Every here and there on forum can here about some problem related with PC or computers and how perps to this and that with your equipment. Think for my self that know something about IT as average technician, admin, but sure can say for my self that I'm power user, so I'd like to reveal some secrets about computers in generally, and give you some tips and tricks before you think that perps is fucking you. Mean of course they do, this is their job, but what if only they got is V2k and playing with your mind how they can do and that, just make you crazy and more paranoid.
So let's start:
Can say that felt power what can do with PC equipment and A/V devices in generally, but this is devices for jamming equipment and for PC that would be flaws in Bluetooth or 802.11 (wireless) standards, and again this 2 flaws is not created by them with software application that I'm going to mention letter in documents but with already made equipment for fucking peoples brains. Don't know name for bluetooth, but in mine country for breaking in 802.11 a/b/g devices equipment is called think viper.

Bluetooth symptoms tising

If you see strange mouse moving, strange noises coming from your speakers, flipping screen(horizontal-verticaly), strange taping on your mobile phone, shortly your PC or mobile phone is definitely compromised with bluetooth flaws.

https://drive.google.com/file/d/0B9UJ0Cu6YID7Q3Z1dU0xLWI5ZDA/edit?usp=sharing

Solution: Because don't use bluetooth I just pull out bluetooth from mine laptop, and this is how it's look likes

Of course you can't pull out bluetooth from mobile phone because it's integrate on motherboard, but found solution that move system files and java classes from mine android phone and backup them and if need bluetooth in function just copy that file's back (of course backup them like they are structured in system folder like /com.mediatek.bluetooth/etc), this solution varies from phone to phone, if someone wants to try that I can help him but phone have to be rooted, or if you have iPhone jailbreak.

802.11 (Wi-fi or wireless)

Think that device is working like fake router presenter so that all client's (wi-fi cards) or router trying to authenticate with that fake device or router, mean not just yours card or router but in whole wi-fi range which is 10 m up to 100 maybe even 300 m depending on terrain and buildings or wi-fi standard, but again still using wi-fi on my mobile phone when I'm at home, but with best protection that wi-fi can offer for average person, and later I will show you that cracking wi-fi is not that easy like someone wants to present on net. Please avoid protection with wep key (no matter 64 or 128 bits) because can be broken with software tools easily. Solution would be WPA-PSK key preferable WPA2-PSK standard with AES not TKIP encryption which can be min 8 up to 63 character. I'm using online tool key generator

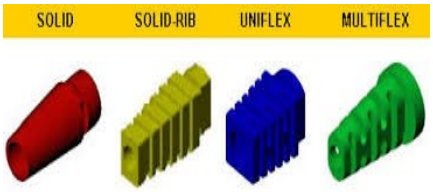
http://www.kurtm.net/wpa-pskgen/

Home networking:

If you are truly IT than you probably felt suddenly breaking internet connection, of course when you need it most ;-), we all know that is cause some device based on EM field. Personally at home have some cheep speedtouch router who is distribute with my ISP and in the past heard often that specific sound, clik when router is restarted.

Solution:

I put my router in old PC MIDI tower and before that wrapped with few layers of Alu foil, acting like some primitive Faraday cage. Connect your PC devices with cable, avoid wi-fi if you can, and you want have to go on public internet any more. Of course for cable choose cat6 U/UTP LSOH or cat6 F/UTP LSOH with RJ45 rubber protector



Password protection:

For start think that yours PC-s on win, linux, osX, smartphones, are much safer than us. Mean even with xp who is old 12 years and officially without Microsoft support from April 1 without antivirus toll is much safer than my head this days, because I have full mind control as of present day can't do anything about that, but I'm sure that weakness with yours mail account and yours speculations that your mail account is hacked is because you have weak password or to be more clear you know your password by heart. Sure maybe they have very talented hacker, but don't think so, or maybe this thing is not related with OS/EH story at all, mean you can always pick trojans, exploits, viruses accidentally.

Let say that you use weak password like this:

123456
password12345

Recently read some text on net with top 10 worsts password and this 2 are on the list, or you maybe using this:

