USHBY
TECHNOLOGY ONLY

Our affiliates

[Tutorial, Walkthrough] Linux Kodachi 101 - Part1

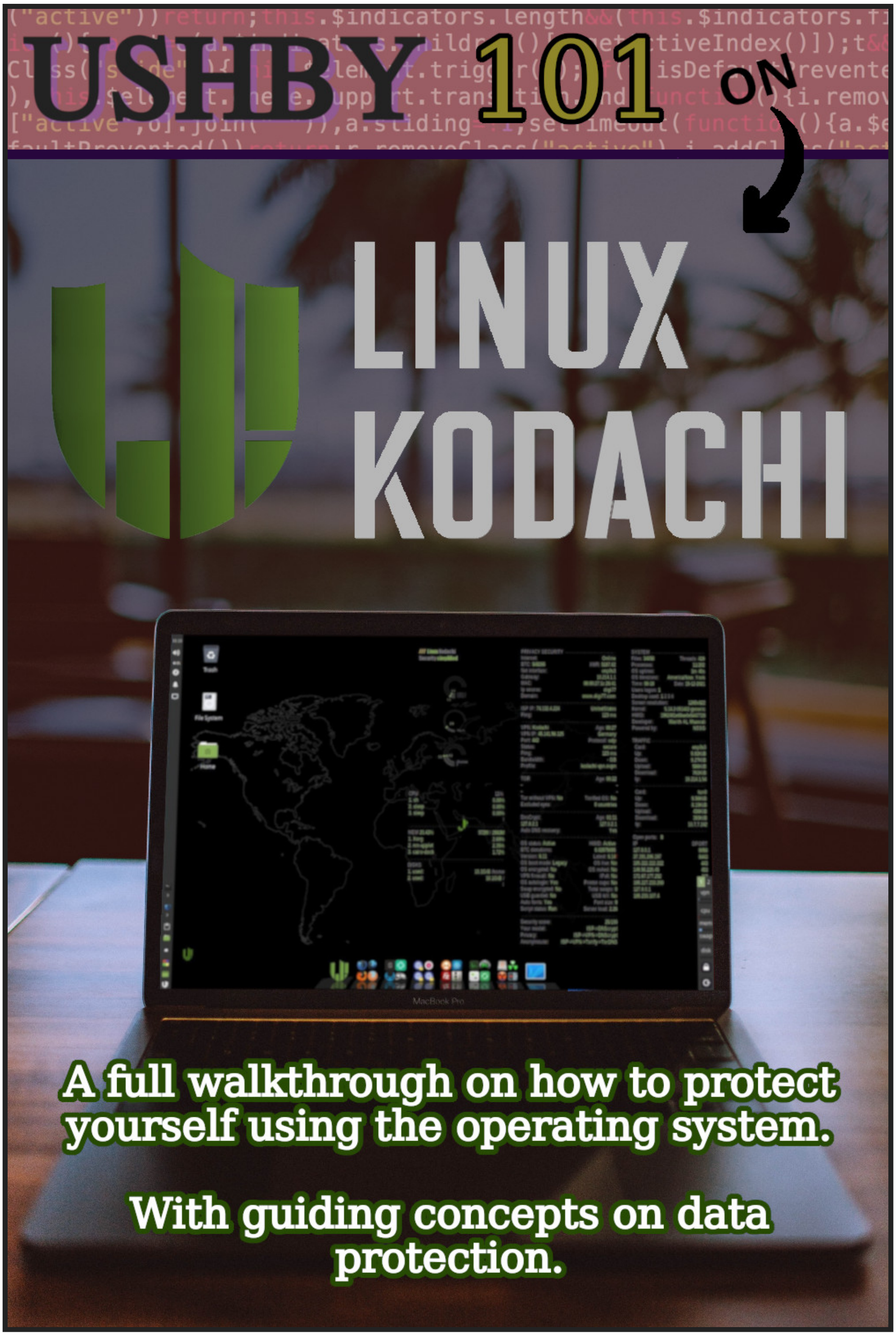
Details

Category: Tutorials

Published: 16 January 2023

Hits: 2674

linux kodachi security cybersecurity security os operating warith al-maawali digi77 privacy anonymity


USHBY 101 ON
LINUX KODACHI
A full walkthrough on how to protect yourself using the operating system.
With guiding concepts on data protection.

Update: Part 2 has just been released ! Click here.

Written by ***Ushby Technical Team***

Published for free by ***Ushby Organization***

Credit goes to ***Warith Al Maawali***, ***DIGI77*** and ***Ushby*** - 2023.

For credits, official details and more info, visit **https://ushby.org** or **https://www.digi77.com**

“By using Kodachi you agree that Kodachi was developed to protect your privacy, if you intend to use it for committing crime or any sort of law violation, then please do stay away from Kodachi [illegible] stop using it immediately, I will take no responsibility of you breaking any country’s laws with this OS.” **Warith Al Maawali**, creator of Kodachi.

Summary

In most cases, if he/she is needy for privacy, secrecy and is worried of being tracked, hacked or compromised .. Then he/she might appreciate what we got here. In addition to the aforementioned needs, Kodachi is a suggesting OS, meaning.. it suggests tools, software and drags you into an already existent world of technology that you might have not heard of. There are tools inside that offer the ability to isolate and transfer files, handle network configurations and run the *GNU/Linux* system more professionally.

“Kodachi is a wide system” **DJ Ware AKA The CyberGizmo**.

Introduction :

Before we give our definition of Kodachi.. let’s be fair to the developer and quote his. According to Warith,

“Linux Kodachi operating system is based on Ubuntu 18.04.6 it will provide you with a secure, anti-forensic, and anonymous operating system considering all features that a person who is concerned about privacy would need to have, in order to be secure.”

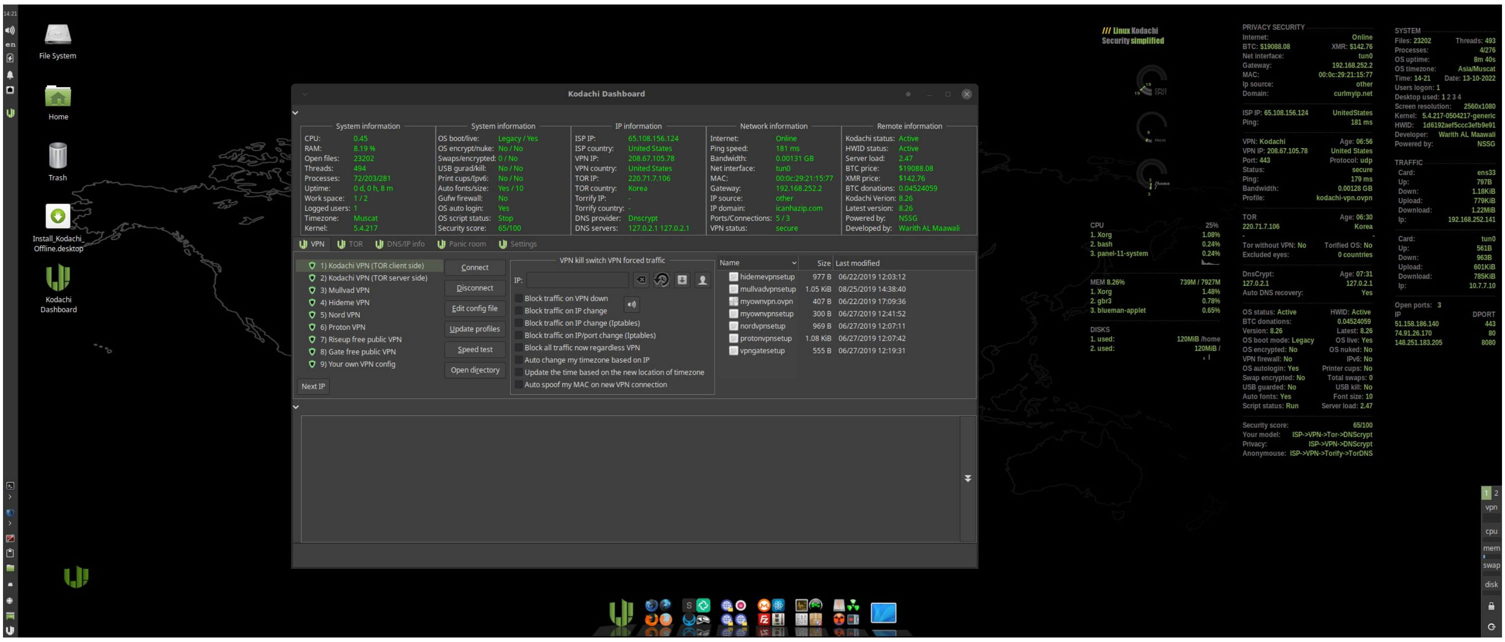
“Kodachi is very easy to use, all you have to do is boot it up on your PC via USB drive, then you should have a fully running operating system with established VPN connection + Tor Connection established + DNScrypt service running. No setup or Linux knowledge is required from your side, it is all been automated for you. The entire OS is functional from your temporary memory RAM, so once you shut it down no trace is left behind, and all your activities are wiped out.”

“Kodachi is a live operating system that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your privacy and anonymity, and helps you to:

- *Use the Internet anonymously.*
- *All connections to the Internet are forced to go through the VPN then Tor network with DNS encryption.*
- *Leave no trace on the computer you are using unless you ask it explicitly.*
- *Use state-of-the-art cryptographic and privacy tools to encrypt your files, emails and instant messaging.”*

“Kodachi is based on the solid Linux Xubuntu/Debian with customized XFCE, this makes Kodachi stable, secure, and unique”.

End of Quote.



```
System information                System information                IP information
CPU:            0.45              OS boot/live:      Legacy / Yes   ISP IP:          65.108.156.124
RAM:            8.19 %            OS encrypt/nuke:   No / No        ISP country:     United States
Open files:     23202             Swaps/encrypted:   0 / No         VPN IP:          208.67.105.78
Threads:        494               USB gurad/kill:    No / No        VPN country:     United States
Processes:      72/203/281        Print cups/Ipv6:   No / No        TOR IP:          220.71.7.106
Uptime:         0 d, 0 h, 8 m     Auto fonts/size:   Yes / 10       TOR country:     Korea
Work space:     1 / 2             Gufw firewall:     No             Torrify IP:      -
Logged users:   1                 OS auto login:     Yes            Torrify country: -
Timezone:       Muscat            OS script status:  Stop           DNS provider:    Dnscrypt
Kernel:         5.4.217           Security score:    65/100         DNS servers:     127.0.2.1 127.0.2.1

Network information                        Remote information
Internet:            Online                Kodachi status:  Active
Ping speed:          181 ms                HWID status:     Active
Bandwidth:           0.00131 GB            Server load:     2.47
Net interface:       tun0                  BTC price:       $19088.08
MAC:                 00:0c:29:21:15:77     XMR price:       $142.76
Gateway:             192.168.252.2         BTC donations:   0.04524059
IP source:           other                 Kodachi Verion:  8.26
IP domain:           icanhazip.com         Latest version:  8.26
Ports/Connections:   5 / 3                 Powered by:      NSSG
VPN status:          secure                Developed by:    Warith AL Maawali
```

```
1) Kodachi VPN (TOR client side)
2) Kodachi VPN (TOR server side)
3) Mullvad VPN
4) Hideme VPN
5) Nord VPN
6) Proton VPN
7) Riseup free public VPN
8) Gate free public VPN
9) Your own VPN config
```

VPN kill switch VPN forced traffic

IP:

- □ Block traffic on VPN down
- □ Block traffic on IP change
- □ Block traffic on IP change (Iptables)
- □ Block traffic on IP/port change (Iptables)
- □ Block all traffic now regardless VPN
- □ Auto change my timezone based on IP
- □ Update the time based on the new location of timezone
- □ Auto spoof my MAC on new VPN connection

Name	Size	Last modified
hidemevpnsetup	977 B	06/22/2019 12:03:12
mullvadvpnsetup	1.05 KiB	08/25/2019 14:38:40
myownvpn.ovpn	407 B	06/22/2019 17:09:36
myownvpnsetup	300 B	06/27/2019 12:41:52
nordvpnsetup	969 B	06/27/2019 12:07:11
protonvpnsetup	1.08 KiB	06/27/2019 12:07:42
vpngatesetup	555 B	06/27/2019 12:19:31

```
CPU                          25%
1. Xorg                    1.08%
2. bash                    0.24%
3. panel-11-system         0.24%

MEM 8.26%          739M / 7927M
1. Xorg                    1.48%
2. gbr3                    0.78%
3. blueman-applet          0.65%

DISKS
1. used:         120MiB /home
2. used:         120MiB /
```

```
PRIVACY SECURITY
Internet:                              Online
BTC: $19088.08               XMR: $142.76
Net interface:                           tun0
Gateway:                        192.168.252.2
MAC:                        00:0c:29:21:15:77
Ip source:                              other
Domain:                           curlmyip.net

ISP IP: 65.108.156.124           UnitedStates
Ping:                                  181 ms

VPN: Kodachi                      Age: 06:56
VPN IP: 208.67.105.78           United States
Port: 443                       Protocol: udp
Status:                                secure
Ping:                                  179 ms
Bandwidth:                         0.00128 GB
Profile:                    kodachi-vpn.ovpn

TOR                               Age: 06:30
220.71.7.106                            Korea
-                                           -
Tor without VPN: No          Torified OS: No
Excluded eyes:                    0 countries

DnsCrypt:                         Age: 07:31
127.0.2.1                           127.0.2.1
Auto DNS recovery:                        Yes

OS status: Active               HWID: Active
BTC donations:                    0.04524059
Version: 8.26                   Latest: 8.26
OS boot mode: Legacy             OS live: Yes
OS encrypted: No                OS nuked: No
VPN firewall: No                    IPv6: No
OS autologin: Yes           Printer cups: No
Swap encrypted: No          Total swaps: 0
USB guarded: No                 USB kill: No
Auto fonts: Yes                Font size: 10
Script status: Run          Server load: 2.47

Security score:                       65/100
Your model:     ISP->VPN->Tor->DNScrypt
Privacy:                 ISP->VPN->DNScrypt
Anonymouse:      ISP->VPN->Torify->TorDNS
```

```
SYSTEM
Files: 23202                  Threads: 493
Processes:                           4/276
OS uptime:                          8m 40s
OS timezone:                   Asia/Muscat
Time: 14-21              Date: 13-10-2022
Users logon: 1
Desktop used: 1 2 3 4
Screen resolution:               2560x1080
Kernel:          5.4.217-0504217-generic
HWID:           1d6192aef5ccc3efb9e91
Developer:               Warith AL Maawali
Powered by:                           NSSG

TRAFFIC
 Card:                               ens33
 Up:                                  797B
 Down:                             1.18KiB
 Upload:                            779KiB
 Download:                         1.22MiB
 Ip:                       192.168.252.141

 Card:                                tun0
 Up:                                  561B
 Down:                                963B
 Upload:                            601KiB
 Download:                          785KiB
 Ip:                            10.7.7.10

Open ports:   3
IP                                   DPORT
51.158.186.140                         443
74.91.26.170                            80
148.251.183.205                       8080
```

Screenshot taken from digi77.com, showing the Kodachi Dashboard.

If I would define Kodachi in my own way, I would say the following:

It is an open source operating system, that can be installed on any computer, all the way from HP laptops, until MacBooks and desktops.

This same system offers secrecy and protection, not only you can hide yourself and what you are doing, but you can protect yourself from being hacked. It can be looked at as the opposite of Kali Linux, Kali allows you to hack and attack, Kodachi will allow you to secure and protect. An entire different approach of work, this system isn’t only for personal issues, but can be for work as well.

There is more to say on the fact that Kodachi is on the other side of things, but I shall continue with my simple definition, and get back to this, later in the book.

This operating system can be the usual one for any person, it has all the office editors, video editors, ftp clients and can install any usual program such as Viber, Thunderbird etc.

Although, it can go from 0 to 100 quickly in terms of security, if you run across a website that you suspect as a source of spyware or hacking. You can open it still, by using one of the Kodachi browsers. Even if this website turns out to be malicious.. you are still on the safe side with a very few concerns.

