

OPINION - TECHNICAL REPORT

NIKOLAOS VASILAKOS

IT and Communications Specialist

Trainer and Associate of the Cybercrime Prosecution Directorate

Researcher - Forensic Technician

Digital Evidence Examiner

Subject of Digital Evidence Research

The investigation of digital convictions and its totality of convictions file concerning the case of Sergio Giuliani Nita who is accused of the acts of: 1. Conspiracy to defraud the United States with respect to tax laws, 2. Conspiracy to commit fraud and 3. Conspiracy to committing money laundering.

Case files taken into account:

1. Sergio Giuliani Nita's application dated 02/08/2021 to the Ministry of Justice, Transparency and Human Rights.
2. No. Prot. 42196/04-08-2021 response of the General Directorate of Special Legal Affairs and Human Rights of the Ministry of Justice.
3. No. Prot. 2307/19-07-2021 Document of the Appellate Prosecutor's Office of Patras.
4. No. Prot. 2299/19-07-2021 Order of Temporary Arrest of the Appellate Prosecutor's Office

Patron.

5. No. Prot. 3880/09-08-2020 translated document of the Community Town Hall Brandoulets.

6. No. Prot. 45001 FEA 2069/15-09-2021 document of the General Directorate of Special Legal Affairs and Human Rights of the Ministry of Justice.

A. The following documents were considered, among others:

1. Interpol arrest warrant No. A 5060/62021.

2. Series of digital photos with dates taken between the time period 2014-2016.

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 3 of 57

3. Series of photos with dated social media posts (facebook) from the defendant's personal account.

B. Based on all the aforementioned, it was requested to be answered with a scientific criterion the following questions:

1. What is the tax refund process? What is needed for each tax refund application in the system, which actors are involved and which processes are activated? Please in the answer also refer to the technical parameters of your specialty.

2. Is it possible to hack the process by script/human/user/hacker/cracker?

3. You can research examples of searches with the nicknames found in case file on the Internet?

4. What is and how does identity theft happen online?

5. Any other observation within the scope of your competence deemed useful for the case.

5.1 What is the captcha, which is in the process, why is it not overcome?

5.2 The process requires a mobile phone for each return. It becomes one to procure american mobile number online;

5.3 Is a unique web browser fingerprint required for each return?

5.4 Can the defendant's affiliation be confirmed?

5.5 Does the defendant have devices?

5.6 What is the botnet cluster the defendant is accused of?

6. What technical skills and knowledge does the cluster or botnet need?

C. BACKGROUND – FINDINGS

D. ANSWERS TO THE QUESTIONS ASKED

1. What is needed for each tax refund application in the system, which agencies involved and what processes are activated? Please in the answer to also refer to the technical parameters of your specialty.

The process of applying for a tax refund in the US can be done in several ways. Two main categories of procedure are filing the application in person to the relevant department and the deposit electronically. As in Greece, procedure can be handled either by the taxpayer himself, or by persons or companies that offer accounting services.

The exact process for filing the application in the IRS online system is under construction constant changes as at least in the last 15 years the said system has been target of long-range cyber-attacks repeatedly.

Material from the critical years 2014 – 2016 was investigated to establish which process was in place then and what safeguards did the IRS system have at that time period. For each tax refund application it was necessary to pres

- Copies of previous tax returns that were filed and related to declarations of income, real estate, tax refund, etc. It is recorded that she at the time, such copies could be obtained in person to the competent agency, by mailing them to the taxpayer's home or in specific cases to be obtained online in case they had registered in the online system. Today most of this process is completed online.

- Full personal details of the taxpayer, ie: name, address tax residence, date of birth, social security number, address e-mail, bank account details, full details of dependent members (spouse – children), previous residential addresses and number

landline corresponding to the place of residence. In case of registration mobile phone, the number code should also correspond to the location residence. (see question 5.2 below)

During the process of online registration of the application, as a security measure the system asked by the applicant to answer questions of a personal nature in order to establish his identity. Examples of such questions could be: "What color was the car you were driving in 2008?", "how much was your monthly loan payment card?", "what is the name your neighbors call you by?" and others similar

In addition, the following were found:

For the tax refund, it was possible to register a bank account which has been opened in online banking. Indications for opening an account and obtaining a card to Green Dot Bank which is a popular choice, should be provided full personal details of the owner, identical to those required in the return application file a tax return with the IRS, answer personal security questions and register cell phone number. To connect a Green Dot account with the transit service

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 6 of 57

of PayPal payments, the same information for the opening an account at Green Dot bank as well as registering a debit number card of the associated bank.

It is noted that it is common in the process of registering a tax refund application on US to be used online proxy platforms that offer friendly to user interaction environment and give step-by-step instructions for entering answers necessary data and supporting documents. Examples of such applications are "Turbo Tax" which it is also the most popular, "TaxAct" etc. (...)

2. It is possible to violate the process by script/human/user/hacker/cracker?

The process of breaching the process is possible but requires high expertise, vs much greater than that of an everyday user. The IRS system in the US has has been targeted repeatedly in the past by cyber-criminals and continues to targeted to date.

A basic prerequisite for breaching the IRS system is gaining access to all required personal data of a taxpayer. This access is obtained either by various techniques of stealing a person's identity information or by purchasing services from illegal circuits on the dark web that provide access to existing bases data with personal information of citizens that have already been intercepted by various methods (one of them is through the use of botnets).

In order for the breach of the system to be massive in nature so as to increase the chances of successful access but also to hide the identity of the perpetrators from the prosecution authorities, it is common to use a botnet system that through malicious software the attacker can simultaneously execute thousands of commands through infected devices from all over the world. This makes simultaneous input possible

on the system with stolen information of thousands of users.

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 7 of 57

In addition, similar incidents of IRS system violations were investigated specifically against critical period 2014 – 2016. Reference found in New York Times article about attack into the IRS system in 2015 with identity theft for over 100,000 taxpayers and a loss of over \$50 million in illegal tax refunds.

Then-IRS Commissioner John Koskinen had stated “We are confident that this is not about amateurs. These are actually organized crime syndicates that it's not just us, but everyone in the financial industry. [...] 80% of incidents of identity theft we deal with and refund fraud is related to organized crime here and around the world. These are excellent sophisticated criminals with access to vast amounts of data.”

3. You can research examples of searches with the aliases that exist do they have on file on the Internet?

Online searches of the nicknames “giulonline” and “juliansweiss”


- Google search results for the nickname “Giulonline”

2015

https://www.avocatnet.ro/forum/discutie_490033/PFA-II-sau-SRL-pentru-tarani.html

opened in Commercial Companies

PFA, II or SRL for farmers?

	giulonline User 00:05, June 8, 2015
---	--

Hello, it's me

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 8 of 57

owner of a small animal farm and want to develop in the future with the help of European non-revolving funds ... in the past I had an LLC that was successfully closed after a long process-sia so in SRL -D I can't fit.

At the moment there are 110 sheep and goats, 12 pregnant sows and 4 pregnant cows.

At the moment I don't sell products or animals, but from next year I want to sell traditionally products made on my own farm.

I am the owner of a place in Pitesti which can be arranged and authorized as a point of consumption of food. (family owned but you can rent in ** solution **)

I state that in the store I will sell my products (for which I am applying for a certificate of manufacturer from the town hall) and the products of other compatriots with a manufacturer's certificate.

Another question would be: do I have to be VAT liable to be able to sell on this site?

Now I don't know what to choose from the 3 options.

please help me with your opinions to choose the best solution for me.

Thanks in advance

Last modified: Monday, June 8, 2015 giulonline , user

https://www.avocatnet.ro/forum/discutie_490171/cod-CAEN-ferma-de-porci-si-desfacere-produse-in-mag-azin-propriu.html#modal

opened in the *New CANE Code 2008*

CAEN code pig farm and products produced in its own shop



giulonline

User

18:25, June 8, 2015

Hello,

I currently have a farm number at town hall for the animals I have but I want to make it legal business and sell the products in my own store through an SRL.

Please tell me which CAEN codes I need for a farm with cows, pigs, sheep, goats and fowls (in other words mixed).

Thank you

2017

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 9 of 57

wex.nz,

<https://btceclub.ru/chatlog/?date=24-12-2017&find=Giulonline&lang=en>

- Google search results for the nickname "julienweiss"

2006

<https://moviechat.org/tt0407732/Dirty-Deeds/58c7fa722214d80b5cf007e1/Soundtrack>

MovieChat Forums > [Dirty Deeds \(2006\) Discussion](#) > Soundtrack???

soundtrack???

posted 16 years ago by relic88

[15 replies](#) [jump to latest](#)

Does anyone know if there is a soundtrack being released? If not, does anybody at least know the names of the artists / songs that are played throughout the film??? Thanks reply share

[+] rip_sta 16 years ago

[-] munkiuik 16 years ago

Superjerk - I'll Get Away With This Bowling For Soup - Almost Wakefield - C'mon Baby Classic - Let It Flow Classic - What Cha Gonna Do? The Grand Skeem - Party All Night The Grand Skeem - Here We Go Cham Pain - Make It Bounce Cham Pain - Show Me 86 (Feat. Classic) - Ridin' Invisible Men - All My Peoples Universal - Yada Yada AD - West G Classic - Rollin' Basko - Ain't No Game AD - Line It Up Valley Lodge - If It Takes All Night Uptown Sinclair - Face Down Uptown Sinclair - Sentimental Uptown Sinclair - Whatever You Want Uptown Sinclair - Superman Uptown Sinclair - Girlfriend Boomish - Popcorn Boomish - Ipanemic David Kopatz - I Like Candy The SmashUp - Icarus Flies Nicole Saletta - Welcome To My Sunny Day Jill Zandeh - Yesterday, Tomorrow and Today Alex Solowitz - Shut Your Mouth Paige Lewis - Take It And Shove It Bryan Datillo - ICGM (Italian Click Gang Mafiosa) Grace & Manners - 9 By 9 Grace & Manners - Away From Here The title song is not listed in the credits... (i got a secret i cant keep, i just committed another dirty deed) reply share

[+] icredibilu00 16 years ago
[-] zeon_peter 16 years ago
man really hard to find these tracks reply share

[-] shuchen90 16 years ago

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 10 of 57

Yeah... are these tracks very old? or what :S reply share

[-] sako_81 16 years ago
I can't find any of these tracks!!! I'm still looking for the song from the 5th deed. reply share

[-] raw_kinetic 16 years ago
WHERE DO I GET ITALIAN CLICK GANG MAFIOASA ? there is no Bryan Datillo who sings this.. please some pointers.. reply share

[-] juliensweiss 16 years ago
well, if someone found at least some of the songs, please post here ... i could find none :) reply share

[-] bornb_2004 16 years ago
People i just need to know the melody before deed 7....the one with meg in car wishing good luck....PLEASE :D reply share

[-] shuchen90 16 years ago
I Need this track Nicole Saletta - Welcome To My Sunny Day pff its very hard to find these tracks reply share

2006

<https://moviechat.org/tt0407732/Dirty-Deeds/58c7fa712214d80b5cf00731/Soundtrack>

Soundtrack

posted 16 years ago by juliensweiss
5 replies | jump to latest


So, after all, did anyone find any of the songs on the soundtrack? :) reply share

[-] icredibilu00 16 years ago
me no reply share

2008 -

<https://www.linuxquestions.org/questions/linux-networking-3/problem-with-routing-via-different-external-interfaces-eth-and-tun-669678/>

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 11 of 57

09-13-2008, 07:45 AM	
juliensweiss LQ Newbie Registered: September 2007 Posts: 2	 (eth and tun) [Log in to get rid of this advertisement]
Rep: Problem with routing	Hello,

I have the following configuration:

```
eth0: xx.xx.xx.18 bcast xx.xx.xx.23 mask 255.255.255.248  
eth0:0 xx.xx.xx.19 bcast xx.xx.xx.23 mask 255.255.255.248
```

```
tun0: yy.yy.yy.84 ptp yy.yy.yy.84 mask 255.255.255.255
```

default route is xx.xx.xx.17

I need a Dante socks server to run on the machine, to accept incoming connections on eth0, and to use tun0 interface for outgoing connections, but at the same time keep the default gateway via eth0.

Dante server does support selecting, different interfaces, so with this configuration:

```
internal: eth0 port = 1090  
external: tun0
```

should work ... but no traffic gets through ...
When I use the eth0:0 interface for outgoing traffic, it works, but when I switch to the tunnel, it doesn't.