Every day I like to watch my favorite documentary in 9 o'clock

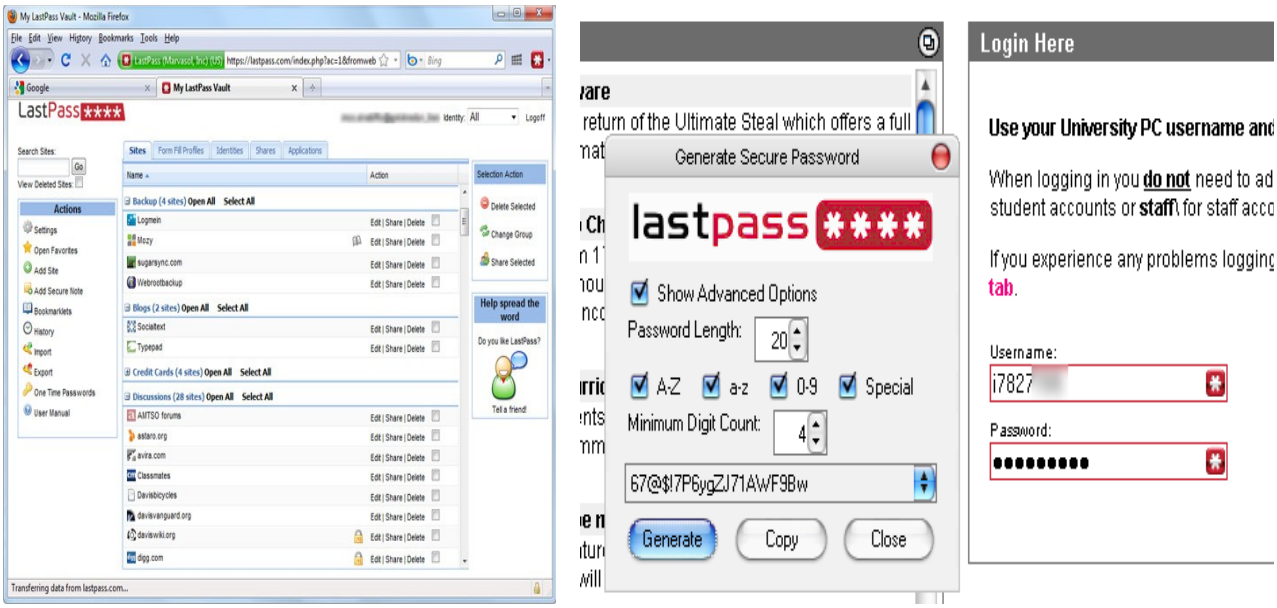
EdIltwmfdi9o

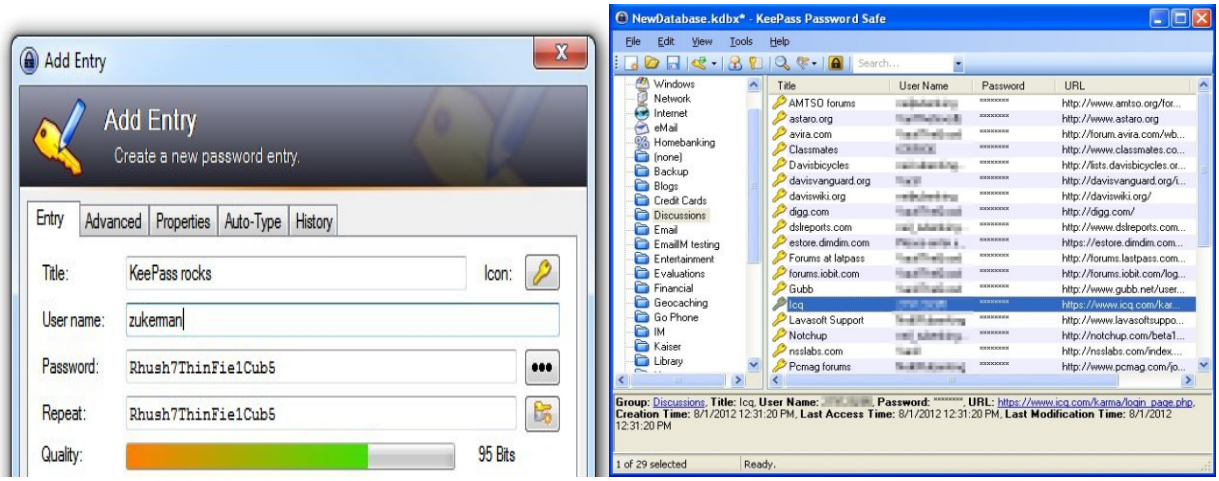
But of course even with that password, which is not bad (it got 2 capital letters and number), that you must repeat inside your head couple of time before you remember it, can be compromise, and of course it is.

But what if used this instead:

Z"E3JW*p9]EwZU^E}Xc_a3(#"Vd#p<3FoXv@ag)-

Of course this is for password's that you will use on a long run, with periodic changes (> 1 month) like mail accounts, forums, various web accounts, wireless passwords, etc. For that services can recommend popular password managers applications like Lastpass (https://lastpass.com/) or keepass (http://keepass.info/). This 2 tools have their pros and cons. Last pass is for start more commercial tool, and for smartphones they want to charge apps, but what bothers me most that my database passwords is stored somewhere online, on the other hand with keepass you are the owner with passwords database, and you can stored database local or in the cloud, but is more difficult for configuration than lastpass. Each of them comes with extension for all major OS and browsers, and support for 2 major smartphones OS providers, lastpass have support for Google authenticator OTP, for keepass don't know that information.





Little TIP:

If you want export lastpass passwords locally in CSV, don't use Chrome, because something is wrong with this 2 in combination.

But what to use when u need quick access to your PC, mean login credentials but still have solid protection, you can't use this because you don't want to enter credentials 20 min.

Z"E3JW*p9]EwZU^E}Xc_a3(#"Vd#p<3FoXv@ag)-

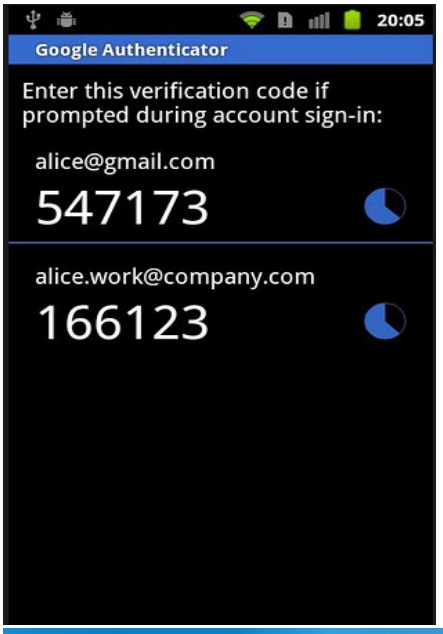
Quick solution would be Google authenticator http://en.wikipedia.org/wiki/Google_Authenticator who offers OTP credentials with 2 side authentication so you can use this password