Running a business, carrying databases, passwords and connecting online regularly, requires a lot of attention not just on the network but in all aspects of a computer. Hackers and thieves will always use that time, the time where you couldn’t make things perfect and left a few precautions, maybe because you forgot or maybe because you couldn’t do them right. With that being said, Kodachi will cover your inabilities, you’ll have an extra friend, that has extra tools.

If you are somewhere, where internet companies, your landlord or even your parents are monitoring your activity, you can manipulate a few settings here and there, use certain connections, and you’ll be the only one who knows what you’re doing. It won’t be just a guess, but it’ll be shown with readings on the desktop, as to why there is nothing to worry about.

If you feel your data is exposed and can’t trust yourself so much. You’ll be introduced to encryption tools that will give you the confidence.

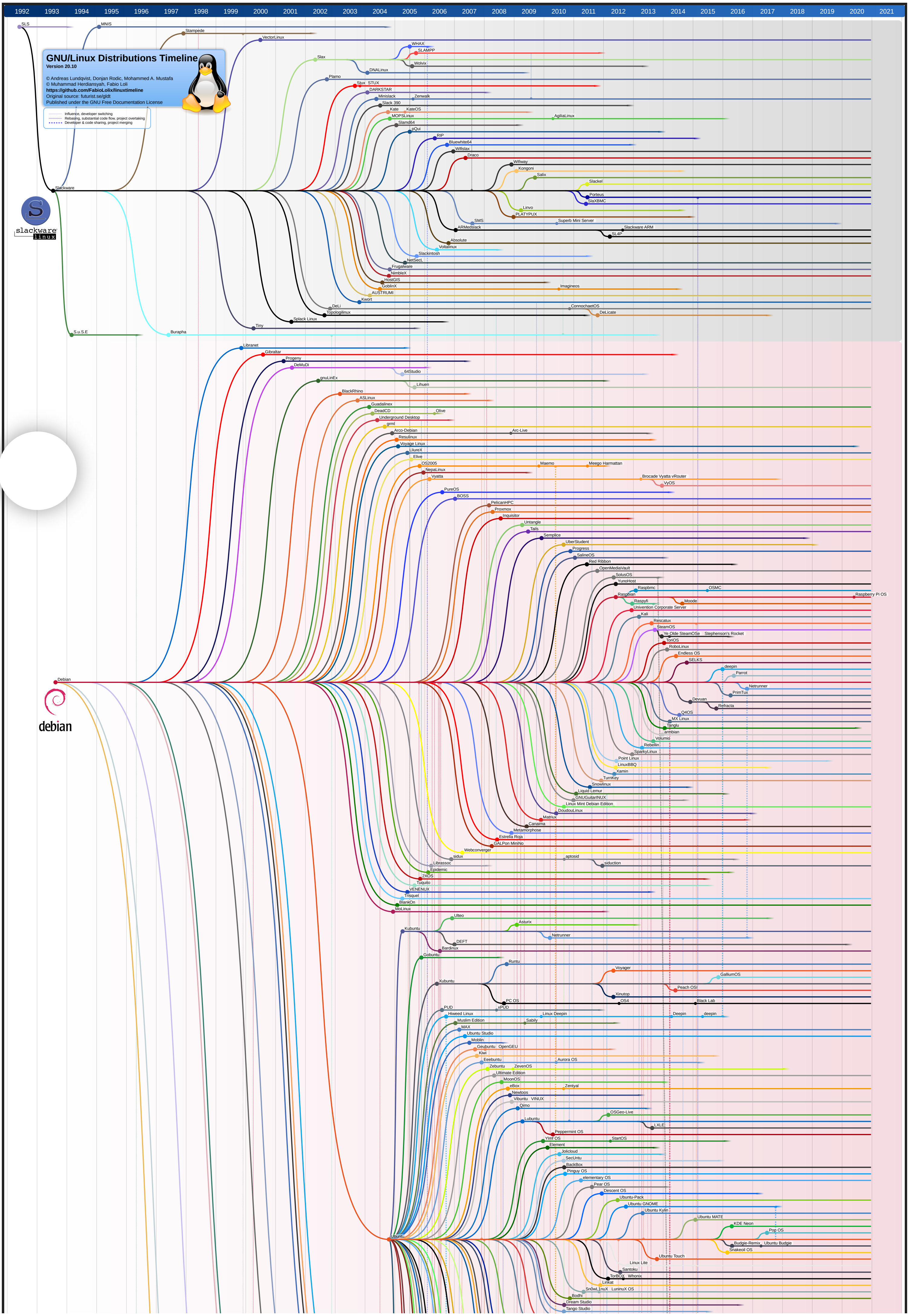
These are just small examples, I refrained from mentioning any terminology, to not scare you, and to give you the summary of what this operating system can do. Of course, there is so much going on and so much else you can do.

How does it work ?

Kodachi works as a *GNU/Linux* distribution. *GNU/Linux* is an operating system for the computer, similar to Microsoft Windows. But the former is an Open Source. It is built more freely, more securely, allows for development and can take up any addition from either the user or the developer. Windows on the other hand is a compiled system, doesn’t allow for development except by the company itself, designed for specific usage and very proprietary to say the least.

The term ***distribution*** is said because *GNU/Linux* depends on the fact that it always changes, it has no restrictions neither by the law nor by the code, to stop it from changing or developing into anything else. So anyone can take *GNU/Linux*, modify it and release it. Therefore *GNU/Linux* system is distributing all these different OS’s by allowing people to do so.

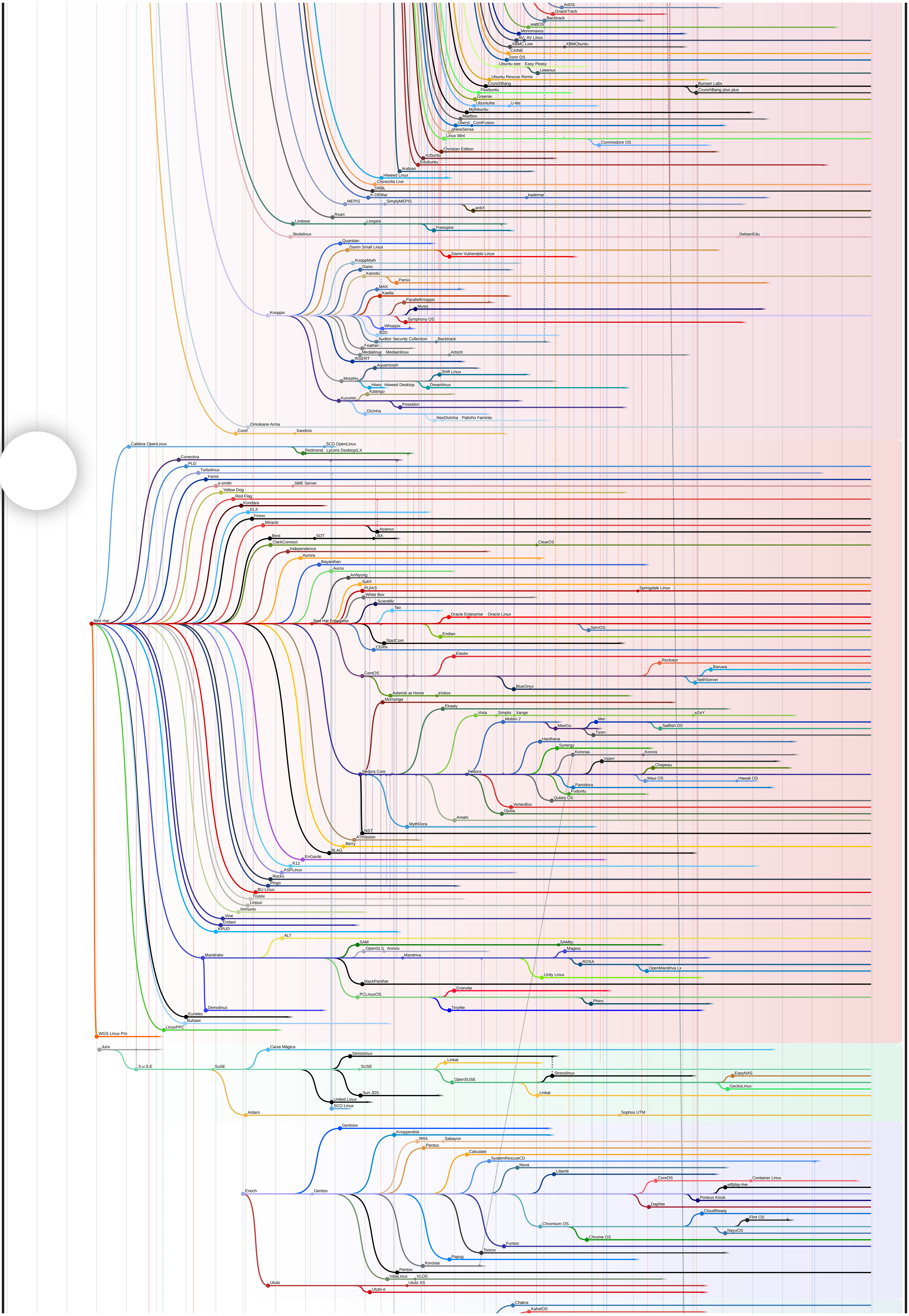
Kodachi is built on top of a *GNU/Linux* distribution called Ubuntu. But when you predict a future for Kodachi, it is definitely becoming its own distribution. It is right now on a fine line between both, but to understand it simply, you can look at as a *GNU/Linux* distro.

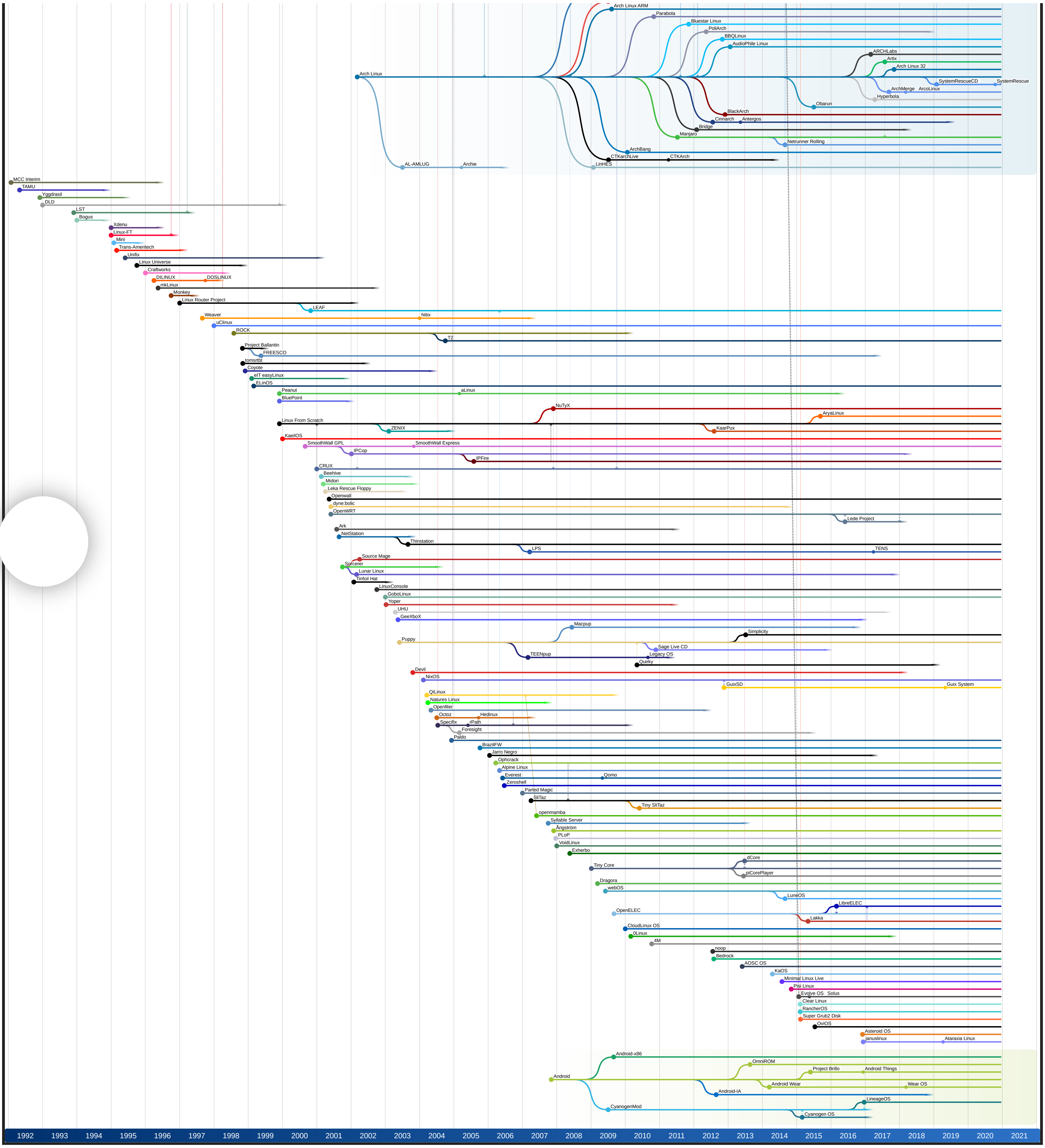


GNU/Linux Distributions Timeline

Version 20.10

© Andreas Lundqvist, Donjan Rodic, Mohammed A. Mustafa
© Muhammad Herdiansyah, Fabio Loli
https://github.com/FabioLolix/linuxtimeline
Original source: futurist.se/gldt
Published under the GNU Free Documentation License