Also, if I add an eth1 with internal ip addresses, like:
eth1: 192.168.1.1 netmask 255.255.255.0, and I try using the ppp0 interface for nat, same result. If I nat via eth0:0 ip, everything works fine...

I would appreciate some help with this.

The OS is CentOS release 4.6 (Final), kernel 2.6.9-67.0.4.EL #1

Thanks,
Julien

Last edited by juliensweiss? 09-13-2008 at 07:48 AM. Reason: added OS version

#2

juliensweiss
LQ Newbie

Registered: September 2008
Posts: 2

Original Poster

rep: ■

Got a solution

After reading a cached google document <http://74.125.95.104/search?q=cache:...nk&cd=28&gl=us> I found a solution. I don't know if its the best one, but it seems to be work.

first, have to tune dante socks server as user sockd, uid 501 and change the configuration to:
internal: eth0 port = 2003
external: eth0

```
echo "151 conn1" >> /etc/iproute2/rt_tables
```

```
ip rule add fwmark 1 table conn1
```

```
iptables -t mangle -A OUTPUT -p tcp --sport ! 2003 -m owner --uid-owner 501 -j MARK --set-mark 1  
iptables -t nat -A POSTROUTING -p tcp --sport ! 2003 -o tun0 -j SNAT --to-source=tun0_ip
```

```
iptables -t mangle -A OUTPUT -p udp --sport ! 2003 -m owner --uid-owner 501 -j MARK --set-mark 1  
iptables -t nat -A POSTROUTING -p udp --sport ! 2003 -o tun0 -j SNAT --to-source=tun0_ip
```

```
ip route add default dev tun0 table conn1
```

```
echo 0 > /proc/sys/net/ipv4/conf/eth0/rp_filter  
echo 0 > /proc/sys/net/ipv4/conf/tun0/rp_filter
```

Now all traffic from the dante servers goes via tun0

If anyone knows a better way, please let me know.

Thank you

2010 -
<https://bugs.launchpad.net/ubuntu/+source/linux/+bug/518196>

Activity log for bug #518196

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 13 of 57

Date	Who	What changed	Old value	New value	Message
2010-02-06 21:33:53	jsweiss	bug			added bug
2010-02-06 21:58:40	Mitch Towner	affected ubuntu-docs	(Ubuntu)	Linux (Ubuntu)	
2010-02-10 19:07:03	Jerem Foshie	linux (Ubuntu) status	New Incomplete		
2010-02-10 19:57:21	jsweiss	attachment added	AlsaDevices.txt	http://launchpadlibrarian.net/39024943/AlsaDevices.txt	
2010-02-10 19:57:26	jsweiss	attachment added	AplayDevices.txt	http://launchpadlibrarian.net/39024944/AplayDevices.txt	
2010-02-10 19:57:32	jsweiss	attachment added	BootDmesg.txt	http://launchpadlibrarian.net/39024945/BootDmesg.txt	
2010-02-10 19:57:36	jsweiss	attachment added	Card0.Amixer.values.txt	http://launchpadlibrarian.net/39024947/hpadlibrarian-Card0.Amixer.values.txt	
2010-02-10 19:57:40	jsweiss	attachment added	Card0.Codecs.codec.0.txt	http://launchpadlibrarian.net/39024948/hpadlibrarian-Card0.Codecs.codec.0.txt	
2010-02-10 19:57:43	jsweiss	attachment added	Card0.Codecs.codec.1.txt	http://launchpadlibrarian.net/39024956/hpadlibrarian-Card0.Codecs.codec.1.txt	
2010-02-10 19:57:47	jsweiss	attachment added	Card1.Codecs.codec.0.txt	http://launchpadlibrarian.net/39024957/hpadlibrarian-Card1.Codecs.codec.0.txt	
2010-02-10 19:57:55	jsweiss	attachment added	CurrentDmesg.txt	http://launchpadlibrarian.net/39024959/CurrentDmesg.txt	
2010-02-10 19:57:58	jsweiss	attachment added	IwConfig.txt	http://launchpadlibrarian.net/39024960/IwConfig.txt	
2010-02-10 19:58:02	jsweiss	attachment added	Lspci.txt	http://launchpadlibrarian.net/39024962/Lspci.txt	
2010-02-10 19:58:06	jsweiss	attachment added	Lsusb.txt	http://launchpadlibrarian.net/39024964/Lsusb.txt	
2010-02-10 19:58:09	jsweiss	attachment added	PciMultimedia.txt	http://launchpadlibrarian.net/39024965/PciMultimedia.txt	
2010-02-10 19:58:13	jsweiss	attachment added	ProcCpuinfo.txt	http://launchpadlibrarian.net/39024968/ProcCpuinfo.txt	
2010-02-10 19:58:16	jsweiss	attachment added	ProcInterrupts.txt	http://launchpadlibrarian.net/39024970/ProcInterrupts.txt	
2010-02-10 19:58:20	jsweiss	attachment added	ProcModules.txt	http://launchpadlibrarian.net/39024971/ProcModules.txt	
2010-02-10 19:58:24	jsweiss	attachment added	RfKill.txt	http://launchpadlibrarian.net/39024973/RfKill.txt	
2010-02-10 19:58:37	jsweiss	attachment added	UdevDb.txt	http://launchpadlibrarian.net/39024986/UdevDb.txt	

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 14 of 57

2010-02-10 19:58:59	jsweiss	attachment added	UdevLog.txt	http://launchpadlibrarian.net/39025010/UdevLog.txt	
2010-02-10 19:59:03	jsweiss	attachment added	XsessionErrors.txt	http://launchpadlibrarian.net/39025013/XsessionErrors.txt	
2010-02-10 19:59:07	jsweiss	linux (Ubuntu) status	Incomplete	New	
2010-02-10	jsweiss	tags		apport-collected	

19-59-17					
Intel iwlagndriver hangs from time to time Bug #518196 reported by jsweiss on 2010-02-06					
32 This bug affects 4 people					
Affects Status Importance Assigned to Milestone linux (Ubuntu) Expired Low Unassigned					
Bug Description					
Binary package hint: ubuntu-docs					
Hello, I have a problem with the iwlagndriver. everything works perfect, except it somehow "hangs" from time to time. There is no exact time frame for hanging, sometimes it works perfectly for days, other times dies 2 times in 10 minutes. The wireless network disconnects, and it does not show any available network (the AP is not the problem, as other devices do work. also there is not a hardware issue, because on windows I did not have this problem). When the wifi adapter hangs, I get this in the dmesg:					
[7952.460205] wlan0: no probe response from AP XX:XX:XX:XX:XX - disassociating [7953.060210] iwlagndriver 0000:05:00.0: Error sending REPLY_RXON: timed out after 500ms. [7953.060223] iwlagndriver 0000:05:00.0: Error setting new RXON (-110) [7953.560245] iwlagndriver 0000:05:00.0: Error sending REPLY_SCAN_CMD: time out after 500ms. [7954.060057] iwlagndriver 0000:05:00.0: Error sending REPLY_RXON: time out after 500ms. [7954.060069] iwlagndriver 0000:05:00.0: Error setting new RXON (-110) [7954.560235] iwlagndriver 0000:05:00.0: Error sending REPLY_RXON: time out after 500ms. [7954.560247] iwlagndriver 0000:05:00.0: Error setting new RXON (-110) [7959.060105] iwlagndriver 0000:05:00.0: Error sending REPLY_RXON: timed out after 500ms. [7959.060116] iwlagndriver 0000:05:00.0: Error setting new RXON (-110) [7959.560264] iwlagndriver 0000:05:00.0: Error sending REPLY_SCAN_CMD: timeout after 500ms. [7960.060248] iwlagndriver 0000:05:00.0: Error sending REPLY_RXON: time out after 500ms. [7960.060260] iwlagndriver 0000:05:00.0: Error setting new RXON (-110)					
The only solution for the wifi network to recover is to remove and then re-insert the module. If I use the wireless on/off switch on the laptop, it still does not work. If I do: rmmod iwlagndriver iwlc core modprobe iwlagndriver modprobe iwlc core the wifi card finds the access point again.					
The system is as follows: Linux user-laptop 2.6.31-19-generic #56-Ubuntu SMP Thu Jan 28 02:39:34 UTC 2010 x86_64 GNU/Linux Ubuntu 9.10					
System is a Sony Vaio VGN-SR59VG (german version), and the wireless adapter is *-network de-					

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 15 of 57

scription: Wireless interface product: Wireless WiFi Link 5100 vendor: Intel Corporation physical id: 0 bus info: pci@0000:05:00.0 logical name: wmaster0 version: 00 serial: xx:xx:xx:xx:xx:xx width: 64 bits clock: 33MHz capabilities: pm msi pci-express bus_master cap_list logical ethernet physical wireless configuration: broadcast=yes driver=iwlagndriver ip=192.168.1.101 latency=0 multicast=yes wireless=IEEE 802.11abgn resources: irq:31 memory:d1500000-d1501fff					
This is getting annoying sometimes, especially because sometimes it works for days, other times it dies 2 times in 10 minutes.					
Any help would be appreciated.					
Julien					
Tags: apport-collected karmic kj-expired regression-potential					
Mitch Towner (kermiac) wrote on 2010-02-06:					#1
not an ubuntu-docs issue					
affects : ubuntu-docs (Ubuntu) → linux (Ubuntu)					
Jeremy Foshee (jeremyfoshee) wrote on 2010-02-10:					#2
jsweiss, Please run 'apport-collect -p linux 518196' so that the collected logs for this issue can be attached to this bug.					
Thanks!					
-JFo					
Changed in linux (Ubuntu):					
status : New → Incomplete					
jsweiss (julienweiss) wrote on 2010-02-10: apport-collect data					#3

```
Architecture: amd64 ArecordDevices: **** List of CAPTURE Hardware Devices **** card 0: Intel [HDA Intel], device 0: ALC262 Analog [ALC262 Analog] Subdevices: 1/1 Subdevice #0: subdevice #0 AudioDevicesInUse: USER PID ACCESS COMMAND /dev/snd/controlC0: user 4085 F... pulseaudio CRDA: Error: [Errno 2] No such file or directory Card0.Amixer.info: Card hw:0 'Intel'/HDA Intel at 0xd5200000 irq 22' Mixer name : 'Realtek ALC262' Components : 'HDA:10ec0262,104d2d00,00100302 HDA:14f12c06,104d1700,00100000' Controls : 18 Simple ctrls : 11 Card1.Amixer.info: Card hw:1 'HDMI'/HDA ATI HDMI at 0xd0030000 irq 17' Mixer name : 'ATI R6xx HDMI' Components : 'HDA:1002aa01,104d2d00,00100100' Controls : 4 Simple ctrls : 1 Card1.Amixer.values: Simple mixer control 'IEC958',0 Capabilities: pswitch pswitch-joined Playback channels: Mono Mono: Playback [off] DistroRelease: Ubuntu 9.10 InstallationMedia: Ubuntu 9.10 "Karmic Koala" - Release amd64 (20091027) MachineType: Sony Corporation VGN-SR59VG_H NonfreeKernelModules: fg1rx Package
```

