# The4960's Hacker Profiling Guide

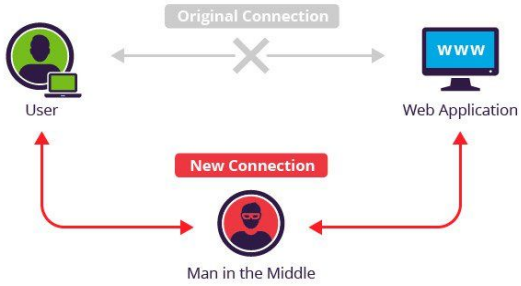
*Authors:*
Christian Aaron Murga

*Editors/Contributors:*
Albert Morales
Jaime Acosta

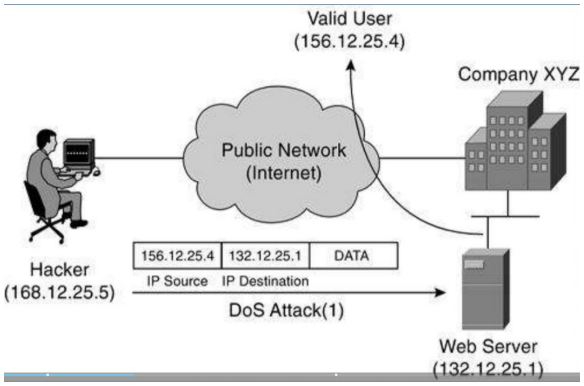
*Tables of contents:*

# *Type of Attacks*

- Man in the Middle Attack - gaining *unauthorized access to network traffic* such that the traffic goes through the attacker before reaching its end point. An attacker can use this to simply listen in on traffic, or can be used to modify traffic with malicious intent.

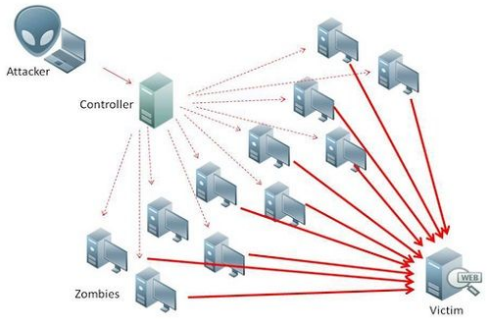



- Spoofing - falsifying or presenting data in such a way that the attacker appears to have a *different identify*.

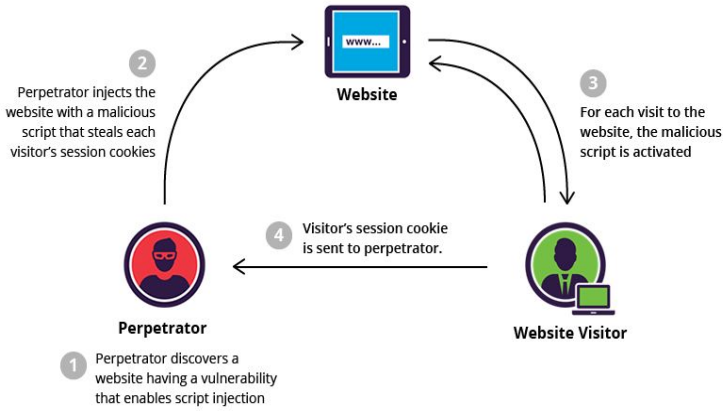



- Phishing Attack - when an attacker, *masquerading as a trusted entity*, dupes a victim into opening an email, instant message, or text message. The recipient is then *tricked into clicking a malicious link*, which can lead to a variety of attacks.

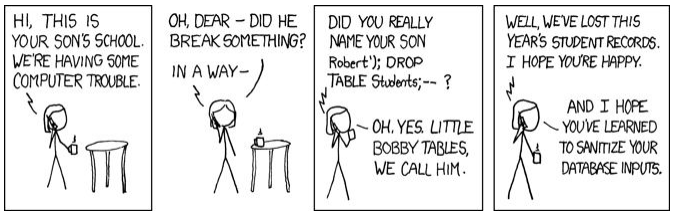
- Denial of Service - maliciously *consuming a system's resources* such that it is unable to serve clients.



- XXS Cross-Site Scripting - *injecting a malicious script* to a vulnerable website. When a normal client visits the website, the *client run the malicious script*.




- SQL Injection - submitting malicious input to a vulnerable server's form such that the server treats the *input as a command rather than data*.




- Brute Force/Dictionary Attack - a form of *password cracking* where an attacker incrementally guess what they password might be from a large set of inputs.

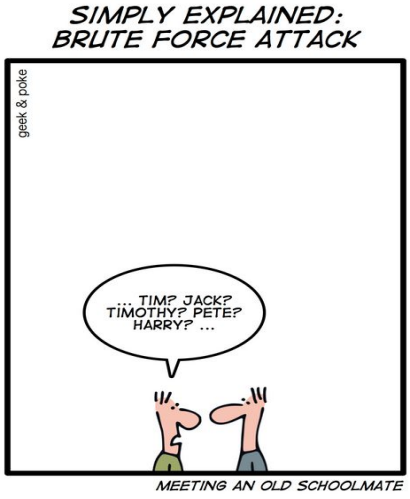
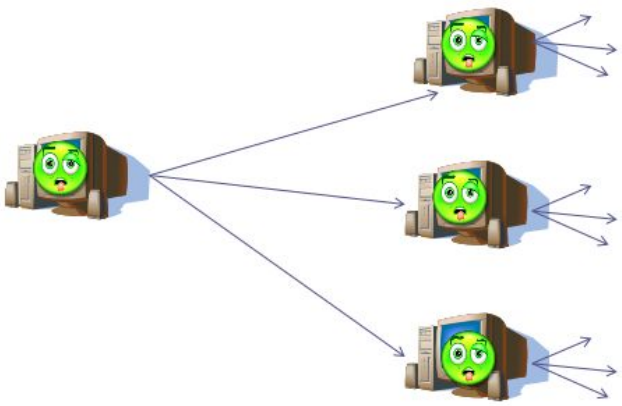