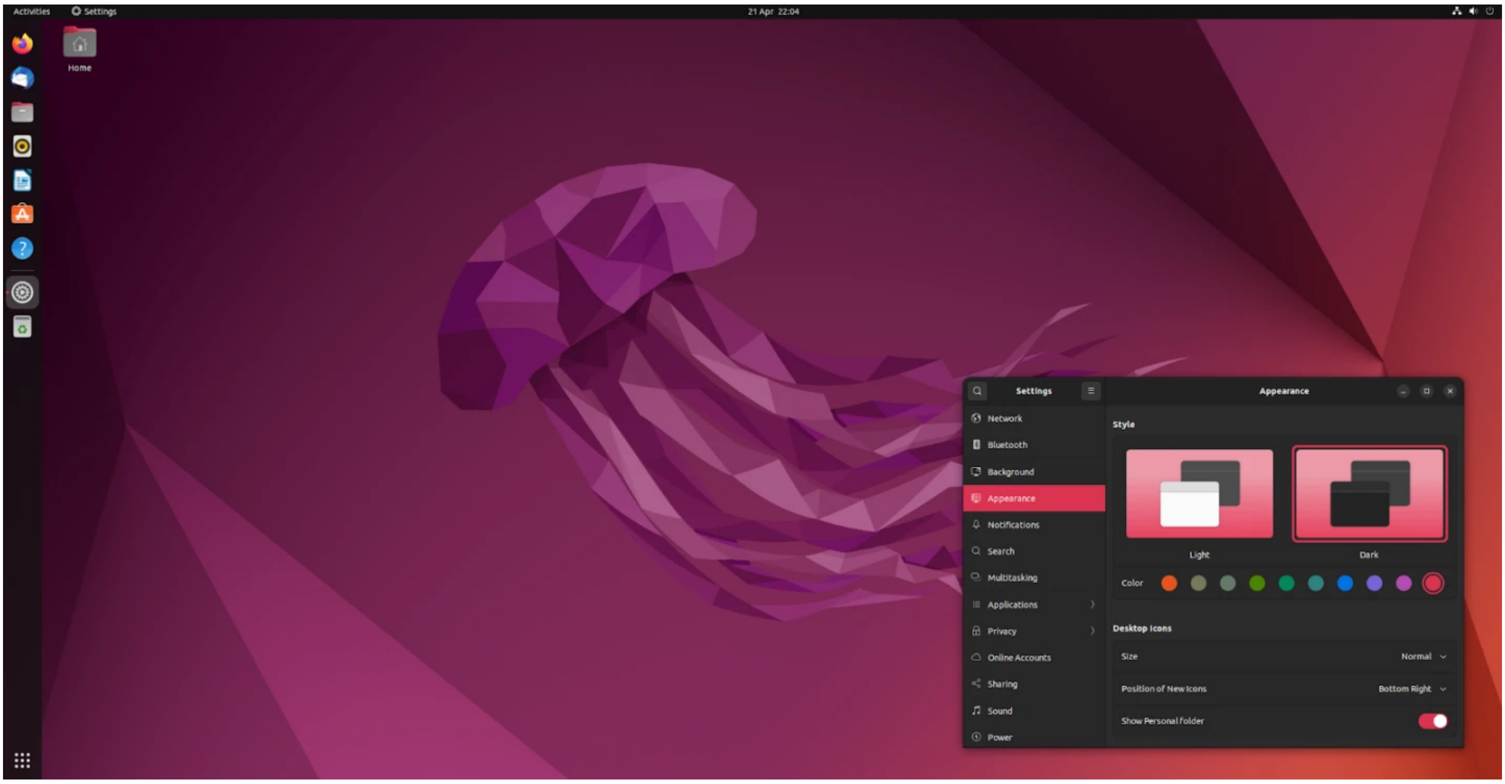

AriOS
GnackTrack
Backtrack
wattOS
Monomaxos
AV AV Linux
XBMC Live
XBMCbuntu
CAINE
Zorin OS
Ubuntu eee
Easy Peasy
Leeenux
Ubuntu Rescue Remix
CrunchBang
Bunsen Labs
CrunchBang plus plus
Fluxbuntu
Greenie
Ubuntulite
U-lite
Mythbuntu
Madbox
Uberyl
ComFusion
gNewSense
Linux Mint
Commodore OS
Christian Edition
nUbuntu
Edubuntu
Arabian
Hiweed Linux
Clonezilla Live
DRBL
K-DEMar
kademar
MEPIS
SimplyMEPIS
antiX
Rxart
Lindows
Linspire
Freespire
Skolelinux
DebianEdu
Quantian
Damn Small Linux
Damn Vulnerable Linux
KnoppMyth
Danix
Kanotix
Parsix
MAX
Kaella
ParallelKnoppix
Musix
Knoppix
Symphony OS
Whoppix
B2D
Auditor Security Collection
Backtrack
Feather
Medialinux
Mediainlinux
ArtistX
INSERT
Aquamorph
Shift Linux
Morphix
Hiwix
Hiweed Desktop
Dreamlinux
Kalango
Kurumin
Poseidon
Dizinha
NeoDizinha
Patinho Faminto
Omoikane Arma
Corel
Xandros
Caldera OpenLinux
SCO OpenLinux
Redmond
Lycoris Desktop/LX
Conectiva
PLD
Turbolinux
Fermi
e-smith
SME Server
Yellow Dog
Red Flag
Kondara
ELX
Finnix
Miracle
Asianux
Best
SOT
LBA
ClarkConnect
ClearOS
Independence
Aurora
Bayanihan
Aurox
AnNyung
SuliX
PUIAS
Springdale Linux
White Box
Scientific
Tao
Oracle Enterprise
Oracle Linux
Red Hat
Red Hat Enterprise
ServOS
Endian
StartCom
CERN
Elastix
Rockstor
Baruwa
CentOS
NethServer
BlueOnyx
Asterisk at Home
trixbox
Momonga
Ekaaty
Vixta
Simplis
Xange
eZeY
Moblin 2
Mer
MeeGo
Sailfish OS
Tizen
Hanthana
Synergy
Kororaa
Korora
Viperr
Chapeau
Fedora Core
Fedora
Maui OS
Hawaii OS
Parsidora
Fuduntu
Qubes OS
VortexBox
Ojuba
Amahi
MythDora
NST
ATmission
Berry
BLAG
EnGarde
K12
ASPLinux
Rocks
Pingo
BU Linux
Trustix
Linpus
Immunix
Vine
Eridani
KRUD
ALT
SAM
SAMity
OpenSLS
Annvix
Mageia
Mandrake
Mandriva
ROSA
OpenMandriva Lx
Unity Linux
blackPanther
Granular
PCLinuxOS
Phinx
Demolinux
TinyMe
Eurielec
Buhawi
LinuxPPC
WGS Linux Pro
Jurix
Caixa Mágica
Stresslinux
S.u.S.E
SuSE
SUSE
Linkat
OpenSUSE
Stresslinux
EasyNAS
GeckoLinux
Sun JDS
Linkat
United Linux
SCO Linux
Astaro
Sophos UTM
Gentoox
Knopperdisk
RR4
Sabayon
Pardus
Calculate
SystemRescueCD
Nova
Liberté
CoreOS
Container Linux
wtfplay-live
Enoch
Gentoo
Porteus Kiosk
Daphile
CloudReady
Flint OS
Chromium OS
NayuOS
Chrome OS
Funtoo
Toorox
Papug
Kororaa
Pentoo
VidaLinux
VLOS
Ututo
Ututo XS
Ututo-e
Chakra
KahelOS



Timeline of the development of main Linux distributions by FabioLolix - CC BY-SA 3.0

You can install Ubuntu on its own, from Ubuntu website that runs under Canonical company. It is in fact safe, pretty safer than windows, very few would argue that. But it isn’t built for the level of security that Kodachi has, that is because first, security requires resources, but at the same time takes off convenience. If Ubuntu will go for extreme security, it will have so many restrictions and no one will be interested to use it.

So does that mean Kodachi is inconvenient and loses usability ? No. That's what the whole idea of Kodachi seems to be about, is how to change quickly between a normal convenient Ubuntu and, turn into a secure system all of a sudden. It is like an airplane, it has a configuration for each phase, when the plane takes off, it sets up an aerodynamic shape for taking off but then readjusts to cruise mode during normal flight. This similar changeability in Kodachi is not only during daily use, but you can carry it on a USB device and boot it up live, this way you have a very forensic approach and become completely anonymouse.



Size Normal

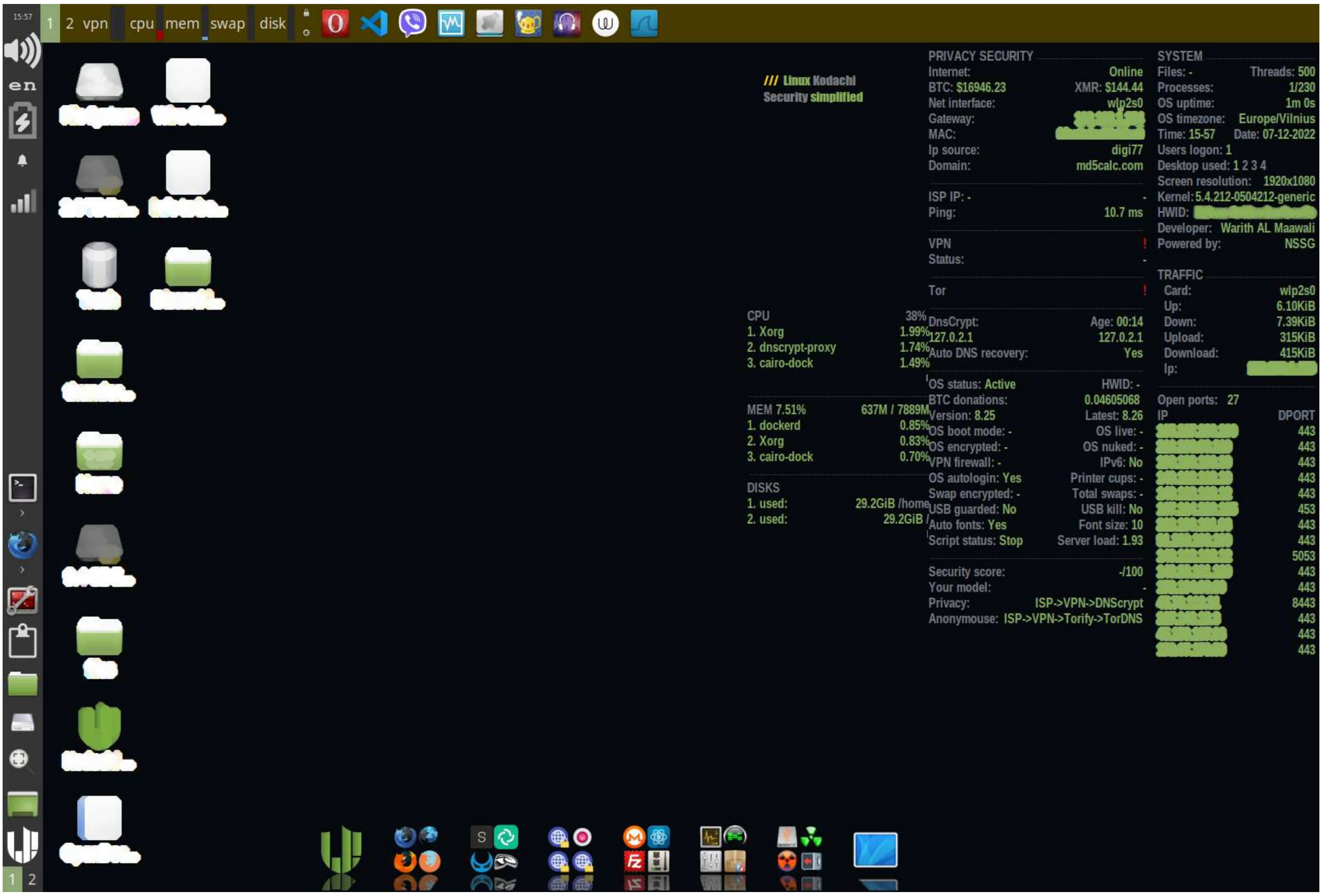
Position of New Icons Bottom Right

Show Personal Folder

A screenshot of a clean Ubuntu 22.04 install, showing the desktop.

There has been many *GNU/Linux* distributions designed for various reasons, such as ***Kali*** for Pen Testing, ***PuppyOS*** and ***Peppermint*** for old and lightweight hardware, etc. Of course, these distributions have started somewhere and got built on top of each other under different sequence, timeline and sometimes even licensing.

ktop Workspace



```
/// Linux Kodachi
Security simplified

PRIVACY SECURITY
Internet:                         Online
BTC: $16946.23            XMR: $144.44
Net interface:                    wlp2s0
Gateway:                      [redacted]
MAC:                          [redacted]
Ip source:                        digi77
Domain:                      md5calc.com

ISP IP: -                              -
Ping:                            10.7 ms

VPN                                    !
Status:                                -

Tor                                    !

CPU                       38%
1. Xorg                 1.99%
2. dnscrypt-proxy       1.74%
3. cairo-dock           1.49%

MEM 7.51%       637M / 7889M
1. dockerd              0.85%
2. Xorg                 0.83%
3. cairo-dock           0.70%

DISKS
1. used:        29.2GiB /home
2. used:            29.2GiB /

DnsCrypt:                 Age: 00:14
127.0.2.1                  127.0.2.1
Auto DNS recovery:               Yes

OS status: Active           HWID: -
BTC donations:            0.04605068
Version: 8.25           Latest: 8.26
OS boot mode: -           OS live: -
OS encrypted: -          OS nuked: -
VPN firewall: -            IPv6: No
OS autologin: Yes    Printer cups: -
Swap encrypted: -    Total swaps: -
USB guarded: No         USB kill: No
Auto fonts: Yes        Font size: 10
Script status: Stop Server load: 1.93

Security score:                 -/100
Your model:                         -
Privacy:          ISP->VPN->DNScrypt
Anonymouse: ISP->VPN->Torify->TorDNS

SYSTEM
Files: -                 Threads: 500
Processes:                      1/230
OS uptime:                      1m 0s
OS timezone:          Europe/Vilnius
Time: 15-57         Date: 07-12-2022
Users logon: 1
Desktop used: 1 2 3 4
Screen resolution:         1920x1080
Kernel: 5.4.212-0504212-generic
HWID: [redacted]
Developer:        Warith AL Maawali
Powered by:                     NSSG

TRAFFIC
  Card:                       wlp2s0
  Up:                        6.10KiB
  Down:                      7.39KiB
  Upload:                     315KiB
  Download:                   415KiB
  Ip:                     [redacted]

Open ports:   27
IP                             DPORT
[redacted]                       443
[redacted]                       443
[redacted]                       443
[redacted]                       443
[redacted]                       443
[redacted]                       453
[redacted]                       443
[redacted]                       443
[redacted]                      5053
[redacted]                       443
[redacted]                       443
[redacted]                      8443
[redacted]                       443
[redacted]                       443
[redacted]                       443
```

Kodachi Desktop which is shown.. Has:

1. The Indication Screen.
2. The Docker; the bottom launcher.
3. XFCE; which is all the rest of the desktop environment

See the table[1-1] below to know what these three components include..

Component	Details		
The Indication Screen	System	Processes	The processes/tasks running on the computer.
		OS uptime	The time from which the computer has last started.
		OS timezone	The timezone of the operating system. This shall not be confused of other timezones in our security practices, some other timezones are only for distraction and specific to browsers and apps.
		Desktops Used	Number of desktop spaces. Different than Windows, GNU/Linux systems allow you to use more than one desktop to help with the user’s perspective.
		Resolution	Number of pixels on your screen, in width and height. There are more than one set of resolutions, they can determine clarity, and fitness for your actual computer screen.
		Kernel	Kernel is the Linux part this operating system. It is the underground level, the system that runs the system. It is closer to the hardware.
		HWID	Hardware ID : Very critical information.. This is a very identifying number, not easy to change permanently and very compromising to physical security if people obtain it. It also gets logged when you deal with connected devices.
		Developer Info	About the Kodachi OS founder : Warith Al Mawaali.
	Traffic	Network Card	The first and major identifier in your network device.
		Upload	Rate and amount of data sent.
		Download	Rate and amount of data received.
		Internet Protocol(ip)	The computer address inside the network. If you are connected to your school wifi, the owner of the wifi will see you and refer to you with this number. Other IP’s can look the same but are different, the one inside this Traffic table denotes to this.
		Open Ports	Ports which are being opened and used in

			your computer. Every internet or network activity, has a specific categorization, for the purpose of separating securing. Also for designation. Therefore computers use the network through specific ports accordingly.
	Privacy Security	Bitcoin & Monero	Because Kodachi is used for securing electronic wallets and handling of Bitcoin and Monero.. the current price is always updated and then indicated.
		Network Interface	The network method that you are using now. For example, Wifi, Ethernet(LAN) or USB When your indication starts with ***wlp*** or ***wno,*** that means it is wifi. If it starts with ***eno,*** that's ethernet, while usb is indicated as ***usb(0)***
		Connection Gateway	Gateway is the address of your router, usually a wifi device.
		MAC address	The address which is unique, so that if your IP changes, site administrators and authorities, can define you with that one. There are other uses for it, but to us.. this is what matters.
		Source of your IP	Kodachi offers the ability to change even your local ip, in case of breach and internal inspection by outsider. That is to be more secure in the worst circumstances. This table shows you the source of where this ip is being generated. This is not your VPN or TOR end point. This is rather the local one and the one that represents the internet service provider.
		Ping Speed	Speed of internet when sample data is sent.
		VPN Status	The status of the current VPN you are using, we'll get into this more later in the book.
		Tor Status	The status and the type of the current TOR that you are using, we'll get into this more later in the book.
		DNS Encryption	Encryption of the Domain Name Server, an address that usually describes your network path to the public, not so much, but it can be compromising to the ones who know. Encrypting that will debilitate people from tracing you.
		Security Score	Security score is a scale measurement calculated by Kodachi, to assume how secure are you from 0 to 100, being on 50 alone is very secure compared to normal computers which scale about 10 at most, when compared to this measurement. With simple methods on Kodachi you can reach 85 easily and be very secure.
The Docker	It categorizes tools, apps and contains the main link to Kodachi Dashboard.		

