DIGITAL NOTESON COMPUTERFORENSICS

B.TECH IIIYEAR-IISEM(2022-23)

COMPUTER FORENSICS(CS 3101E)

SYLLABUS:

UNIT-I

Computer Forensics Fundamentals: What is Computer Forensics?,Use of ComputerForensicsinLawEnforecement,ComputerForensicsAssistancetoHumanRecources/EmploymentProceedings,ComputerForensicsServices,BenefitsofprofessionalForensics Methodology,StepstakenbyComputerForensicsSpecialists.

Types of Computer Forensics Technology: - Types of Business Computer ForensicTechnology.TypesofMilitaryComputerForensicTechnology,TypesofLawEnforcement-ComputerForensicTechnology,TypesofBusinessComputerForensicTechnology.

Computer Forensics Evidence and capture: Data Recovery Defined-Data Back-up andRecovery-TheRole ofBack-upinData Recovery-TheData-RecoverySolution.

UNIT-II

Evidence Collection and Data Seizure: Why Collect Evidence? Collection Options-Obstacles-TypesofEvidence-TheRulesofEvidence-VolatileEvidence-GeneralProcedure-CollectionandArchiving-MethodsofCollections-Artfacts-CollectionSteps -ControllingContamination: Thechainofcustody.
DuplicationandPreservationofDigitalEvidence: PreservingtheDigitalCrimeScene-Computer Evidence processing steps-Legal Aspects of collecting and PreservingComputerforensicEvidence.
ComputerimageVerificationandAuthentication: SpecialneedsofEvidentialAuthentication-PracticalConsideration-PracticalImplementation.

UNIT-III

Computerforensicanalysisandvalidation: Determiningwhatdata tocollectandanalyze, validating forensic data, addressing data-hiding techniques, performing remoteacquisitions

NetworkForensics: Networkforensicoverview,performingliveacquisitions,developing standard procedures for network forensics,using network tools,examiningthe honeynetproject.

Processing crime at incident scenes: Identifying digital evidence, collecting evidence inprivate-sector incident scenes, processing law enforcement crime scenes, preparing for asearch, securing a computer incident or crime scene, seizing digital evidence at the scene,storingdigitalevidence,obtaininga digitalhash,reviewinga case.

UNIT-IV

Current Computer Forensic Tools: evaluating computer forensic tool needs, computerforensic software tools, computer forensic hardware tools, validating and testing forensicsoftware.

E-mail investigations: Exploring the role of email in investigations, exploring the role ofclient and server in email, investigating email crimes and violations, understanding emailservers,usingspecializedemailforensictools.

Cellphoneandmobiledeviceforensics: Understandingmobiledeviceforensic,understandin gacquisitionproceduresforcellphonesandmobile devices.

UNIT-V

Workingwithwindowsanddossystems:understandingfilesystems,exploringMicrosoft file structures examining NTFS disks, understanding whole disk encryption,windowsregistry,Microsoftstartuptasks,MS Dosstartuptasks,virtualmachines.

TEXTBOOKS:

1. ComputerForensics,ComputerCrimeInvestigationbyJohnR,Vacca,FirewallMedia,New Delhi.
2. Computer Forensics and Investigations by Nelson, Phillips Enfinger, Steuart, CENGAGELearning.

REFERENCEBOOKS:

1. RealDigitalForensicsbyKeithj.Jones,RichardBejitlich, CurtisW.Rose,Addison-Wesley PearsonEducation
2. Forensic Compiling,A Tractitioneris Guide by Tony Sammes and BrainJenkinson,SpringerInternationaledition.
3. ComputerEvidenceCollection&PresentationbyChrostopherL.T.Brown,FirewallMedia .
4. HomelandSecurity,Techniques&TechnologiesbyJesusMena,FirewallMedia.
5. SoftwareForensicsCollectingEvidencefromtheSceneofaDigitalCrimebyRobertM.Slade,T MH2005
6. WindowsForensicsbychadSteel,WileyIndiaEdition.

INDEX

UNIT-

1INTRODUCTIO

N

WHATISCOMPUTERFORENSICS?

- Computer forensics is the process of methodically examining computer media (harddisks,diskettes,tapes,etc.)forevidence.Inotherwords,computerforensicsisthecollection, preservation,analysis,and presentationofcomputer-relatedevidence.
- Computer forensics also referred to as computer forensic analysis, electronic discovery,electronic evidence discovery, digital discovery, data recovery, data discovery, computeranalysis,andcomputerexamination.
- Computer evidence can be useful in criminal cases, civil disputes, and human resources/employmentproceedings.

USEOF COMPUTERFORENSICSINLAW ENFORCEMENT

ComputerforensicsassistsinLawEnforcement. Thiscaninclude:

- Recoveringdeleted filessuchasdocuments,graphics,andphotos.
- Searching unallocated space on the hard drive, places where an abundance of data oftenresides.
- Tracing artifacts, those tidbits of data left behind by the operating system. Our expertsknow how to find these artifacts and,more importantly, they know how to evaluate thevalueoftheinformationtheyfind.
- Processing hidden files — files that are not visible or accessible to the user — that containpast usage information. Often, this process requires reconstructing and analyzing the datecodes for each file and determining when each file was created, last modified, last accessedandwhendeleted.
- Runningastring-searchfore-mail,whennoe-mailclientisobvious.

COMPUTERFORENSICSASSISTANCETOHUMANRESOURCES/EMPLOYMENT PROCEEDINGS

Computers can contain evidence in many types of human resources proceedings, includingsexualharassmentsuits,allegationsofdiscrimination,andwrongfulterminationclaims.Evidence can be found in electronic mail systems, on network servers, and on individualemployee's computers.

EMPLOYERSAFEGUARDPROGRAM

Employers must safeguard critical business information. An unfortunate concern today is thepossibilitythatdatacouldbedamaged,destroyed,ormisappropriatedby adiscontentedindividual. Before an individual is informed of their termination, a computer forensic specialistshould come on-site and create an exact duplicate of the data on the individual's computer. Inthis way, should the employee choose to do anything to that data before leaving, the employeris protected. Damaged or deleted data can be re-placed, and evidence can be recovered to showwhat occurred. This method can also be used to bolster an employer's case by showing theremoval of proprietary information or to protect the employer from false charges made by theemployee. You should be equipped to find and interpret the clues that have been left behind.This includes situations where files have been deleted, disks have been reformatted, or otherstepshavebeentakentoconcealordestroytheevidence.Forexample,didyouknow?

- ✓ WhatWebsiteshavebeenvisited?
- ✓ Whatfileshavebeendownloaded?
- ✓ Whenfileswerelastaccessed?
- ✓ Ofattemptstoconcealordestroyevidence?
- ✓ Ofattemptstofabricate evidence?
- ✓ That theelectroniccopyofadocumentcancontaintextthatwasremovedfromthe finalprintedversion?
- ✓ Thatsomefaxmachinescancontainexactduplicatesofthelastseveralhundredpagesreceived?

- ✓ Thatfaxessentorreceived viacomputermayremainonthecomputerindefinitely?
- ✓ Thatemailisrapidlybecomingthecommunications mediumofchoiceforbusinesses?
- ✓ Thatpeopletendtowritethingsinemailthattheywouldnever considerwritinginamemorandumorletter?
- ✓ Thatemailhasbeenused successfullyincriminalcasesaswellasincivillitigation?
- ✓ Thatemailis oftenbackedupontapesthatare generallykeptformonthsoryears?
- ✓ Thatmanypeoplekeeptheirfinancialrecords,includinginvestments,oncomputers?

COMPUTERFORENSICSSERVICES

Computerforensicsprofessionalsshouldbeabletosuccessfullyperformcomplexevidencerecovery procedureswiththeskillandexpertise thatlendscredibilitytoyourcase.

For example,theyshould beabletoperformthefollowingservices:

1. DATASEIZURE

- ✓ Followingfederalguidelines,computerforensicsexpertsshouldactastherepresentative,using theirknowledgeofdatastoragetechnologiestotrackdownevidence.
- ✓ Theexpertsshouldalsobe ableto assistofficials duringtheequipmentseizureprocess.

2. DATADUPLICATION/PRESERVATION

- ✓ Whenonepartymustseizedatafromanother,twoconcernsmustbeaddressed:
  - thedatamustnotbealteredinanyway
  - theseizuremustnotputanundueburdenontherespondingparty
- ✓ Thecomputerforensicsexpertsshouldacknowledgebothoftheseconcernsbymakinganexactd uplicateoftheneededdata.
- ✓ Whenexpertsworksontheduplicatedata,theintegrityoftheoriginalismaintained.

3. DATARECOVERY

- ✓ Usingproprietarytools,yourcomputer forensicsexpertsshouldbeabletosafelyrecover

andanalyzeotherwiseinaccessibleevidence.

- ✓ Theabilitytorecoverlostevidenceismadepossiblebytheexpert'sadvancedunderstandingofstoragetechnologies.