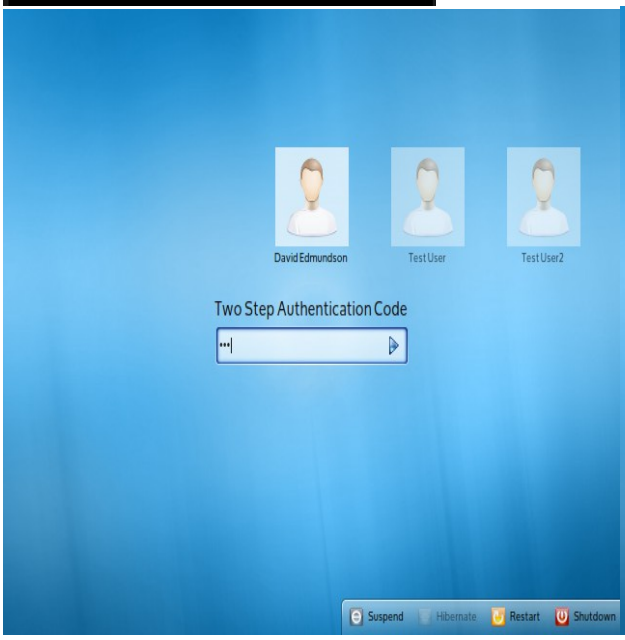
EdIltwmfdi9o

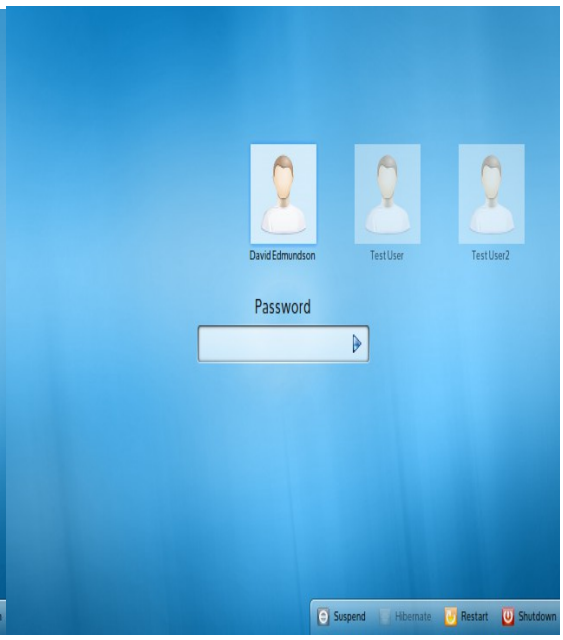
with bonus credentials on your smartphones and all look like this:

TIP:

If you loose your phone or you don't have access to your phone when you configure Google authenticator on OS for first time you will get emergency key and with that key you can enter in your system.







How to detect and remove viruses:

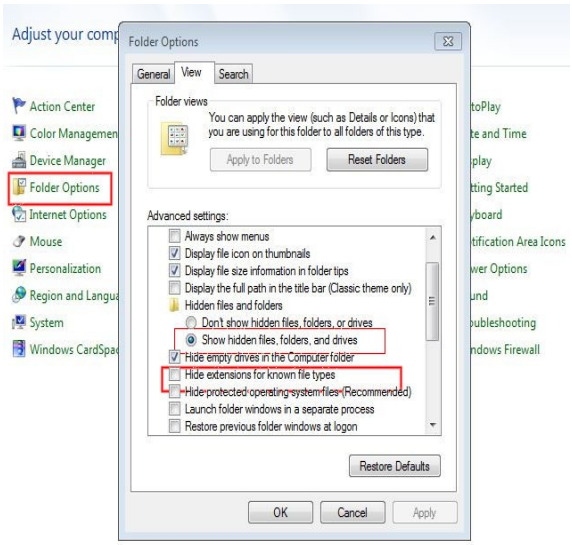
All viruses mostly affect Windows OS, and this tips are for Microsoft OS-s. If you suspect that you have viruses but not sure in that you can always do something on your own.

1. If you have access to Windows GUI check with antivirus tool first, any antivirus software is better than no antivirus at all (www.avast.com - free home edition, www.avira.com, microsft essentials - http://windows.microsoft.com/en-us/windows/security-essentials-download)

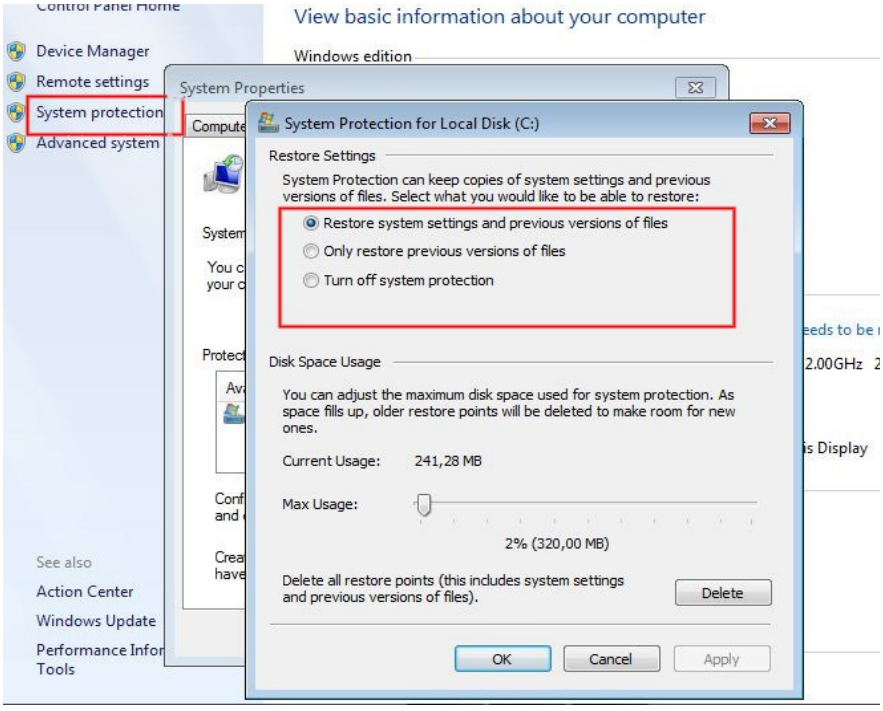
2. Download and run MGTools http://forums.majorgeeks.com/showthread.php?t=137630 which is compilation antivirus and antispywere tools and after utility finish you will get log files on Desktop for investigation