Kodachi dashboard	Kodachi dashboard will have its own sections and pages in this book, but it is the control panel of all Kodachi. From it, you can connect and configure your VPN, TOR, repair and modify your network, observe the current insecurity information and set security measures and even system features as you want.
Browsers	The various browser developed by Kodachi. As follow : • Kodachi Lite browser : for casual secure browsing ◦ It surfs using VPN, when VPN connection is established beforehand. It doesn't surf through Tor. However, the only time when it does surf through Tor, is when the entire system is torified. System Torification is a feature in Kodachi. ◦ The lite browser has extension installed and set, they provide more privacy and security, they are: ▪ **Disable WebRTC** ▪ **IP Location Lookup** ▪ **MYKI Password Manager & Authenticator** ▪ **Proxy SwitchyOmega** ▪ **uBlock Origin** ◦ The lite browser also rasters every time you close it, nothing is saved, no cache memory, no history, no data. • Kodachi Loaded Tor is quite slower, it surfs the Tor capability when Tor is connected. It has some and sometimes all the Lite browser's extension but with more others, they are: ▪ **AdNauseam** ▪ **Bloody Vikings!** ▪ **Buster: Captcha Solver for Humans** ▪ **Cookie AutoDelete** ▪ **CSS Exfil Protection** ▪ **Decentraleyes** ▪ **Disable WebRTC** ▪ **Firefox Multi-Account Containers** ▪ **Font Fingerprint Defender** ▪ **GNU libreJS** ▪ **HTTPS Everywhere** ▪ **IP Location Lookup** ▪ **MYKI Password Manager & Authenticator** ▪ **PeerName: Surf blockchain-Based Domains** ▪ **Private Bookmarks** ▪ **Proxy SwitchyOmega** ▪ **Random User-Agent** ▪ **Searchonymous** ▪ **Searchonymous2** ▪ **Trace – Online Tracking Protection** ▪ **uBlock Origin** ▪ **User-Agent Switcher** ▪ **webGL Fingerprint Defender**

	- WebGL Fingerprint Defender • Kodachi Browser Ghacks. It is similar to the loaded one but has the Ghacks plugin, more security. Configurable. • Kodachi Browser – Proxychains. It torifies everything. Configurable. • Tor Browser & Sphere Tor Browser Tor Browsers that are regardless to Kodachi Tor System.	
Seucrity Apps	• Session manager • Element • Demonsaw • Tox • Pidgin Internet • CoyIM • OnionShare • TOR Circiutes • VeraCrypt • ZuluCrypt • zuluMount • siriKali • MAT • ExifCleaner • Steghide-HUI • KeePassXC • GPA • Firetools • OpenSnitch • CUFW • Stacer • BleachBit • BleachBit (as root)	This set of tool is mentioned and somehow described, in the other articles or papers in Ushby Cassiopeia
Security Services	• Syncthing, data sharing technology based on Peer-to-peer method. It allows you to send files immediately, under a safe route, not only encrypted in information but also encrypted in principle. • **Gnu Net**, a similar to Syncthing as far as a basic usage is concerned. • **i2p**,a technology of anonymity just as Tor, for those that can't implement Tor, i2p might do it for them. It's the old PGP method of securing. • **Noisy Crawlers**, creates a load of traffic that causes distraction, when one is private and anonymous.. using this will distract any entity or network that is monitoring you. This helps everyone from not paying attention to the site you are working on. • **SSH**, a port, these settings will allow to open and close it immediately, simple Kodachi users aren't required to know about it, they are secure without touching it.	
System Apps	This set of tool is mentioned and somehow described, in the other articles or papers in Ushby Cassiopeia	
Other Apps	This set of tool is mentioned and somehow described, in the other articles or papers in Ushby Cassiopeia	
Extra	• Storage Tools	This set of tool is

	Extra Tools	• Storage Tools. • System Nuke. • Disable System. • Safe box encryption. • Panic Repair.	This set of tool is mentioned and somehow described, in the other articles or papers in Ushby Cassiopeia
XFCE	Panel 0	• Hardware button ◦ Audio ◦ Wifi ◦ Notification ◦ Time ◦ Battery/Power • Network Repair Button • Browser Quicklink • Clipboard history • Disks • System and OS menu	
	Panel 1	• Indicators ◦ CPU usage ◦ RAM usage ◦ Disk usage • Workspace Switcher	

Kodachi Dashboard

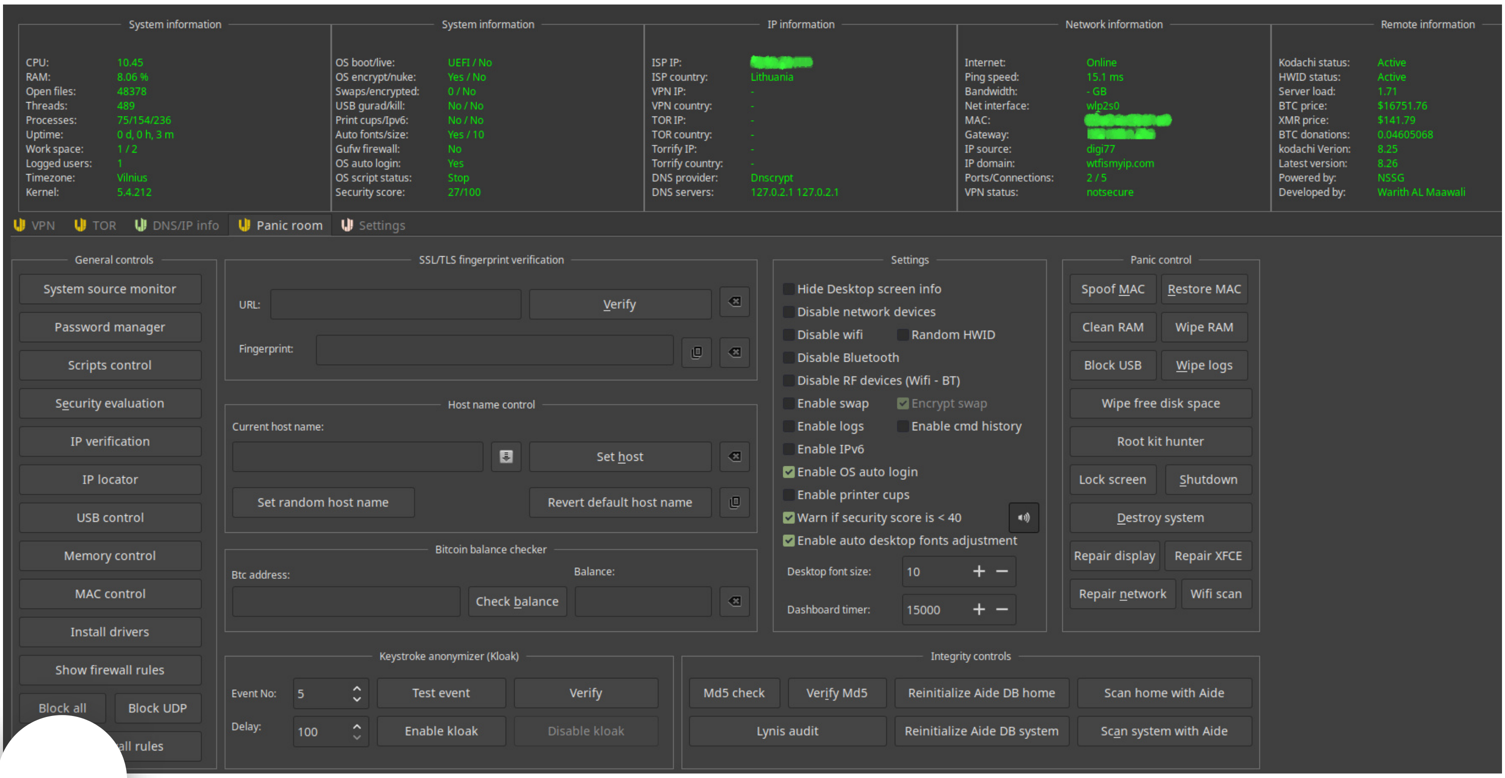
Kodachi Dashboard is where it all gets down to, the commands and shell scripts that run the features of this operating system are convoluted. They are dynamic, conditional and sophisticated. The dashboard is the graphical user interface and final control panel of all those scripts and codes that run the system.

It consists of five tabs, ***VPN, Tor, DnsCrypt, Panic Room and Settings***. You wouldn’t wanna go through them all for each use, depending on your needs and plan of work, you will go around and prepare yourself for takeoff.

It makes things faster, security always takes off usability and time. It requires repeated steps and revision. Here though, it is not. At the same time we are not talking about simple security precautions, this is the user’s safety. If things go south and the user gets compromised, loses can be pricey. So it might be questioned "why all this is being appreciated when it exists in lesser tactics at other OS’s ?", The answer is.. First, they don’t, second it’s so much security here. So to see that level of it being established fast ad accurate will allow you to jump from a casual Xubuntu use to extreme security.

The tabs start with ***VPN***, but I have decided to start with the ***Panic Room***, because it helps one understand, why all the security is needed in the first place, or in other words, how much security is there to begin with.

- **The Panic Room**



System information

CPU: 10.45
RAM: 8.06 %
Open files: 48378
Threads: 489
Processes: 75/154/236
Uptime: 0 d, 0 h, 3 m
Work space: 1 / 2
Logged users: 1
Timezone: Vilnius
Kernel: 5.4.212

System information

OS boot/live: UEFI / No
OS encrypt/nuke: Yes / No
Swaps/encrypted: 0 / No
USB gurad/kill: No / No
Print cups/Ipv6: No / No
Auto fonts/size: Yes / 10
Gufw firewall: No
OS auto login: Yes
OS script status: Stop
Security score: 27/100

IP information

ISP IP: [redacted]
ISP country: Lithuania
VPN IP: -
VPN country: -
TOR IP: -
TOR country: -
Torrify IP: -
Torrify country: -
DNS provider: Dnscrypt
DNS servers: 127.0.2.1 127.0.2.1

Network information

Internet: Online
Ping speed: 15.1 ms
Bandwidth: - GB
Net interface: wlp2s0
MAC: [redacted]
Gateway: [redacted]
IP source: digi77
IP domain: wtfismyip.com
Ports/Connections: 2 / 5
VPN status: notsecure

Remote information

Kodachi status: Active
HWID status: Active
Server load: 1.71
BTC price: $16751.76
XMR price: $141.79
BTC donations: 0.04605068
kodachi Verion: 8.25
Latest version: 8.26
Powered by: NSSG
Developed by: Warith AL Maawali

Event No: 5
Delay: 100

Settings

☐ Hide Desktop screen info
☐ Disable network devices
☐ Disable wifi ☐ Random HWID
☐ Disable Bluetooth
☐ Disable RF devices (Wifi - BT)
☐ Enable swap ☑ Encrypt swap
☐ Enable logs ☐ Enable cmd history
☐ Enable IPv6
☑ Enable OS auto login
☐ Enable printer cups
☑ Warn if security score is < 40
☑ Enable auto desktop fonts adjustment
Desktop font size: 10
Dashboard timer: 15000

To remove confusion out of the way, we should say that the *System Information* above are unified across all the tabs. So, as we switch from one tab to another, they aren’t changing. They are still shown because they are a crucial part of the Dashboard’s monitoring capabilities.

It is called the *Panic Room* because here is where you go, when you suspect something is wrong or when you want to be more careful and isolative. The panels are split into five as the example shows. Some of these panels and settings take time for a user to need them or to know that they are needed. Some here are essential while others are non-essential, but they can be a paranoid user’s casual back and forth.

The *Panic Control* section which is at the upper right, has two MAC features, with one click you can obtain and show a fake MAC address, to your local network and to whoever traces you back this much. Anytime you want to unveil, you can click the button next to it; Restore MAC. Not only helps with secrecy but it can be handy when the network router or other administrators ban you from using the WiFi, with spoofing the MAC you can regain access to the internet. Some routers and administrators [illegible] users from WiFi either manually or automatically, when major changes happen in your device, due to increased bandwidth or something similar.

RAM memory is used simultaneously between programs, if you happen to use two programs that one has an outer accessibility and, you felt that the third party can access the data, a one click cleaning of RAM gets rid of the concerns. This also helps fasten your OS, reduce fan speed and stop the computer RAM from freezing, as some temporary files do remain sometimes.

According to *Stackify*, **“Linux logs provide a timeline of events for the Linux operating system, applications and system and are a valuable troubleshooting tool when you encounter issues. When issues arise, analyzing log files is the first thing an administrator needs to do”**.

Issues arising can leave all traces behind if someone else uses the computer behind us, that’s why the Panic Room has ability to clean all of them. As it’s shown in the screenshot.

Deleted files remain, they can be restored, the only way to guarantee they are gone is to overwrite them with other data that is useless, deleting disk option does that, it might take some time if you get a Terabyte or so, but the option is always there for you.

Some options in the panic panel and some others are self explanatory, we shall get back to them in *Part 2,* when implementations start taking place. But let’s highlight the following:

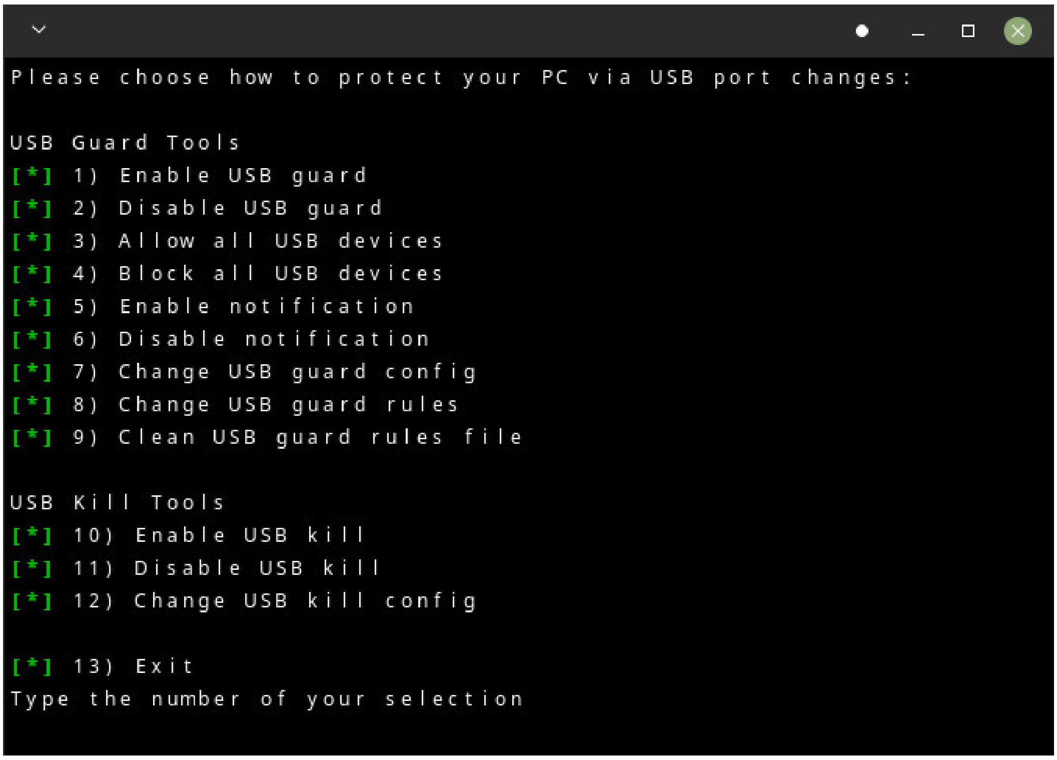
- **Swap Enabling**

Swap memory is RAM memory that is still needed but not as much as the other, so it gets transferred to SWAP to help optimize for speed and usage. You can look at it as a secondary RAM or RAM’s assistant. Enabling it is an option that exists eveyrwhere in Linux, but with Kodachi you have the opportunity to encrypt that as well, this way nothing gets out.

- **Random HWID**

Hardware ID is very compromising and make it harder for you to hide your self if someone finds out. You will have to constantly change it just to prove you weren’t somewhere else before. This option helps you to always use a fake one just incase someone was too good of a tracker and went that far.