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 16 of 57

<pre>linux (not installed) ProcCmdLine: BOOT_IMAGE=/vmlinuz-2.6.31-19-generic root=UUID=2cebe356-2708-47eb-9821-27eba1d664e8 ro quiet splash ProcEnviron: SHELL=/bin/bash PATH=(custom, user) LANG=en_US.UTF-8 ProcVersionSignature: Ubuntu 2.6.31-19.56-generic RelatedPackageVersions: linux-backports-modules-2.6.31-19-generic N/A linux-firmware 1.25 Uname: Linux 2.6.31-19-generic x86_64 UserGroups: adm admin cdrom dialout lpadmin plugdev sambashare www-data WifiSyslog: dmi.bios.date: 08/05/2009 dmi.bios.vendor: American Megatrends Inc. dmi.bios.version: R4090Y1 dmi.board.asset.tag: N/A dmi.board.name: VAIO dmi.board.vendor: Sony Corporation dmi.board.version: N/A dmi.chassis.asset.tag: N/A dmi.chassis.type: 10 dmi.chassis.vendor: Sony Corporation dmi.chassis.version: N/A dmi.modalias: dmi:bvnAmericanMegatrendsInc.:bvrR4090Y1:bd08/05/2009:svnSonyCorporation:pnVGN-SR59VG_H:pvrC60389VN:rvn-SonyCorporation:rnVAIO:rvrN/A:cvnSonyCorporation:ct10:cvrN/A: dmi.product.name: VGN-SR59VG_H dmi.product.version: C60389VN dmi.sys.vendor: Sony Corporation</pre>			
jsweiss (julienweiss) wrote on 2010-02-10: AlsaDe- devices.txt			#4
<p>* AlsaDevices.txt Edit (643 bytes, text/plain)</p>			
jsweiss (julienweiss) wrote on 2010-02-10: AplayDe- devices.txt			#5
<p>* AplayDevices.txt Edit (263 bytes, text/plain)</p>			
jsweiss (julienweiss) wrote on 2010-02-10: BootDmesg.txt			#6
<p>* BootDmesg.txt Edit (51.9 KiB, text/plain)</p>			
jsweiss (julienweiss) wrote on 2010-02-10: Card0.Amixer.values.txt			#7
<p>* Card0.Amixer.values.txt Edit (2.2 KiB, text/plain)</p>			
jsweiss (julienweiss) wrote on 2010-02-10: Card0.Co- decs.codec.0.txt			#8
<p>* Card0.Codecs.codec.0.txt Edit (10.6 KiB, text/plain)</p>			
jsweiss (julienweiss) wrote on 2010-02-10: Card0.Co- decs.codec.1.txt			#9
<p>* Card0.Codecs.codec.1.txt Edit (146 bytes, text/plain)</p>			

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 17 of 57

jsweiss (julienweiss) wrote on 2010-02-10: Card1.Co- decs.codec.0.txt			#10
---	--	--	-----

* Card1.Codecs.codec.0.txt Edit (761 bytes, text/plain)		
jsweiss (juliensweiss) wrote on 2010-02-10: CurrentDmesg.txt		#
* CurrentDmesg.txt Edit (79.3 KiB, text/plain)		
jsweiss (juliensweiss) wrote on 2010-02-10: IwConfig.txt		#
* IwConfig.txt Edit (617 bytes, text/plain)		
jsweiss (juliensweiss) wrote on 2010-02-10: Lspci.txt		#
* Lspci.txt Edit (15.6 KiB, text/plain)		
jsweiss (juliensweiss) wrote on 2010-02-10: Lsub.txt		#
* Lsub.txt Edit (742 bytes, text/plain)		
jsweiss (juliensweiss) wrote on 2010-02-10: PciMultimedia.txt		#
* PciMultimedia.txt Edit (1.2 KiB, text/plain)		
jsweiss (juliensweiss) wrote on 2010-02-10: ProcCpuinfo.txt		#
* ProcCpuinfo.txt Edit (1.5 KiB, text/plain)		
jsweiss (juliensweiss) wrote on 2010-02-10: Re: [Bug		#

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 18 of 57

518196] Re: Intel iwlagndriver hangs from time that time		#
Done. Thanks Jeremy Foshee wrote: > jsweiss, > Please run 'apport-collect -p linux 518196' so that the collected logs for this issue can be attached to this bug. >> Thanks! >> -JFo >> ** Changed in: linux (Ubuntu) > Status: New => Incomplete >>		
jsweiss (juliensweiss) wrote on 2010-02-10: ProcInterrupts.txt		#
* ProcInterrupts.txt Edit (1.7 KiB, text/plain)		
jsweiss (juliensweiss) wrote on 2010-02-10: ProcModules.txt		#
* ProcModules.txt Edit (5.1 KiB, text/plain)		
jsweiss (juliensweiss) wrote on 2010-02-10: RfKill.txt		#
* RfKill.txt Edit (175 bytes, text/plain)		
jsweiss (juliensweiss) wrote on 2010-02-10: UdevDb.txt		#

• UdevDb.txt Edit (124.4 KiB, text/plain)			
isweiss (julienweiss) wrote on 2010-02-10: UdevLog.txt			# 1 2 3 4 5 6 7 8 9 10
• UdevLog.txt Edit (232.1 KiB, text/plain)			
isweiss (julienweiss) wrote on 2010-02-10: Xsession-Errors.txt			# 1 2 3 4 5 6 7 8 9 10
• XsessionErrors.txt Edit (3.2 KiB, text/plain)			

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 19 of 57

<pre> Changed in linux (Ubuntu): sta- Incomplete → New here: tags : added: apport-collected Jeremy Foshee (jeremyfoshee) on 2010-02-10 tags : added: karmic </pre>			
dave945 (dave-dtabor) wrote on 2010-02-17:			# 1 2 3 4 5 6 7 8 9 10
<p>I think I may have the same or a similar bug. Ubuntu Karmic was working very well until yesterday and think a kernel patch may have done me in. Here's the info I have:</p>			
dave945 (dave-dtabor) wrote on 2010-02-17:			# 1 2 3 4 5 6 7 8 9 10
• laptop-diags.txt Edit (9.4 KiB, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02-17: apport-collect data			# 1 2 3 4 5 6 7 8 9 10
<pre> Architecture: i386 ArecordDevices: **** List of CAPTURE Hardware Devices **** card 0: Intel [HDA Intel], device 0: CONEXANT Analog [CONEXANT Analog] Subdevices: 1/1 Subdevice #0: subdevice #0 Au- dioDevicesInUse: USER PID ACCESS COMMAND /dev/snd/controlC0: tabord 1998 F... pulseaudio CRDA: Error: [Errno 2] No such file or directory Card0.Amixer.info: Card hw:0 'Intel'/'HDA Intel at 0xfc220000 irq 17' Mixer name : 'Conexant CX20561 (Hermosa)' Components : 'HDA:14f15051,17aa2100,00100000 HDA:14f12c06,17aa2122,00100000' Controls : 14 Simple ctrls : 7 CheckboxSubmission: 78f0d12e26671bc09b495230bb082922 CheckboxSystem: bb422ca46d02494cdb459927a98bc2f DistroRelease: Ubuntu 9.10 HibernationDevice: RE- SUME=UUID=0a6b324d-4259-494d-945f-5fd16b10475c InstallationMedia: Ubuntu 9.10 "Karmic Koala" - Release i386 (20091028.5) MachineType: LENOVO 20823GU Package: linux (not installed) PccardctlI- dent: Socket 0: no product info available PccardctlStatus: Socket 0: no card ProcCmdLine: </pre>			

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 20 of 57

BOOT_IMAGE=/boot/vmlinuz-2.6.31-19-generic root=UUID=4eca727b-6dec-49c4-931c-7cd930d4675e ro

```

quiet splash ProcEnviron: SHELL=/bin/bash LANG=en_US.UTF-8 ProcVersionSignature: Ubuntu
2.6.31-19.56-generic RelatedPackageVersions: linux-backports-modules-2.6.31-19-generic N/A linux-
firmware 1.25 Uname: Linux 2.6.31-19-generic i686 UserGroups: adm admin cdrom dialout lpadmin plug-
dev sambashare dmi.bios.date: 04/22/2009 dmi.bios.vendor: LENOVO dmi.bios.version: 7VET66WW
(2.16 ) dmi.board.name: 20823GU dmi.board.vendor: LENOVO dmi.board.version: Not Availa-
ble dmi.chassis.asset.tag: No Asset Information dmi.chassis.type: 10 dmi.chassis.vendor:
LENOVO dmi.chassis.version: Not Available dmi.modalias:
dmi:bvnLENOVO:bvr7VET66WW(2.16):bd04/22/2009:svnLENOVO:pn20823GU:pvrThink-
PadT500:rvnLENOVO:rn20823GU:rvrNotAvailable:cvnLENOVO:ct10:cvrNotAvailable: dmi.product.name:
20823GU dmi.product.version: ThinkPad T500 dmi.sys.vendor: LENOVO

```

dave945 (dave-dtabor) wrote on 2010-02-17: AlsaDe- vices.txt			# 2 / 7
* AlsaDevices.txt Edit (517 bytes, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02-17: AplayDe- vices.txt			# 1 0 1 0
* AplayDevices.txt Edit (281 bytes, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02- 17: BootDmesg.txt			# 1 0 1 0
* BootDmesg.txt Edit (63.6 KiB, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02- 17: Card0.Amixer.values.txt			# 1 0 1 0
* Card0.Amixer.values.txt Edit (1.5 KiB, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02- 17: Card0.Codecs.codec.0.txt			# 1 0 1 0
* Card0.Codecs.codec.0.txt Edit (5.0 KiB, text/plain)			

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 21 of 57

dave945 (dave-dtabor) wrote on 2010-02- 17: Card0.Codecs.codec.1.txt			# 1 0 1 0
* Card0.Codecs.codec.1.txt Edit (146 bytes, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02-17: Cur- rentDmesg.txt			# 1 0 1 0
* CurrentDmesg.txt Edit (15.5 KiB, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02-17: IwCon- fig.txt			# 1 0 1 0
* IwConfig.txt Edit (567 bytes, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02-17: Lspci.txt			# 1 0 1 0
* Lspci.txt Edit (19.3 KiB, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02-17: Lusb.txt			#

			#100
• Lsub.txt Edit (719 bytes, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02-17: PciMulti-media.txt			#101
• PciMultimedia.txt Edit (588 bytes, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02-17: ProcCpuinfo.txt			#102
• ProcCpuinfo.txt Edit (1.4 KiB, text/plain)			

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 22 of 57

dave945 (dave-dtabor) wrote on 2010-02-17: ProcInterrupts.txt			#103
• ProcInterrupts.txt Edit (1.7 KiB, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02-17: ProcModules.txt			#104
• ProcModules.txt Edit (3.2 KiB, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02-17: RfKill.txt			#105
• RfKill.txt Edit (182 bytes, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02-17: UdevDb.txt			#106
• UdevDb.txt Edit (120.1 KiB, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02-17: UdevLog.txt			#4 3
• UdevLog.txt Edit (250.8 KiB, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02-17: WifiSyslog.txt			#107
• WifiSyslog.txt Edit (426.1 KiB, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02-17: XsessionErrors.txt			#108
• XsessionErrors.txt Edit (1.1 KiB, text/plain)			
dave945 (dave-dtabor) wrote on 2010-02-17:			#109

			6						
<p>* laptop-diags.txt Edit (9.4 KiB, text/plain) this is a lenovo T500 laptop that dual-boots Ubuntu 9.10 Karmic and.. and ... W... W... Windows Visssss ta Vista, which DOES connect to my network. The Wireless access point is an apple airport base station extreme 802.11b/g/n of recent vintage. Dave</p>									
dave945 (dave-dtabor) wrote on 2010-02-17:			#4171						
<p>* laptop-diags.txt Edit (9.4 KiB, text/plain) this is a lenovo T500 laptop that dual-boots Ubuntu 9.10 Karmic and.. and ... W... W... Windows Visssss ta Vista, which DOES connect to my network. The Wireless access point is an apple airport base station extreme 802.11b/g/n of recent vintage. Dave</p>									
Russell Robinson (russellr-openconcepts) wrote on 2010-02-17:			#14101						
<p>Similar problem on Dell Latitude E6500. /var/log/messages message is: ADDRCONF(NETDEV_UP): wlan0: link is not ready Didn't happen in Jaunty - only since upgrading to Karmic, and then only recently (last week or so). Recent kernel update?</p>									
jsweiss (julienweiss) wrote on 2010-02-17: Re: [Bug 518196] Re: Intel iwlag driver hangs from time that time			#14101						
<p>Forgot to mention the AP is a HUAWAI D100 router. But I guess it is not too important, as I have a Nokia phone, another laptop and this same laptop on Windows with no issues. Also I have not tried other Linux distributions, as the laptop is new.</p>									
Jeremy Foshee (jeremyfoshee) wrote on 2010-02-25:			#14101						
<p>set to triaged with a low initial importance. This has been added to my list for review. -JFo</p> <table border="1"> <tr> <td colspan="2">Changed in linux (Ubuntu):</td> </tr> <tr> <td>status :</td> <td>New → Triaged</td> </tr> <tr> <td>importance :</td> <td>Undecided → Low</td> </tr> </table> <p>Jeremy Foshee (jeremyfoshee) on 2010-02-25 tags : added: regression-potential</p>				Changed in linux (Ubuntu):		status :	New → Triaged	importance :	Undecided → Low
Changed in linux (Ubuntu):									
status :	New → Triaged								
importance :	Undecided → Low								