3. Erase any temp files with crap cleaner utility http://www.piriform.com/, or manually like c:\windows\temp, c:\Users\USER ACCOUNT NAME\AppData\Local\temp and temporary internet files (for vista and win 7) for xp is C:\Documents and settings\USER ACCOUNT NAME\Application data\temp and temporary internet files

You need to enable hidden files and unchecked Hide protected in folder options like this in control panel > folder options



4. Suggestion to disconnect System restore in windows - right click on my computer>properties>System protection>Configure>Turn off system protection



Reason would be today already OOOLD trick that viruses author like to put in c:\System volume information folder viruses and you probably guess that this is location for system restore files so when you turn your system back in last known good state also return virus back. You can always delete content of system volume information manually(not folder), but you need to have security credentials for that on xp you need only right click>sharing>share> click apply> of course windows would complain something but you will get access to enter, for win 7 and vista you need right click >security>edit>add>advanced>find now>add admin account that you use>give full access to that folder>apply OK

5. run command sf (first put windows install DVD, CD in reader) in terminal like run>cm (run as administrator)>sf /scan file, XP users can't repair system files only verify files with that command. Basically that command checks system files in system32 folder with files from DVD or CD.

6. Close all internet consumers like browsers, mail clients, Microsoft system update (right click on my computer>windows update>change settings>Never check for updates), just temporary of course to check if some other resources try to contact some remote IP address on net with command run>cm (run as administrator)>net stat -a

7. Run command msconfig to see all starting services (when you choose services click on “hide all microsft services”) and application on startup.

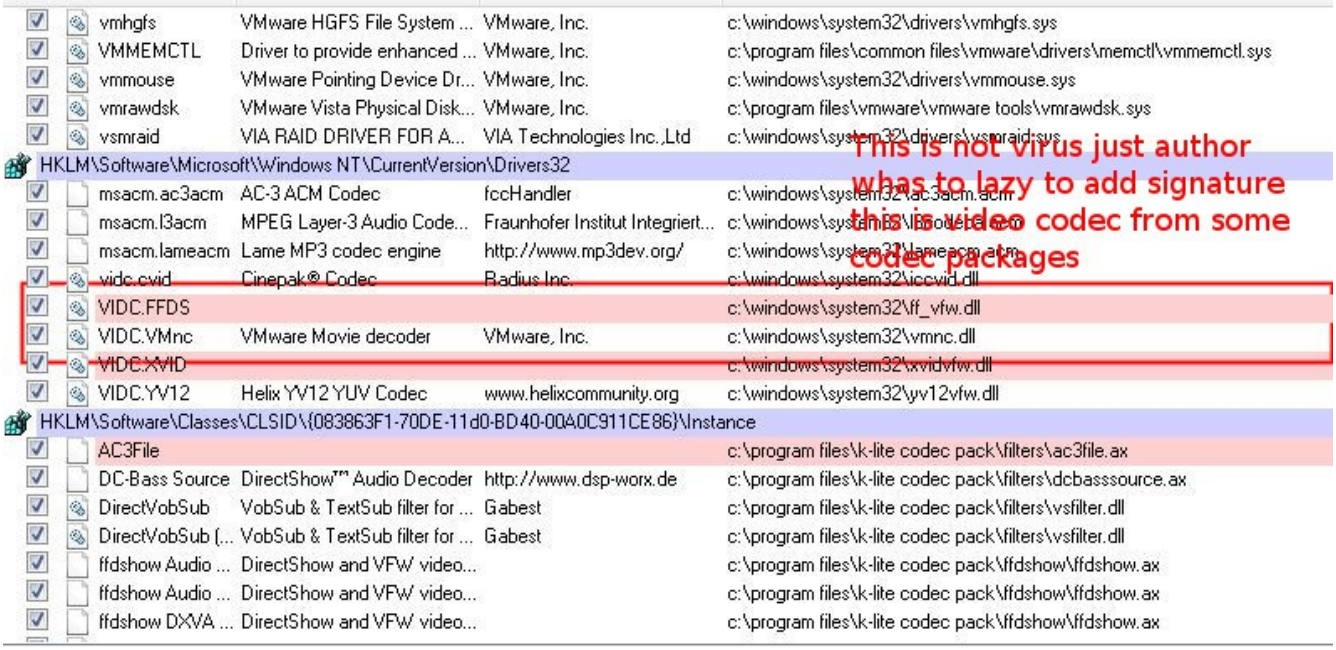
8. One old trick, open windows explorer windows>system32>click right click on name in top right corner to choose more columns (choose company name and authors), and choose to filter only unspecified company. Reason is simple, when someone is going to rob you he/she will not carry ID card on forehead, mean if viruses is here they probably don't have author or company signature, also