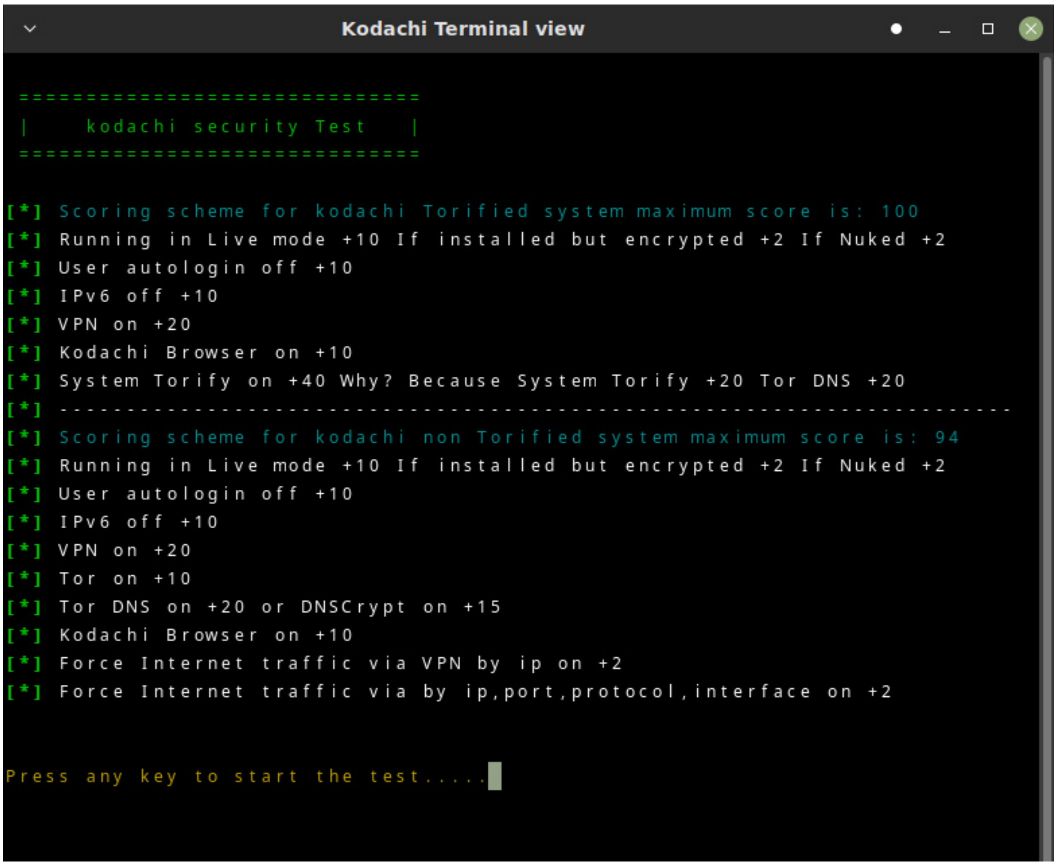
- **USB control**



```
Please choose how to protect your PC via USB port changes:

USB Guard Tools
[*] 1) Enable USB guard
[*] 2) Disable USB guard
[*] 3) Allow all USB devices
[*] 4) Block all USB devices
[*] 5) Enable notification
[*] 6) Disable notification
[*] 7) Change USB guard config
[*] 8) Change USB guard rules
[*] 9) Clean USB guard rules file

USB Kill Tools
[*] 10) Enable USB kill
[*] 11) Disable USB kill
[*] 12) Change USB kill config

[*] 13) Exit
Type the number of your selection
```

The USB tool list, speaks directly to the *kernel* through *systemd*. From the terminal tool list, you can achieve any of the displayed options.

- **Security Evaluation**

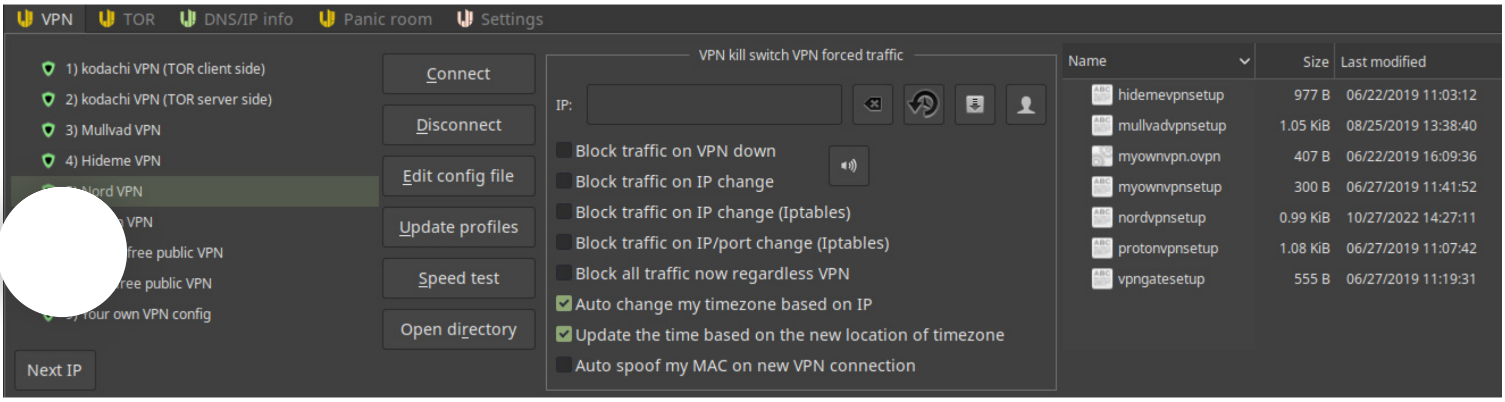


```
 ==============================
 |    kodachi security Test    |
 ==============================

[*] Scoring scheme for kodachi Torified system maximum score is: 100
[*] Running in Live mode +10 If installed but encrypted +2 If Nuked +2
[*] User autologin off +10
[*] IPv6 off +10
[*] VPN on +20
[*] Kodachi Browser on +10
[*] System Torify on +40 Why? Because System Torify +20 Tor DNS +20
[*] -----------------------------------------------------------------
[*] Scoring scheme for kodachi non Torified system maximum score is: 94
[*] Running in Live mode +10 If installed but encrypted +2 If Nuked +2
[*] User autologin off +10
[*] IPv6 off +10
[*] VPN on +20
[*] Tor on +10
[*] Tor DNS on +20 or DNSCrypt on +15
[*] Kodachi Browser on +10
[*] Force Internet traffic via VPN by ip on +2
[*] Force Internet traffic via by ip,port,protocol,interface on +2


Press any key to start the test.....
```

- **Block UDP**

UDP is a port format that co-exists with another type called TCP, whenever you see these two abbreviations, you are looking at a major port issue, whether good or bad. Because both are crucial. Blocking UDP stops data from being transmitted over that specific port number, UDP still sends data, it is usually less concerning than TCP, since the sent data isn’t organized with time and sequence, but any forensic specialist can figure them out. Blocking certain UDP also has to do with server configuration and few software running accordingly or not.

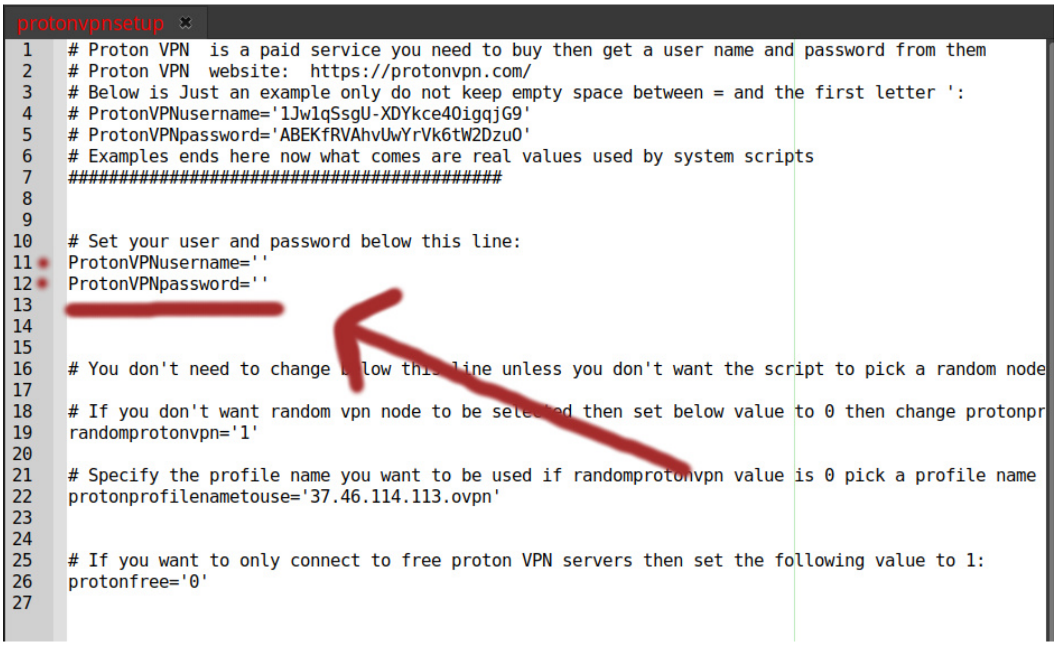
“UDP, or User Datagram Protocol, is another one of the major protocols that make up the internet protocol suite. UDP is less reliable than TCP, but is much simpler.” freeCodeCamp - https://www.freecodecamp.org



□ Block traffic on VPN down
□ Block traffic on IP change
□ Block traffic on IP change (Iptables)
□ Block traffic on IP/port change (Iptables)
□ Block all traffic now regardless VPN
☑ Auto change my timezone based on IP
☑ Update the time based on the new location of timezone
□ Auto spoof my MAC on new VPN connection

Name	Size	Last modified
hidemevpnsetup	977 B	06/22/2019 11:03:12
mullvadvpnsetup	1.05 KiB	08/25/2019 13:38:40
myownvpn.ovpn	407 B	06/22/2019 16:09:36
myownvpnsetup	300 B	06/27/2019 11:41:52
nordvpnsetup	0.99 KiB	10/27/2022 14:27:11
protonvpnsetup	1.08 KiB	06/27/2019 11:07:42
vpngatesetup	555 B	06/27/2019 11:19:31

There is the ability to connect to any of the 9 listed VPN’s. The first, second, seventh, and the last are for free.



```
# Proton VPN  is a paid service you need to buy then get a user name and password from them
# Proton VPN  website:  https://protonvpn.com/
# Below is Just an example only do not keep empty space between = and the first letter ':
# ProtonVPNusername='1Jw1qSsgU-XDYkce4OigqjG9'
# ProtonVPNpassword='ABEKfRVAhvUwYrVk6tW2Dzu0'
# Examples ends here now what comes are real values used by system scripts
###########################################


# Set your user and password below this line:
ProtonVPNusername=''
ProtonVPNpassword=''



# You don't need to change below this line unless you don't want the script to pick a random node

# If you don't want random vpn node to be selected then set below value to 0 then change protonpr
randomprotonvpn='1'

# Specify the profile name you want to be used if randomprotonvpn value is 0 pick a profile name
protonprofilenametouse='37.46.114.113.ovpn'


# If you want to only connect to free proton VPN servers then set the following value to 1:
protonfree='0'
```

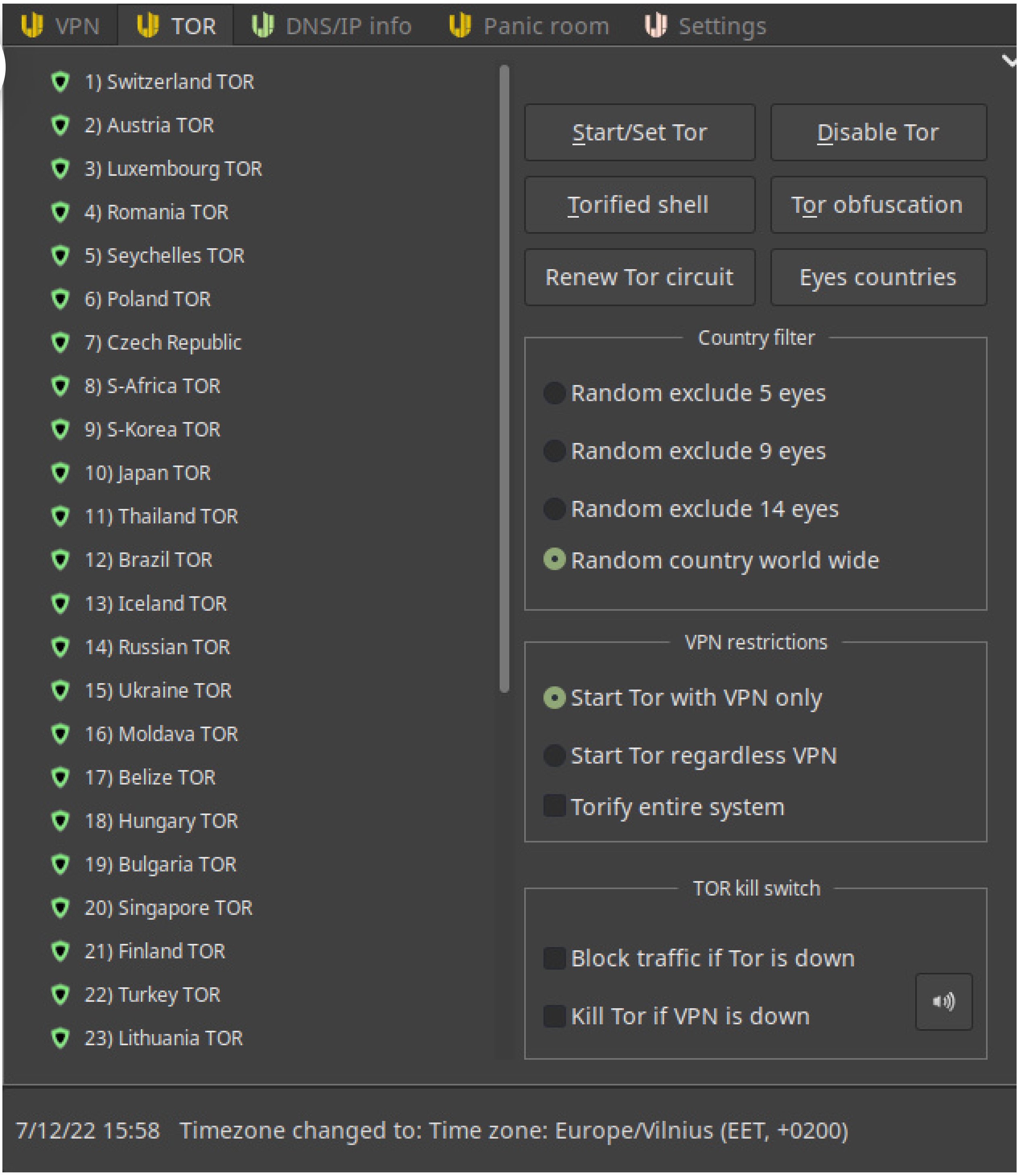
If you obtain or purchased any of the rest you can configure them by editing the config file, you will be asked to add the username and password, which is always given when you purchase a service from these providers, such as ProtonVPN, see the image..

> *The VPN list is sorted by priority, it descends with the least trustable VPN’s.*
>
> *Of course, the trustability changes from one person to another, depending on the individual and the country of the connection.*
>
> *The section in the middle has options regarding running the chosen VPN.*

If one is running a browser or an application during a connection and the VPN connection falls down. Any sent data will have information regarding your network and computer, such as http headers, user-agent, location and more. Therefore the section is listing the ability to automatically kill the internet connection if VPN somehow disconnects. There's the ability also for the case of IP change, which you might not want to happen when you are presenting yourself as one entity from a sepcific location.

There is the ability to change the timezone of your computer, something that users forget to bare in mind. If you connect from a VPN in USA for instance.. and your timezone isn’t changed, the webmaster can determine first, that you are not where you are saying you're from, and second.. you could be at a specific longitude. The latter can help the webmaster round down possible locations you might be at. When you change your timezone however, it might not be the same as the proclaimed IP, but it certainly won't compromise you, location wise.