4. DOCUMENTSEARCHES

- ✓ Computerforensicsexpertsshouldalsobeabletosearchover200,000electronicdocumentsinseconds ratherthanhours.
- ✓ The speed and efficiency of these searches make the discovery process less complicatedandlessintrusivetoallpartiesinvolved.

5. MEDIACONVERSION

- ✓ Computer forensics experts should extract the relevant data from old and un-readabledevices,convertitintoreadableformats,and placeitontonewstoragemediaforanalysis.

6. EXPERTWITNESSSERVICES

- ✓ Computer forensics experts should be able to explain complex technical processes in aneasy-to-understandfashion.
- ✓ This should help judges and juries comprehend how computer evidence is found, what itconsists of,andhow itis relevanttoa specificsituation.

7. COMPUTEREVIDENCESERVICEOPTIONS

Computer forensics experts should offer various levels of service, each designed to suit yourindividualinvestigativeneeds.Forexample,they shouldbeabletoofferthefollowingservices:

- ✓ **Standard service**: Computer forensics experts should be able to work on your caseduringnor-malbusinesshoursuntilyourcriticalelectronicevidenceisfound.
- ✓ **On-siteservice**:Computerforensicsexpertsshouldbeabletotraveltoyourlocationto

per-formcompletecomputerevidenceservices.Whileon-site,theexpertsshouldquicklybe able to produceexactduplicatesofthedatastoragemediainquestion.

- ✓ **Emergency service**: Your computer forensics experts should be able to give your casethe highest priority in their laboratories. They should be able to work on it withoutinterruptionuntilyourevidenceobjectivesaremet.
- ✓ **Priority service**: Dedicated computer forensics experts should be able to work on yourcase during normal business hours (8:00 A.M. to 5:00 P.M., Monday through Friday)untiltheevidenceis found.Priorityservicetypicallycutsyourturnaroundtimeinhalf.
- ✓ **Weekend service**: Computer forensics experts shouldbe able towork from 8:00A.M.to 5:00 P.M., Saturday and Sunday, to locate the needed electronic evidence and willcontinue14ComputerForensics,SecondEditionworkingonyourcaseuntilyourevidenceo bjectives aremet.

8. OTHERMISCELLANEOUSSERVICES

Computerforensicsexpertsshouldalsobeabletoprovideextendedservices.Theseservicesinclude:

- ✓ Analysisofcomputersanddataincriminalinvestigations
- ✓ On-siteseizureofcomputerdataincriminalinvestigations
- ✓ Analysisofcomputersand dataincivillitigation.
- ✓ On-siteseizureofcomputerdataincivillitigation
- ✓ Analysisofcompanycomputersto determineemployeeactivity
- ✓ Assistanceinpreparing electronicdiscoveryrequests
- ✓ Reportinginacomprehensiveandreadilyunderstandablemanner
- ✓ Court-recognizedcomputerexpertwitnesstestimony
- ✓ Computer forensicsonbothPCandMacplatforms
- ✓ Fastturnaroundtime.

BENEFITSOFPROFESSIONALFORENSICMETHODOLOGY

Aknowledgeablecomputerforensics professionalshouldensure thatasubjectcomputersystemis carefullyhandledtoensurethat:

1. Nopossibleevidenceisdamaged,destroyed,orotherwisecompromisedbytheprocedure s usedtoinvestigatethe computer.
2. Nopossiblecomputervirusisintroducedtoasubjectcomputerduringthe analysisprocess.
3. Extractedandpossiblyrelevantevidenceisproperlyhandledandprotectedfromlatermechanic alorelectromagneticdamage.
4. Acontinuingchainofcustodyisestablishedand maintained.
5. Businessoperationsareaffectedforalimitedamountoftime,ifatall.
6. Anyclient-attorneyinformationthatisinadvertentlyacquiredduringaforensicexplorationisethicall yandlegallyrespectedandnotdivulged.

STEPSTAKENBYCOMPUTERFORENSICSSPECIALISTS

The computer forensics specialist should take several careful steps to identify and attempt toretrieve possible evidence that may exist on a subject's computer system. For example, thefollowingsteps shouldbetaken:

1. **Protect**thesubjectcomputersystem duringtheforensicexaminationfrom any possiblealteration,damage,data corruption,orvirusintroduction.
2. **Discover**allfilesonthesubjectsystem.Thisincludesexistingnormalfiles,deletedyetremainin gfiles,hidden files,password-protectedfiles,and encryptedfiles.
3. **Recover**allofdiscovereddeletedfiles.
4. **Reveal**thecontentsofhiddenfilesaswellastemporaryorswapfilesusedbyboththeapplicationp rograms andtheoperatingsystem.
5. **Access**the contentsofprotectedorencryptedfiles.
6. **Analyze**allpossiblyrelevantdatafoundinspecialareasofadisk.Thisincludesbutisnotlimitedt

owhatiscalledunallocatedspaceonadisk,aswellasslackspaceinafile

(the remnant area at the end of a file in the last assigned disk cluster, that is unused bycurrent file data, but once again, may be a possible site for previously created andrelevantevidence).

7. **Print out** an overall analysis of the subject computer system, as well as a listing of allpossiblyrelevantfilesanddiscoveredfiledata.
8. **Provide** an opinion of the system layout; the file structures discovered; any discovereddataandauthorshipinformation;anyattemptstohide,delete,protect,andencryptinformation; and anything else that has been discovered and appears to be relevant to theoverallcomputersystemexamination.
9. **Provide**expertconsultationand/ortestimony, asrequired.

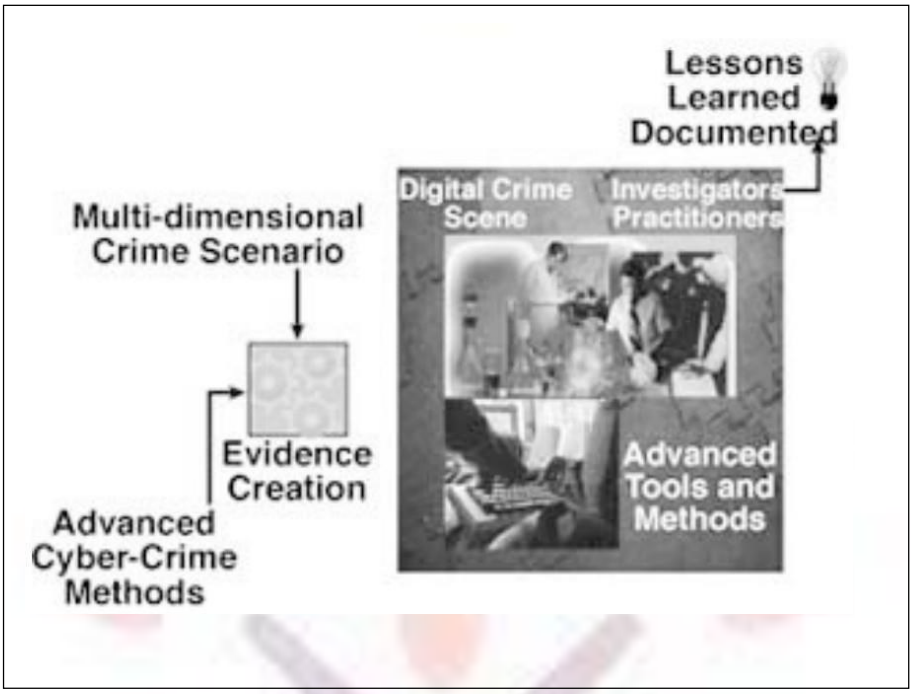
TYPESOFCOMPUTERFORENSICTECHNOLOGY

TYPESOFMILITARYCOMPUTERFORENSICTECHNOLOGY

- Key objectives of cyber forensics include rapid discovery of evidence, estimation ofpotentialimpactofthemaliciousactivityonthevictim,andassessmentoftheintentandidentityoftheperpetrator.
- Real-timetrackingof potentially maliciousactivity isespecially difficultwhen thepertinent information has been intentionally hidden, destroyed, or modified in order toeludediscovery.
- National Law Enforcement and Corrections Technology Center (NLECTC) works withcriminaljustice professionalsto identifyurgentand emergingtechnologyneeds.
- NLECTCcentersdemonstratenewtechnologies,testcommerciallyavailabletechnologies andpublishresults—linkingresearchandpractice.
- National Institute of Justice (NIJ) sponsors research and development or identifies bestpractices toaddressthoseneeds.
- The information directorate entered into a partnership with the NIJ via the auspices oftheNLECTC,totestthenewideasandprototypetools.TheComputerForensicsExperiment2000(CFX-2000)resultedfromthispartnership.