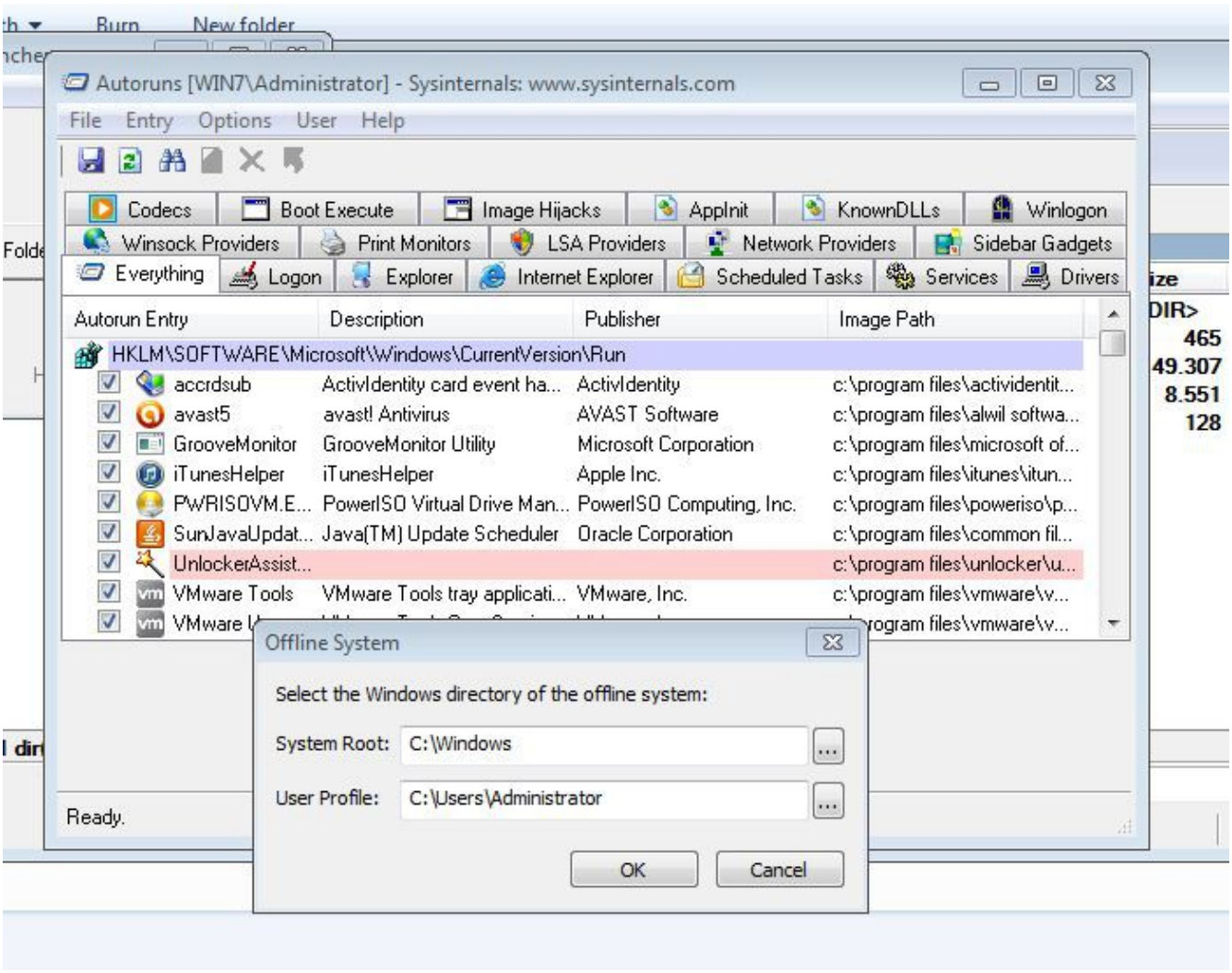
you spend lots of time checking with antivirus system32 which can be really big, instead you just scan that unsigned files. Sometimes regularly software developers let say from Microsoft will not signed or put company name but you will figure it out by your self

Next step

If nothing from above not helping than is time to go in safe mode or even better to boot system from DVD/CD or maybe USB hard or stick. Every power user should have Hirens boot CD http://www.hiren.info/pages/bootcd, all utility from CD are FREE, know that some of you like only legitimate not pirate software, but if someone wants to expands horizons with let say paid free software they can look for hirens restored editions with lots of good software on it.

To boot from DVD/CD you need to enter in BIOS and put CD/DVD device or USB drive (if you put bootable hirens on it) to boot before hard drive. Depending on manufacturer they are different keyboard key to enter into BIOS. For Desktop that would be usually DEL button, on laptop F2, but of course could be ESC or F10, mean find in manual if you are not sure. Than choose run mini XP to load system into RAM memory. Some good tools on hirens would be backup all drivers, or in startup folder autoruns all and than choose offline system and offline user account or profiles. This is old great utility popularly called “swiss army knife” for admins from Sysinternals company that was taken over from Microsoft corporation, just to shut down concurrency and think that Microsoft not developing that utility anymore. You can choose antivirus utility, etc





Forget to mention that you looking for strange places for executable files (CMD;VBS;BAT;EXE, etc) like C:\Documents and settings\USER ACCOUNT NAME\Application data\temp, also look in c:\Users\ACCOUNT USER NAME\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\startup\.

Windows installation

I will not mention installing regularly windows installation with DVD/CD, when something is gone wrong or maybe DVD/CD unit is not working, or you need backup your data and you don't have spare hard drive for backup.

1. If you have enough space for new installation without formatting and leave all old data than procedure is following. Boot from hirens mini xp, than rename all folder like c:\windows to c:\windows.old, c:\users to c:\users.old and do the same with rest of folders, create new folder and put all files from root folder inside. Next procedure is boot from DVD/CD drive and choose option leave current files systems intact, and rest of procedure you probably know.From backup folders that you leave you will probably need only c:\users\USERS ACOOUNT NAME folder and content from it, because inside is EVERYTHING from previous installation like files, mails, templates, history browsers files, bookmarks, etc. I will mention couple of worth mentioning paths for savings files.

Microsoft applications

http://office.microsoft.com/en-001/outlook-help/locating-the-outlook-data-files-HA103412630.aspx

Google Chrome

c:\Users\USERS ACCOUNT NAME\AppData\Local\Google\Chrome\User Data\

Mozilla Firefox

C:\Users\Administrator\AppData\Roaming\Firefox\Profiles

If you need drivers from previous installation and you didn't saved drivers with utility from hirens you need again enable hidden files in folder options and than navigate to old folder c:\windows.old\inf\. Inf file is just text document who tells to OS where is other system files needed for device to be recognized by Windows and running, and after that you need to navigate to couple other folders to find files like *.cat and *.says.