- **TOR**



1) Switzerland TOR
2) Austria TOR
3) Luxembourg TOR
4) Romania TOR
5) Seychelles TOR
6) Poland TOR
7) Czech Republic
8) S-Africa TOR
9) S-Korea TOR
10) Japan TOR
11) Thailand TOR
12) Brazil TOR
13) Iceland TOR
14) Russian TOR
15) Ukraine TOR
16) Moldava TOR
17) Belize TOR
18) Hungary TOR
19) Bulgaria TOR
20) Singapore TOR
21) Finland TOR
22) Turkey TOR
23) Lithuania TOR

Country filter

○ Random exclude 5 eyes
○ Random exclude 9 eyes
○ Random exclude 14 eyes
● Random country world wide

VPN restrictions

● Start Tor with VPN only
○ Start Tor regardless VPN
☐ Torify entire system

TOR kill switch

☐ Block traffic if Tor is down
☐ Kill Tor if VPN is down

7/12/22 15:58 Timezone changed to: Time zone: Europe/Vilnius (EET, +0200)

Whether you have been using Tor or not, using it with Kodachi can ruffle some feathers if you do that incorrectly. The danger here is you thinking it works when it doesn’t. That’s all you got to pay attention to, you don’t need to question the scripts running the back-end. To break it down, ***Tor*** here is different than ***Torify,*** if you are looking to be anonymouse together with VPN.

The list on the left shows the exit nodes, exit nodes is where the browser or applications used, are coming from. *Tor* won’t hide your activity to your internet provider. But when Tor is used together with *VPN*, you are now hiding your activity from the ISP, and are both unknown to the website. That’s why, this board offers integrated options. Whether you want to turn the *VPN* down if Tor goes down or if that is okay for you. Whether you want to restrain *Tor* if *VPN* is off so that you don’t forget, or if you want *Tor* to run regardless to *VPN*.

After *Tor* has been used for the weirdest and most heinous crimes by some, some countries stepped up and created associations, of a somewhat successful system to track down and collect data more accurately to find people. They use intersection of antennas and networks to circle around and round down locations. This principle has been picked up by two more associations.

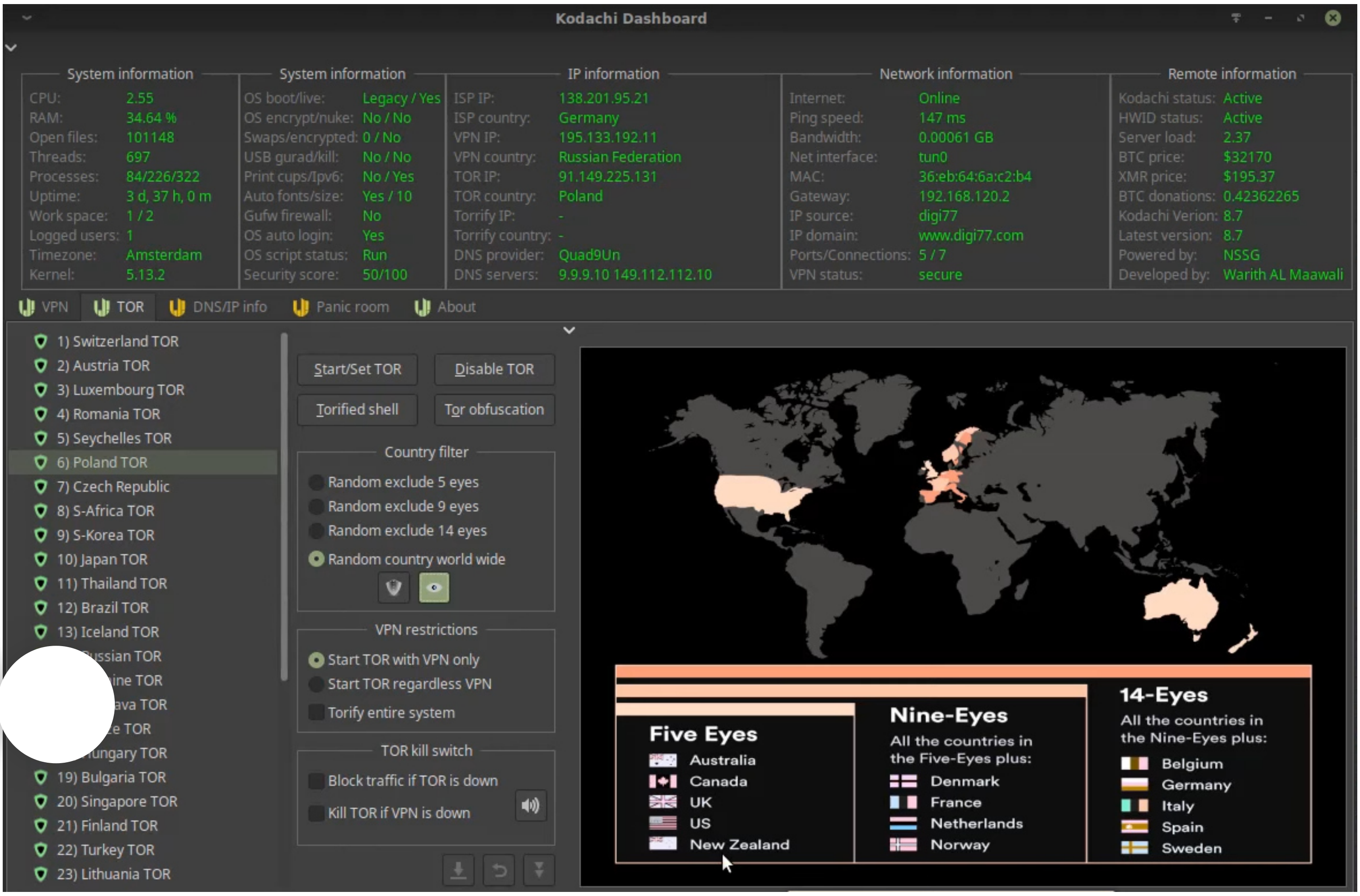
They turn out to be three associations, one that has 5 countries, one that has 9 and one with 14.

Kodachi has the ability to exclude these eyes when you want to work, of course when such measures are taken, one would have to wait a longer time for the connection to be established. It might also be slower than the usual Tor.

“The Nine Eyes and Fourteen Eyes Alliances are essentially extensions of the original Five Eyes Alliance. While these countries may not all share as much information with each other as the Five Eyes Alliance, they still actively and willingly participate in international intelligence-sharing.” vpnmentor.com

These Eyes also depend on data analysis,

“All SIGINT agencies rely on telecommunication companies and internet service providers to gain access to individuals’ private data. By installing fiber-optic splitters at ISP junction points, the SIGINT agency can make an exact copy of the data being processed at that point. This data is then analyzed using deep packet inspection and stored at different data centers.” Richie Koch at ProtonVPN



System information
CPU: 2.55
RAM: 34.64 %
Open files: 101148
Threads: 697
Processes: 84/226/322
Uptime: 3 d, 37 h, 0 m
Work space: 1 / 2
Logged users: 1
Timezone: Amsterdam
Kernel: 5.13.2

System information
OS boot/live: Legacy / Yes
OS encrypt/nuke: No / No
Swaps/encrypted: 0 / No
USB gurad/kill: No / No
Print cups/Ipv6: No / Yes
Auto fonts/size: Yes / 10
Gufw firewall: No
OS auto login: Yes
OS script status: Run
Security score: 50/100

IP information
ISP IP: 138.201.95.21
ISP country: Germany
VPN IP: 195.133.192.11
VPN country: Russian Federation
TOR IP: 91.149.225.131
TOR country: Poland
Torrify IP: -
Torrify country: -
DNS provider: Quad9Un
DNS servers: 9.9.9.10 149.112.112.10

Network information
Internet: Online
Ping speed: 147 ms
Bandwidth: 0.00061 GB
Net interface: tun0
MAC: 36:eb:64:6a:c2:b4
Gateway: 192.168.120.2
IP source: digi77
IP domain: www.digi77.com
Ports/Connections: 5 / 7
VPN status: secure

Remote information
Kodachi status: Active
HWID status: Active
Server load: 2.37
BTC price: $32170
XMR price: $195.37
BTC donations: 0.42362265
Kodachi Verion: 8.7
Latest version: 8.7
Powered by: NSSG
Developed by: Warith AL Maawali

VPN | TOR | DNS/IP info | Panic room | About

1) Switzerland TOR
2) Austria TOR
3) Luxembourg TOR
4) Romania TOR
5) Seychelles TOR
6) Poland TOR
7) Czech Republic
8) S-Africa TOR
9) S-Korea TOR
10) Japan TOR
11) Thailand TOR
12) Brazil TOR
13) Iceland TOR
ssian TOR
ine TOR
ava TOR
e TOR
ungary TOR
19) Bulgaria TOR
20) Singapore TOR
21) Finland TOR
22) Turkey TOR
23) Lithuania TOR

Start/Set TOR | Disable TOR
Torified shell | Tor obfuscation

Country filter
○ Random exclude 5 eyes
○ Random exclude 9 eyes
○ Random exclude 14 eyes
● Random country world wide

VPN restrictions
● Start TOR with VPN only
○ Start TOR regardless VPN
□ Torify entire system

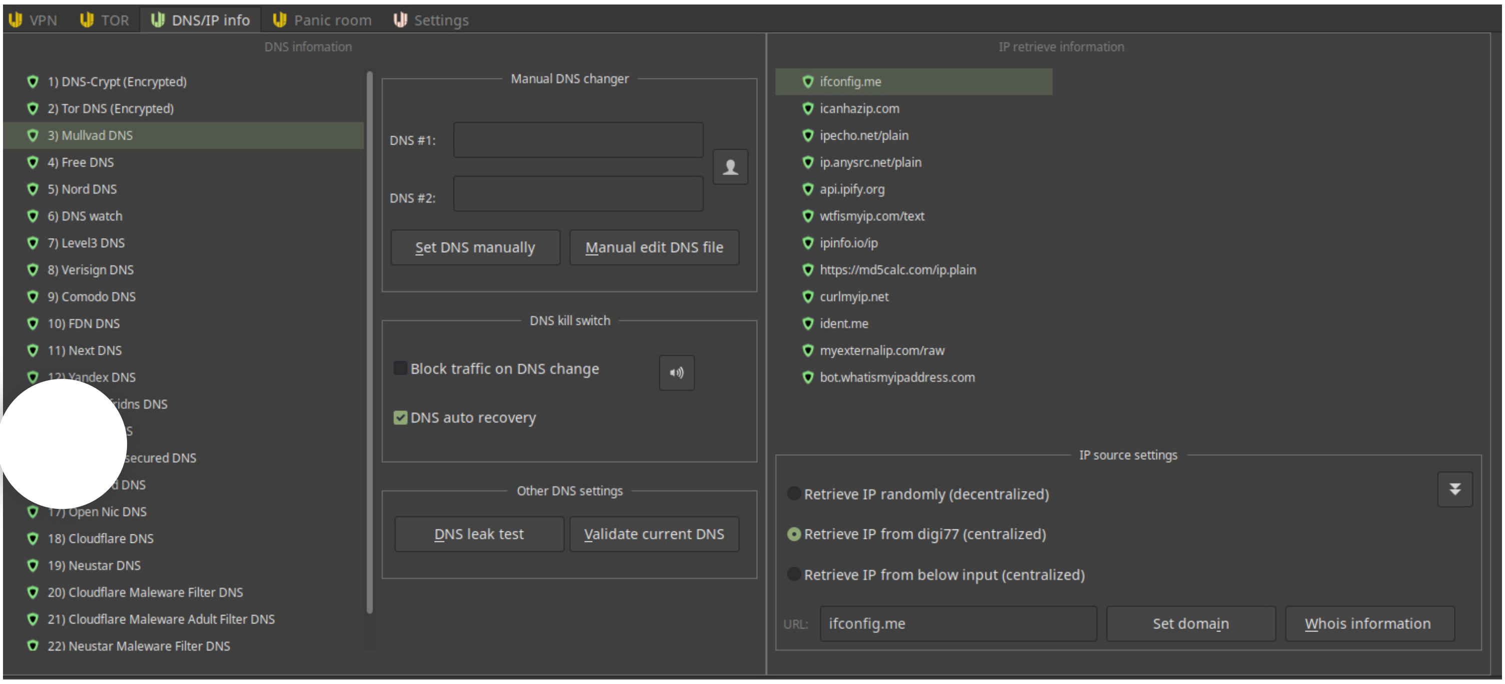
TOR kill switch
□ Block traffic if TOR is down
□ Kill TOR if VPN is down

Eyes Map on the right and Exclusion Filter on the left – Linux Kodachi

Contrary to popular belief, the five, nine and fourteen eyes countries aren’t separate entities and are not working distinctly from each other. The difference is in the datalink and scope of analysis not the co-operations. There are other umbrellas that come by, such as European Union for example, authorities cooperate together and engineers know how to hand data. The key is to switch accordingly and split your work between them in a way that data analysis wouldn’t make sense.

If you aren’t torifying the entire system, but still want to run scans using *nmap* for example. You can use the *Torified Shell* from the dashboard, all your commands will be wrapped inside *Tor*.

- **DnsCrypt**



DNS infomation

1) DNS-Crypt (Encrypted)
2) Tor DNS (Encrypted)
3) Mullvad DNS
4) Free DNS
5) Nord DNS
6) DNS watch
7) Level3 DNS
8) Verisign DNS
9) Comodo DNS
10) FDN DNS
11) Next DNS
12) Yandex DNS
ridns DNS
S
secured DNS
d DNS
17) Open Nic DNS
18) Cloudflare DNS
19) Neustar DNS
20) Cloudflare Maleware Filter DNS
21) Cloudflare Maleware Adult Filter DNS
22) Neustar Maleware Filter DNS

Manual DNS changer

DNS #1:

DNS #2:

DNS kill switch

□ Block traffic on DNS change

☑ DNS auto recovery

Other DNS settings

IP retrieve information

ifconfig.me
icanhazip.com
ipecho.net/plain
ip.anysrc.net/plain
api.ipify.org
wtfismyip.com/text
ipinfo.io/ip
https://md5calc.com/ip.plain
curlmyip.net
ident.me
myexternalip.com/raw
bot.whatismyipaddress.com

IP source settings

○ Retrieve IP randomly (decentralized)

● Retrieve IP from digi77 (centralized)

○ Retrieve IP from below input (centralized)

URL: ifconfig.me

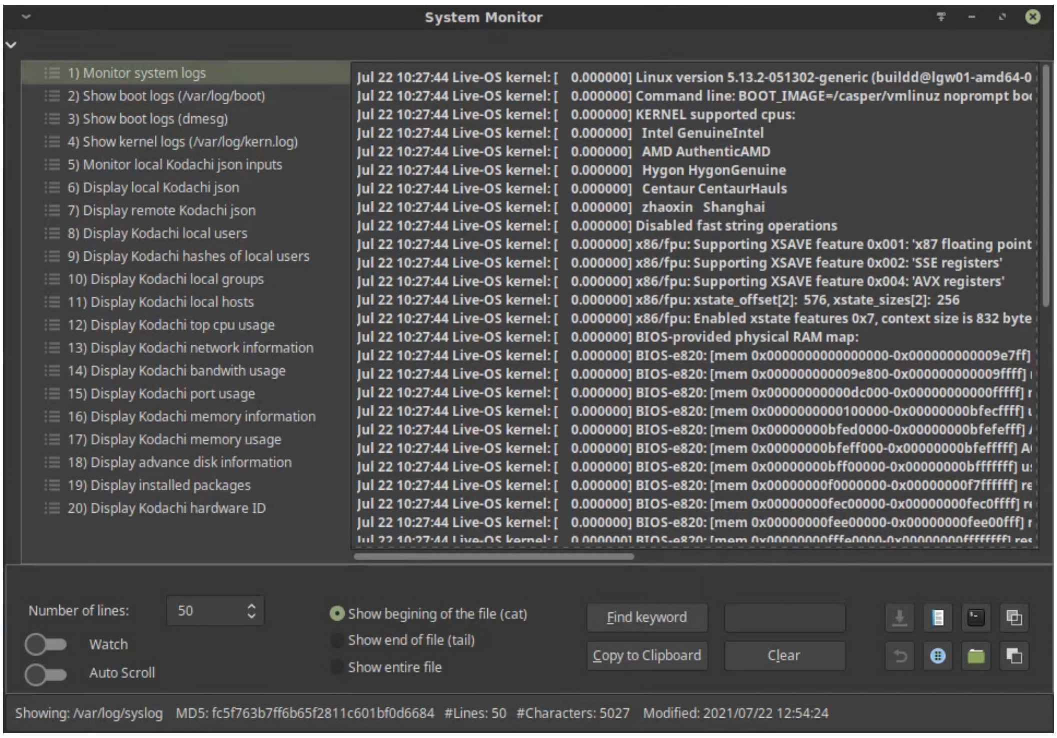
According to dnscrypt.org, **“DNSCrypt is a protocol that authenticates communications between a DNS client and a DNS resolver. It prevents DNS spoofing. It uses cryptographic signatures to verify that responses originate from the chosen DNS resolver and haven't been tampered with. It is an open specification, with free and open source reference implementations, and it is not affiliated with any company nor organization.”**

A lot claim that the ISP can see what sites one is visiting, the internet searches and more. Even if they’re using *https* and, allegedly that is done via DNS lookups on port 53.