COMPUTERFORENSICEXPERIMENT-2000(CFX-2000)

- ✓ CFX-2000isanintegratedforensicanalysisframework.
- ✓ The central hypothesis of CFX-2000 is that it is possible to accurately determine themotives, intent, targets, sophistication, identity, and location of cyber criminals andcyberterroristsbydeployinganintegratedforensicanalysisframework.
- ✓ The cyber forensic tools involved in CFX-2000 consisted of commercial off-the-shelfsoftware and directorate-sponsored R&D prototypes. CFX includes SI-FI integrationenvironment.
- ✓ The*SynthesizingInformationfromForensicInvestigations*(SI-FI)integrationenvironment supports the collection, examination, and analysis processes employedduringacyber-forensicinvestigation.
- ✓ TheSI-FIprototypeusesdigitalevidence bags(DEBs),which are *secure*and *tamperproofcontainers*usedtostoredigitalevidence.
- ✓ Investigators can seal evidencein theDEBsandusethe SI-FI implementation tocollaborateoncomplexinvestigations.
- ✓ AuthorizeduserscansecurelyreopentheDEBsforexamination,whileautomaticauditofallactions ensures thecontinuedintegrityoftheircontents.
- ✓ The teams used other forensic tools and prototypes to collect and analyze specificfeatures of the digital evidence, perform case management and time lining of digitalevents,automateeventlinkanalysis,and performsteganographydetection.
- ✓ The results of CFX-2000 verified that the hypothesis was largely correct and that it ispossible toascertaintheintentandidentityofcybercriminals.
- ✓ As electronic technology continues its explosive growth, researchers need to continuevigorous R&D of cyber forensic technology in preparation for the onslaught of cyberreconnaissanceprobes andattacks.



TYPES OF LAW ENFORCEMENT COMPUTER FORENSICTECHNOLOGY

Computerforensicstoolsandtechniqueshavebecomeimportantresourcesforuseininternalinvestigations,civillawsuits,andcomputersecurityriskmanagement.Lawenforcement and military agencies have been involved in processing computer evidence foryears.

ComputerEvidenceProcessingProcedures

Processing procedures and methodologies should conform to federal computer evidenceprocessingstandards.

1. PreservationofEvidence

- ✓ Computerevidenceisfragileandsusceptibletoalterationorerasurebyanynumberofoccurrences.
- ✓ Computer evidencecanbeusefulincriminalcases,civildisputes,andhumanresources/

employmentproceedings.

- ✓ Black box computer forensics software tools are good for some basicinvestigationtasks,buttheydonotofferafullcomputerforensicssolution.
- ✓ SafeBacksoftwareovercomessomeoftheevidenceweaknessesinherentinblackboxcomputerforensicsapproaches.
- ✓ SafeBacktechnologyhasbecomeaworldwidestandardinmakingmirrorimagebackups since1990.

TROJANHORSE PROGRAMS

- ✓ The computer forensic expert should be able to demonstrate his or her ability to avoiddestructiveprogramsandtrapsthatcanbeplantedbycomputerusersbentondestroyingdataandevidence.
- ✓ Such programs can also be used to covertly capture sensitive information, passwords,andnetworklogons.

COMPUTERFORENSICSDOCUMENTATION

- ✓ Withoutproperdocumentation,itisdifficulttopresentfindings.
- ✓ Ifthesecurityorauditfindingsbecometheobjectofalawsuitoracriminalinvestigation,thendocumentationbecomes evenmoreimportant.

FILESLACK

- ✓ Slack space in a file is the remnant area at the end of a file in the last assigned diskcluster, that is unused by current file data, but once again, may be a possible site forpreviouslycreatedandrelevantevidence.
- ✓ Techniques and automated tools that are used by the experts to capture and evaluate fileslack.

DATA-HIDINGTECHNIQUES

- ✓ Trade secret information and othersensitive data caneasily be secreted using anynumber of techniques. It is possible to hide diskettes within diskettes and to hide entirecomputer hard disk drive partitions. Computer forensic experts should understand suchissuesand toolsthathelpintheidentificationofsuchanomalies.

OMMERCEINVESTIGATIONS

- ✓ **Net Threat Analyzer** can be used to identify past Internet browsing and email activitydone through specific computers. The software analyzes a computer's disk drives andother storage areas that are generally unknown to or beyond the reach of most generalcomputerusers.NetThreatAnalyzeravail-ablefreeof chargetocomputercrimespecialists,schoolofficials,andpolice.

DUAL-PURPOSEPROGRAMS

- ✓ Programs can be designed to perform multiple processes and tasks at the same time.Computerforensicsexpertsmusthavehands-onexperience withtheseprograms.

TEXTSEARCHTECHNIQUES

- ✓ Tools that can be used to find targeted strings of text in files, file slack, unallocated filespace,andWindowsswapfiles.

FUZZYLOGICTOOLSUSEDTOIDENTIFYUNKNOWNTEXT

- ✓ Computer evidence searches require that the computer specialist know what is beingsearchedfor.Many timesnotall isknown aboutwhatmay bestored on agivencomputersystem.
- ✓ In such cases, fuzzy logic tools can provide valuable leads as to how the subject computerwasused.

2. DiskStructure

- ✓ Computerforensicexpertsmustunderstandhowcomputerharddisksandfloppydiskettes are structured and how computer evidence can reside at various levels withinthe structureofthedisk.
- ✓ They should also demonstrate their knowledge of how to modify the structure and hidedata inobscureplaces onfloppydiskettes andharddiskdrives.

3. DataEncryption

- ✓ Computer forensic experts should become familiar with the use of software to cracksecurityassociatedwiththe differentfilestructures.

4. MatchingaDiskettetoaComputer

- ✓ Specialized techniques and tools that make it possible to conclusively tie a diskette to acomputer that was used to create or edit files stored on it. Computer forensic expertsshouldbecomefamiliarhowto usespecialsoftwaretoolstocompletethisprocess.

5. DataCompression

- ✓ Computer forensic experts should become familiar with how compression works andhow compression programs can be used to hide and disguise sensitive data and alsolearnhow password-protectedcompressedfilescanbebroken.

6. ErasedFiles

- ✓ Computer forensic experts should become familiar with how previously erased files canbe recovered by using DOS programs and by manually using data-recovery technique &familiarwithclusterchaining.

7. InternetAbuseIdentificationandDetection

- ✓ Computer forensic experts should become familiar with how to use specialized softwaretoidentifyhow atargetedcomputerhasbeenusedontheInternet.
- ✓ This process will focus on computer forensics issues tied to data that the computer userprobably doesn't realize exists (file slack, unallocated file space, and Windows swapfiles).

8. TheBootProcessandMemoryResidentPrograms

- ✓ Computer forensic experts should become familiar with how the operating system canbemodifiedtochangedataanddestroydataatthe whimofthepersonwhoconfiguredthesystem.
- ✓ Such a technique could be used to covertly capture keyboard activity from corporateexecutives, for example. For this reason, it isimportant that the experts understandthesepotentialrisks andhowtoidentifythem.

TYPESOFBUSINESSCOMPUTERFORENSICTECHNOLOGY

Thefollowingaredifferenttypesofbusinesscomputerforensicstechnology:-

REMOTEMONITORINGOFTARGETCOMPUTERS

- ✓ *DataInterceptionbyRemoteTransmission*(*DIRT*)isapowerfulremotecontrolmonitoring tool that allows stealth monitoring of all activity on one or more targetcomputers simultaneously fromaremotecommandcenter.
- ✓ No physical access is necessary. Application also allows agents to remotely seize andsecuredigitalevidencepriortophysicallyenteringsuspectpremises.

CREATINGTRACKABLEELECTRONICDOCUMENTS

- ✓ *BinaryAudit Identification Transfer*(*BAIT*) isapowerful intrusion detection tool thatallows users tocreate*trackable*electronicdocuments.
- ✓ BAIT identifies (including their location) unauthorized intruders who access, download,andviewthesetaggeddocuments.
- ✓ BAITalsoallowssecuritypersonneltotracethechainofcustodyandchainofcommand ofallwhopossess thestolenelectronicdocuments.

THEFTRECOVERYSOFTWAREFORLAPTOPS ANDPCS

- ✓ Whatitreallycoststo replaceastolencomputer:
  - Thepriceofthereplacementhardware&software.
  - The cost of recreating data, lost production time or instruction time, reportingand investigating the theft, filing police reports and insurance claims, increasedinsurance,processingandorderingreplacements,cuttingacheck, andthelike.
  - Thelossofcustomergoodwill.
  - Ifathiefisevercaught,thecostoftimeinvolvedinprosecution.

- ✓ PCPHONEHOME
  - PC PhoneHome is a software application that will track and locate alost or stolenPC or laptop any-where in the world. It is easy to install. It is also

completelytransparenttotheuser.

- If your *PC PhoneHome*-protected computer is lost or stolen, all you need to do ismake a report to the local police and call CD's 24-hour command center. CD'srecoveryspecialistswillassistlocallawenforcementintherecoveryofyourproperty.

