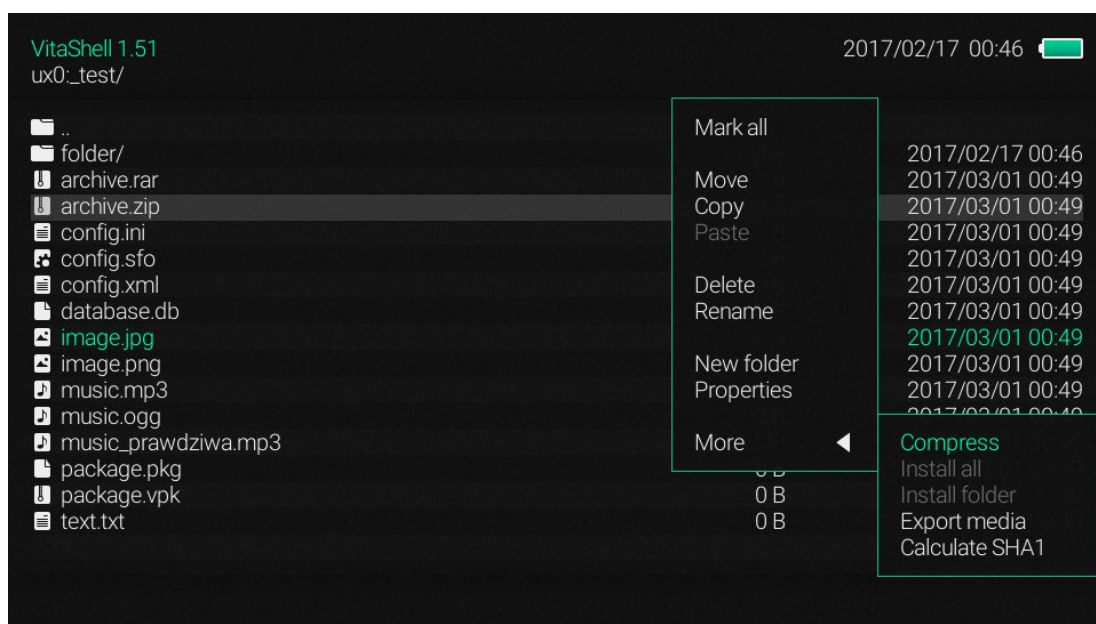
Skoro miecz już gotowy na cięcie truchła, przyszedł czas do obowiązkowych ozdób podkreślających charakter jego właściciela. A więc oprogramowanie dodatkowe, bez którego nie ma mowy o żadnej personifikacji (względem potrzeb, nie tylko wyglądu jak sugeruje nagłówek).

### Programy w paczkach VPK

Czyli forma w jakiej można znaleźć programy, uruchamiane przez użytkownika z bąbli. Tak naprawdę są to zwykłe archiwa ZIP (a więc łatwe w modyfikacji w razie potrzeb), które podczas instalacji, rozpakowuje manager plików, wrzucając w odpowiednie miejsce i tworząc wpisy w bazie danych.



A więc jakie to wynalazki można na tej scenie znaleźć, warte zainteresowania? Na samym początku najważniejszy, czyli najlepszy manager plików jakim jest [VitaShell](#). Pozwala montować dodatkowe partycje/urządzenia, katalogi z PFS (dodatkowy system szyfrowania, którego Sony używa do zabezpieczania gier i danych użytkownika), posiada wbudowany serwer FTP (bardzo wolny) i host USB, umożliwia także odświeżanie bazy danych, przeglądanie plików graficznych, odtwarzanie muzyki, edycję plików tekstowych i SFO. Oczywiście jego główną funkcją jest zarządzanie danymi na podmontowanych zasobach konsoli. Wszystkie pozostałe managery plików, wbudowane w inne programy (np. [ONEMenu](#)) są cieniem VitaShella.





Drugim dosyć ciekawym programem jest [VITAident](#), dzięki któremu poznasz swój unikalny numer konsoli i numer identyfikacyjny w sieci SEN (o ile twoja Vita została aktywowana), plus oczywiście cały zestaw innych danych o konsoli.