The aforementioned is not true for Linux Kodachi, as it runs DnsCrypt and TorCrypt with each connection.

“Your provider won't see anything if you are using VPN because your traffic is encrypted, they might see your dns requests, unless you use DNScrypt which is part of Kodachi” Warith Al Maawali.

System Monitor


System Monitor
1) Monitor system logs
2) Show boot logs (/var/log/boot)
3) Show boot logs (dmesg)
4) Show kernel logs (/var/log/kern.log)
5) Monitor local Kodachi json inputs
6) Display local Kodachi json
7) Display remote Kodachi json
8) Display Kodachi local users
9) Display Kodachi hashes of local users
10) Display Kodachi local groups
11) Display Kodachi local hosts
12) Display Kodachi top cpu usage
13) Display Kodachi network information
14) Display Kodachi bandwith usage
15) Display Kodachi port usage
16) Display Kodachi memory information
17) Display Kodachi memory usage
18) Display advance disk information
19) Display installed packages
20) Display Kodachi hardware ID
Watch
Auto Scroll
Find keyword
Copy to Clipboard
Clear

```
Jul 22 10:27:44 Live-OS kernel: [    0.000000] Linux version 5.13.2-051302-generic (buildd@lgw01-amd64-0
Jul 22 10:27:44 Live-OS kernel: [    0.000000] Command line: BOOT_IMAGE=/casper/vmlinuz noprompt bo
Jul 22 10:27:44 Live-OS kernel: [    0.000000] KERNEL supported cpus:
Jul 22 10:27:44 Live-OS kernel: [    0.000000]   Intel GenuineIntel
Jul 22 10:27:44 Live-OS kernel: [    0.000000]   AMD AuthenticAMD
Jul 22 10:27:44 Live-OS kernel: [    0.000000]   Hygon HygonGenuine
Jul 22 10:27:44 Live-OS kernel: [    0.000000]   Centaur CentaurHauls
Jul 22 10:27:44 Live-OS kernel: [    0.000000]   zhaoxin   Shanghai
Jul 22 10:27:44 Live-OS kernel: [    0.000000] Disabled fast string operations
Jul 22 10:27:44 Live-OS kernel: [    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point
Jul 22 10:27:44 Live-OS kernel: [    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Jul 22 10:27:44 Live-OS kernel: [    0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Jul 22 10:27:44 Live-OS kernel: [    0.000000] x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
Jul 22 10:27:44 Live-OS kernel: [    0.000000] x86/fpu: Enabled xstate features 0x7, context size is 832 byte
Jul 22 10:27:44 Live-OS kernel: [    0.000000] BIOS-provided physical RAM map:
Jul 22 10:27:44 Live-OS kernel: [    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009e7ff]
Jul 22 10:27:44 Live-OS kernel: [    0.000000] BIOS-e820: [mem 0x000000000009e800-0x000000000009ffff] r
Jul 22 10:27:44 Live-OS kernel: [    0.000000] BIOS-e820: [mem 0x00000000000dc000-0x00000000000fffff] r
Jul 22 10:27:44 Live-OS kernel: [    0.000000] BIOS-e820: [mem 0x0000000000100000-0x00000000bfecffff] u
Jul 22 10:27:44 Live-OS kernel: [    0.000000] BIOS-e820: [mem 0x00000000bfed0000-0x00000000bfefefff] A
Jul 22 10:27:44 Live-OS kernel: [    0.000000] BIOS-e820: [mem 0x00000000bfeff000-0x00000000bfefffff] A
Jul 22 10:27:44 Live-OS kernel: [    0.000000] BIOS-e820: [mem 0x00000000bff00000-0x00000000bfffffff] us
Jul 22 10:27:44 Live-OS kernel: [    0.000000] BIOS-e820: [mem 0x00000000f0000000-0x00000000f7ffffff] re
Jul 22 10:27:44 Live-OS kernel: [    0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] re
Jul 22 10:27:44 Live-OS kernel: [    0.000000] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] r
Jul 22 10:27:44 Live-OS kernel: [    0.000000] BIOS-e820: [mem 0x00000000fffe0000-0x00000000ffffffff] res
```

Number of lines: 50

● Show begining of the file (cat)
○ Show end of file (tail)
○ Show entire file

Showing: /var/log/syslog MD5: fc5f763b7ff6b65f2811c601bf0d6684 #Lines: 50 #Characters: 5027 Modified: 2021/07/22 12:54:24

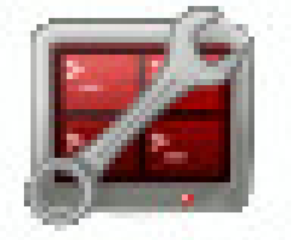
Everything that is done to the Kodachi dashboard, gets sent to the system as a JSON parameter, the System Monitor shows all these parameters and more. Therefore it has all the logs of anything that is taking place, it allows you to see anything that Kodachi is running. For example, if you wanna know what happens when you click Kodachi client or server side VPN.. click that option while having the System Monitor open, you will see the logs and changes., It can be displayed in terminal view as well, with dates of modification. The logs that can be displayed include the following:

- System logs, Dmesg (Which monitors the network card amongst other things). Kernel Logs, Queries that are sent to the json files as parameters and current logs with their local hashes. If any one has trust issues towards Kodachi, this dashboard will break those issues. The monitor is basically running commands but they are integrated here together to give a wider perspective.

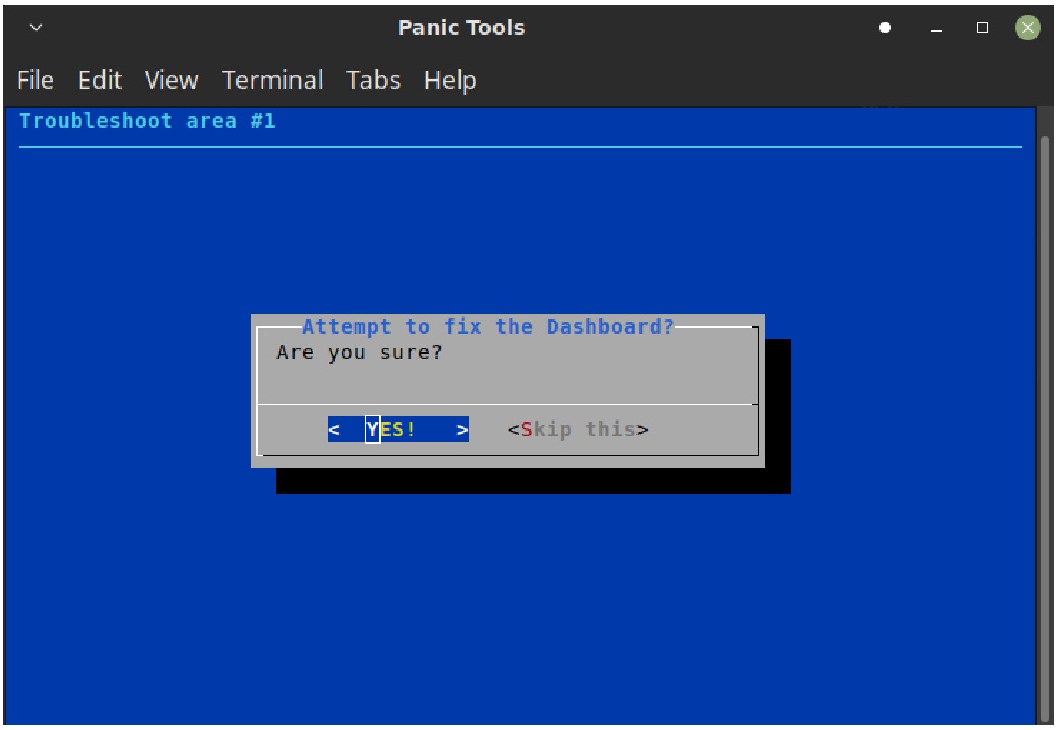
Good To Know

- **Panic Tools**

Not to be confused with Panic Room, Panic Tools are a set of steps you can go through to fix everything by either reset or troubleshooting. The symbolic link to them is on the left Panel of the GUI, shown as a red board with a wrench tool.



They are handy for the network, gui and the dashboard. You don’t have to finish all the steps, if your problem gets fixed.. just close it and get back to work.



```
Troubleshoot area #1

Attempt to fix the Dashboard?
Are you sure?

<  YES!   >    <Skip this>
```

A screenshot of the panic tools

- **Password Manager**

In previous versions of Kodachi, changing the root password will stop functionalities from working. That’s no longer a problem now, with the password manager that is in the panic room, you can change password of both Kodachi user and Root user. There is also a password generator that makes things fast for you, right underneath.

- **Network-Manager**

Different than Windows operating system, *GNU/Linux* handles the network connection differently and directly using its hardware-to-software program called *systemd*. Most of the network config used to be done in text files. Of cource, now there’s a network manager that is adapted in most *GNU/Linux* systems, including Kodachi. Adding, editing or managing networks is done through that.

The network manager won’t require much work from you, if you are not planning on using Kodachi with another computers or a mobiles. Nevertheless, there’s the possibility to use the torified and vpn’d secured network access for your mobile phone, of that of Kodachi. Such a process can be tedious, but if you set it up correctly.. it offers great ability. Kodachi can also run hotspots that use its secured network, where every device that connects to it, ends up using the internet torified, vpn’d and secured just as the dashboard is configured. That is quite handy for offices and large corporations. Again, it requires good engineers to make it stable and problemless.

- **Kodachi Bookmarks**

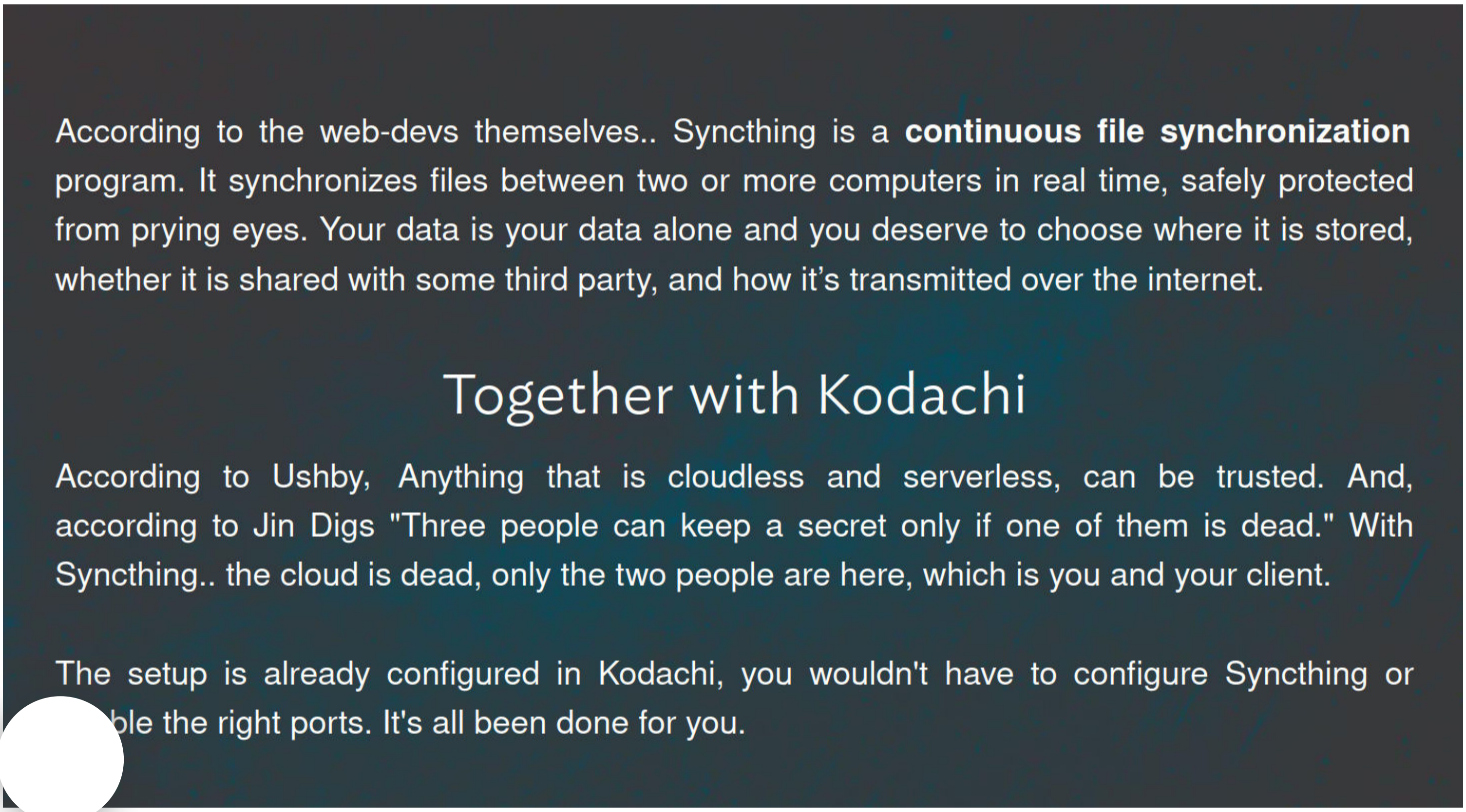
The lite and ghacks browsers are equipped with bookmarks that are already saved. Very useful for quick work, and as you use the system for different reasons at different occasions, you’ll realize that they are very common work. A big list of email providers that are uniquely different, social sites on web and onion network along with security sites and more. The last one on the right will lead you to the developer’s info and digi77’s homepage, an interesting one to look at.

Syncthing

With syncthing you can share files from one device to another directly, without having a server or a cloud in the middle to withhold or save the data. It’s similar to peer-to-peer method of working, it uses local tunneling and depends on the tool to handle the rerouting. This tool is not to be trusted completely, but comparatively and with Tor and VPN.. it’s almost impossible for someone to know you unless the data itself is compromising. The tool runs a local server in your machine.

Syncthing is by far one of the strongest security tools made and hence installed in Kodachi. It can as well be integrated with *LDAP* User Authentication and SSH Access.

For Syncthing to be able to synchronize files with another device, it must be told about that device. This is accomplished by exchanging “device IDs”. A device ID is a unique, cryptographically-secure identifier that is generated as part of the key generation the first time you start Syncthing. It is printed in the log above, and you can see it in the web GUI by selecting “Actions” (top right) and “Show ID”. Two devices will only connect and talk to each other if they are both configured with each other’s device ID. Since the configuration must be mutual for a connection to happen, device IDs don’t need to be kept secret. They are essentially part of the public key. To get your two devices to talk to each other click “Add Remote Device” at the bottom right on both devices, and enter the device ID of the other side. You should also select the folder(s) that you want to share. The device name is optional and purely cosmetic. You can change it later if desired.



According to the web-devs themselves.. Syncthing is a **continuous file synchronization** program. It synchronizes files between two or more computers in real time, safely protected from prying eyes. Your data is your data alone and you deserve to choose where it is stored, whether it is shared with some third party, and how it's transmitted over the internet.