FORENSICSERVICESAVAILABLE

Servicesincludebutarenotlimitedto:

- Lostpasswordandfilerecovery
- Locationand retrievalofdeletedand hidden files
- Fileandemaildecryption
- Emailsupervisionandauthentication
- Threateningemailtracedtosource
- IdentificationofInternetactivity
- Computerusagepolicyandsupervision
- RemotePCandnetworkmonitoring
- Trackingandlocationofstolenelectronicfiles
- Honeypotstingoperations
- Locationandidentityofunauthorizedsoftwareusers
- Theftrecoverysoftwareforlaptops andPCs
- Investigativeandsecuritysoftwarecreation
- Protectionfromhackersandviruses.

COMPUTERFORENSICEVIDENCE&CAPTURE

DataRecoveryDefined

- Datarecoveryistheprocessinwhichhighlytrainedengineersevaluateandextractdatafromdamagedmediaandreturnitinanintactformat.
- Many people, even computer experts,fail to recognize data recoveryas an option during a data crisis. But it is possible to retrieve files that havebeen deleted and passwords that have been forgotten or to recover entire harddrivesthathavebeenphysicallydamaged.

DataBack-upandRecovery

Back-upObstacles

- **Back-up Window**: The back-up window is the period of time whenback-ups can be run. The back-up window is generally timed to occur duringnonproductionperiodswhennetworkbandwidthandCPUutilizationarelow.
- **Networkbandwidth**:Ifanetworkcannothandletheimpactoftransporting hundreds of gigabytes of data over a short period of time, theorganization'scentralizedbackupstrategyisnotviable.
- **System throughput**: Three I/O bottlenecks are commonly found intraditionalbackupschemes.Theseare

1. The ability of the system being backed up to push data to the backupserver
2. The ability of the backup server to accept data from multiple systemssimultaneously
3. The available throughput of the tape device(s) onto which the data

ismoved

- **Lack-ofResources**:Manycompaniesfailtomakeappropriateinvestmentsindataprotectionuntilitistoolate.

TheRoleofBack-upinDataRecovery

Therearemanyfactorsthataffectback-up.Forexample:

- **Storagecostsaredecreasing**:Thecostpermegabyteof primary(online)storagehasfallendramaticallyoverthepastseveralyearsandcontinuestodosoasdiskdrivetechnologiesadvance.
- **Systems have to be on-line continuously**: Because systems must becontinuously online, the dilemma becomes that you can no longer take filesofflinelongenoughtoperformbackup.
- **The role of Back-up has changed**: The role of backup now includesthe responsibility for recovering user errors and ensuring that good data hasbeensavedandcanquicklyberestored.

CONVENTIONALTAPEBACK-UPINTODAY'SMARKET

- ✓ A typical tape management system consists of a dedicated workstationwith the front-end interfaced to the network and the back-end controlling arepository of tape devices. The media server runs tape managementsoftware.Itcanadministerbackupdevicesthroughoutanenterpriseand canruncontinuous parallelbackups and restores.
- ✓ An alternative to tape backup is to physically replicate or mirror alldata and keep two copies online atall times. The advantage is that the datadoes nothave tobe restored, so there are noissues withimmediate dataavailability.

ISSUESWITHTODAY'SBACK-UP

- ✓ **NETWORKBACKUP**createsnetworkperformanceproblems.Usingthe

productionnetworktocarrybackupdata,aswellasfornormaluser

dataaccess,canseverelyoverburdentoday'sbusynetworkresources.

- ✓ **OFFLINE BACKUP** affects data accessibility. The time that the hostis offline for data backup must be minimized. This requires extremely high-speed,continuousparallelbackupofthe rawimageofthedata.
- ✓ **LIVE BACKUPS** allow data access during the backup process butaffectperformance.Thedownsidetothelivebackupisthatitputsatremendous burdenonthehost.
- ✓ **MIRRORING**doesn't protect against user error and replication ofbad data. Fully replicated online data sounds great, albeit at twice the cost permegabyteofasinglecopyofonlinedata.

NEWARCHITECTURESANDTECHNIQUESAREREQUIRED

- ✓ Backupatextremelyhighspeedisrequired.Recoverymustbeavailable at file level. The time that systems off-line for back-up must beeliminated.
- ✓ Remote hot recovery sites are needed for immediate resumptionofdata access.Backup of critical data is still required toensure againstdataerrorsandusererrors.
- ✓ To achieve effective backup and recovery, the decoupling of data from its storagespaceisneeded.
- ✓ It is necessary to develop techniques to journal modified pages, so thatjournaling can be invoked within the primary storage device, without hostintervention.
- ✓ Part of the primary storage area must be set aside for data to be backedup.Thisareamustbeaslargeasthelargestbackupblock.Weshouldhave fastnonrandomrestorationofcriticaldata.

TheDataRecoverySolution

SHRINKINGEXPERTISE,GROWINGCOMPLEXITY

a. Thecomplexsystemsthathaveevolvedoverthepast30yearsmustbe

monitored, managed, controlled, and optimized. But most of the brightyoung graduates this term haven't had much exposure to mainframeconcepts.

b. Backups often take place while an application is running. Applicationchanges take place on the fly. If an outage occurs, the company standstolosetens ofthousands ofdollars anhour.

FAILURES:

Disk storage is more reliable than ever, buthardware failures are still possible.A simplemistake can be made by an application programmer, system programmer, or operations person.Logic errors in programs or application of the wrong update at the wrong time can result in asystem crash or, worse. Disasters do really occurs! Floods, tornadoes, earthquakes, tsunamis,andeventerrorismcandostrike.Wemustbeready.

BUDGETSANDDOWNTIME

We have fewer resources (people, processing power, time, and money) to do more work thanever before, and we must keep your expenses under control. Systems must remain available tomake moneyandservecustomers.Downtimeismuchtooexpensivetobetolerated.

RECOVERY:THINKBEFOREYOUBACK-UP

One of the most critical data-management tasks involves recovering data in the event of aproblem. You must evaluate your preparations, make sure that all resources are available inusable condition, automate processes as much as possible, and make sure you have the rightkindofresources.

Evaluateyourpreparation

If all of the resources (image copies, change accumulations, and logs) are available at recoverytime, these preparations certainly allow for a standard recovery. Finding out at recovery timethatsomecriticalresourceismissingcanbedisastrous!

Don'tletyourresources fallthroughthecracks

Identifying different types of conditions is critical to ensuring a successful recovery. Checkingyourassets tomakesure they'rereadyshouldbepartofyourplan.

AutomatedRecovery

Withproperplanningandautomation,recoveryismadepossible,relianceonspecificpersonnelisreduced,andthe human-error factorisnearlyeliminated.

Data integrity and your business relay on building recovery job control language (JCL). In theevent of a disaster, the Information Management System (IMS) recovery control (RECON) datasetsmustbemodifiedinpreparationfortherecovery.

CleaningyourRECONdatasetscantakehoursifdonemanually,andit'sanerror-proneprocess.

MakeRecoveriesEfficient

Multithreading tasks shorten the recovery process. Recovering multiple databases with onepass through your log data certainly will save time. Taking image copies, rebuilding indexes,andvalidatingpointersconcurrentlywiththe recoveryprocessfurtherreducedowntime.

TakeBack-ups

The first step to a successful recovery is the backup of your data. Your goal in backing up datais to do so quickly, efficiently, and usually with minimal impact to your customers. You mightneed only very brief out-ages to take instant copies of your data, or you might have intelligentstorage devices that allow you to take a snapshot of your data. Both methods call for tools toassistinthemanagementofresources.

BACK-UPANDRECOVERYSOLUTION

BMC software has developed a model called the *Back-up and Recovery Solution* (BRS) for theInformationManagementSystem(IMS)product.

ImageCopy

BRS contains an Image Copy component to help manage your image copy process.BRS can take batch, on-line (fuzzy), or incremental image copies; Snapshot copies; orInstantSnapshotcopies.

The Image Copy component of BRS offers a variety of powerful features: dynamic allocation ofall input and output data sets, stacking of output data sets, high performance access methods(fasterI/O),copyingbyvolume,compressionof outputimagecopies,anddatabasegroupprocessing--- allwhileinterfacingwithDBRCandprocessingasynchronously.

ChangeAccumulation

The BRS *Change Accumulation* component takes advantage of multiple engines, large virtualstorageresources,andhigh-speedchannelsandcontrollersthatareavailableinmanyenvironments.

Useofmultipletackcontrolblock(TCB)structuresenablesoverlappingofasmuchprocessingaspossible,reducingbothelapsedandCPUtime.

Recovery

→TheBRS*Recovery*component,whichfunctionallyreplacestheIMS*DatabaseRecovery* utility for null- function (DL/I) databases and data-entry databases (DEDBs),allow recovery of multiple databases with one pass of the log and change accumulationdata setswhile dynamicallyallocatingalldata setsrequiredforrecovery.

→ BRS recovers multiple databases to any point in time. BRS can determine the bestchoicefora Point-in-Time (PIT)recovery.FullDBRS supportincludes:

RECOVERYMANAGER

→ *RecoveryManager*componentlets youautomateandsynchronizerecoveriesacross applications and databases by creating meaningful groups of related databases andcreatingoptimizedJCLtoperformtherecoveryofthesegroups.