2. Method is installation from hard drive. I will mention xp installation and give link for vista and win 7 installation. Boot from Hirens, if you don't have DVD/CD drive or not running properly or not running at all, you need to copy all i386 folders from installation DVD/CD to hard drive (of course you need first to get hands on good DVD/CD and copy i386 folder on USB drive). After that need to find winnt.exe and start installation. Installing vista and win 7 is more difficult because they using actually two partiotions. First one is bookable and is usuallay 100 MB large and second one is system partition.

http://www.instructables.com/id/Install-Windows-7-without-USB-or-DVD-without-upgra/

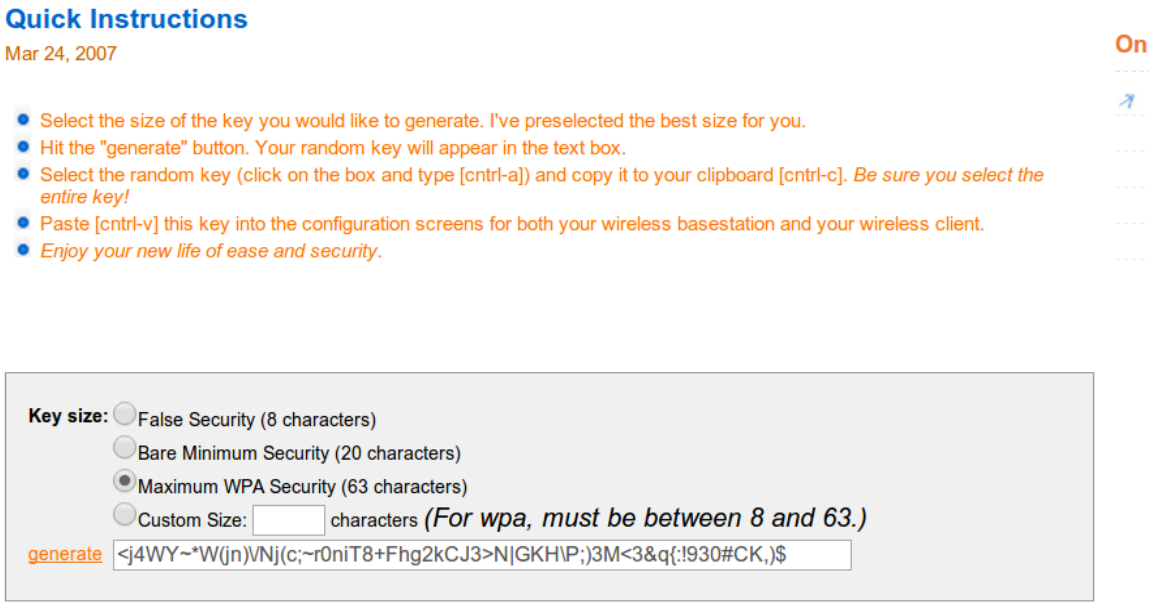
3. Method is with utility on hirens in menu>others for xp and vista and win 7 installation. That is 2 different utilities and with this utilities you have couple of tweaking option for installation.

Couple of examples that is not that EASY to crack wi-fi password

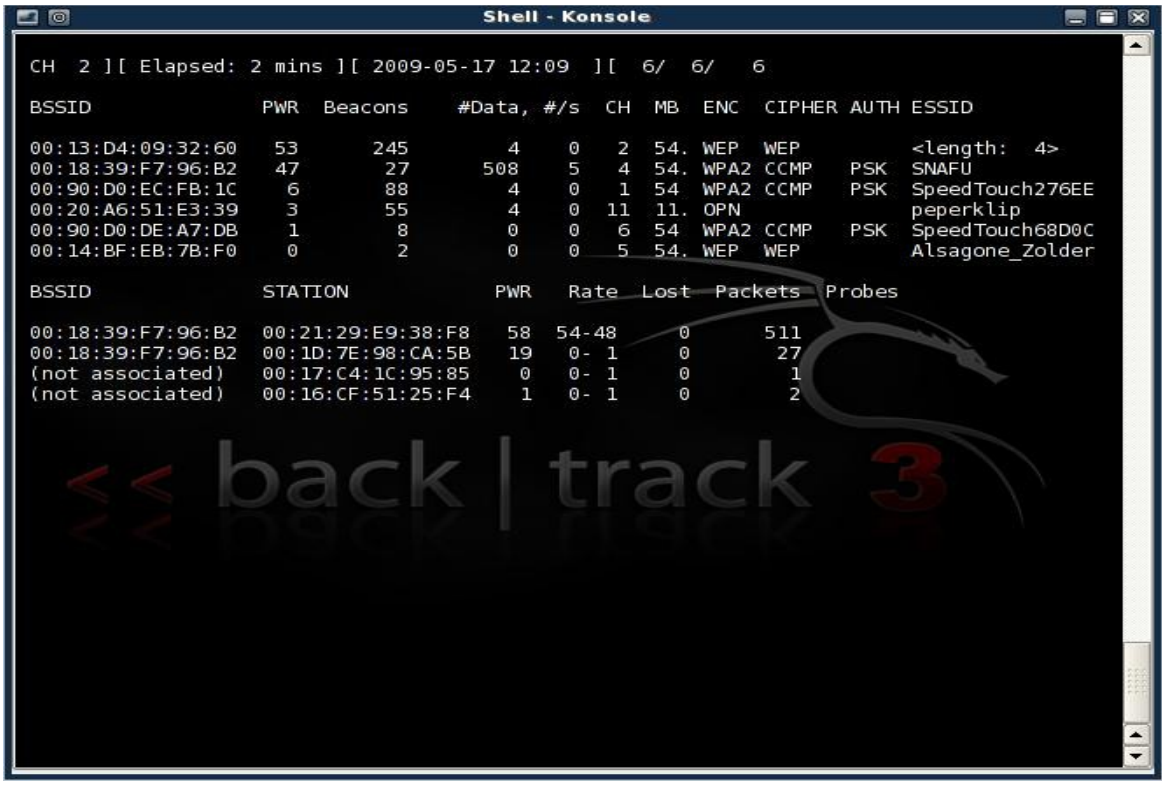
Title of course is goes for WPA cracking not WEP key. WEP flaws no matter if you using 64 or 128 bits can be broken with regular wi-fi card that not support injection, just sniffing and gathering packages (IVS), when owner is on the net for maybe 1 hours depending on traffic you need to gather around 15k of IVS, but if you have wi-fi card that support injection you can crack wep network for 10 minutes. All you need is utilities like airdumpand aircrack-ng if you just sniffing and collecting ivs, and if you like to put in second gear and of course have equipment for that (injection) you need also aireplay-ng.