Together with Kodachi

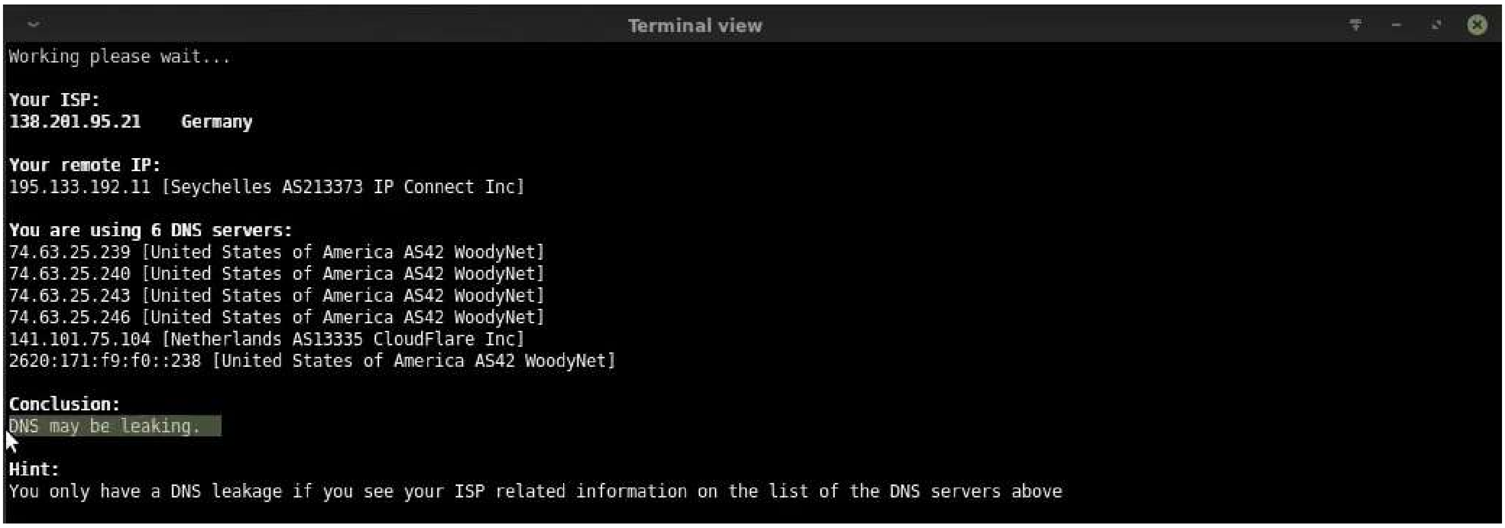
According to Ushby, Anything that is cloudless and serverless, can be trusted. And, according to Jin Digs "Three people can keep a secret only if one of them is dead." With Syncthing.. the cloud is dead, only the two people are here, which is you and your client.

The setup is already configured in Kodachi, you wouldn't have to configure Syncthing or ble the right ports. It's all been done for you.

- **Noisy Crawl**

Generating fake traffic for distraction, if someone managed to monitor your traffic -which rarely happens- you can still distract them from following you, and from focusing on your visited pages or transferred data.

- **Dns Leak Test**



```
Working please wait...

Your ISP:
138.201.95.21    Germany

Your remote IP:
195.133.192.11 [Seychelles AS213373 IP Connect Inc]

You are using 6 DNS servers:
74.63.25.239 [United States of America AS42 WoodyNet]
74.63.25.240 [United States of America AS42 WoodyNet]
74.63.25.243 [United States of America AS42 WoodyNet]
74.63.25.246 [United States of America AS42 WoodyNet]
141.101.75.104 [Netherlands AS13335 CloudFlare Inc]
2620:171:f9:f0::238 [United States of America AS42 WoodyNet]

Conclusion:
DNS may be leaking.

Hint:
You only have a DNS leakage if you see your ISP related information on the list of the DNS servers above
```

“A DNS leak refers to a security flaw that allows DNS requests to be revealed to ISP DNS servers, despite the use of a VPN service to attempt to conceal them. Although primarily of concern to VPN users, it is also possible to prevent it for proxy and direct internet users. The vulnerability allows an ISP, as well as any on-path eavesdroppers, to see what websites a user may be visiting. This is possible because the browser's DNS requests are sent to the ISP DNS server directly, and not sent through the VPN.“ Wikipedia.

As it says above, the requests you send and get back can pass through the ISP, that’s because your VPN wouldn’t have encrypted all the data. This is the DNS leak phenomena. There are online tests you can do to see if any leakage is taking place. However the Kodachi DNS leak test is more robust and accurate. If any info regarding your ISP IP is showing in the test, then you do have a leakage.

One fix is to re-establish the connection over again.

- **Hiding your key strokes**

When the frequency of the keystroke slows down to a certain threshold, key loggers in that case can’t know what you’re typing. Kodachi Dashboard offers the ability to slow the typing to any frequency you want. Very helpful when messing with unknown websites. It might slow your work down, but the chance of someone knowing what you’re typing are rounded down to 0.

- **System Nuke (Destroy)**

If you have an installed and an encrypted Kodachi installation. Enabling Sysem Nuke is one way to protect the system and you from being forced physically. System Nuke is a procedure only ignited when a certain password is entered, one that is different than the usual one.
When the nuke password is entered for the login, the system’s encryption headers will be manipulated and randomized, no one will be able to access the system anymore. This can be handy for ones that are afraid from being physically threatened to start the system.

Note: System Nuke only works for an encrypted installation.

Terminals

Kodachi has more than just one terminal, they also don't save history of commands. The terminals are modified and work accordingly. There is also the torified shell that runs commands under a *Tor* network

- **Embedded Scores and Connection status**

The terminals in Kodachi are equipped with a network status. It shows you what connection are you under. Commands entered from the terminal in those cases will run under the same network.

- **Terminator & Tilix**

These two installed terminals have a powerful ability to arrange terminal sessions. You can open more than one terminal in one window.

What Can You Add.

There are many additions to be implemented to Kodachi, to achieve security goals. Those additions will be mentioned in *Part 2* (*Docker* and *Kubernates*). Ones that aren’t mentioned could be *Kali*, *Android Studio*, *Briar*, *Whonix Windows* and more.

Frequently Asked Questions (Depicted from real inquiries)

Q1. I installed Kodachi on *VirtualBox* and is freezing just a few seconds after startup.

Answer: If you put lower than 8GB of Ram and 2 CPU’s for Kodachi You're likely to freeze, the browsers consume so much memory. You can check it out using the `htop` command in the terminal. The 8th version will be quite good with 8GB, 7th was quite good with 4GB.

Q2. It seems that internet goes down a few seconds after I try to spoof the MAC address, consistently.

Answer: That has to do with your router and your computer's *ARP (Address Resolution Protocol)*. It still thinks you're the old *MAC Address*. To fix this, change your IP or reconnect to WiFi after you spoof, might as well change your *MAC Address* before you turn the WiFi on.

If nothing fixed that, you can do these steps, they will surely work:

1: run this command `ip -s -s neigh flush all`

2: run this command `sudo systemctl stop network-manager`

3: spoof your mac address from the dashboard

4: run this command sudo `systemctl restart network-manager`

Also if your router has static addresses, change them to DHCP. Same for your laptop.

Q3. BTC transactions are too slow/expensive and Monero is way to suspicious to withdraw from an exchange. Last time I checked it costed about 3 dollars to send a BTC transaction and it took about an hour to confirm. Monero transactions are suspicious to governments by default. So, if I

withdraw Monero from my KYCed account then I become a suspect, automatically.

Answer: 3 dollars and an hour is not so much for a safe route. Technology ends there. I wonder why would you be worried though.. There are ways to get around that, but I won't share them with you until I ask you to fill out an KYC form.

Q: Why are the DNS servers IP's compared against my IP? Shouldn't they be compared to the IP from the DNS of my ISP? Such a logic is also different from the one employed in the website, which appears in the Kodachi browser.

Answer: That's not your IP, that's the ISP's IP. ISP uses domain name servers (DNS) on their forefront, these ones on the forefront will eventually lead to this ISP IP, so that they then communicate with you. DNS are on both ends, your ISP and the web application for example. If you see any information that is somewhat describing your ISP company, ISP IP, region or district.. then that means the DNS is leading back to this IP. Your IP is whatever you see when you type ifconfig. If you open another device and visit the same site. You'll see the same IP. ISP provides IP to your last antenna, these antennas have inner DHCP leading to your router, your router has also DHCP leading to your device and so on. Type `tracepath google.com` and you'll see the full connection or maybe type `traceroute google.com`.

Q5. I thought whatever traffic I send to my VPN is encrypted. Now I wonder if that's even a possibility.

Answer: Depends on the connection to that VPN. If you use VPN with secure socket layers (https) and/or TLS.. you're good.

Q6. If my ISP can know what sites am I visiting, then so should my VPN.

Answer: Your ISP doesn't have your private certificate. There's no way. Although, they can make huge guesses, because they see a lot of details.

Q7. It seems that, after all, my ISP can see what sites I visit, my internet searches and more. Even if I am using https. This is done via DNS lookups on port 53.

Answer: That's why you have dnsCrypt on Linux Kodachi.

Q8. I was just surprised to read that using https would prevent my ISP from knowing the sites I visit because they don't have my private certificate. That’s weird ?

Answer: There is a difference between a weblink and sent data using https (API's) A webpage is an address, it has title and metadata. But, data that is sent directly using https won't be seen. It will be encrypted.

Q9. I have a black blank screen on boot ?

Answer: On the grub menu, press e. When you are on the first entry.. Use the keyboard arrows, and move to the line where it says `linux`, you will find written quiet splash, delete that and write `nomodeset`. Now press ctrl + x to boot. If this didn't work, instead of `nomodeset`, type `iommu=soft`.

Q10. How can I implement my own VPN nodes in Kodachi ?

Answer: For this you can use openVPN which is installed in Kodachi already. You will have to extract your nodes into `/etc/openvpn`. Then every time you want to connect run the following command:

```
sudo ovpn /etc/openvpn/ovpn_udp/ <udp node>
```

Or `sudo ovpn /etc/openvpn/ovpn_tcp/ <tcp node>`

Q11. Does Kodachi require any form of kernel hardening ?

Answer: No.

Q12. What is the safest and most paranoid way to use Kodachi

Answer: On a usb stick (Anti-forensic mode).

Q13. Is it possible to increase your live usb disk size ?

Answer: Does this storage that you want, have to be in the home or root directory ? If you just want storage place, using Gparted.. do this:

- Delete your entire usb.
- Create two partitions,
- Make the first as FAT and give it 10gb
- Make the second as ext4 and give it all the rest of the size
- Now, using the terminal, you need to mount the [illegible] FAT partition.
- Look at its name from Gparted. It's usually called `/dev/sda1` or `/dev/sdc1`
- From the terminal run (`sudo mkdir /mnt/sda1 ; sudo mount /dev/<your partition name>/mnt/sd1`)
- Using `unetbootin`.. burn the Kodachi ISO to the FAT partition.
- After running Kodachi live.. use *VeraCrypt* to encrypt the `ext4` created partition.

Now you have an encrypted extra Hard Drive, it weighs whatever size you gave it. Anytime you want to open it run *VeraCrypt* from Kodachi Docker Menu and open it using your prescribed password.

- You can also use the terminal to quickly boot the encrypted extra space by running: `sudo veracrypt /dev/sda1`
- Note: the `sda1` might be different for `sdc1` or `sdb1`, run `fdisk -l` to see which name have been assigned to your extra partition.

Given Under Creative Commons License

Attribution 3.0 Unported (CC BY 3.0)

https://creativecommons.org

You are free to:

- Share — copy and redistribute the material in any medium or format.
- Adapt — remix, transform, and build upon the material for any purpose, even commercially.
- The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

- Attribution — You must give **appropriate credit**, provide a link to the license, and **indicate if changes were made**. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- No additional restrictions — You may not apply legal terms or **technological measures** that legally restrict others from doing anything the license

Prev

Next

Main Menu

Tutorials

Software Analysis Reviews

Analytic Gallery

Informational Resources

Donate money

Donate now with..
PayPal™
VISA
MasterCard
AMERICAN EXPRESS

bc1q7cznuect9ny396ufsdxdzhwhvcf4g59ujfgvnn

Kodachi Solutions

Forum

- Index
- Recent Topics
- Search

Recent podcasts.

Sorry, that’s not currently available.

Luckily, lots of other stuff is.

Sorry, that’s not currently available.

Luckily, lots of other stuff is.

Login Form

Username

Password

□ Remember Me

LOGIN WITH FACEBOOK

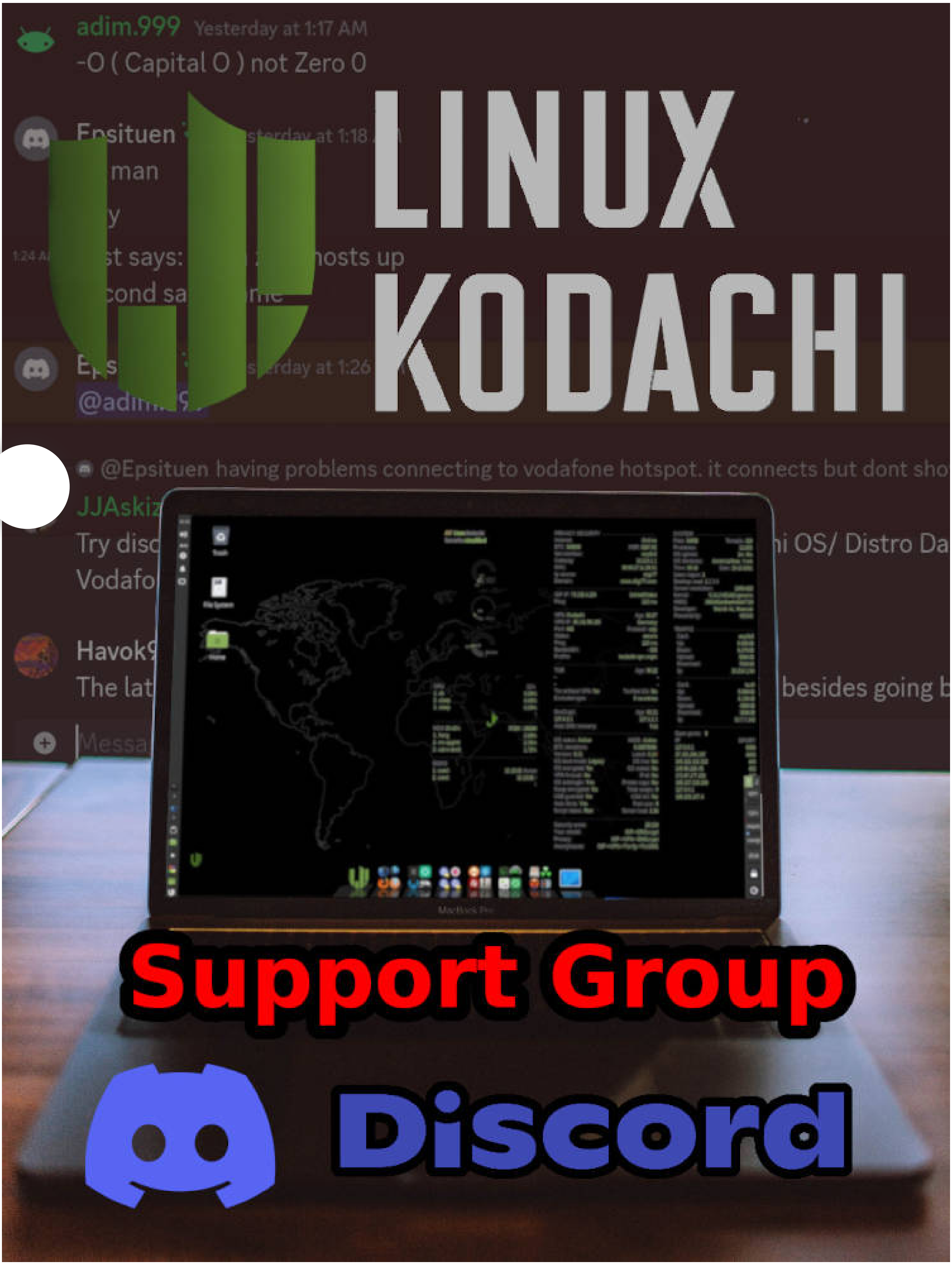
LOGIN WITH GITHUB

SIGN IN WITH GOOGLE

WEB AUTHENTICATION

LOG IN

Forgot your password?
Forgot your username?
Create an account


LINUX
KODACHI
Support Group
Discord

Credits

Powered by

Operating Systems

Contact us

About us

Support Control Room

Data Policy

echnical Team