→ *RecoveryManager*componentprovidesapositiveresponsefortheIMScommands thatareusedtodeallocateandstartyourdatabases.

→ *RecoveryManager*componentfullyautomatestheprocessofcleaningtheRECON datasets forrestartfollowinga disasterrecovery.

→ *RecoveryManager*componentalsoallowsyoutotestyourrecoverystrategyand

notifiesyouwhenmediaerrorshavejeopardizedyourrecoveryresources.

POINTERCHECKING

BRS offers the capability to verify the validity of database pointers through the*ConcurrentPointer Checking* function for both full-function databases and Fast Path data-entry databases(DEDBs).

INDEXREBUILD

If indexes are ever damaged or lost, the *Index Rebuild* function of BRS allows you rebuild themratherthanrecover them.

RECOVERYADVISOR

The *Recovery Advisor* component of BRS allows you to monitor the frequency of your imagecopies andchangeaccumulations.

It helps you to determine whether allyour databases are being backed-up. By using anynumber of back-up and recovery tools available, you can better manage your world and bereadytorecover!

Unit-II

EVIDENCECOLLECTIONANDDATA SEZIURE

WhyCollectEvidence?

Thesimplereasons forcollectingevidenceare:

→**Future Prevention**: Without knowing what happened, you have no hope of ever beingable tostopsomeoneelsefromdoingitagain.

→**Responsibility**: The attacker is responsible for the damage done, and the only way tobring him to justice is with adequate evidence to prove his actions. The victim has aresponsibilitytothecommunity.Informationgatheredafteracompromisecanbeexaminedan dusedbyotherstopreventfurtherattacks.

CollectionOptions

Onceacompromisehasbeendetected,you havetwooptions:

→**Pull the system off the network and begin collecting evidence**: In this case you mayfind thatyou haveinsufficientevidence or, worse, that the attacker lefta deadmanswitchthatdestroys anyevidenceoncethesystemdetectsthatitsoffline.

→**Leave it online and attempt to monitor the intruder**: you may accidentally alert theintruderwhilemonitoringandcausehimtowipehistracksanywaynecessary,destroyingevi denceas hegoes.

Obstacles

→ Computer transactions are fast, they can be conducted from anywhere, can be encryptedoranonymous,andhavenointrinsicidentifyingfeaturessuchashandwritingandsignat urestoidentifythoseresponsible.

- → Anypapertrailofcomputerrecordstheymayleavecan beeasilymodifiedordestroyed,ormaybeonlytemporary.
- → Auditing programs may automatically destroy the records left when computertransactions arefinishedwiththem.
- → Investigatingelectroniccrimeswillalways bedifficultbecauseoftheeaseofalteringthedataandthe factthattransactionsmaybe doneanonymously.
- → Thebestwecandoistofollowtherulesofevidencecollectionandbeasassiduousaspossible.

TypesofEvidence

- **Real Evidence:** Real evidence is any evidence that speaks for itself without relying onanything else. In electronic terms, this can be a log produced by an auditfunction—providedthatthelogcanbeshowntobefreefromcontamination.
- **Testimonial Evidence:** Testimonial evidence is any evidence supplied by a witness. Aslong as the witness can be considered reliable, testimonial evidence can be almost aspowerfulas realevidence.
- **Hearsay:** Hearsay is any evidence presented by a person who was not a direct witness.Hearsayisgenerallyinadmissibleincourtandshouldbe avoided.

TheRulesofEvidence

1. **Admissible**:Admissibleisthemostbasicrule.Theevidencemustbeabletobeusedincourt.
2. **Authentic**:Youmustbeabletoshowthattheevidencerelatesto theincidentinarelevantway.

3. **Complete**:It'snotenough tocollectevidencethatjustshowsoneperspectiveof theincident.

4. **Reliable**:Yourevidencecollectionandanalysisproceduresmustnotcastdoubtontheevidence's authenticityandveracity.

5. **Believable**:Theevidenceyoupresentshouldbeclearlyunderstandableandbelievabletoajury.

Usingthepprecedingfiverules,wecanderivesomebasicdo'sanddon'ts:

- **Minimize handling and corruption of original data:** Once you've created a mastercopy of the original data,don'ttouchitor the original.Any changesmade to theoriginals willaffecttheoutcomesofanyanalysislater donetocopies.
- **Account for any changes and keep detailed logs of your actions:** Sometimes evidencealteration is unavoidable. In these cases, it is absolutely essential that the nature, extent,andreasonsforthechangesbedocumented.
- **Complywiththefiverulesofevidence:**Followingtheserulesisessentialtoguaranteeingsuccessfulevidencecollection.
- **Donotexceedyourknowledge**:Ifyoueverfindyourself–outofyourdepth,‖eithergo and learn more before continuing (if time is available) or find someone who knows theterritory.
- **Follow your local security policy:** If you fail to comply with your company's securitypolicy,youmayfindyourselfwithsomedifficulties.
- **Capture as accurate an image of the system as possible:** Capturing an accurate imageofthesystemisrelatedtominimizingthehandlingorcorruptionoforiginaldata.
- Be prepared to testify: If you're not willing to testify to the evidence you have collected,you might as well stop before you start. No one is going to believe you if they can'treplicateyouractionsandreachthesameresults.
- **Work fast:** The faster you work, the less likely the data is going to change. Volatileevidencemayvanishentirelyifyoudon'tcollectitintime.Ifmultiplesystemsare

involved,workparallel.

- **Proceed from volatile to persistent evidence:** Always try to collect the most volatileevidencefirst.
- **Don'tshutdownbeforecollectingevidence**:Youshouldnever,evershutdownasystem before you collect the evidence. Not only do you lose any volatile evidence, butalso the attacker may have trojaned the startup and shutdown scripts, plug-and-playdevices may alter the system configuration, and temporary file systems may be wipedout.
- **Don't run any programs on the affected system:** The attacker may have left trojanedprograms and libraries on the system;you may inadvertently trigger something thatcouldchangeordestroytheevidenceyou'relookingfor.

VolatileEvidence

Alwaystrytocollectthemostvolatileevidencefirst.Anexampleanorderofvolatilitywouldbe:

1. Registersandcache
2. Routingtables
3. Arpcache
4. Processtable
5. Kernelstatisticsandmodules
6. Mainmemory
7. Temporaryfilesystems
8. Secondarymemory
9. Routerconfiguration
10. Networktopology

GeneralProcedure

- ✓ **IdentificationofEvidence**:Youmustbeabletodistinguishbetweenevidenceandjunkdata

- ✓ **PreservationofEvidence**:Theevidenceyoufindmustbepreservedascloseaspossible toitsoriginal state.
- ✓ **AnalysisofEvidence**:Analysisrequiresin-depthknowledgeofwhatyouarelookingforandhowtogetit.
- ✓ **PresentationofEvidence**:Themannerofpresentationisimportant,anditmustbeunderstandablebyalaymantobeeffective.

CollectionandArchiving

Oncewe'vedevelopedaplanofattackandidentifiedtheevidencethatneedstobecollected.

LogsandLogging: Youshouldrunsomekindof systemloggingfunction. Itisimportant to keep these logs secure and to back them up periodically. Messages andlogsfromprogramscanbe usedtoshow whatdamage anattackerdid.

Monitoring: By monitoring we can gather statistics, watch out for irregular, and tracewhere an attacker is coming from and what he is doing. Unusual activity or the suddenappearance of unknown users should be considered definite cause for closer inspection.Youshoulddisplayadisclaimerstatingwhatmonitoringisdonewhenuserslogon.

MethodsofCollection

Therearetwobasicformsofcollection:freezingthesceneandhoneypotting.

FreezingtheScene

- ✓ It involves taking a snapshot of the system in its compromised state. You should thenstarttocollectwhateverdataisimportantontoremovablenonvolatilemediainastandardformat.

- ✓ All data collectedshouldhave a cryptographicmessagedigestcreated,andthosedigests shouldbecomparedtotheoriginalsforverification.

Honeypotting

- ✓ Itistheprocessof creating areplicasystem andluring theattackerintoitfor furthermonitoring.
- ✓ Theplacementof misleadinginformationandtheattacker's responsetoitisagoodmethodfordeterminingtheattacker'smotives.

Artifacts

- ➢ Thereisalmostalwayssomethingleftbehindbytheattackerbeitcodefragments,trojanedprograms,runningprocesses,or snifferlogfiles.Theseareknownasartifacts.
- ➢ Neverattempttoanalyzeanartifactonthecompromisedsystem.
- ➢ Artifactsarecapableofanything,andwewanttomakesuretheireffectsarecontrolled.