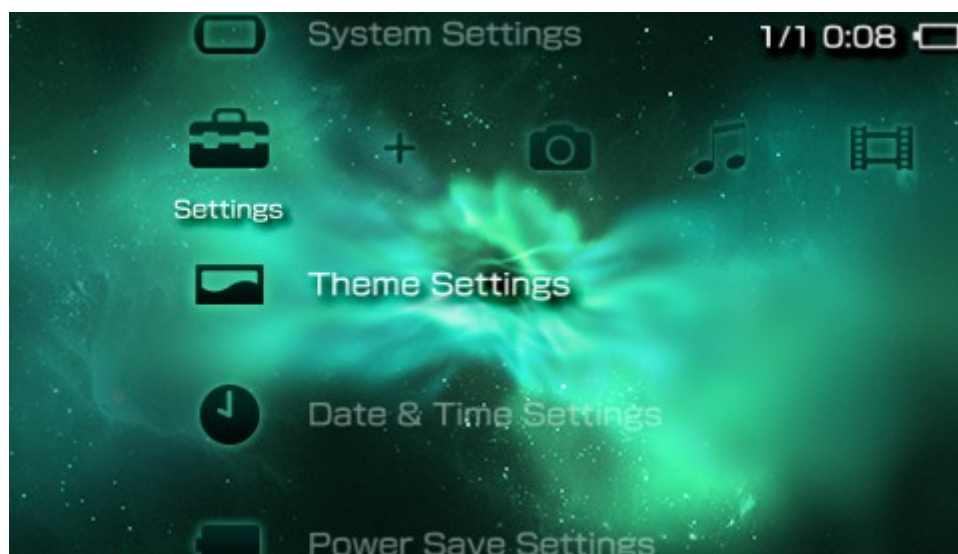
Trzeci w kolejce stoi [Custom Themes Manager](#), który umożliwia zmianę wyglądu menu. Koniec z odrażająco prostackim motywem Vity, a także koniec z kupowaniem niskiej jakości motywów ze sklepu – od teraz można stworzyć swój własny i wrzucić do folderu "custom themes" na karcie pamięci (przykład: "ux0:/customthemes/[Phalaris Nebula v1.2](#)/") lub skorzystać z bogatego i stale powiększającego się [repozytorium](#) (również z poziomu aplikacji).

Do edycji wszystkich ustawień konsoli (np. ręczne uzupełnienie NP Account ID) przydatny może okazać się [RegistryEditor](#).

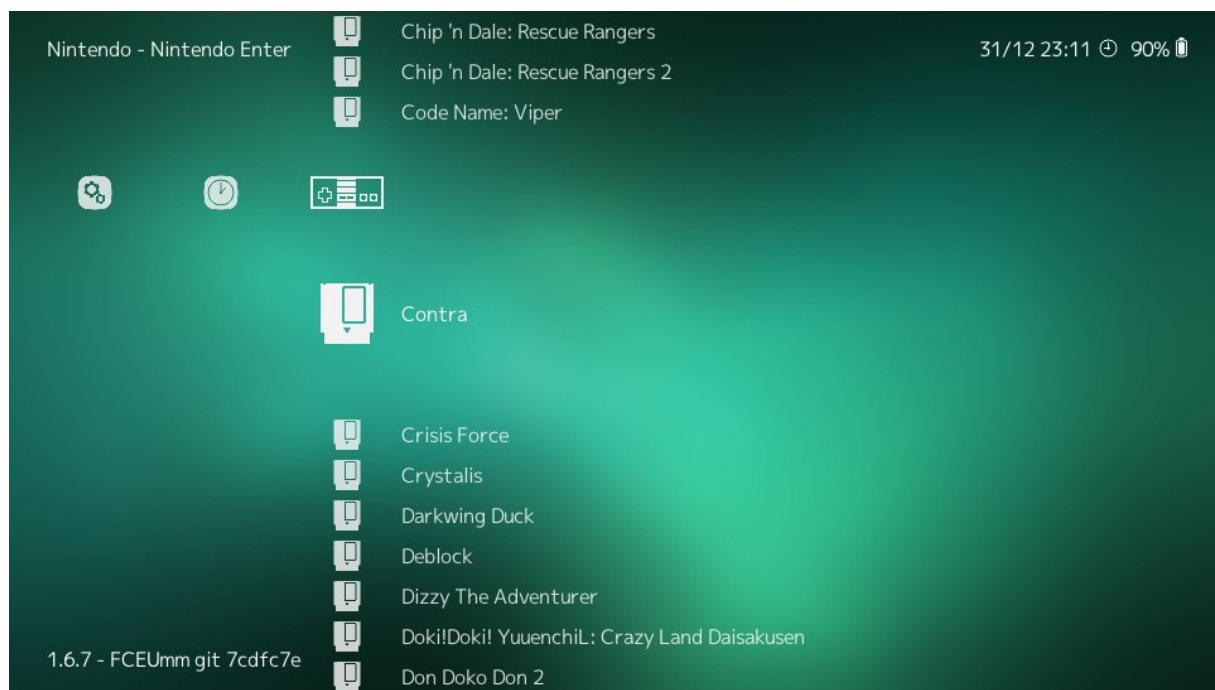
Aby usunąć blokadę uruchamiania większości gier na PlayStation TV, nieoceniony jest [AntiBlacklist](#).