Table 12.1 The Matrix of Cybercrime: Level of Opportunity by Type of Crime (Wall, 2005)

| | Integrity-Related (Harmful Trespass) | Computer-Related (Acquisition Theft/ Deception) | Content-Related 1 (Obscenity) | Content-Related 2 (Violence) |
|---|---|---|---|---|
| More opportunities for traditional crime (e.g., through communications) | Phreaking Chipping | Frauds Pyramid schemes | Trading sexual materials | Stalking Personal Harassment |
| New opportunities for traditional crime (e.g., organization across boundaries) | Cracking/Hacking Viruses H Activism | Multiple large-scale frauds 419 scams, Trade secret theft, ID theft | Online Gender trade Camgirl sites | General hate speech Organized pedophile rings (child abuse) |
| New opportunities for new types of crime | Spams (List construction and content) Denial of Service, Information Warfare, Parasitic Computing | Intellectual Property Piracy Online Gambling E-auction scams Small-impact bulk fraud | Cyber-Sex, Cyber-Pimping | Online grooming, Organized bomb talk/ Drug talk Targeted hate speech |

# *Types of Malware*

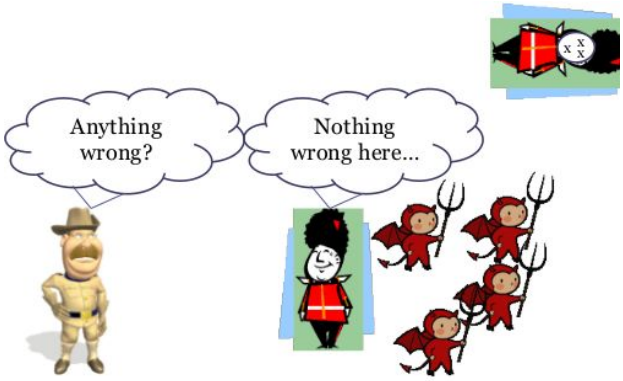
- Virus - Attached to a program. Spreads when a user launches an infected program – keeps a low profile and usually infects new programs or disks.
- Worm - Does not need to attach to an existing program. Sends a copy of itself to another computer and then launches that copy.



- Ransomware - encrypts files and demands payment to decrypt them. This is a subset of scamware.

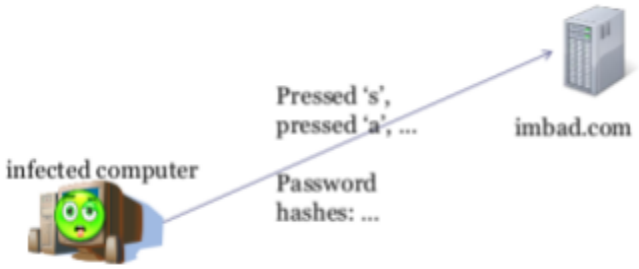
- Backdoor - allow the attacker to execute commands usually with little or no authentication