CollectionSteps

1. **FindtheEvidence:**Useachecklist.Notonlydoesithelpyoutocollectevidence,butitalsocanbe used todouble-check thateverythingyouare lookingforisthere.
2. **FindtheRelevantData:**Onceyou've foundtheevidence,youmustfigureoutwhatpartof itisrelevanttothecase.
3. **CreateanOrderofVolatility:**Theorderofvolatilityforyoursystemisagoodguideandens ures thatyouminimizelossofuncorruptedevidence.
4. **Remove external avenues of change:** It is essential that you avoid alterations to theoriginaldata.
5. **CollecttheEvidence:**Collecttheevidenceusingtheappropriatetoolsforthejob.
6. **Documenteverything:**Collection procedures may be questionedlater,soitisimportant that you document everything you do. Timestamps, digital signatures, andsignedstatements areallimportant.

ControllingContamination:TheChainofCustody

Oncethedatahasbeencollected,itmustbeprotectedfromcontamination.Originalsshouldnever beusedinforensicexamination;verifiedduplicatesshouldbeused.

Agoodwayofensuringthatdata remainsuncorruptedistokeepachainofcustody.Thisisadetailedlistofwhatwasdonewiththe originalcopies once theywere collected.

Analysis

- Oncethedatahasbeensuccessfullycollected,itmustbeanalyzedtoextracttheevidenceyo u wishtopresentandtorebuildwhatactuallyhappened.

Time

- Toreconstructtheeventsthatledtoyoursystembeingcorrupted,youmustbeable tocreateatimeline.
- Never,everchangetheclockonanaffectedsystem.

ForensicAnalysisofBack-ups

- When we analyze back-ups, it is best to have a dedicated host for the job. We need adedicated host which is secure, clean and isolated from any network for analyzing back-ups.
- Document everything you do. Ensure that what you do is repeatable and capable ofalwaysgivingthesame results.

ReconstructingtheAttack

After collecting the data, we can attempt to reconstruct the chain of events leading to andfollowing the attacker's break-in. We must correlate all the evidence we have gathered.Include all of the evidence we've found when reconstructing the attack---no matter

howsmallitis.

SearchingandSeizing

Thereisnoone methodologyforperformingacomputerforensic investigationandanalysis.

There are too many variables for to be just one way. Some of the typical variable that comesto the mind includes operating systems; software applications; cryptographic algorithms andapplications; and hardware platforms. But moving beyond these obvious variables springotherequallychallengingvariables:law,internationalboundaries,publicity,andmethodology.

Thereareafewwidelyacceptedguidelinesforcomputer forensicanalysis:

- ✓ Acomputerforensicexaminerisimpartial.Ourjobis toanalyzethemediaandreportourfindingswithnopresumptionofguiltorinnocence.
- ✓ Themediausedincomputerforensicexaminationsmustbesterilizedbefore eachuse.
- ✓ Atrue image (bitstream)oftheoriginalmediamustbemade andusedfortheanalysis.
- ✓ Theintegrityoftheoriginal mediamustbemaintainedthroughouttheentireinvestigation.

BeforetheInvestigation

→Forthesakeoffirstargument,youmusthaveskilledtechniciansin-houseandatopnotchlab therightequipment,therightcomputerforensictools, andsoon.

→Districtattorneys mayrequiremoredocumentationonthechainofevidencehandling.

→Whenyouhaveacasearise,youknowwhatisrequiredandcanworkthecasefromtheinceptioninsupportoftheserequirements.

MethodologyDevelopment

- Define yourmethodology,andworkingaccordingtothismethodology.
- Heremethodologydefinesamethod,asetofrules:guidelinesthatareemployedbyadiscipline.

DocumentEverything

The chain of evidence is so important in computer forensic investigations. If resourcesallow, have two computer forensic personnel assigned to each case every step of the way.Important in the documentation are the times that dates steps were taken; the names of thoseinvolved;andunderwhoseauthoritywerethe steps taken?

EvidenceSearchandSeizure

Priortosearchandseizure,youalreadyhavetheproperdocumentsfilledaswellaspermissionfromtheauthoritytosearchandseizethesuspect'smachine.

Step1:Preparation

You should check all media that is to be used in the examination process. Document thewiping andscanning process.Checktomake sure thatall computerforensictools arelicensedforuseandalllabequipmentisinworkingorder.

Step2:Snapshot

We should photograph the scene, whether it is a room in a home or in a business.Youshould also note the scene. Take advantage of your investigative skills here. Note pictures,personal items, and the like. Photograph the actual Evidence. For example, the evidence is aPCinahomeoffice.Takeaphotographofthemonitor.Removethecasecovercarefullyandphotographtheinternals.

Step3:Transport

If you have the legal authority to transport the evidence to your lab, you should pack theevidence securely. Photograph/videotape and document the handling of evidence leaving thescenetothetransportvehicle andfromtransportvehicletothelabexaminationfacility.

Step4:Examination

Youshouldpreparetheacquiredevidenceforexaminationinyourlab.Therearemany

options to on what tool to use image the drive. You could use *EnCase*, the Unix commandDD, *ByetBack*, or also *SafeBack*. It is wise to have a variety of tools in your lab. Each ofthese tools has its respective strengths. The important note to remember here is: Turn offvirus-scanning software. We must record the time and date of the COMS. Do not boot thesuspectmachine.

When making the image, make sure that the tool you use does not access the file system ofthetargetevidencemedia.Aftermakingtheimage,sealtheoriginalmediainanelectrostatic-safe container, catalog it, and initial the container. Finally, the examination oftheacquiredimagebegins.

DUPLICATIONANDPRESERVATIONOFDIGITALEVIDENCE

PreservingtheDigitalCrimeScene

- ✓ Aftersecuringthecomputer, weshouldmakeacompletebitstreambackupofallcomputerdata beforeitis reviewedorprocessed.
- ✓ Bitstreambackupsaremuchmorethoroughthanstandardbackups.
- ✓ Theyinvolvecopyingofeverybitofdataonastoragedevice,anditisrecommendedthattwosuch copiesbemadeoftheoriginalwhenharddiskdrivesareinvolved.
- ✓ Anyprocessingshouldbe performedononeofthebackupcopies.
- ✓ **IMDUMP** was the first software for taking bit stream back-ups developed by MichaelWhite.

SafeBack

- ➢ **SafeBack**hasbecomealawenforcementstandardandisusedbynumerousgovernmentintelligenceagencies,militaryagencies,andlawenforcementagenciesworldwide.
- ➢ SafeBackprogramcopiesandpreservesalldatacontainedontheharddisk.
- ➢ Evenitgoessofarastocircumventattemptsmadetohidedatainbadclustersandevensectorswith invalidCRCs.

SnapBack

- Anotherbitsteamback-upprogram,called**SnapBack**,isalsoavailableandisusedbysomelawenforcementagenciesprimarilybecauseofitseaseofuse.
- ItspricesseveralhundredsofdollarshigherthanSafeBack.
- Ithaserror-checkingbuiltintoeveryphaseoftheevidenceback-upandrestorationprocess.
- Theharddisk driveshould beimagedusingspecializedbitstreamback-upsoftware.
- Thefloppydiskettescanbeimagedusingthestandard DOSDISKCOPYprogram.
- WhenDOSDISKCOPYisused,itisrecommendedthatthe**MSDOSVersion6.22**beusedand(data verification) switchshouldbeinvokedfromthecommandline.
- Knowandpracticeusingallofyourforensicsoftwaretoolsbeforeyouusethemintheprocessing ofcomputerevidence.
- Wemayonlygetonechancetodoitright.

ComputerEvidenceProcessingSteps

There really are no strict rules that must be followed regarding the processing of computerevidence.

Thefollowingaregeneralcomputer evidenceprocessingsteps:

1. Shutdownthecomputer.

Depending on the computer operating system, this usually involves pulling the plug orshuttingdownanetworkcomputerusingrelevantcommandsrequiredbythenetworkinvolved. Generally, time is of the essence, and the computer system should be shut down asquicklyas possible.

2. Documentthehardwareconfigurationofthesystem.

Be-foredismantlingthecomputer,itisimportantthatpicturesaretakenofthecomputer

from all angles to document the system hardware components and how they are connected.Labeling each wire is also important, so that it can easily be reconnected when the systemconfigurationisrestoredtoitsoriginalconditionatasecurelocation.

3. Transport thecomputersystemtoasecurelocation.

A seized computer left unattended can easily be compromised. Don't leave the computerunattendedunlessitislockedupina securelocation.

4. Makebitstreambackupsofhard disksandfloppydisks.

All evidence processing should be done on a restored copy of the bit stream backup ratherthan on the original computer. Bit stream backups are much like an insurance policy and areessentialforanyserious computerevidenceprocessing.

***5.* Mathematicallyauthenticatedataonallstoragedevices.**

You want to be able to prove that you did not alter any of the evidence after the computercame into your possession. Since 1989, law enforcement and military agencies have used a32-bitmathematicalprocess todotheauthenticationprocess.