Z typowo gromowych programów liczą się zaledwie trzy. [Virtual GC](#), który pozwala na kopię posektorową i uruchomienie gry z takiego obrazu cartridge'a (niestety obrazy są ogromne i nic nie da się na to poradzić). [MaiDumpTool](#) (jest też nieoficjalna [angielska wersja](#)), który pozwala na kopiowanie i instalację gier tak jak jak dowolną cyfrową ze sklepu (niestety jest inwazyjny i nie wszystkie tytuły działają). [Vita Save Manager](#) – służy archiwizacji i przywracania save'ów w odszyfrowanej formie (dosyć ważne bo na tej konsoli kasując grę, kasują się również save'y...). Także jest inwazyjny i także nie zadziała ze wszystkimi grami (z żadną szyfrowaną i z żadną oryginalną).

Jeśli chodzi o emulację to tutaj są zaledwie dwie aplikacje godne uwagi. [Adrenaline](#), która utylizuje wbudowany emulator PSP, przynosząc w pełni funkcjonalny CFW z tej konsoli, na którym można uruchamiać gry z PSX (\*.pbp), natywne gry dla PSP (z obrazów \*.iso i \*.cso), jego moduły i zwykłe aplikacje. Jest nawet cały XMB, choć nie wszystkie w nim opcje są sprawne (ale to już ograniczenia nałożone przez emulator Sony, wszystkie dotyczą usług sieciowych LAN/WLAN).



[RetroArch](#) to nakładka na mnóstwo różnych emulatorów i portów gier. Jedne działają w miarę ok, inne nie nadają się do komfortowego grania (np. emulator GBA na PSP (gpSP) jest szybszy niż mGBA w RetroArch...). Z moich obserwacji najlepiej radzą sobie „rdzenie” FCEUmm (emulator FC/NES), SNES9x 2005 (emulator SF/SNES; nowsze rwą animację), PicoDrive (emulator MD/Genesis/32X) i o dziwo PCSX-ReARMed (emulator PSX, który czasem jest lepszym wyborem niż POPS w Adrenalinie).



Jest jeszcze kilka samodzielnych emulatorów jak np. [ScummVM](#) i [pFBA](#). Ale żadnego z nich nie używałem. Ponoć emulator komputerów Apple (na procesorach Motoroli 68K, czyli np. System 7), zwany [Basilisk II Vita](#), także jest niczego sobie. Niestety także nie testowałem.

Są i porty gier o otwartym kodzie, darmowych (ewentualnie shareware) i wbrew pozorom wysokiej lub przynajmniej dobrej jakości. Nie jest ich wiele, wręcz garstka, ale zawsze są to dodatkowe godziny dobrej zabawy. I tak jak zawsze, nieśmiertelne: Doom ([Vita Doom](#)), Hexen II ([vitaHexenII](#)), Quake ([vitaQuake](#)), Quake II ([vitaQuakeII](#)), Prince of Persia ([SDL Prince of Persia Vita](#)). To zestaw już można by rzec standardowy na każdą zhakowaną platformę. :) Oprócz nich są też fanowskie Zeldy ([Zelda: Navi's Quest](#), [Zelda: Oni Link Begins](#), [Zelda: Return of The Hylian](#), [Zelda: Time to Triumph](#)), chiński RPG ([The Legend of Sword and Fairy](#)) i japońska metroidvania ([Hydra Castle Labyrinth](#)).