- Rootkit - designed to conceal existence of other malware

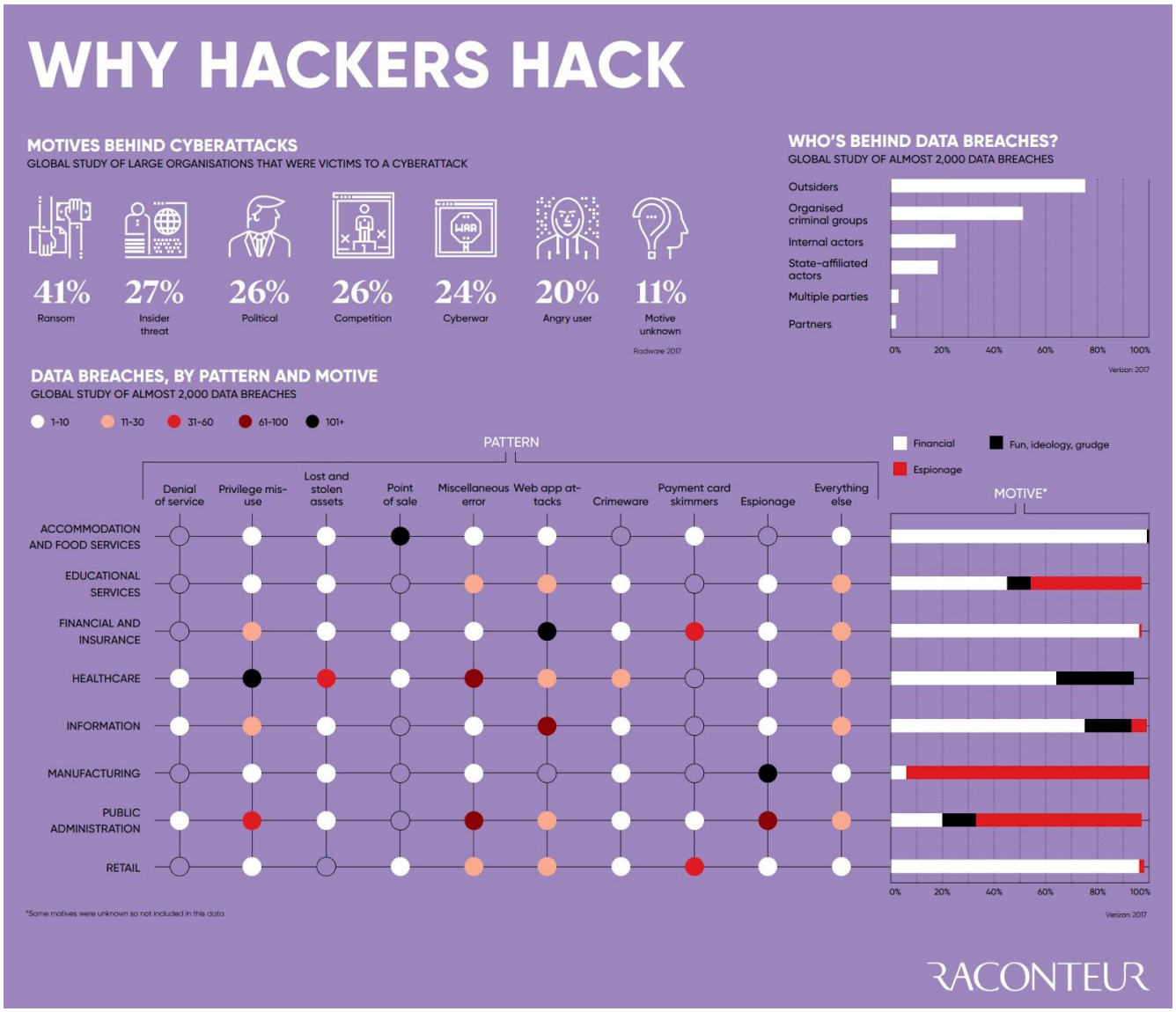


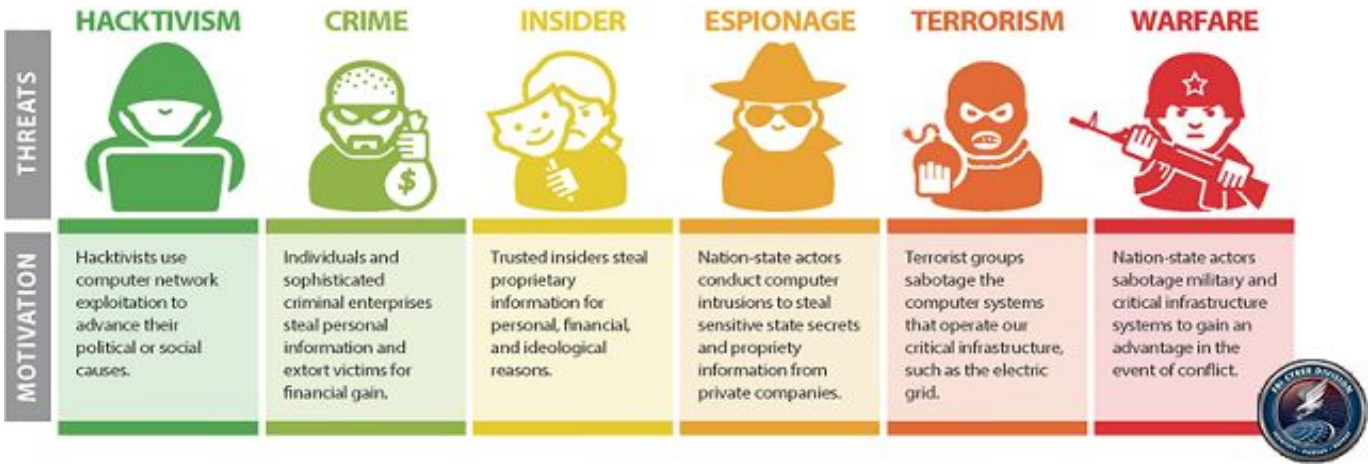

- Adware - “Software typically installed that displays advertisements browser pop-ups).”


- Keylogger - collects keystroke information and gives to attacker.



# *Motivations*



# *Cybercriminal Profiles*

From “Computer Incident Response and Forensics Team Management : Conducting a Successful Incident Response”

- *Script kiddie* - not technologically sophisticated; uses existing scripts; ego driven; usually have the intent to trespass or invade privacy.
- *Cyberpunks* - technologically proficient; usually young; ego driven. Tend to engage in trespassing, invasion, theft, sabotage. Often viruses and DOS against established companies.
- *Old timers* - most technologically proficient; motivation is ego driven and perfecting the cyber-trespassing ‘art.’ Typically middle aged or older; have extensive technology backgrounds. Sometimes deface websites; usually do not cause much harm due to skill.
- *Unhappy insider* - very dangerous since they are inside an organization's defenses, any and and employment level, motivation is revenge and/or monetary gain. Intend to steal from or harm company. Engage in extortion or exposure of company secrets. Depend on direct access - Internet is secondary (also to obtain tools, transfer, etc).
- *Ex-insider* - separated from company unwillingly (e.g. layoff, bad performance/conduct); motive is revenge and purpose to harm company; if termination is foreseen, they may perform other destructive acts (e.g. logic bombs, delete data); benefit from private company information
- *Cyber-thieves* - any age, does not require vast technological experience. Motivation is profit (e.g. stealing data, monetary theft). Adept at social engineering, but use network tools as well. Often try to gain employment at targeted company; some work from the outside.
- *Cyberhucksters* - spammers and malware distributors. Focused on monetary gain. Good at social engineering and spoofing. Use spyware. Sometimes infect systems so they can sell the cure.
- *Con man* - Motivated by monetary gain. “Theft is their trademark.” Often run scams and perform phishing attacks to commit identity and credit card theft. Very good at social engineering and spoofing. Harder to catch because they are usually antonymous. Typically no specific victim; some will target high value targets by spear phishing.
- *Cyberstalker* - driven by ego and deviance. Want to invade their victim’s privacy to satisfy personal/psychological need (e.g. jealousy). Use keyloggers, Trojan horses, sniffers; very resourceful and diverse.
- *Code warriors* - skilled with long histories with technology (often times with degrees). Initially focused on ego and revenge. Now more capitalistic, performing theft or sabotage. Not an ‘art’, more of a profession. Code exploitation and trojan horse creators. Any age, but typically 30-50. Usually socially inept and social deviants.
- *Mafia soldier* - some characteristics from con-man and code warrior. Highly organized with criminal purpose of making money. Typically engage in theft, extortion, and privacy invasion with goal of blackmail.
- *Warfighter* - Any age; very bright and skilled. Motivation is infowar (e.g. after strategic advantages for their country and their allies). All types of cyber weapons (e.g. trojan horses, DOS attacks, and use of disinformation.