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 24 of 57

Chase Douglas (chasedouglas) wrote on 2010-02-26:			#51
<p>Could anyone affected please test two things:</p> <ol style="list-style-type: none"> linux-backports-modules-wireless-karmic-generic (newer versions of the wireless drivers) <ol style="list-style-type: none"> Go to System -> Administration -> Software Sources Ensure the box for "Community-maintained Open Source software (universe)" is checked Install the linux-backports-modules-wireless-karmic-generic (either through apt-get install or through Synaptic Package Manager) Restart and test the new drivers Lucid <ol style="list-style-type: none"> Download one of the daily lucid isos from http://cdimage.ubuntu.com/daily-live/current/ and test this in Lucid (you don't need to install it, just boot it up to test) <p>If either of these seems to have the issue fixed we can then begin to focus on finding a particular patch to it fix the issue. Thank you</p>			
dave945 (dave-dtabor) wrote on 2010-02-27:			#14101
<p>Download full text (20.9 KiB) This did not get it working for me. Strangely, if I boot with a wired connection, my wireless works, even if I disconnect eth0: Feb 27 17:02:19 tabord-laptop kernel: [14.108311] ADDRCONF(NETDEV_UP): eth0: link is not ready Feb 27 17:02:19 tabord-laptop kernel: [14.109658] iwlagm 0000:03:00:0: firmware: requesting lbm-iwlwifi-5000-</p>			


```

2. ucode Feb 27 17:02:19 tabord-laptop kernel: [ 14.2533] Calling country code file firmware/ibm-
ibm-iwlwifi-5000-1. ucode Feb 27 17:02:19 tabord-laptop kernel: [ 14.249646] iwlnagn 0000:03:00:0: loaded
firmware version 8.24.2.12 Feb 27 17:02:19 tabord-laptop kernel: [ 14.397123] Registered led device: iwl-
phy0::radio Feb 27 17:02:19 tabord-laptop kernel: [ 14.397141] Registered led device: iwl-phy0::as-
soc Feb 27 17:02:19 tabord-laptop kernel: [ 14.397156] Registered led device: iwl-phy0::RX Feb 27
17:02:19 tabord-laptop kernel: [ 14.397169] Registered led device: iwl-phy0::TX Feb 27 17:02:19 tabord-
laptop kernel: [ 14.416539] ADDRCONF(NETDEV_UP): wlan0: link is not ready Feb 27 17:02:19 tabord-
laptop kernel: [ 14.499530] mtrr: no more MTRRs available Feb 27 17:02:19 tabord-laptop kernel:
[ 14.499583] mtrr: no more MTRRs available Feb 27 17:02:20 tabord-laptop kernel: [ 15.470226] Blue-
tooth: BNEP (Ethernet Emulation) ver 1.3 Feb 27 17:02:20 tabord-laptop kernel: [ 15.470229] Bluetooth:
BNEP filters: protocol multicast Feb 27 17:02:20 tabord-laptop kernel: [ 15.475449] Bridge firewalling reg-
istered Feb 27 17:02:20 tabord-laptop kernel: [ 15.534876] ppdev: user-space parallel port driver Feb 27
17:02:22 tabord-laptop kernel: [ 17.317221] e1000e: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow
Control: RX/TX Feb 27 17:02:22 tabord-laptop kernel: [ 17.317395] ADDRCONF(NETDEV_CHANGE):
eth0: link becomes ready Feb 27 17:02:26 tabord-laptop kernel: [ 21.242404] IBM TrackPoint firmware:
0x0e, buttons: 3/3 Feb 27 17:02:26 tabord-laptop kernel: [ 21.482140] input: TPPS/2 IBM TrackPoint as
/devices/platform/i8042/serio1/serio2/input/input15 Feb 27 17:02:43 tabord-laptop kernel:
[ 38.318873] ADDRCONF(NETDEV_CHANGE): wlan0: link becomes ready Feb 27 17:02:43 tabord-lap-
top kernel: [ 38.318905] cfg80211: Calling CRDA for country: US Feb 27 17:02:43 tabord-laptop kernel:
[ 38.320698] cfg80211: Regulatory domain: US Feb 27 17:02:43 tabord-laptop kernel: [ 38.320700]

```

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 25 of 57

```

(start_freq - end_freq @ bandwidth), (max_antenna_gain, max_eirp) Feb 27 17:02:43 tabord-laptop ker-
nel: [ 38.320703] (5170000 KHz - 5250000 KHz @ 40000 KHz), (10000 mBi, 10000 mBm) Feb 27 17:02:43
tabord-laptop kernel: [ 38.320706] (5735000 KHz - 5835000 KHz @ 40000 KHz), (10000 mBi, 10000
mBm) Feb 27 17:02:43 tabord-laptop kernel: [ 38.320709] cfg80211: Regulatory domain: US Feb 27
17:02:43 tabord-laptop kernel: [ 38.320711] (start_freq - end_freq @ bandwidth), (max_antenna_gair,
max_eirp) Feb 27 17:02:43 tabord-laptop kernel: [ 38.320713] (2402000 KHz - 2472000 KHz @ 40000
KHz), (300 mBi, 2700 mBm) Feb 27 17:02:43 tabord-laptop kernel: [ 38.320716] (517...

```

[dave945 \(dave-dtabor\)](#) wrote on 2010-02-27:

[Download full text \(34.6 KiB\)](#)

After unplugging eth0, wlan0 runs for about a minute then quits. Here is the sequence of events:

```

Feb 27 17:31:43 tabord-laptop kernel: [ 47.352057] wlan0: no IPv6 routers present Feb 27 17:31:50 tabord-
laptop kernel: [ 54.364177] e1000e: eth0 NIC Link is Down Feb 27 17:31:50 tabord-laptop NetworkMan-
ager: <info> (eth0): carrier now OFF (device state 8, deferring action for 4 seconds) Feb 27 17:31:55
tabord-laptop NetworkManager: <info> (eth0): device state change: 8 -> 2 (reason 40) Feb 27 17:31:55
tabord-laptop NetworkManager: <info> (eth0): deactivating device (reason: 40). Feb 27 17:31:55 tabord-
laptop NetworkManager: <info> (eth0): canceled DHCP transaction, dhcp client pid 1794 Feb 27 17:31:55
tabord-laptop NetworkManager: <WARN> check_one_route(): (eth0) error -34 returned from
rtnL_route_del(): Success#012 Feb 27 17:31:55 tabord-laptop avahi-daemon[968]: Withdrawing address
record for 10.0.1.17 on eth0. Feb 27 17:31:55 tabord-laptop avahi-daemon[968]: Leaving mDNS multicast
group on interface eth0.IPv4 with address 10.0.1.17. Feb 27 17:31:55 tabord-laptop avahi-daemon[968]:
Interface eth0.IPv4 no longer relevant for mDNS. Feb 27 17:31:55 tabord-laptop NetworkManager: <info>
Policy set 'Auto Tabor (5 GHz)' (wlan0) as default for routing and DNS. Feb 27 17:32:04 tabord-laptop
wpa_supplicant[1356]: CTRL-EVENT-SCAN-RESULTS Feb 27 17:32:28 tabord-laptop anacron[2450]:
Anacron 2.3 started on 2010-02-27 Feb 27 17:32:28 tabord-laptop anacron[2450]: Normal exit (0 jobs
run) Feb 27 17:32:28 tabord-laptop kernel: [ 91.927340] CPU0 attaching NULL sched-domain. February 27
17:32:28 tabord-laptop kernel: [ 91.927344] CPU1 attaching NULL sched-domain. Feb 27 17:32:28 tabord-
laptop kernel: [ 91.934050] thinkpad_acpi: EC reports that Thermal Table has changed Feb 27 17:32:28
tabord-laptop kernel: [ 91.940567] CPU0 attaching sched-domain: Feb 27 17:32:28 tabord-laptop kernel:
[ 91.940570] domain 0: span 0-1 level MC Feb 27 17:32:28 tabord-laptop kernel: [ 91.940572] groups: 0
1 Feb 27 17:32:28 tabord-laptop kernel: [ 91.940576] CPU1 attaching sched-domain: Feb 27 17:32:28
tabord-laptop kernel: [ 91.940577] domain 0: span 0-1 level MC Feb 27 17:32:28 tabord-laptop kernel:
[ 91.940579] groups: 1 0 Feb 27 17:32:44 tabord-laptop wpa_supplicant[1356]: CTRL-EVENT-SCAN-RE-
SULTS Feb 27 17:32:44 tabord-laptop wpa_supplicant[1356]: Trying to associate with 00:1f:f3:f8:a1:db
(SSID='Tabor (5 GHz)' freq=5745 MHz) Feb 27 17:32:44 tabord-laptop NetworkManager: <info> (wlan0):
supplicant connection state: completed -> associating Feb 27 17:32:44 tabord-laptop wpa_suppli-
cant[1356]: CTRL-EVENT-DISCONNECTED - Disconnect event - remove keys Feb 27 17:32:44 tabord-
laptop NetworkManager: <info> (wlan0): supplicant connection state: associating -> disconnected Feb 27
17:32:44 tabord-laptop kernel: [ 107.648220] wlan0: deauthenticating from f8:1e:df:fa:e6:1c by local choice
(reason=3) Feb 27 17:32:44 tabord-laptop kernel: [ 107.651297] wlan0: direct probe to AP 00:1f:f3:f8:a1:db
(tr try 1) Feb 27 17:32:44 tabord-laptop kernel: [ 107.652818] wlan0: direct probe responded Feb 27 17:32:44
tabord-laptop kernel: [ 107.652825] wlan0: authenticate w...

```

<p>dave945 (dave-dtabor) wrote on 2010-02-28:</p>			#10111
<p>Download full text (44.9 KiB) This time, I booted to linux and it worked (don't know for how long it will last):</p> <pre>Feb 27 22:45:43 tabord-laptop kernel: [12.470749] iwlag: Intel(R) Wireless WiFi Link AGN driver for Linux, 1.3.27ks Feb 27 22:45:43 tabord-laptop kernel: [12.470752] iwlag: Copyright(c) 2003-2009 Intel Corporation Feb 27 22:45:43 tabord-laptop kernel: [12.470830] iwlag: 0000:03:00:0: PCI INT A -> GSI 17 (level, low) -> IRQ 17 Feb 27 22:45:43 tabord-laptop kernel: [12.470906] iwlag: 0000:03:00:0: Detected Intel Wireless WiFi Link 5100AGN REV=0x54 Feb 27 22:45:43 tabord-laptop kernel: [12.513637] iwlag: 0000:03:00:0: Tunable channels: 13 802.11bg, 24 802.11a channels Feb 27 22:45:43 tabord-laptop kernel: [12.547322] input: HDA Intel Headphone as /devices/pci0000:00/0000:00:1b.0/sound/card0/input10 Feb 27 22:45:43 tabord-laptop kernel: [12.547382] input: HDA Intel Mic as /devices/pci0000:00/0000:00:1b.0/sound/card0/input11 Feb 27 22:45:43 tabord-laptop kernel: [12.547429] input: HDA Intel Mic as /devices/pci0000:00/0000:00:1b.0/sound/card0/input12 Feb 27 22:45:43 tabord-laptop kernel: [12.547473] input: HDA Intel Headphone as /devices/pci0000:00/0000:00:1b.0/sound/card0/input13 Feb 27 22:45:43 tabord-laptop kernel: [12.720221] pcmcia_socket pcmcia_socket0: cs: IO port probe 0x100-0x3af: clean. Feb 27 22:45:43 tabord-laptop kernel: [12.721953] pcmcia_socket pcmcia_socket0: cs: IO port probe 0x3e0-0x4ff: excluding 0x4d0-0x4d7 Feb 27 22:45:43 tabord-laptop kernel: [12.722685] pcmcia_socket pcmcia_socket0: cs: IO port probe 0x820-0x8ff: clean. Feb 27 22:45:43 tabord-laptop kernel: [12.723262] pcmcia_socket pcmcia_socket0: cs: IO port probe 0xc00-0xcf7: clean. Feb 27 22:45:43 tabord-laptop kernel: [12.723993] pcmcia_socket pcmcia_socket0: cs: IO port probe 0xa00-0xaff: clean. Feb 27 22:45:43 tabord-laptop kernel: [12.816328] ADDRCONF(NETDEV_UP): eth0: link is not ready Feb 27 22:45:43 tabord-laptop kernel: [12.817604] iwlag: 0000:03:00:0: firmware: requesting lbm-iwlwifi-5000-2.ucode Feb 27 22:45:43 tabord-laptop kernel: [12.860701] iwlag: 0000:03:00:0: firmware: requesting lbm-iwlwifi-5000-1.ucode Feb 27 22:45:43 tabord-laptop kernel: [12.934285] Synaptics Touchpad, model: 1, fw: 7.0, id: 0x1c0b1, caps: 0xd04791/0xb00000 Feb 27 22:45:43 tabord-laptop kernel: [12.934290] serio: Synaptics pass-through port at isa0060/serio1/input0 Feb 27 22:45:43 tabord-laptop kernel: [12.949384] iwlag: 0000:03:00:0: loaded firmware version 8.24.2.12 Feb 27 22:45:43 tabord-laptop kernel: [13.000010] input: SynPS/2 Synaptics TouchPad as /devices/platform/i8042/serio1/input/input14 Feb 27 22:45:43 tabord-laptop kernel: [13.058703] usb 4-2: new full speed USB device using uhci_hcd and address 3 Feb 27 22:45:43 tabord-laptop kernel: [13.098558] Registered led device: iwl-phy0::radio Feb 27 22:45:43 tabord-laptop kernel: [13.098574] Registered led device: iwl-phy0::assoc Feb 27 22:45:43 tabord-laptop kernel: [13.098588] Registered led device: iwl-phy0::RX Feb 27 22:45:43 tabord-laptop ke...</pre>			
<p>Chase Douglas (chasedouglas) wrote on 2010-03-01:</p>			#10111
<p>@dave945: There's something interesting in your logs. Both boot dmesg logs when the wireless wasn't working properly had loaded the iwlwifi-5000-2.ucode properly. When you installed the linux-backports-modules package it</p>			