## Programy w postaci modułów SKPRX, SUPRX i PRX

Czyli programy, które ładowane są przy starcie systemu lub które działają tylko w określonych np. grach. Moduły (lub jak kto woli: wtyczki) podzielić można na dwa rodzaje: takie, które działają w przestrzeni użytkownika (\*.suprx) i takie, które są rozszerzeniem kernela (\*.skprx). Po więcej szczegółowych informacji odsyłam do stosownego [poradnika](#). Znajdziesz tam opisy sekcji pod którymi się umieszcza wtyczki, lokalizację plików etc. Włączając w to także te dla PSP (\*.prx), ponieważ Adrenalina wspiera także moduły napisane dla CFW tej konsoli w wersjach 6.60 i 6.61.

```
VitaShell 1.83                                     2015/01/01 00:03
ur0:tai/config.txt

0005  *KERNEL
0006  # ur0:tai/unmount.skprx
0007  # ux0:app/PSPEMUFCW/sce_module/adrenaline_kernel.skprx
0008  # ur0:tai/gamesd_ux0.skprx
0009  # ur0:tai/usbmc.skprx
0010  # ur0:tai/nonpdrm.skprx
0011  # ur0:tai/nopsmdrm.skprx
0012  # ur0:tai/dsmotion.skprx
0013  # ur0:tai/psvgamesd.skprx
0014
0015  *main
0016  ur0:tai/henkaku.suprx
0017  ur0:tai/pngshot.suprx
0018
0019  *NPXS10015
0020  ur0:tai/henkaku.suprx
0021
```

Modułów, które już zostały wpisane do pliku "ur0:/tai/config.txt" podczas instalacji HENkaku nie usuwaj, nie komentuj, ani tym bardziej nie kasuj fizycznie z konsoli. Zaś pliku "boot\_config.txt" nawet nie dotykaj w myślach (zepsuty oznacza **uceglenie konsoli**).

A o to lista subiektywnie przydatnych wtyczek (wszystkich jest oczywiście znacznie więcej), wraz z krótkim opisem do czego służą:

<b>DSMotion</b>	Umożliwia odczyt akcelerometru w DS3 i DS4 jako żyroskopu Vity. Przydatna wtyczka dla posiadaczy PSTV.
<b>FakeCamera</b>	Oszukuje PSTV w grach, które używają kamery.
<b>NoNpDrm</b>	Służy do generowania fałszywych plików licencyjnych dla gier z PSV, w razie utraty konta i/lub dostępu do sieci SEN.
<b>NoPsmDrm</b>	Służy do generowania fałszywych plików licencyjnych dla gier z platformy PlayStation Mobile (już niedostępnych do pobrania).
<b>PNGShot</b>	Umożliwia wykonywanie bezstratnych zrzutów ekranu (w ten sam sposób co oryginalna funkcja systemu).
<b>PSVGameSD</b>	Wymagana do działania opisywanego wcześniej Virtual GC.
<b>Storage Manager</b>	Umożliwia przypisywanie różnych urządzeń do różnych punktów montowania (zastępuje wiele innych wtyczek tego rodzaju jak np. <b>USBMC</b> czy <b>GameCard-MicroSD</b> ).

## Przekuwanie

A może by tak **przekuć** całość w coś nowocześniejszego jak np. firmware **3.65**? Z chwilą kiedy to piszę, nie ma sensu, bowiem choć w nowsze gry niż dla fw 3.60 można by już zagrać, tak **nie ma możliwości ani wgrania Ensō, ani co gorsza sposobu na odratowanie środowiska** w razie sformatowania karty pamięci (PSV) i/lub pamięci wewnętrznej (PSTV) innego niż kopia CMA (a nawet wgrania nowego programu jeśli użytkownik pozbawił się w jakiś sposób sprawnego menedżera plików). Oczywiście **nie można wgrać HENkaku na OFW 3.65**, trzeba to zrobić na 3.60 (właśnie dlatego jest to podróż ryzykowna). Być może w przyszłości znalezione zostaną nowsze exploity (szczególnie na Non Secure Boot Loader), ale na chwilę obecną pozostają same przechwałki o kilku odkrytych entry points na **3.67** (prawdopodobnie znów webkit). Jakby tego było mało, nie wszystkie moduły i programy zostaną przepisane na nowszy fw niż **3.60** dlatego przynajmniej jeszcze przez jakiś czas zalecam na nim pozostać.