# *Motivational Typologies*

From “Profiling and Serial Crime : Theoretical and Practical Issues”

- Power Reassurance
    - “This offender is driven by a relational fantasy and feels that the victim is special because of it.”
    - “There is no intent to punish or degrade, and they are the least likely to physically harm their victim since this would shatter the illusion that the relationship was somehow wanted”
    - “The attack is intended to restore diminishing feelings of masculinity, and power is achieved by taking power away from the victim.”
- Power Assertive
    - Offender “feel inadequate and both seek affirmation about their masculinity and worth.”
    - “offender tries to establish a relationship with the victim, and in this way hopes to shore up their low self-worth.”
    - “offenders try to make themselves feel better by making others feel bad.”
    - “is not concerned about the victim’s welfare in any form. Moderate to excessive force may be used in controlling the victim, and the attacks will occur at any time and location that is convenient and safe.”
- Anger Retaliatory
    - “does not want to include the victim or want their input. They will use excessive levels of force, even beyond that needed to gain control over a victim, or that required to get compliance.”
    - “Offenders hate the target (individual or group) against whom the offense is committed and will hold them accountable for real wrongs, or misplace their aggression as would happen in the case of a perceived wrong.”
    - “focus is an individual or a group that has either done something wrong or that the offender believes has done something wrong.”
- Pervasively Angry
    - “The offense is the manifestation of anger not directed at a specific target, group, or institution, but results from cumulative life stresses in any or all aspects of being.”
- Gang and Opportunistic
    - Reassurance Oriented - seeking emotional support due to low self-esteem
    - Pervasively Angry - group used as a platform to legitimize behavior
    - The gang espouses a philosophy that is concordant with their own
    - Joins gang for monetary gain
- Profit
    - Struggling to make ends meet
    - Does not have to be actual cash

# *Digital Forensics Workflow*

From “Computer Incident Response and Forensics Team Management : Conducting a Successful Incident Response”

1. **Prepare** —Specific forensics training, overarching corporate policies and procedures, as well as practice investigations and examinations will prepare you for an “event.” Specialized forensics or incident handling certifications are considered of great value for forensics investigators. Identify —When approaching an incident scene— review what is occurring on the computer screen. If data is being deleted, pull the power plug from the wall; otherwise perform real-time capture of system “volatile” data first.
2. **Preserve** —Once the system-specific “volatile” data is retrieved, then turn off machine, remove it from scene, and power it up in an isolated environment. Perform a full system bit-stream image capture of the data on the machine, remembering to “hash” the image with the original data for verification purposes.
3. **Select** —Once you have a verified copy of the available data, start investigation of data by selecting potential evidence files, datasets, and locations data could be stored. Isolate event-specific data from normal system data for further examination.
4. **Examine** —Look for potential hidden storage locations of data such as slack space, unallocated space, and in front of File Allocation Table (FAT) space on hard drives. Remember to look in registry entries or root directories for additional potential indicators of data storage activity. Classify —Evaluate data in potential locations for relevance to current investigation. Is the data directly related to case, or does it support events of the case, or is it unrelated to the case?
5. **Analyze** —Review data from relevant locations. Ensure data is readable, legible, and relevant to investigation. Evaluate it for type of evidence: Is it direct evidence of alleged issue or is it related to issue?
6. **Present** —Correlate all data reviewed to investigation papers (warrants, corporate documents, etc.). Prepare data report for presentation— either in a court of law or to corporate officers.

# *Skills/Areas of Knowledge*

- Encryption
- Web development
- Malware writing
- Programming
- Computer vision
- Data mining
- Machine learning
- Reverse engineering
- Networking
- Penetration testing
- Social engineering
- Wireless communications

# File Extensions

- elf - Linux executable
- exe - Windows executable
- lnk - Reference/link to another file
- txt - Text file
- php - Webpage
- html - Webpage
- bat - Windows shell script
- dll - Windows dynamically link library
- ps1 - Windows Powershell script
- dat - General information file
- py - Python script
- java - Java source code
- webm - Video file

# Network Protocols

8 Layer model: Physical, Data, Network, Transport, Session, Presentation, Application
(Please Do Not Teach Stupid People Acronyms)
4 Layer model: Network access layer, Network layer, Transport layer, Application layer

| Port | Name | Description |
|---|---|---|
| 8 | echo | Test connection between client and server |
| 17 | qotd | Quote of the day |
| 18 | msp | Message send protocol |
| 21 | ftp | File transfer |
| 22 | ssh | Remote shell |
| 23 | telnet | Old remote terminal connection |
| 25 | smtp | Mail transfer |
| 53 | domain/DNS | Domain name system - resolves domain names |
| 66 | sql-net | SQL database server |
| 67 | dhcps | Dynamic Host Configuration Protocol server - assigns IP addresses |
| 68 | dhcpc | Dynamic Host Configuration Protocol client - assigned IP addresses |
| 69 | tftp | Trivial File Transfer Protocol |
| 79 | finger | User information look up |

| | | |
|---|---|---|
| 80 | http | Hypertext transfer protocol - websites |
| 88 | kerberos | Authentication protocol |
| 110 | pop3 | Email service |
| 111 | rpcbind | Bind port to program |
| 123 | ntp | Network time protocol |
| 137 | netbios-ns | Network Basic Input/Output System |
| 138 | netbios-dgm | Network Basic Input/Output System |
| 139 | netbios-ssn | Network Basic Input/Output System |
| 143 | imap | Email service |
| 162 | snmp | Simple Network Management protocol |
| 194 | irc | Internet relay chat |
| 443 | https | Secure HTTP |
| 445 | microsoft-ds | SMB over IP |
| 497 | retrospect | Backup software |
| 514 | syslog | Logger for network devices |
| 515 | printer | ... |
| 520 | rip | Controls routing tables |
| 1434 | ms-sql-m | Microsoft sql monitor |
| 1723 | pptp | Point-to-Point Tunneling Protocol |
| 1900 | upnp | Universal Plug and Play |
| 8080 | http-proxy | …. |

# *Partition Formats*

- NTFS - robust and effective. Windows install format.  Somewhat low compatibility with other systems. (1993)

- FAT32 (File Allocation Table 32) - all operating systems (universal); Max volume: depends, typically 2TB, but 32GB in Windows. Max file size 4GB. Not a journaling file system (more prone to corruption). Does not support file permissions. (1977)
- EXFAT - flash drive optimized. More compatible than NTFS, but less than FAT32. (2006)
- EXT4 - Max file size: 16TB. Max volume: 1EB (exabyte) = 1,024PB (petabyte) = 1,048,576 TB (terabyte). Linux install format. Optional journaling file system. (2008)
- EXT3 - Max file size: 2TB. Max volume: 32TB. Journaling file system. (2001)
- Linux-swap - used when RAM is full.