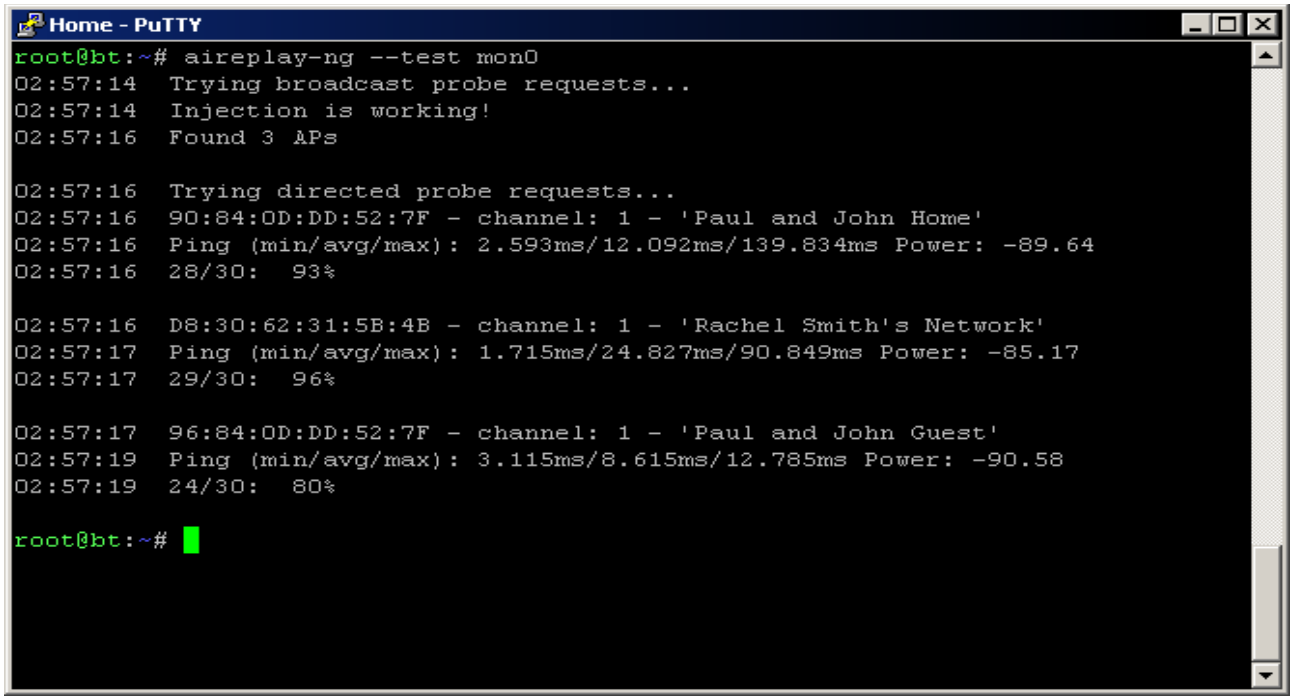
For WPA cracking you need to catch 4 hand shaking between router and wi-fi clients, and after that you need good password dictionary for cracking, and if you choose min character (8), like PASSWORD, of course that your network would be compromise, but for that attacker don't even need pass file. I read somewhere that Dual core with 2.7 GHZ can process around 500 password per second, but this can be of course even faster if you use Graphic cards with CUDA capabilities instead CPU with utility john the ripper and comparing passwords from database not ordinary large text dictionary file. Answer why they are using graphic card is very simple because this days GPU is much faster than CPU.

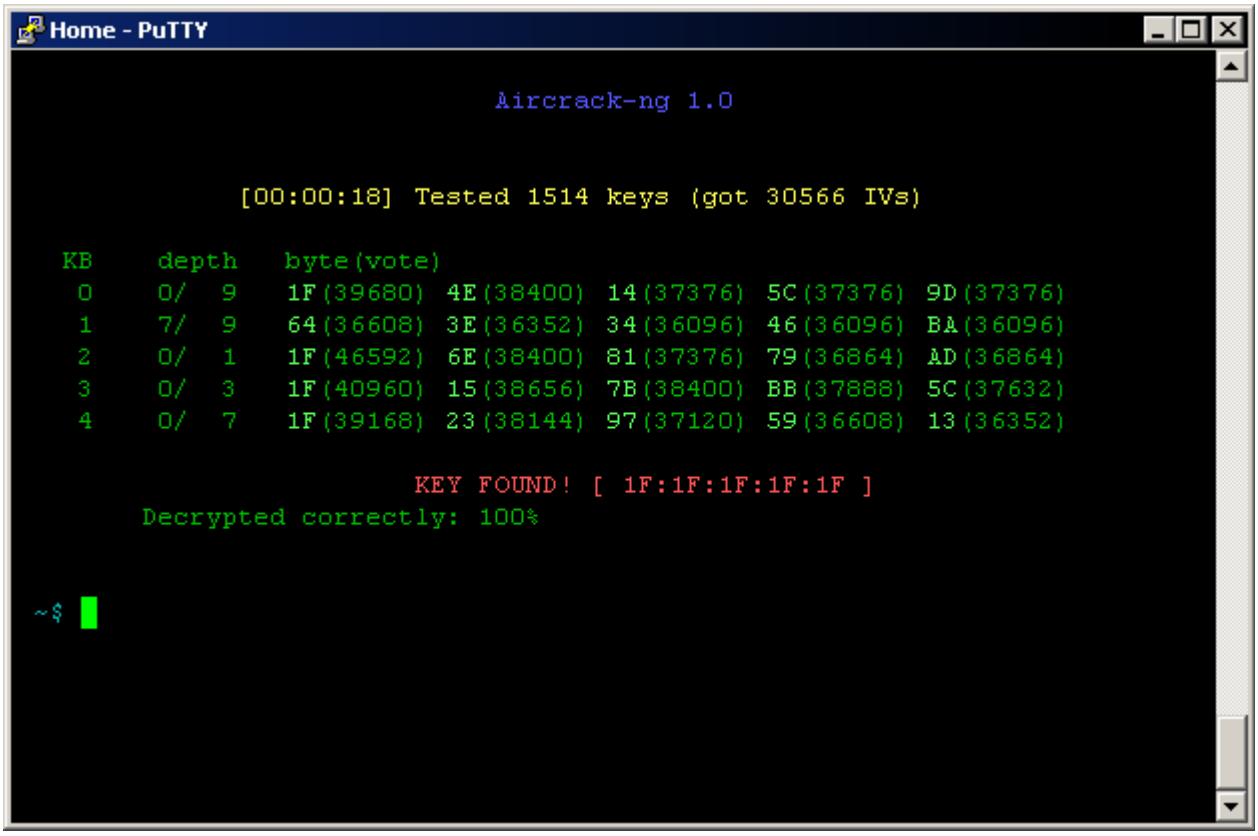
Everything that I write before is from my personally experience and I'm not some security expert, just tried some pentesting utilities from backtrack or kali distribution based on ubuntu, and I never ever didn't manage to break WPA key, can't say that is not possible, real hacker can break WPA key, but don't think that “our friend” can break this.