6. Document thesystemdateandtime.

If the system clock is one hour slow because of daylight-savings time, then file timestampswill also reflect the wrong time. To adjust for these inaccuracies, documenting the systemdateandtimesettingsatthetime thecomputeristakenintoevidenceisessential.

7. Makealistofkeysearchwords.

itisallbutimpossibleforacomputerspecialisttomanuallyviewandevaluateeveryfileona computer hard disk drive. Gathering information from individuals familiar with the case tohelp com-pile a list of relevant keywords is important. Such keywords can be used in thesearchofallcomputerhard diskdrivesandfloppydiskettesusingautomated soft-ware.

8. EvaluatetheWindowsswapfile.

TheWindowsswapfileisapotentiallyvaluablesourceofevidenceandleads.Whenthe

computer is turned off, the swap file is erased. But the content of the swap file can easily becapturedandevaluated.

9. Evaluatefileslack.

It is a source of significant security leakage and consists of raw memory dumps that occurduring the work session as files are closed. File slack should be evaluated for relevantkeywords to supplement the keywords identified in the previous steps. File slack is typicallya good source of Internet leads. Tests suggest that file slack provides approximately 80 timesmoreInternetleadsthantheWindowsswapfile.

10. Evaluateunallocatedspace(erasedfiles).

Unallocated space should be evaluated for relevant keywords to supplement the keywordsidentifiedintheprevious steps.

11. Searchfiles,fileslack,andunallocatedspaceforkeywords.

The list of relevant keywords identified in the previous steps should be used to search allrelevant computer hard disk drives and floppy diskettes. It is important to review the outputofthetextsearchutilityandequallyimportanttodocumentrelevantfindings.

12. Documentfilenames, dates,andtimes.

From an evidence standpoint, file names, creation dates, and last modified dates and timescan be relevant. The output should be in the form of a word-processing-compatible file thatcan beused to helpdocumentcomputerevidenceissuestied tospecificfiles.

13. Identifyfile,program,andstorageanomalies.

Encrypted, compressed, and graphic files store data in binary format. As a result, text datastored in these file formats cannot be identified by a text search program. Manual evaluationof these files is required. Depending on the type of file involved, the contents should beviewedandevaluatedforits potentialasevidence.

14. Evaluateprogramfunctionality.

Depending on the application software involved, running programs to learn their purposemaybenecessary.Whendestructiveprocessesthataretiedtorelevantevidencearediscover ed, this canbeusedtoprovewillfulness.

15. Documentyourfindings.

It is important to document your findings as is-sues are identified and as evidence is found.Documentingallofthesoftwareusedinyourforensicevaluationoftheevidence,includingth e version numbers of the programs used, is also important. Be sure you are legallylicensed to USE the forensic software. Screen prints of the operating software also helpdocumenttheversionofthesoftware andhowitwasusedtofind or processtheevidence.

16. Retain copiesofsoftwareused.

As part of your documentation process, it is recommended that a copy of the software usedbe included with the output of the forensic tool involved. Duplication of results can bedifficult or impossible to achieve if the soft-ware has been upgraded and the original versionusedwas notretained.

LegalAspectsofCollectingandPreservingComputerFore nsic Evidence

Definition

- Achainofcustodyisaroadmapthatshowshowevidencewascollected,analyzed,andpreservedi norder tobepresentedas evidenceincourt.
- Preservingachainofcustodyforelectronicevidence requiresprovingthat:
  - ✓ Noinformationhasbeenaddedorchanged.
  - ✓ Acompletecopywasmade.
  - ✓ Areliablecopyingprocesswasused.
  - ✓ Allmediawassecured.

LegalRequirements

- Whenevidenceiscollected,certainlegalrequirementsmustbemet.Theselegalrequirementsarevast,complex,andvaryfromcountrytocountry.
- CERT Advisory CA-1992-19 suggests the following text be tailored to a corporation'sspecificneeds undertheguidanceoflegalcounsel:
  - ✓ This system isfor the use of authorized users only. Individuals usingthis computer system without authority, or in excess of their authority,are subject to having all of their activities on this system monitored andrecorded bysystempersonnel.
  - ✓ In the course of monitoring individuals improperly using this system, orin the course of system maintenance, the activities of authorized usersmayalsobemonitored.
  - ✓ Anyone using this system expressly consents to such monitoring and isadvised that if such monitoring reveals possible evidence of criminalactivity, system personnel may provide the evidence of such monitoringtolawenforcementofficials.
- Thelegalityofworkplacemonitoringdependsprimarilyonwhetheremploymentpolicies exist thatauthorize monitoringandwhether that policy has beenclearlycommunicatedtoemployees.
- To prove that the policy has been communicated, employees should sign a statementindicating that they have read, understood, and agreed to comply with corporatepolicyandconsenttosys-temmonitoring.

EvidenceCollectionProcedure

Whenthetimearrivestobegincollectingevidence,thefirstrulethatmustbefollowedis

Donotrush.

→The investigation team will need a copy of their incident-handling procedure, anevidencecollectionnotebook,andevidenceidentificationtags.

→Theymayalsoneedtobringtoolstoproducereliablecopiesofelectronicevidence,includingmediatouseinthecopyingprocess.

→Insomecases,legalcounselwillwantphotographsofthesystempriorto searchandseizure.Thenincludea *Polaroidcamera*inthelistoftools.

TheIncidentCoordinator

Policyandprocedureshouldindicatewhoistoactasincidentcoordinator.

TheIncidentcoordinator

- ✓ willcontacttheothermembersoftheresponseteamasoutlinedintheIncidentResponse Policy,whenanincidentis reported.
- ✓ willberesponsibleforensuringthatevery detailoftheincident-handlingprocedureisfollowed,uponarrival attheincidentsite.
- ✓ willassignteammembersthevarioustasksoutlinedintheincident-handlingprocedure.
- ✓ serveastheliaisontothelegalteam,lawenforcementofficials,management,andpublic relationspersonnel.

Ultimateresponsibilityforensuringthatevidenceisproperlycollectedandpreserved,andthatthe chain ofcustodyisproperlymaintained,belongstotheincidentcoordinator.

TheEvidenceNotebook

- Oneteammemberwill beassignedthe taskofmaintainingtheevidencenote-book.
- Thispersonwillrecordthe who,what,where,when,andhowoftheinvestigationprocess. Ataminimum,itemstoberecordedinthenotebookincludethefollowingtask.

a) Whoinitiallyreportedthesuspectedincidentalongwithtime,date,andcircumstancessurrounding thesuspectedincident?

b) Detailsoftheinitialassessmentleadingtotheformalinvestigation.

c) Namesofallpersonsconductingtheinvestigation.

d) Thecasenumber oftheincident.

e) Reasonsfortheinvestigation.

f) A list of all computer systems included in the investigation, along with complete systemspecifications.Alsoincludeidentification tagnumbersassignedtothesystemsorindividualparts ofthesystem.

g) Networkdiagrams.

h) Applicationsrunningonthecomputersystemspreviouslylisted.

i) A copy of the policy or policies that relate to accessing and using the systems previouslylisted.

j) Alistofadministratorsresponsiblefortheroutinemaintenanceofthesystem.

k) A detailed list of steps used in collecting and analyzing evidence. Specifically, this listneeds to identify the date and time each task was performed, a description of the task,whoperformedthetask,wherethetaskwasperformed,andtheresults oftheanalysis.

l) Anaccesscontrol listofwhohadaccesstothecollectedevidenceatwhatdateandtime.

- Aseparatenotebookshouldbeusedforeachinvestigation.Itshouldbeboundinsuchawaythatiti s obviousifapageorpageshavebeenremoved.
- This notebook is a crucial element in maintaining chain of custody. Therefore, it must beasdetailedaspossibletoassistinmaintaining thischain.

EvidenceCollection

- ✓ Anotherteammember (ormembers)willbeassignedthetaskofevidencecollection.
- ✓ Toavoidconfusion,thenumberofpeopleassignedthistaskshouldbekepttoaminimum.
- ✓ Thismember(ormembers)shouldalsobehighlyproficientwithcopyingandanalysis

tools.

- ✓ Thispersonwilltagallevidenceandworkwiththepersonresponsiblefortheevidencenotebookt oensurethatthisinformationisproperlyrecorded.
- ✓ Next, the person will also be responsible for making a reliable copy of all data to be usedasevidence.
  - ✓ Thedatawillincludecompletecopiesofdrivesoncompromisedorsuspectsystems,aswellas allrelevantlogfiles.
  - ✓ Thiscanbedoneon-siteortheentiresystemcanbemovedtoaforensicslab,asneedsdictate.
  - ✓ A binarycopyofthe dataistheproperwaytopreserveevidence.
  - ✓ Areliablecopyprocesshasthreecriticalcharacteristics.
    - Theprocessmustmeetindustrystandardsfor qualityandreliability.
    - Thecopiesmustbecapableofindependentverification.
    - Thecopiesmustbetamperproof.
  - ✓ Once all evidenceis collectedandlogged,itcan be securely transported to the forensicslab.
  - ✓ Adetaileddescriptionofhowdatawastransportedandwhowasresponsibleforthetransport,alo ngwithdate,time,and route,shouldbeincludedinthelog.