| Amount of RAM in the System | Recommended Amount of Swap Space |
|---|---|
| 4GB of RAM or less | a minimum of 2GB of swap space |
| 4GB to 16GB of RAM | a minimum of 4GB of swap space |
| 16GB to 64GB of RAM | a minimum of 8GB of swap space |
| 64GB to 256GB of RAM | a minimum of 16GB of swap space |
| 256GB to 512GB of RAM | a minimum of 32GB of swap space |

## NTFS vs FAT vs exFAT

| Criteria | NTFS5 | NTFS | exFAT | FAT32 | FAT16 | FAT12 |
|---|---|---|---|---|---|---|
| **Operating System** | Windows 2000<br>Windows XP<br>Windows 2003 Server<br>Windows 2008<br>Windows Vista<br>Windows 7 | Windows NT<br>Windows 2000<br>Windows XP<br>Windows 2003 Server<br>Windows 2008Windows Vista<br>Windows 7 | Windows CE 6.0<br>Windows Vista SP1<br>Windows 7<br>WinXP+KB955704 | DOS v7 and higher<br>Windows 98<br>Windows ME<br>Windows 2000<br>Windows XP<br>Windows 2003 Server<br>Windows Vista<br>Windows 7 | DOS All versions of Microsoft Windows | DOS All versions of Microsoft Windows |
| **Limitations** | | | | | | |
| **Max Volume Size** | 2 ^ 64 clusters – 1 cluster | 2 ^ 32 clusters – 1 cluster | 128PB | 32GB for all OS. 2TB for some OS | 2GB for all OS. 4GB for some OS | 16MB |
| **Max Files on Volume** | 4,294,967,295<br>2 ^ 32 -1 | 4,294,967,295<br>2 ^ 32 -1 | Nearly Unlimited | 4194304 | 65536 | |
| **Max File Size** | 2 ^ 64 bytes<br>(16 ExaBytes) minus 1KB | 2 ^ 44 bytes<br>(16 TeraBytes) minus 64KB | 16EB | 4GB minus 2 Bytes | 2GB (Limit Only by Volume Size) | 16MB (Limit Only by Volume Size) |
| **Max Clusters Number** | 2 ^ 64 clusters – 1 cluster | 2 ^ 32 clusters – 1 cluster | 4294967295 | 4177918 | 65520 | 4080 |
| **Max File Name Length** | Up to 255 | Up to 255 | Up to 255 | Up to 255 | Standard - 8.3<br>Extended - up to 255 | Up to 254 |
| **File System Features** | | | | | | |
| **Unicode File Names** | Unicode Character Set | Unicode Character Set | Unicode Character Set | System Character Set | System Character Set | System Character Set |
| **System Records Mirror** | MFT Mirror File | MFT Mirror File | No | Second Copy of FAT | Second Copy of FAT | Second Copy of FAT |
| **Boot Sector Location** | First and Last Sectors | First and Last Sectors | Sectors 0 to 11 Copy in 12 to 23 | First Sector and Copy in Sector #6 | First Sector | First Sector |
| **File Attributes** | Standard and Custom | Standard and Custom | Standard Set | Standard Set | Standard Set | Standard Set |
| **Alternate Streams** | Yes | Yes | No | No | No | No |
| **Compression** | Yes | Yes | No | No | No | No |
| **Encryption** | Yes | No | No | No | No | No |
| **Object Permissions** | Yes | Yes | Yes | No | No | No |
| **Disk Quotas** | Yes | No | No | No | No | No |
| **Sparse Files** | Yes | No | No | No | No | No |
| **Reparse Points** | Yes | No | No | No | No | No |
| **Volume Mount Points** | Yes | No | No | No | No | No |
| **Overall Performance** | | | | | | |
| **Built-In Security** | Yes | Yes | Yes minimal ACL only | No | No | No |
| **Recoverability** | Yes | Yes | Yes if TFAT activated | No | No | No |
| **Performance** | Low on small volumes High on Large | Low on small volumes High on Large | High | High on small volumes Low on large | Highest on small volumes Low on large | High |
| **Disk Space Economy** | Max | Max | Max | Average | Minimal on large volumes | Max |
| **Fault Tolerance** | Max | Max | Yes if TFAT activated | Minimal | Average | Average |

# *Windows Programs*

- Programming/Development
    - XAMPP - used to develop and host websites. Website files stored in *C:\xampp\htdocs*
    - Python - scripting programing language
    - PHP - web-focused programing language
    - Java JDK/JRE - object oriented programing language
    - Eclipse - Integrated development environment for programming
    - GitHub Desktop - version control software; usually used when programming
    - Blender - 3D modeling program
    - Unity Game Engine - cross-platform game engine for game development
    - Matlab - Programming language with mathematical focus
    - Visual Studio - Integrated development environment for programming
    - Sublime Text Editor - typically for programming
    - Cygwin - GNU Linux tools for Windows
- Pen-testing
    - Metasploit - penetration testing software. Has a folder at *~/.msf4* containing logs, history, and other settings.
    - Wireshark - network analysis software
    - Nmap - network scanner
    - Tor Browser - proxy-based browser built on Firefox
    - Burp Suite - web application testing tool
    - Cain & Able - penetration testing and password recovery tool
    - Mimikatz - penetration testing tool targeting Windows
    - IDA pro - reverse engineering tool
- Defensive
    - Snort - intrusion detection/prevention system
    - AVG AntiVirus
    - Malwarebytes - antivirus
    - TrueCrypt - used to encrypt harddrives
    - Autopsy - forensics analysis software
    - FKTImager - forensics software for data previews and imaging
    - RegRipper - forensics software for extracting registry data
- Utils
    - Putty - SSH and telnet client. RegRipper has a plugin to detect SSH keys
    - Icecream Screen Recorder - used to record/takes pictures of screen
    - Win32 Disk Imager - tool for imaging USB flash drives
    - Rufus - tool for creating bootable USB flash drives
    - CCleaner - a utility program used to clean Windows