Some more examples from that 3 utilities mention before in action







Don't be afraid this third picture is cracked wep key in hex format

If you are still not feeling safe I can recommend to move on second level and install some home based firewall from old PC-s with 2 or more network cards based on realtek 8169 chipset with 1 Gb bandwith, and install VERY good FREE firewalls like Pfsense based on freebsd unix distribution, it's

really easy to handle compare to others distributions, and it's using PF, and you can try radius authentication, but have to install package separately, it's not coming with default installation.

vyatta which don't offer GUI any more from version 6.3 core which is free, based on debian, any way GUI was real mass before that, didn’t have a chance to work with paid distribution and they said that will made completely new GUI, it's using IP tables

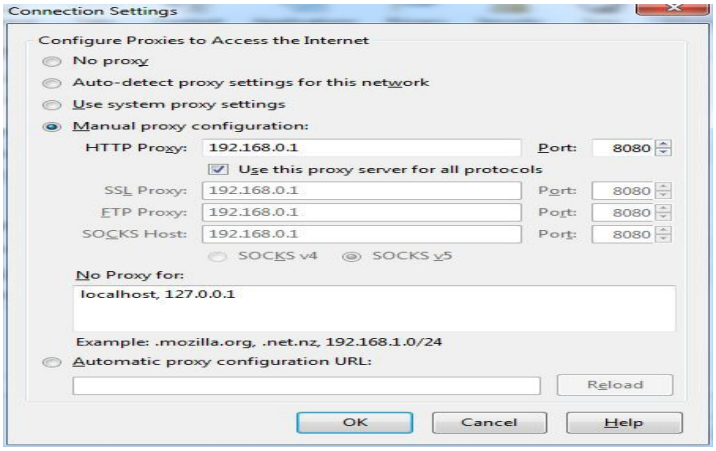
mine favorite is mikrotik, but it's not free distribution, but comparing to others using really low hardware resources.

Some tips for safe surfing

- If you like to keep low profile on net, first you need to change MAC address from your LAN card, because it's like unique car registration, for linux distribution best utility is macchanger, tried 2 for Windows can't remember names, but can confirm that I didn't manage to change Intel LAN card mac address which is very popular on notebooks in middle price range.

- Secondly can recommend TOR project which is very popular among people who are aware that internet is not safe place https://www.torproject.org/ (Shortly we talking about lots of routers around the world who sharing some capabilities for whole community, and traffic is encrypted). If you are going to use TOR in future be patient because bandwith is pretty bad.

- For Smartphones can recommend apps siphon which is VPN network, acting like that your public address coming from UK, and can't be installed regularly around globes without tweaks. This is sometimes important if you are using smartphones as tathering and sharing your data internet with computer
- You can use also free IP proxies and enter IP address that you choose in https://hidemyass.com/proxy-list, and on mozilla will look something like this



- If you are using Windows OS on laptops and you are surfing on public internet, choose public network, because this option have more rigorous option in MS firewall which is not bad on windows 7 with UAC on, although UAC is here more for Microsoft to wash hands when user trying to complain something about security and OS in not responding mode.
- Avoid using checking mails on hotspot who using regular protocols for authentication like POP

110, SMTP 25, IMAP 143, because your password is travel around net in pure text, and someone with sniffing software or packet inspection and analyzing software like wireshark can see your password easily, of course wireshark you need to know how to use, but on backtrack or kali distribution you can find kiddy tools for hacking like etercap and with few click someone can see not only regular plain text auth. But encrypted as well to, so if you must check mail on public places and you don't have proxy in function at least use mail with secure protocols.

- Webmail in USA are not safe to much, try to choose webmail provider who is located in other part of the world, can recommend safe-mail.net but with free account you will get only 2 MB for mailbox.

Some more usefull command for the end:

for windows in CMD>ipconfig /all (show more information about network cards and connections)
ipconfig /renew (request for new IP address from DHCP services)
ipconfig /flushdns (reset DNS servers on client when you change DNS providers but you can't still access internet)

This is everything from me for know, hope that I reveal something that you didn't know already. Purpose of this short manual was just to aware average IT that Perps are not all-powerfull considering IT, and I'm aware of mind control, but still can figure it out when they try to full me with lots of crap with V2K, mean when everything else is falls they always have that, just to made you paranoid. English is not my native so you will have to forgive me.

Robin.