<p>started to look for lbm-iwlwifi-5000-2.ucode firmware file instead (note the prefixed "lbm-"). It then fell back to lbm-iwlwifi-5000-1.ucode, which it found. I am wondering if this is a firmware issue.</p> <p>By default you should have both iwlwifi-5000-1.ucode and iwlwifi-5000-2.ucode in /lib/firmware/. Assuming you do, try the following test:</p> <ol style="list-style-type: none"> 1. move /lib/firmware/iwlwifi-5000-2.ucode to /lib/firmware/iwlwifi-5000-2.ucode.backup 2. restart <p>If it gets better, do the opposite. Move the ucode file back to where it was and then restart to confirm that the wireless behaves poorly again. Please post your results in this bug report.</p> <p>Thank you</p>			
<p>Changed in linux (Ubuntu):</p> <p>status : Triaged → Incomplete</p>			
<p>dave945 (dave-dtabor) wrote on 2010-03-02:</p>			#56
<p>Chase, Thanks for the tip. I did as you suggested. I renamed the file and restarted the laptop and networking worked. Then I named it back and rebooted: no wlan0. Feeling we were on to something, I renamed the file back to .backup and rebooted thinking to write in and report a positive diagnosis. Unfortunately, wlan0 is still not functioning, even though it appears to be OK as reported by syslog. This makes me wonder if (a) it could be hardware, or (b) if the driver could have messed up the hardware. As an additional data point Windows Vista on this same laptop which has always connected before, stopped working today. Thanks Dave</p>			

PS: let me know if you would like me to upload any logs.
 Oh, also, you mentioned lbm-prefixed drivers in your previous note. I don't seem to have any. here's what i have:

```
tabord@tabord-laptop:/lib/firmware$ ls -lart *iwlwifi* -rw-r--r-- 1 root root 459992 2009-11-30 06:29 iwlwifi-6000-4.ucode -rw-r--r-- 1 root root 337400 2009-11-30 06:29 iwlwifi-5150-2.ucode -rw-r--r-- 1 root root 353240 2009-11-30 06:29 iwlwifi-5000-2.ucode.backup -rw-r--r-- 1 root root 345008 2009-11-30 06:29 iwlwifi-5000-1.ucode -rwxr-xr-x 1 root root 187972 2009-11-30 06:29 iwlwifi-4965-2.ucode -rw-r--r-- 1 root root 187608 2009-11-30 06:29 iwlwifi-4965-1.ucode -rwxr-xr-x 1 root root 150100 2009-11-30 06:29 iwlwifi-3945-2.ucode -rw-r--r-- 1 root root 149652 2009-11-30 06:29 iwlwifi-3945-1.ucode -rw-r--r-- 1 root root 335056 2009-11-30 06:29 iwlwifi-1000-3.ucode
tabord@tabord-laptop:/lib/firmware$ ls -lart lbm* ls: cannot access lbm*: No such file or directory
```

Chase Douglas (chasedouglas) wrote on 2010-03-02:			#10101
---	--	--	--------

@dave945:
 Please attach a dmesg log now. I'd like to see what's in the log now that wifi isn't working.
 Also, try running 'rfkill list'. Maybe something (perhaps windows?) set a block.

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 28 of 57

dave945 (dave-dtabor) wrote on 2010-03-03:			#10101
--	--	--	--------

```
* dmesg Edit (64.0 KiB, text/plain)
Chase, tabord@tabord-laptop:~$ rfkill list 0: tpacpi_bluetooth_sw: Bluetooth Soft blocked: no Hard blocked: no 1: phy0: Wireless LAN Soft blocked: no Hard blocked: no 2: hci0: Bluetooth Soft blocked: no Hard blocked: no

Also, Vista wifi is working today. I will attach /var/log/dmesg

Thanks, David
```

Chase Douglas (chasedouglas) wrote on 2010-03-03:			#10101
---	--	--	--------

@dave945:
 Something odd is going on here. In the first dmesg where things started to work, the -2 firmware wasn't found and the following was output:

```
Feb 27 22:45:43 tabord-laptop kernel: [ 12.817604] iwlagnd 0000:03:00:0: firmware: requesting lbm-iwlwifi-5000-2.ucode Feb 27 22:45:43 tabord-laptop firmware.sh[1074]: Cannot find firmware file 'lbn-iwlwifi-5000-2.ucode' Feb 27 22:45:43 tabord-laptop kernel: [ 12.860701] iwlagnd 0000:03:00:0: firmware: requesting lbn-iwlwifi-5000-1.ucode Feb 27 22:45:43 tabord-laptop kernel: [ 12.949384] iwlagnd 0000:03:00:0: loaded firmware version 8.24.2.12
```

However, in your last dmesg (where things are broken), we see:

```
[ 12.917423] iwlagnd 0000:03:00:0: firmware: requesting lbn-iwlwifi-5000-2.ucode [ 12.938337] iwlagnd 0000:03:00:0: lbn-iwlwifi-5000-2.ucode firmware file req failed: -2 [ 12.938341] iwlagnd 0000:03:00:0: firmware: requesting lbn-iwlwifi-5000-1.ucode [ 13.049180] iwlagnd 0000:03:00:0: Loaded firmware lbn-iwlwifi-5000-1.ucode, which is deprecated. Please use API v2 instead. [ 13.049185] iwlagnd 0000:03:00:0: loaded firmware version 8.24.2.12
```

Note that in this log we see it complain about how the -1 ucode is deprecated. If the same driver was used in both tests, we should see the message output in both logs. Do you know if the driver itself has changed between these tests? Did you update your kernel or linux-backports-modules?

dave945 (dave-dtabor) wrote on 2010-03-04:			#10101
--	--	--	--------

Chase, I haven't updated anything, but I see your point. Should I install linux-backports again? Thanks Dave

On 3/3/2010 9:41 AM, Chase Douglas wrote: [...]

<p>Chase Douglas (chasedouglas) wrote on 2010-03-04:</p>			#1014
<p>@dave945:</p> <p><i>I'm not really sure what the best way forward is now. You can try various combinations of firmware and drivers to see if anything works, and if you find anything be sure to let us know. The latest compat-wireless tree may include some fixes that affect you. Some newer drivers can be found in the linux-backports-modules package available in the karmic pre-proposed ppa: https://launchpad.net/~kernel-ppa/+archive/pre-proposed/.</i></p> <p><i>However, your issues are a little beyond my experience. I suggest going through the documentation at http://linuxwireless.org/en/users/Documentation/Reporting_bugs to check some more variables and then report a bug to the linux-wireless mailing list. If you report a bug to the mailing list, please include a link to your message in a comment here.</i></p>			
<p>jsweiss (juliensweiss) wrote on 2010-03-05:</p>			#1015
<p>Hello,</p> <p><i>Tried all the firmware images, with the same result. Also tried ndiswrapper, but it looks like this driver is not supported.</i></p> <p><i>However, i tried a different thing ... i changed on the wifi router (Huawei D100) the WiFi security settings from Encryption mode : WPA-PSK, WPA Encryption: TKIP to WPA2-PSK, Encryption AES. I don't know if this is the reason, but until now, everything looks good. I also changed the firmware to the latest version (8.24.2.12). Ill post back after I test it for more time, as the problem usually appears totally random (sometimes once or twice in 2, 3 days, other times twice in 10 minutes). The Huawei router is also Linux based</i></p> <p><i>for more details you can check the Huawei website. Note: I have also been for 3 days in a hotel which had a wifi hotspot that was totally open, and it worked without any problems ...</i></p> <p><i>JChase Douglas wrote: [...]</i></p>			
<p>Chase Douglas (chasedouglas) wrote on 2010-03-05:</p>			#1016

<p>@jsweiss:</p> <p><i>Thanks for that input. There are often issues with various combinations of wireless cards and routers. That's it something we should always keep in mind when we are working on wireless issues. I'm sure others have brands they like, but I try to use Apple routers personally because they seem to be the most compatible and stable brand of routers I've ever used.</i></p>			
<p>Chase Douglas (chasedouglas) wrote on 2010-03-05:</p>			#1017
<p>@dave945:</p> <p><i>Can you try what jsweiss has tried? First, trying to use WPA2-PSK using AES, and then trying other routers if possible?</i></p>			
<p>jsweiss (juliensweiss) wrote on 2010-03-05:</p>			#1018
<p>@Chase</p>			

True, I really didn't think about the router issue until now. To be honest, in Windows 7 I did not have the chance to try it too much, because i just deleted it and installed Linux ... I cannot use an Apple router, as i have a 3G/WCDMA connection and so far the Huawei router makes sense. I will switch to an Option router soon, which has the same features and as I understand, it is a lot better (and quite more expensive).

If this change does not work, the next on the list is a Netgear 3G/UMTS router which I have handy (got it in the store and can take it back in 2 weeks if its not good). But I hope that for now I solved the issue with the WPA2-PSK - AES combination.

I don't know if my issue is similar to Dave's issue, as for him there were instances when the wifi did not work at all ... For me it worked all the time, and died at random periods of time, as explained.

I will keep on testing, and keep everyone updated, this might not be a module/firmware issue after all ...

J

Chase Douglas wrote: > @jsweiss: >> Thanks for that input. There are often issues with various combinations > of wireless cards and routers. That's something we should always keep in > mind when we are working on wireless issues. I'm sure others have brands > they like, but I try to use Apple routers personally because they seem > to be the most compatible and stable brand of routers I've ever used. >>

[jsweiss \(julienweiss\)](#) wrote on 2010-03-05:

Chase:

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 31 of 57

Also, when I had a DSL or Cable connection, the Linksys routers looked very good for me ... I do not remember the exact model, but it was a router with Gigabit ethernet, suitable for gaming, and was the only one that did not crash when used at full speed (6Mbit DSL) or when used with torrents ...