Registry entries from a computer.
    - Filezilla - FTP client
    - 7zip - archive utility
    - BitTorrent - Torrenting software
- Virtualization
    - Virtualbox
    - VMware
    - XenCenter - capable to nested virtualization
    - Bluestacks - Android virtual machines
- Communication
    - Pidgin - universal chat client (cross-platform)
    - Thunderbird - email client (cross-platform)
    - Microsoft Outlook - email client
- Gaming
    - Minecraft - popular cross-platform game
    - League of Legends - popular competitive PC game
    - Steam - video game distribution platform
    - DaedalusX64 R747 - game emulation software
- General
    - Chrome - best web browser
    - Firefox - decent web browser
    - Teamviewer - remote desktop software
    - Skype - text and video communication software
    - VLC Media Player
    - GIMP - raster graphics editor
    - Inkscape - vector graphics editor
    - Microsoft Office - document editor

# *Windows 7 Programs (Default)*

In “C:\Program Files”

- Common Files
- DVD Maker
- Internet Explorer
- Microsoft Games
- MSBuild
- Reference Assemblies
- Windows Defender
- Windows Journal
- Windows Mail
- Windows Media Player
- WIndows NT
- Windows Photo Viewer
- Windows Portable Devices
- Windows Sidebar

In “C:\Program Files (x86)”

- Common Files
- Internet Explorer
- MSBuild
- Reference Assemblies
- Windows Defender
- Windows Journal
- Windows Mail
- Windows Media Player
- WIndows NT
- Windows Photo Viewer
- Windows Portable Devices
- Windows Sidebar

In “C:\Windows\System32”

AdapterTroubleshooter.exe,aitagent.exe,alg.exe,appidcertstorecheck.exe,appidpolicyconverter.exe,ARP.EXE,at.exe,AtBroker.exe,attrib.exe,audiodg.exe,auditpol.exe,autochk.exe,autoconv.exe,autofmt.exe,AxInstUI.exe,baaupdate.exe,bcdboot.exe,bcdedit.exe,BdeHdCfg.exe,BdeUISrv.exe,BdeUnlockWizard.exe,BitLockerWizard.exe,BitLockerWizardElev.exe,bitsadmin.exe,bootcfg.exe,bridgeunattend.exe,bthudtask.exe,cacls.exe,calc.exe,CertEnrollCtrl.exe,certreq.exe,certutil.exe,change.exe,charmap.exe,chglogon.exe,chgport.exe,chgusr.exe,chkdsk.ex

e,chkntfs.exe,choice.exe,cipher.exe,cleanmgr.exe,cliconfg.exe,clip.exe,cmd.exe,cmdkey.exe,cmdl32.exe,cmmon32.exe,cmstp.exe,cofire.exe,colorcpl.exe,comp.exe,compact.exe,CompMgmtLauncher.exe,ComputerDefaults.exe,conhost.exe,consent.exe,control.exe,convert.exe,credwiz.exe,cscript.exe,csrss.exe,ctfmon.exe,cttune.exe,cttunesvr.exe,dccw.exe,dcomcnfg.exe,ddodiag.exe,Defrag.exe,DeviceDisplayObjectProvider.exe,DeviceEject.exe,DevicePairingWizard.exe,DeviceProperties.exe,DFDWiz.exe,dfrgui.exe,dialer.exe,diantz.exe,dinotify.exe,diskpart.exe,diskperf.exe,diskraid.exe,Dism.exe,dispdiag.exe,DisplaySwitch.exe,djoin.exe,dllhost.exe,dllhst3g.exe,dnscacheugc.exe,doskey.exe,dpapimig.exe,DpiScaling.exe,dpnsvr.exe,driverquery.exe,drvinst.exe,dvdplay.exe,dvdupgrd.exe,dwm.exe,DWWIN.EXE,dxdiag.exe,Dxpserver.exe,Eap3Host.exe,efsui.exe,EhStorAuthn.exe,esentutl.exe,eudcedit.exe,eventcreate.exe,eventvwr.exe,expand.exe,extrac32.exe,fc.exe,find.exe,findstr.exe,finger.exe,fixmapi.exe,fltMC.exe,fontview.exe,forfiles.exe,fsutil.exe,ftp.exe,fvenotify.exe,fveprompt.exe,FXSCOVER.exe,FXSSVC.exe,FXSUNATD.exe,getmac.exe,GettingStarted.exe,gpresult.exe,gpscript.exe,gpupdate.exe,grpconv.exe,hdwwiz.exe,help.exe,HOSTNAME.EXE,hwrcomp.exe,hwrreg.exe,icacls.exe,icardagt.exe,icsunattend.exe,ie4uinit.exe,ieUnatt.exe,iexpress.exe,InfDefaultInstall.exe,ipconfig.exe,irftp.exe,iscsicli.exe,iscsicpl.exe,isoburn.exe,klist.exe,ksetup.exe,ktmutil.exe,label.exe,LocationNotifications.exe,Locator.exe,lodctr.exe,logagent.exe,logman.exe,logoff.exe,LogonUI.exe,lpksetup.exe,lpremove.exe,lsass.exe,lsm.exe,Magnify.exe,makecab.exe,manage-bde.exe,mblctr.exe,mcbuilder.exe,mctadmin.exe,MdRes.exe,MdSched.exe,mfpmp.exe,MigAutoPlay.exe,mmc.exe,mobsync.exe,mountvol.exe,mpnotify.exe,MpSigStub.exe,MRINFO.EXE,msconfig.exe,msdt.exe,msdtc.exe,msfeedssync.exe,msg.exe,mshta.exe,msiexec.exe,msinfo32.exe,mspaint.exe,msra.exe,mstsc.exe,mtstocom.exe,MuiUnattend.exe,MultiDigiMon.exe,NAPSTAT.EXE,Narrator.exe,nbtstat.exe,ndadmin.exe,net.exe,net1.exe,netbtugc.exe,netcfg.exe,netiougc.exe,Netplwiz.exe,NetProj.exe,netsh.exe,NETSTAT.EXE,newdev.exe,nltest.exe,notepad.exe,nslookup.exe,ntoskrnl.exe,ntprint.exe,ocsetup.exe,odbcad32.exe,odbcconf.exe,openfiles.exe,OptionalFeatures.exe,osk.exe,p2phost.exe,PATHPING.EXE,pcalua.exe,pcaui.exe,pcawrk.exe,pcwrun.exe,perfmon.exe,PING.EXE,PkgMgr.exe,plasrv.exe,PnPUnattend.exe,PnPutil.exe,poqexec.exe,powercfg.exe,PresentationHost.exe,PresentationSettings.exe,prevhost.exe,print.exe,PrintBrmUi.exe,printfilterpipelinesvc.exe,PrintIsolationHost.exe,printui.exe,proquota.exe,psr.exe,PushPrinterConnections.exe,qappsrv.exe,qprocess.exe,query.exe,quser.exe,qwinsta.exe,rasautou.exe,rasdial.exe,raserver.exe,rasphone.exe,rdpclip.exe,rdpinit.exe,rdpshell.exe,rdpsign.exe,rdrleakdiag.exe,RDVGHelper.exe,ReAgentc.exe,recdisc.exe,recover.exe,reg.exe,regedt32.exe,regini.exe,RegisterIEPKEYs.exe,regsvr32.exe,rekeywiz.exe,relog.exe,RelPost.exe,repair-bde.exe,replace.exe,reset.exe,resmon.exe,RMActivate.exe,RMActivate_isv.exe,RMActivate_ssp.exe,RMActivate_ssp_isv.exe,RmClient.exe,Robocopy.exe,ROUTE.EXE,RpcPing.exe,rrinstaller.exe,rstrui.exe,runas.exe,rundll32.exe,RunLegacyCPLElevated.exe,runonce.exe,rwinsta.exe,sbunattend.exe,sc.exe,schtasks.exe,sdbinst.exe,sdchange.exe,sdclt.exe,sdiagnhost.exe,SearchFilterHost.exe,SearchIndexer.exe,SearchProtocolHost.exe,SecEdit.exe,secinit.exe,services.exe,sethc.exe,SetIEInstalledDate.exe,setspn.exe,setupcl.exe,setupugc.exe,setx.exe,sfc.exe,shadow.exe,shrpubw.exe,shutdown.exe,sigverif.exe,slui.exe,smss.exe,SndVol.exe,SnippingTool.exe,snmptrap.exe,sort.exe,SoundRecorder.exe,spinstall.exe,spoolsv.exe,sppsvc.exe,spreview.exe,srdelayed.exe,StikyNot.exe,subst.exe,svchost.exe,sxstrace.exe,SyncHost.exe,syskey.exe,systeminfo.exe,SystemPropertiesAdvanced.exe,SystemPropertiesComputerName.exe,SystemPropertiesDataExecutionPrevention.exe,SystemPropertiesHardware.exe,SystemPropertiesPerformance.exe,SystemPropertiesProtection.exe,SystemPropertiesRemote.exe,systray.exe,tabcal.exe,takeown.exe,TapiUnattend.exe,taskeng.exe,taskhost.exe,taskkill.exe,tasklist.exe,taskmgr.exe,tcmsetup.exe,TCPSVCS.EXE,timeout.exe,TpmInit.exe,tracerpt.exe,TRACERT.EXE,tscon.exe,tsdiscon.exe,tskill.exe,TSTheme.exe,TsUsbRedirectionGroupPolicyControl.exe,TSWbPrxy.exe,TsWpfWrp.exe,typeperf.exe,tzutil.exe,ucsvc.exe,UI0Detect.exe,unlodctr.exe,unregmp2.exe,upnpcont.exe,UserAccountControlSettings.exe,userinit.exe,Utilman.exe,VaultCmd.exe,VaultSysUi.exe,vds.exe,vdsldr.exe,verclsid.exe,verifier.exe,vmicsvc.exe,vssadmin.exe,VSSVC.exe,w32tm.exe,waitfor.exe,wbadmin.exe,wbengine.exe,wecutil.exe,WerFault.exe,WerFaultSecure.exe,wermgr.exe,wevtutil.exe,wextract.exe,WFS.exe,where.exe,whoami.exe,wiaacmgr.exe,wiawow64.exe,wimserv.exe,WindowsAnytimeUpgradeResults.exe,wininit.exe,winload.exe,winlogon.exe,winresume.exe,winrs.exe,winrshost.exe,WinSAT.exe,winver.exe,wisptis.exe,wksprt.exe,wlanext.exe,wlrmdr.exe,wowreg32.exe,WPDShextAutoplay.exe,wpnpinst.exe,write.exe,wscript.exe,WSManHTTPConfig.exe,wsmprovhost.exe,wsqmcons.exe,wuapp.exe,wuauclt.exe,WUDFHost.exe,wusa.exe,xcopy.exe,xpsrchvw.exe,xwizard.exe

# *Windows Registry Hives*

- C:\Windows\System32\config\
    - SAM - user account information
    - SYSTEM -
    - SOFTWARE -
    - SECURITY -
- C:\Users\<username>\
    - NTUSER.DAT
- C:\Users\<username>\AppData\Local\Microsoft\Windows\
    - USRCLASS.DAT

# *Linux Programs*

**Text Editors**

- Gedit - GUI based
- Leafpad - GUI based
- Nano/Pico - Command line based; uses hidden folder : ~/.nano
- Emacs - Command line based, but has a GUI version; uses hidden folder: ~/.emacs.d
- vi/vim - Command line based

**Web Browsing**

- w3m - Interactive command line based. uses hidden folder: ~/.w3s
- curl - command line based. Prints webpage to stdout
- wget - command line based. Prints webpage to file
- Firefox/Iceweasel - GUI based; Firefox uses hidden folder: ~/.mozilla
- Chrome - GUI based
- Tor Browser - Firefox based. Used to increase anonymity

**Pen-testing**

- Metasploit - used to create malware and perform well know exploits; uses hidden folder: ~/.ms4
- Nmap - used to perform network reconnaissance
- Zenmap - GUI version of Nmap; uses hidden folder: ~/.zenmap
- Crunch - used to generate words lists/dictionaries.
- John - used to crack passwords, usually given a wordlist. uses hidden folder: ~/.john
- Tshark and tcpdump - captures network traffic
- Wireshark - GUI version tshark
- Apktool and Dex2jar - used to reverse engineer Android applications
- OllyDbg - used for reverse engineering Windows 32-bit applications
- Angr - binary analysis framework utilizing symbolic execution
- CORE - used to simulate computer networks