J

Chase Douglas wrote: > @jsweiss: >> Thanks for that input. There are often issues with various combinations > of wireless cards and routers. That's something we should always keep in > mind when we are working on wireless issues. I'm sure others have brands > they like, but I try to use Apple routers personally because they seem > to be the most compatible and stable brand of routers I've ever used. >>

[dave945 \(dave-dtabor\)](#) wrote on 2010-03-11:

@Chase, I switched my Apple Airport Base station extreme from WPA/WPA2 Personal to WPA2 Personal and booted from Windows Vista into Ubuntu Karmic. After unplugging the eth0 cable, the wlan0 connection is working. If memory serves, this would work for a little while and then go bad. So far however, this seems to be working! So to summarize, if we set the router to the highest level of security, the driver can connect. It's only in WPA "fallback mode" that the problem manifests.

```
13.852635] iwlag: Intel(R) Wireless WiFi Link AGN driver for Linux, 1.3.27ks [ 13.852638] iwlag: Copyright(c) 2003-2009 Intel Corporation [ 13.852702] iwlag: 0000:03:00:0: PCI INT A -> GSI 17 (level, low) -> IRQ 17 [ 13.852710] iwlag: 0000:03:00:0: setting latency timer to 64 [ 13.852733] iwlag: 0000:03:00:0: Detected Intel Wireless WiFi Link 5100AGN REV=0x54 [ 13.891900] iwlag: 0000:03:00:0: Tunable channels: 13 802.11bg, 24 802.11a channels [ 13.891959] alloc irq_desc for 33 on node -1 [ 13.891961] alloc kstat_irqs on node -1 [ 13.891979] iwlag: 0000:03:00:0: irq 33 for MSI/MSI-X [ 13.898444] phy0: Selected rate control algorithm 'iwl-agn-rs' [ 13.902784] pcmcia_socket pcmcia_socket0: cs: IO port probe 0x100-0x3af: clean. [ 13.907234] pcmcia_socket pcmcia_socket0: cs: IO port probe 0x3e0-0x4ff: excluding 0x4d0-0x4d7 [ 13.907930] pcmcia_socket pcmcia_socket0: cs: IO port probe 0x820-0x8ff: clean. [ 13.908582] pcmcia_socket pcmcia_socket0: cs: IO port probe 0xc00-0xcf7: clean. [ 13.909277] pcmcia_socket pcmcia_socket0: cs: IO port probe 0xa00-0xaff: clean. [ 14.011004] Synaptics Touchpad, model: 1, fw: 7.0, id: 0x1c0b1, caps: 0xd04791/0xb00000 [ 14.011014] serio: Synaptics pass-through port at isa0060/serio1/input0 [ 14.019469] EXT4-fs (sda5): internal journal on sda5:8 [ 14.052474] input: SynPS/2 Synaptics TouchPad as /devices/platform/i8042/serio1/input/input14 [ 14.228774] e1000e 0000:00:19:0: irq 31 for MSI/MSI-X [ 14.287750] e1000e 0000:00:19:0: irq 31 for MSI/MSI-X [ 14.287979] ADDRCONF(NETDEV_UP): eth0: link is not ready [ 14.289348] iwlag: 0000:03:00:0: firmware: requesting lbm-iwlfwifi-5000-2.ucode [ 14.304014] iwlag: 0000:03:00:0: lbm-iwlfwifi-5000-2.ucode firmware file req failed: -2 [ 14.304018] iwlag: 0000:03:00:0: firmware: requesting lbm-iwlfwifi-5000-1.ucode [ 14.329993] iwlag: 0000:03:00:0: Loaded firmware lbm-iwlfwifi-5000-1.ucode, which is deprecated. Please use API v2 instead. [ 14.329997] iwlag: 0000:03:00:0: loaded firmware version 8.24.2.12
```

I'm going to re-instate the lbm-iwlfwifi-5000-2.ucode firmware driver and see what happens...

Dave

Chase Douglas wrote: > @dave945: >> Can you try what jsweiss has tried? First, trying to use WPA2-

PSK using > AES, and then trying other routers if possible? > >									
jsweiss (juliensweiss) wrote on 2010-03-11:			#1010#						
Hello, Now testing with a Belkin wifi router, everything seems ok. Security is open.									
jsweiss (juliensweiss) wrote on 2010-04-05:			#1110#						
Hello, After extensive testing with various WiFi routers, I consider this issue resolved. I don't know about the others, but I am sure that my problem was a wrong combination of router and security settings. Me too don't know if this happens only on Linux or also on Windows, as I did not get to test the windows behavior for long, and the problem showed up at random times. Thanks everyone for the advice.									
On 03/05/2010 01:19 PM, Chase Douglas wrote: > @dave945: > > Can you try what jsweiss has tried? First, trying to use WPA2-PSK using > AES, and then trying other routers if possible? > >									
Scott Moser (smoser) wrote on 2010-04-14:			#1210#						
@Chase, I had previously seen this from time to time on Karmic, and still on lucid. It bit me twice today while I was away from the machine, someone had to reload modules for me. I use WEP auth, dd-wrt router (linksys wlan-54G). If you need anything, feel free to ping me and I can test.									
Jeremy Foshee (jeremyfoshee) wrote on 2010-06-14:			#1310#						
This bug report was marked as Incomplete and has not had any updated comments for quite some time. As a result this bug is being closed. Please reopen if this is still an issue in the current Ubuntu release http://www.ubuntu.com/getubuntu/download . Also, please be sure to provide any requested information that may have been missing. To reopen the bug, click on the current status under the Status column and change the status back to "New". Thank you.									
[This is an automated message. Apologies if it has reached you inappropriately? please just reply to this message indicating so.]									
<table border="1"> <tr> <td>tags :</td> <td>added: kj-expired</td> </tr> <tr> <td>Changed in linux (Ubuntu):</td> <td></td> </tr> <tr> <td>sta- here:</td> <td>Incomplete → Expired</td> </tr> </table>				tags :	added: kj-expired	Changed in linux (Ubuntu):		sta- here:	Incomplete → Expired
tags :	added: kj-expired								
Changed in linux (Ubuntu):									
sta- here:	Incomplete → Expired								

<p>Conclusions of search results analysis of nicknames "giulonline" and "juliensweiss"</p> <p>The following references were found for the nickname "giulonline":</p> <ul style="list-style-type: none"> - 2015: Sending messages to the Forum "avocatnet.ro" in order to search for information for the expansion in the form of a business of the animal farm that the questioner has in his possession. - 2017: Display of the nickname on the sites wex.nz and btceclub.ru – unspecified content-menu
--

The following references were found for the nickname "julienweiss":

- 2006: Posting on the "MovieChat" Forum about movie music compilations.
- 2008: Sending messages to the "linuxquestions.org" Forum about solving problems of server connectivity on the internet through the CentOS version 4.6.
- 2010: Registration of electronic program errors (bugs) on the platform "bugs.launchpad.net" on Linux – Ubuntu OS and extensive discussion with other users about solving online and offline connectivity issues correct operation of drivers.

4. What is and how does identity theft happen online?

Definition: Identity theft and identity fraud are catch-all terms the types of crimes in which someone illegally receives and uses personal

another person's data in some way that involves fraud or deception, usually for economic benefit.

Ways of online identity theft: There are various techniques of online identity theft identity which are directly related to the degree of technical knowledge of the internet safety of both the user and the perpetrator.

Such techniques may have little to no technical background but in others cases to make the most of available technology.

Indicative common methods:

- Phishing: The perpetrator sends the user - victim a deceptive message email or text or social media message that contains links that can be used to download malicious software. This software may mine personal data from your computer information and send it without the victim's knowledge to a remote computer operated by the perpetrator. In other cases the above links they lead to virtual websites that resemble legitimate ones and deceive the user to lead him to voluntarily enter personal information, as it has the impression that it is registering them on legitimate websites (eg a banking institution).
- Wi-Fi Hacking: Some public wireless network (Wi-Fi) connections may are not encrypted and this may allow an attacker to spy on and intercept data that a user sends or receives on his computer. A common practice requires perpetrators to create fake public connection points (Wi-Fi hotspots) with names that look like these of a legitimate network.

5. Any other observation in the field of your competence deemed useful for the case

Searching for domain names: _____

1. Related domain names:

Source: indictment domain name: "secure.net.im"

Secure.net.im
dawismultiservice.com
Dhplus.com
pkiplus.net

2. Date of last domain DNS changes:

Source: <https://whoisrequest.com/history/>

Dhplus.com 30 Aug, 2021
Pkiplus.net 30 Aug, 2021
dawismultiservice.com Mar 18, 2014

Source:
<https://dnshistory.org/historical-dns-records/soa/secure.net.im>

Secure.net.im
2021-04-25 -> 2021-06-25
2021-07-20 -> 2021-09-26

3. Associated ip addresses :

Central Source : Related domain names.

Source:
<https://www.robtx.com/ip-lookup/>

Source:
<https://www.robtx.com/dns-lookup/secure.net.im>

82.221.131.22 Iceland
dhplus.com
secure.net.im
ns1.pkiplus.net

82.221.131.23 Iceland
dawismultiservice.com

82.221.131.31 Iceland
mail.secure.net.im

182.237.0.79 Hong Kong
dns1.secure.net.im

182.237.0.80 Hong Kong
mx.dawismultiservice.com
ns2.pkiplus.net
mail.secure.net.im

37,228,129,228 Seychelles
is1.dhplus.com
ns2.pkiplus.net

37,228,129,229 Seychelles
ns1.pkiplus.net

37,228,129,230 Seychelles
dawismultiservice.com

82.103.128.249 Denmark
Ns3.pkiplus.net

209.200.231.56 United States
Ns3.pkiplus.net

Method

The domain name safe.net.im was searched for and from there it was associated and investigated each IP address and domain name.

The search was made in:

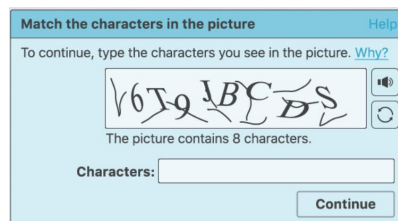
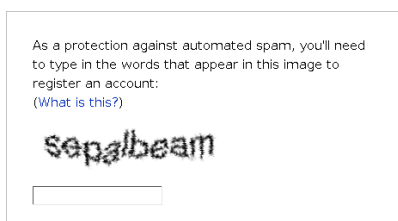
google.com, robtex.com, dnshistory.org and whoisrequest.com and all information on these the report is public information.

5.1 What is the captcha, which is in the process, why is it not overcome?

What is CAPTCHA?

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a mechanism used on websites on the internet usually when registration process of a user and allows the system to decide whether the registration it is done by a human or an automated system (computer).

Classic type CAPTCHAs were invented in 1997 and are still in use on some websites to this day, they ask users to identify a series distorted letters. The letters are distorted so bots don't they can recognize them. To pass the test, users must interpret the garbled text, to type the correct letters into a form field and submit the form. If the letters do not match, users are prompted to try again. Such CAPTCHAs are common in login forms, registration forms account, online polls and e-checkout pages trade.

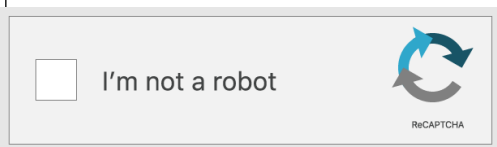
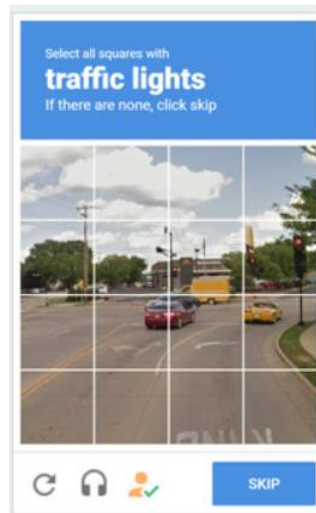


Indicative CAPTCHA examples

reCAPTCHAs are a free service offered by Google as a replacement for traditional CAPTCHAs. reCAPTCHA technology was acquired by Google in 2009.

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 38 of 57

reCAPTCHA is more advanced than standard CAPTCHA tests. Unlike the normal ones CAPTCHA, reCAPTCHA sources the text from real-world images: street address images, text from printed books, text from old newspapers etc.



Sample reCAPTCHA formats

reCAPTCHA also takes into account the movement of the user's cursor (mouse) as well as this is approaching the checkbox. Even the most immediate movement by a human being has some randomness at the microscopic level: tiny unconscious movements that the robots cannot be easily imitated. reCAPTCHA can also evaluate the cookies and history stored by her browser device to determine if the user is likely to be a bot. If the test still cannot determine whether the user is human or not, it may present an additional challenge such as the image recognition test. The most

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 39 of 57

modern forms of CAPTCHA, in combination with the above, also evaluate the general online user's behavior.