**Shells**

- Bash - Bourne Again Shell - very popular and usually the default shell; uses hidden files: ~./bash_profile, ~/.bashrc, ~/.bash_history
- Sh - The original shell.
- Ssh - Secure shell - a protocol/program used to run a remote shell on an unsecure network. Replaced rlogin, telnet, and rsh protocols; uses hidden folder: ~/.ssh
- Fish - friendly interactive shell
- Zsh - has features from bash, tcsh, and ksh
- Ksh - Korn shell
- Tcsh/Csh - Uses C-like syntax

**Utility**

- *Networking*
  - Nc - arbitrary TCP and UDP connections and listens
  - Scp - transfer file over the network. Uses ssh
  - Ifconfig - view and configure network interfaces
  - Route - view and configure IP routing table
- *File related*
  - Mkdir - make folder/directory
  - Cd - change working directory of shell
  - Cp - copy file (e.g. cp source.file new_dst.file)
  - Mv - move/rename file

        - Touch - update timestamp of file. If the file does not exist, it is create empty.
        - Ln - create a link to a file
        - Find - search for files
        - more/less - view scrollable file
        - zip/tar/bzip/gzip - used to compress a file/files
        - Dd - read from hardware devices and output to file format
    - *Text related*
        - Yes - print text repeatedly
        - Grep/egrep/fgrep/rgrep - print lines matching a pattern
        - Cat - print the content of a file/files
        - Echo - print text
        - Wc - word count - prints the lines, words, and character count of the input
        - Diff - print the difference between two inputs
    - *Task management*
        - cron - a utility to schedule tasks
        - Watch - execute a command repeatedly
        - Bg - run a task in the background
        - Fg - run a task in the foreground
        - Kill - stop running a task
        - Ps/jobs - print current processes
        - Exec - Replace the current process with a new process
        - Exit - quit shell
    - *Misc.*
        - Systemd, Init - control system's and programs' state
        - Apt, dpkg - package manager for Debian based Linux distribution (install/uninstall programs).
        - Yum - deprecated package manager for Redhat based Linux distributions
        - Pacman - package manager for Arch based linux distributions
        - Docker - use to manage program sandbox
        - Man - used to view the manual for programs
        - Passwd - change the password of a user
        - Fdisk - used to manage disk partitions
        - Mount - mount a drive (e.g. usb or hard drive usually found in the /dev folder) onto a folder.
        - md5sum - compute the md5 checksum of an input
        - shasum - compute the sha1 checksum of an input

# *Glossary*

From “Computer Incident Response and Forensics Team Management : Conducting a Successful Incident Response”

- Attacker : “Person or entity performing any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.”
- Botnet : Shorted term for Robot Network, this is a network of compromised computers and servers that are remotely controlled by unauthorized personnel where the compromised devices are performing activities not under the
- Computer Forensics : “The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.”
- Digital Signature : “A digital signature is a mathematical encryption mechanism for proving the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and nonrepudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.”
- Cybercrime profiling : “the investigation, analysis, assessment and reconstruction of data from a behavioral/psychological perspective extracted from computer systems, networks and the humans committing the crimes”
    - “The inductive approach assumes that individuals who committed the same crimes in the past share characteristics with individuals who are committing the same crime now. Examples of such profiles are those created for serial killers and rapists. The deductive approach uses evidence collected at the crime scene to develop a specific profile that can be used for offender identification. Understanding inductive profiles helps as the deductive approach frequently looks to them for clues in developing a more specific offender profile”
- Intent : The intent to commit a crime: malice, as evidenced by a criminal act; intent to deprive or defraud the true owner of his property. A person intends a consequence they foresee that it will happen if the given series of acts or omissions continue, and desires it to happen.
- Intrusion : The unauthorized act of bypassing the security mechanisms of a system for the purposes of causing an incident.
- Logic Bomb : A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.
- Malware : Malicious software which is designed to damage or disable computers with the intent to steal information or gain control of the device. Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. Examples include virus, worm, Trojan

horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

- Nonrepudiation : “Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the information. This protection against an individual falsely denying having performed a particular action provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.”
- Penetration Test : A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.
- Piracy : Illegally reproducing copyrighted work. Music, photographs, movies, and software are all potentially copyrighted and can be pirated.
- Privacy : The act of guaranteeing that the interests of persons and organizations are protected and secluded from outside disclosure.
- Spam : Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
- Spear phishing : A targeted phishing attack on a select group of victims, usually executives.
- Spoofing : There are two meanings to spoofing in our context:
    - Either faking the sending address of a transmission to gain illegal entry into a secure system or
    - the deliberate inducement of a user or resource to take incorrect action.
    - Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.
- Spyware : Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
- Zombie : An infected computer that floods another computer with packets in an attempt to infect or crash it without the consent or knowledge of the infected computer’s owner.

# *References*


- 
- https://www.diffen.com/difference/FAT32_vs_NTFS
- https://www.howtogeek.com/235596/whats-the-difference-between-fat32-exfat-and-ntfs/
- http://www.pointsoftware.ch/en/4-ext4-vs-ext3-filesystem-and-why-delayed-allocation-is-bad/
- http://www.ntfs.com/ntfs_vs_fat.htm
- Petherick, Wayne. Profiling and Serial Crime : Theoretical and Practical Issues, Elsevier Science & Technology, 2012. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/fbial-ebooks/detail.action?docID=1111846. Created from fbial-ebooks on 2018-06-30 20:38:56.
- Johnson, Leighton. Computer Incident Response and Forensics Team Management : Conducting a Successful Incident Response, William Andrew, 2013. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/fbial-ebooks/detail.action?docID=1115165. Created from fbial-ebooks on 2018-06-30 20:03:59.
- Shipley, Todd G., and Art Bowker. Investigating Internet Crimes : An Introduction to Solving Crimes in Cyberspace, William Andrew, 2013. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/fbial-ebooks/detail.action?docID=1115158. Created from fbial-ebooks on 2018-06-30 16:11:30.
- Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by Babak Akhgar, et al., William Andrew, 2014. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/fbial-ebooks/detail.action?docID=1744499. Created from fbial-ebooks on 2018-06-30 15:40:55.
- Johnson, Leighton. Computer Incident Response and Forensics Team Management : Conducting a Successful Incident Response, William Andrew, 2013. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/fbial-ebooks/detail.action?docID=1115165. Created from fbial-ebooks on 2018-06-30 14:41:06.