CAPTCHA Violation

There are three main categories of CAPTCHA breaking techniques:

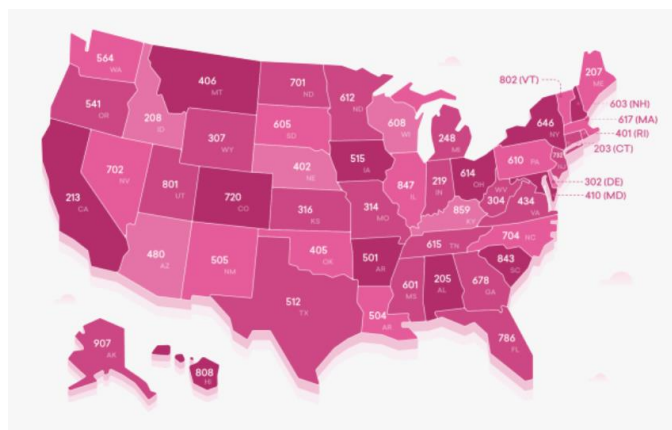
- The purchase and use of online bulk CAPTCHA solving services which they take advantage of low-cost human resources in developing countries and they create so-called "Click Farms" where a large number of workers is paid to manually click the required CAPTCHA tests.
- Exploiting developer errors when installing CAPTCHA on each application it is called upon to protect.
- The use of advanced artificial intelligence (AI) with "smart" programs that can "imitate" a person's way of thinking and functioning. The first successful demonstration of automated CAPTCHA solving took place in 2018 at the ACM CCS show. Earlier than this time, the necessary technology did not exist with significant rates successful resolution.

5.2 The process requires a mobile phone for each return. It becomes someone to get US mobile number online;

It is possible to get US mobile number online through various companies provide this service. These numbers are called "virtual phone numbers" and are available in specific countries depending on the respective provider. Basis of applicable law however, in order for a user to enter into a contract with one such company, should provide at least scanned copy of passport or national identity card and documents proving the place of residence of the user in question.

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 40 of 57

Obtaining a cell phone number in the US can also be done in person at relevant sales outlet. Each number contains within the digits the relevant code which corresponds to a specific area of the holder's place of residence.



Indicative area code footprint map of the US

For example, a resident of Manhattan, New York will receive a cell phone number with local code "212" etc.

5.3 Is a unique web browser fingerprint required for each return?

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 41 of 57

A device fingerprint, machine fingerprint, or fingerprint
A browser footprint is information collected about a computer for the purpose of its identification. This means that when a user connects to the Internet, the device it uses delivers a bundle of specific data on the download server about the websites you visit.

Browser fingerprinting is a powerful method that websites use to collect information about type and version of the browser, as well as the operating system, the active ones plugins, time zone, language, screen resolution and various other active settings.

Websites use the information that browsers provide for identifying unique users and tracking online behavior; their. This process is therefore called "program fingerprinting browsing".

In the case under consideration, the use of 200,000 different fingerprints is mentioned of device footprints, i.e. 200000 different ones would need to be used devices in order to have these elements and such a large number is extremely difficult to create artificially, without actually existing corresponding physical machines. (...)

5.4 Can the defendant's affiliation be confirmed?

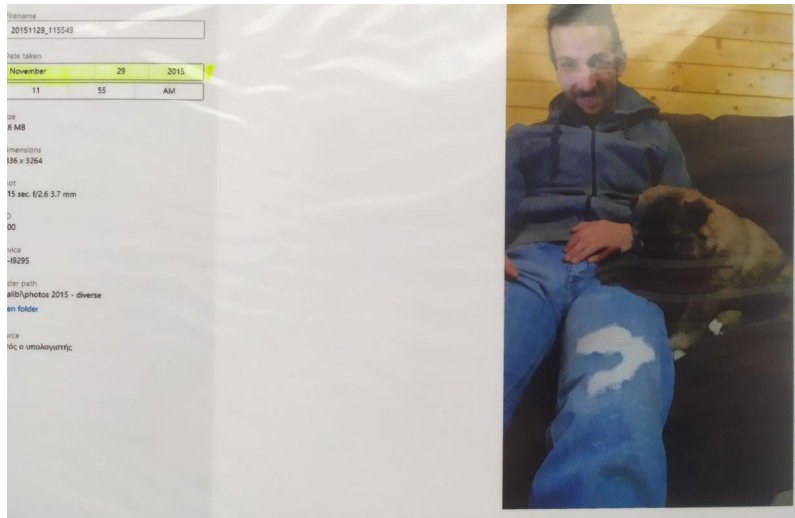
Are there any digital traces of the defendant's whereabouts at the time?

Series of photographs examined depict the defendant in Romania. Specifically, the metadata of the digital photos were examined. Metadata is a series of data stored within the digital file

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 42 of 57

photo and may contain, among other things, information about its time receiving it. The metadata of the digital photographs examined places the accused in Romania during the period 2014 -2016.





Indicative photograph of the defendant with metadata of date taken (left)

Digital photos registered in the "Google Photos" application were also examined which records the date the photo was taken/registered.

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 43 of 57



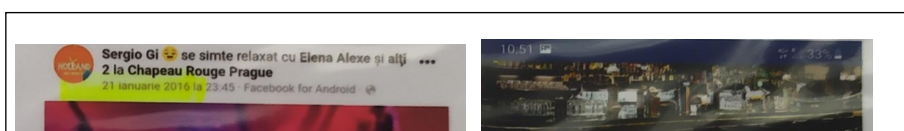
Sample Google Photos collection dated photos

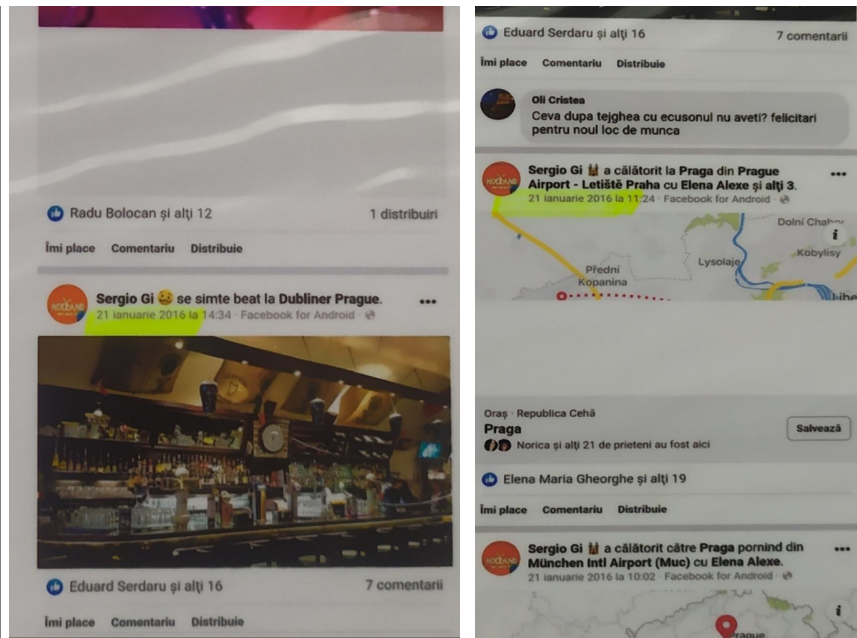
In addition, publications on social media (facebook) by personal account of the accused under the name "Sergio Gi". The publications in question they are dated and consist of photographs that place the accused in Romania during the period 2014-2016.



Indicative photo of a dated facebook post from the "Sergio Gi" account

In addition, publications were identified where the defendant has allowed the application of facebook to record its location footprint through the use of GPS and display map showing its location at the time of publication. The location places him in Prague on 21 January 2016.





Indicative posts with location tagging

5.5 Does the defendant have devices?

No, just a mobile phone with which the photos were taken in Romania, photos and dates on the drive.

5.6 What is the botnet cluster being accused of?

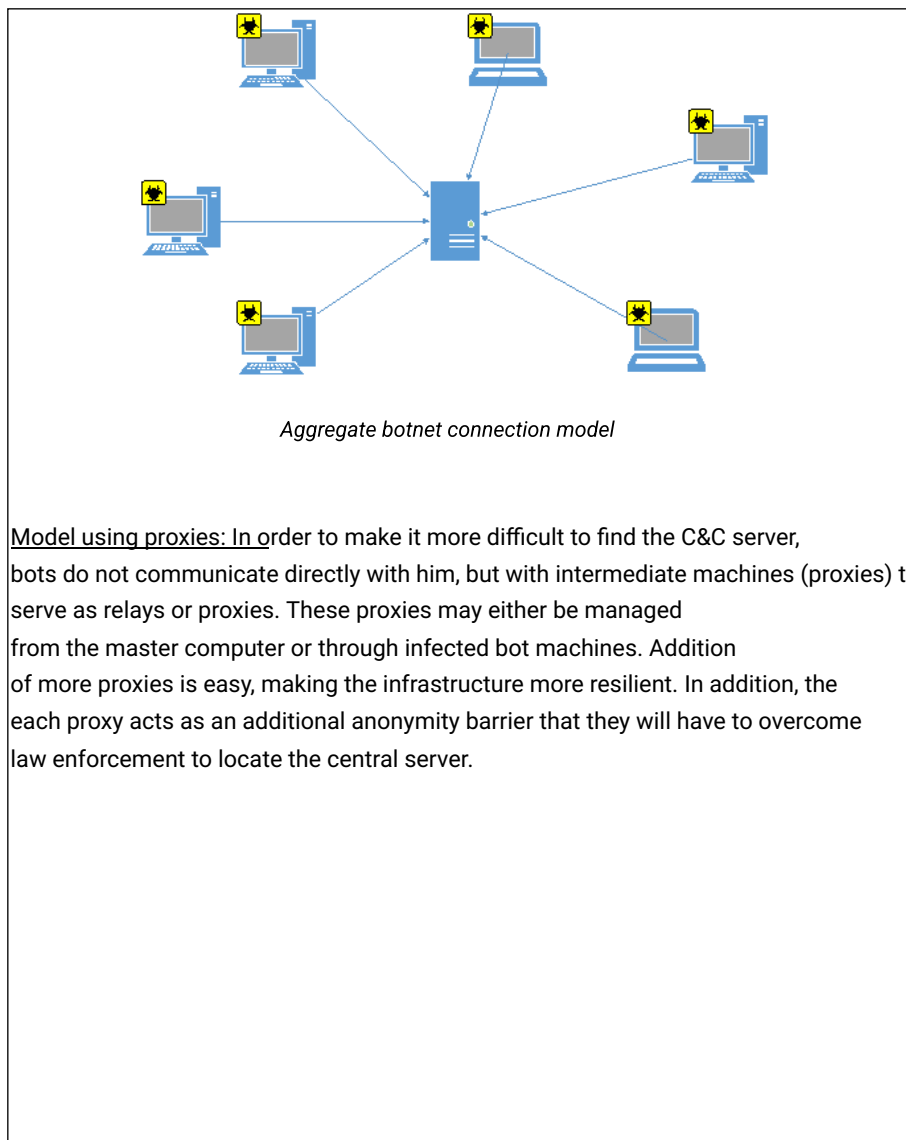
A botnet cluster or simply botnet ("bot network") is a network of computers that have infected by malware (bots) under the control of a single attacking party, known as a bot-herder. A bot is a piece of malware software that receives commands from a central computer (master) and once executed, it gives the bot-header the same access to the computer's resources as the real one its owner. Therefore bots can read and write files, execute programs, block keys, access camera, send email etc.

For this purpose, bots connect to Command and Control (C&C or CC or C2). There are various models of botnets.

Aggregate Model: This model is the oldest and simplest. Bots give

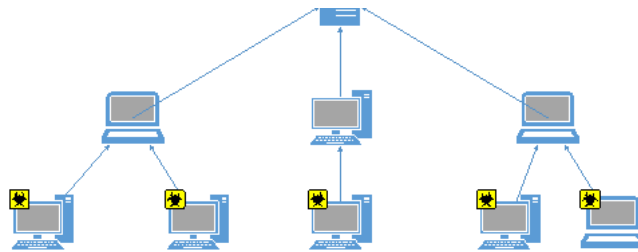
report periodically to a central server (server). Their disadvantage is that if it stops, to have the main server running, the bots are rendered useless. Also the use of a single server makes the botnet easier for law enforcement to detect.

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 47 of 57



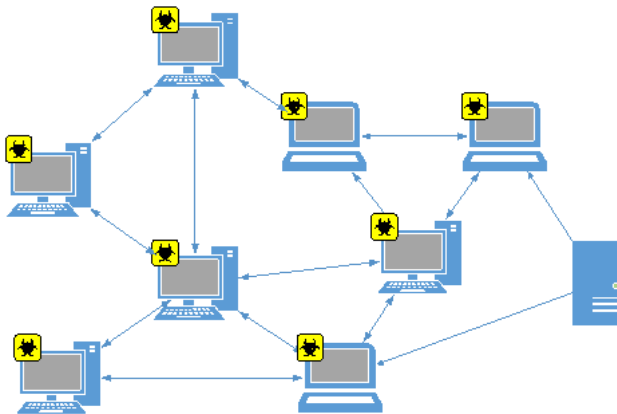
OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 48 of 57





Botnet me interface using proxies

Peer-to-peer model: It is the most sophisticated type of botnet architecture. Here the bots they communicate with each other and not with the C&C server. Information and commands control are propagated in the network from bot to bot. To maintain control of the botnet, the master it only needs to be able to communicate with any infected machine. This makes taking down the entire botnet very difficult.



Botnet interface with peer-to-peer model

The scale of a botnet (many consist of millions of bots) allows an attacker to performs large-scale actions. Since botnets remain under the control of a remote attacker, bots can receive updates and change the their behavior immediately.

Common botnet actions include:

- Spam e-mail: although e-mail considered today as an older form of attack, spam botnets are some of the larger in scope. They are mainly used for spamming, which often include malware. The Cutwail botnet, for example, can to send up to 74 billion messages per day. They are also used for bot propagation to recruit more computers into the botnet.
- DDoS attacks: leverage the massive scale of the botnet to overload a network or target server, making it inaccessible to users. DDoS attacks are targeted organizations for personal or political incentives or for ransom in exchange for its termination attack.
- Financial hacking: include botnets specifically designed for direct theft funds from businesses and credit card information. The finances

botnets, such as the ZeuS botnet, are responsible for attacks through which millions of dollars were stolen directly from multiple businesses in very short periods of time periods.

- Targeted intrusions: smaller botnets designed to specifically compromise high-value organization systems from which attackers can penetrate and to further invade the network. These intrusions are extremely dangerous for them organizations, as attackers specifically target their valuable assets; including financial data, research and development, the intellectual property and personal customer information.

6. What technical skills and knowledge does the cluster or botnet need?

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 50 of 57

To create a cluster/botnet one should have considerable technical computer knowledge above the average user.

- He should know techniques to disguise his online identity on the internet (e.g. by using sophisticated VPN services that offer significantly increased secrecy than average).
- He should find a reliable "host" to host the software that will control the botnet (either by hacking consecutive users or by paying companies with low oversight of it hosting content or in collaboration with "hosts" who offer pure hosting to illegal activities for large amounts and are only available in "underground" channels communication that the average user does not have access to).
- For secure communication with the "host" you need a sufficient number of domain names which allow DNS service control and true location masking techniques of the servers used (e.g. "fast flux" type)
- He should know how to handle the software he will handle and create the botnet that will either be bought or found with "cracked" passwords from channels of questionable legitimacy.
- He should know ways (eg phishing) to gain illegal access to PCs that will be used to build the botnet without being noticed.

In addition, it should be noted that for the organization and execution of an attack against the US IRS system, requires the creation and management of a large botnet range with sophisticated systems to avoid detection by law enforcement authorities. Those actions require not only increased expertise but also action through illegality organized cybercrime rings with strong internet connections "underworld" and access to capital to finance or finance services mediation, acquisition of required technical equipment, etc.

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 51 of 57

CONCLUSION - END

Internet research of the pseudonyms listed in the case file does not prove some involvement in illegal actions and the findings point to either conversations with other users for entertainment or to solve technical problems of their PC said user with the internet (connectivity, server operation, etc.) by use Linux operating systems.

No sign or trace associated with illegal internet was observed activities or an indication that the defendant possesses the necessary increased expertise create or operate a highly sophisticated botnet and perform illegal actions as described in the case file.

Messages about farm work don't show any effort obtaining information on the procedures of corporate and tax legislation of USA.

There is evidence placing the accused in Romania at critical time period 2014 – 2016 as well as in Prague on January 21, 2016.

Devices and a wanted technician were not found in his possession at the time of his arrest equipment that links him to illegal activities or proves increased computer skills.

There is no evidence of a physical presence or connection to the US and his movements accused is said to be exclusively within Europe.

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 52 of 57

BIBLIOGRAPHY / SOURCES

<https://www.paloaltonetworks.com/cyberpedia/what-is-botnet>

<https://pixelprivacy.com/resources/browser-fingerprinting/>

<https://www.anura.io/blog/captcha-and-recaptcha-how-fraudsters-bypass-it>

<https://www.irs.gov/>

<https://www.cloudflare.com/learning/bots/how-captchas-work/>

<https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets>

<https://www.forbes.com/advisor/taxes/tax-prep-checklist/>

<https://www.google.com/search?q=HOW+TO+DOWNLOAD+YOUR+IRS+TAX+TRANSCRIPT>

<https://www.greendot.com/helpcenter/top-questions/how-do-i-activate-register-a-card>

<https://arstechnica.com/information-technology/2013/04/a-beginners-guide-to-building-bot-nets-with-little-assembly-required/>

<https://us.norton.com/blog/id-theft/what-is-identity-theft#>

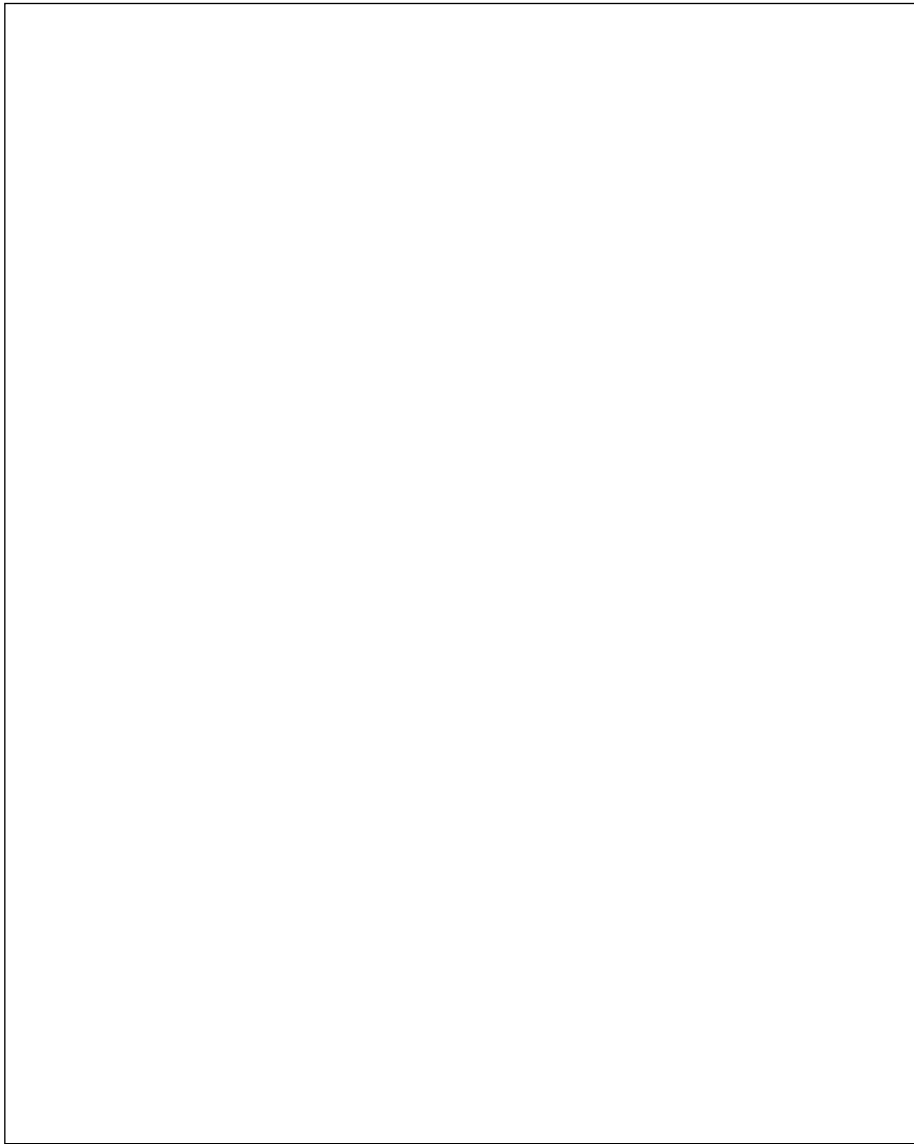
<https://www.nytimes.com/2015/05/27/business/breach-exposes-irs-tax-returns.html>

OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 53 of 57

Appendix 1

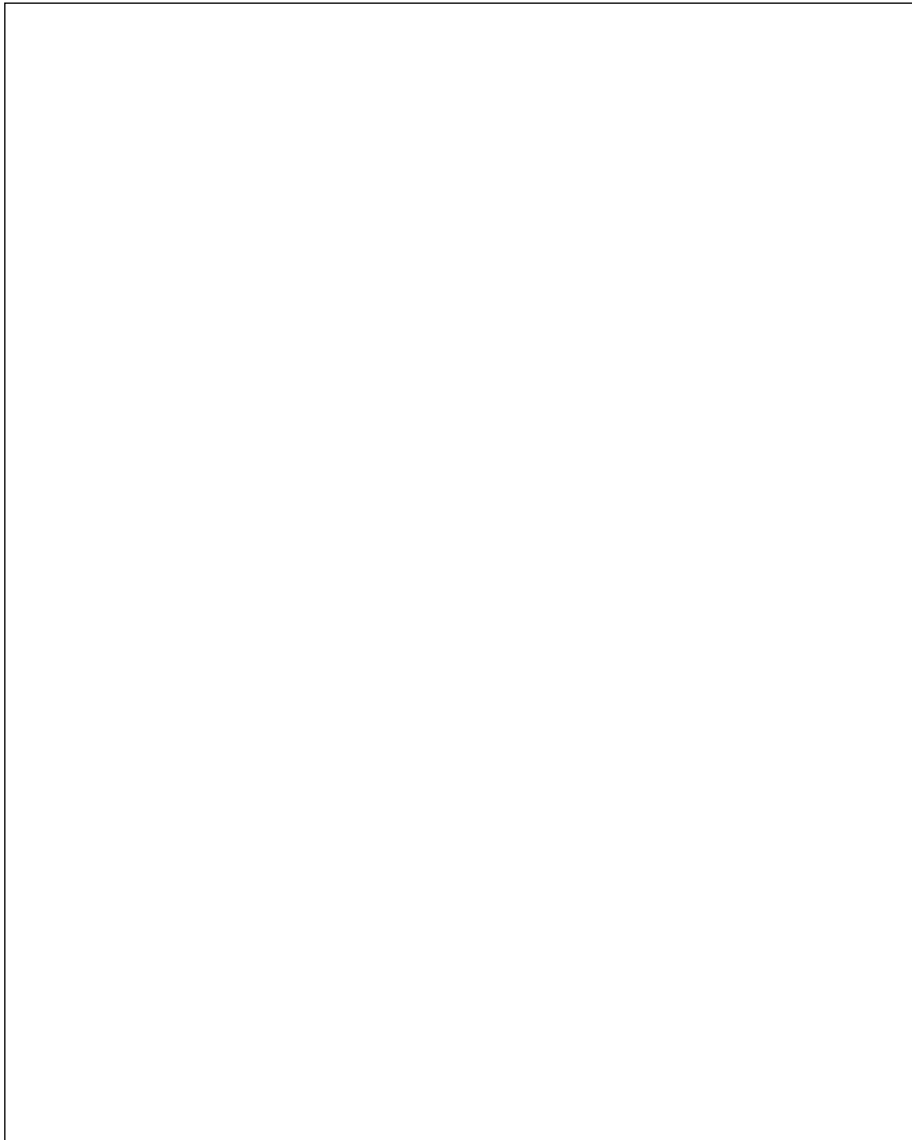
Curriculum vitae

1. Nikolaos Vasilakos





OPINION – TECHNICAL REPORT NIKOS VASILAKOS page 56 of 57



Athena , 2022

The undersigned technical advisor

Nikolaos Vasilakos