StorageandAnalysisofData

- ➢ Thelabmustprovidesomeformofaccesscontrol;alogshouldbekeptdetailingentranceandexitt imes ofallindividuals.
- ➢ Itis importantthatevidenceneverbeleftinanunsecuredarea.
- ➢ Ifadefenselawyercanshowthatunauthorizedpersonshadaccesstotheevidence,itcouldeasily be declaredinadmissible.

- As analysis of evidence is performed,investigators mustlog the details of their actionsintheevidence notebook.Thefollowingshould beincludedataminimum:
- Thedateandtimeofanalysis
- Toolsusedinperforming theanalysis
- Detailedmethodologyoftheanalysis
- Resultsoftheanalysis.
- Finally, once all evidence has been analyzed and all results have been recorded in theevidencenotebook,acopyofthenotebookshouldbemadeandgiventothelegalteam.
- If the legal team finds that sufficient evidence exists to take legal action, it will beimportant to maintain the chain of custody until the evidence is handed over to theproperlegalauthorities.
- Legal officials should provide a receipt detailing all of the items received for entry intoevidence.

COMPUTERIMAGEVERIFICATIONANDAUTHENTICATION

SpecialNeedsofEvidentialAuthentication

→Duringaninvestigation,itisdecidedthatevidence mayresideonacomputersystem.

→ It may be possible to seize or impound the computer system, but this risks violating thebasic principle of *innocent until proven guilty*, by depriving an innocentparty of theuse ofhis orher system.

→It should be perfectly possible to copy all the information from the computer system inamannerthatleavestheoriginalsystemuntouchedandyetmakesallcontentsavailableforfor ensicanalysis.

→Thecourtsmayrightlyinsistthatthecopiedevidenceisprotectedfromeitheraccidental or deliberate modification and that the investigating authority should provethatthishasbeendone.Thus,itisnotthecontentthatneedsprotection,butits

integrity.

→Thisprotectiontakestwoforms:

- Asecuremethodofdeterminingthatthedatahasnotbeenalteredbyevenasinglebitsince thecopywastaken.
- Asecuremethodofdeterminingthatthecopyisgenuinelytheonetakenatthetimeandont he computerinquestion.

→Theseelementsarecollectivelyreferredasthe*DigitalImageVerificationandAuthentication Protocol***.**

DIGITALIDSANDAUTHENTICATIONTECHNOLOGY

- ✓ Without an assurance of the software's integrity, and withoutknowing who publishedthesoftware,it'sdifficultforcustomersto knowhowmuchtotrustsoftware.
- ✓ It'sdifficulttomakethechoiceofdownloadingthesoftwarefromtheInternet.
- ✓ For example (when using MicrosoftAuthenticode coupled with Digital IDs™fromVeriSign®),throughtheuseof digitalsignatures,softwaredevelopersareabletoincludeinformationaboutthemselvesandthei rcodewiththeirprograms.
- ✓ Whencustomersdownloadsoftwaresignedwith**Authenticode**andverifiedby**VeriSign**, they should be assured of content source, indicating that the software reallycomesfrom the publisherwhosignedit,and**content integrity**,indicating thatthesoftwarehasnotbeenalteredorcorruptedsinceitwassigned.

Authenticode

→MicrosoftAuthenticodeallowsdeveloperstoincludeinformationaboutthemselvesandtheircod ewiththeirprogramsthroughtheuseofdigitalsignatures.

→Through*Authenticode,*theuseris informed:

1. Ofthetrueidentityofthepublisher

2. Ofaplace tofind outmoreabout thecontrol

3. Theauthenticityofthepreceding information

→Userscanchoosetotrustallsubsequentdownloadsofsoftwarefromthesamepublisher and all software published by commercial publishersthat has been verifiedbyVeriSign.

PublicKeyCryptography

- ✓ In publickeycryptographicsystems,everyentityhastwocomplementarykeys(a publickeyandprivatekey)thatfunctiononlywhentheyareheldtogether.
- ✓ Publickeysarewidely distributedtousers,whereasprivatekeysarekeptsafeandonlyusedbytheir owner.
- ✓ Anycodedigitallysignedwiththepublisher'sprivatekeycanonlybesuccessfullyverifiedusing thecomplementarypublickey.
- ✓ Codethatsuccessfullyverifiedusingthepublisher'spublickey,couldonlyhavebeendigitallysi gnedusingthepublisher'sprivatekey,andhasnotbeentamperedwith.

CertificateAuthorities

→ Certification Authorities such as VeriSign are organizations that issue digital certificatesto applicants whoseidentity they are willing to vouch for.Each certificateislinked tothe certificateoftheCAthatsignedit.

→VeriSign hasthefollowingresponsibilities:

1. Publishingthecriteria forgranting,revoking,andmanagingcertificates
2. Grantingcertificatesto applicationswhomeetthepublishedcriteria
3. Managingcertificates
4. StoringVeriSign'srootkeys inanexceptionallysecuremanner
5. Verifyingevidencesubmitted byapplicants
6. Providingtoolsforenrollment

7. Acceptingthe liabilityassociatedwiththeseresponsibilities
8. Time-stampingdigitalsignatures.

DigitalID

→ ADigitalID/Certificate isaformofelectroniccredentialsfortheInternet.

→ADigitalIDisissuedbyatrustedthirdpartytoestablishtheidentityoftheIDholder.

→Thethirdpartywhoissuescertificatesisknownasa CertificateAuthority(CA).

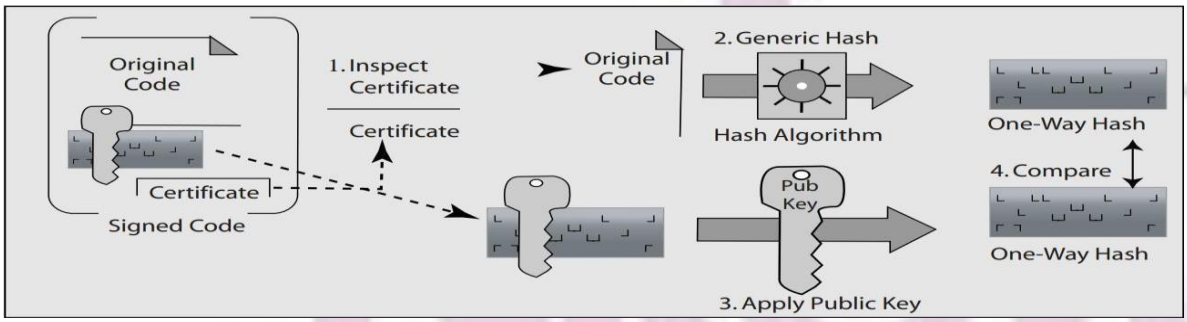
→Digital IDtechnologyisbasedonthetheoryofpublickeycryptography.

→ThepurposeofaDigital IDistoreliablylinkapublic/privatekeypairwithitsowner.

→WhenaCAsuchasVeriSignissuesaDigitalIDs,itverifiesthattheownerisnotclaimingafalseidentity.

→WhenaCAissuesyouadigitalcertificate,itputsitsnamebehindthestatement thatyouaretherightfulownerofyourpublic/private keypair.

HowAuthenticodeworkswithVeriSign DigitalIDs?



Authenticode:VeriSignDigitalIDprocess

1. PublisherobtainsaSoftwareDeveloperDigitalIDfromVeriSign
2. Publishercreates code
3. UsingtheSIGNCODE.EXEutility, thepublisher
    - Creates ahashofthecode,usinganalgorithmsuchas MD5orSHA

- Encryptsthehasusinghis/herprivatekey
- Createsapackagecontainingthecode,theencryptedhash,andthepublisher'scertificat e

4. Theend user encountersthepackage
5. The end user's browser examines the publisher's Digital ID. Using the VeriSign rootPublic Key, which is already embedded in Authenticode enabled applications, the enduser browser verifies the authenticity of Software Developer Digital ID (which is itselfsignedbytheVeriSignrootPrivateKey)
6. Using the publisher's public key contained withinthe publisher's Digital ID, the enduserbrowserdecryptsthesignedhash.
7. The end browser runs the code through the same hashing algorithm as the publisher,creatinganewhash.
8. Theenduserbrowsercomparesthetwohashes.If they areidentical,thebrowsermessages that the content has been verified by VeriSign,and the enduserhas theconfidence that the code was signed by the publisher identified in the Digital ID, and thecodehasn'tbeenalteredsinceitwassigned.

TimeStamping: Becausekeypairsarebasedonmathematicalrelationshipsthatcantheoretically be ―cracked‖with a great deal of time and effort, it isa well-established securityprinciplethatdigitalcertificatesshouldexpire.

PracticalConsideration

- Itisusefultopresentsomefundamentalrequirementsofaforensicdatacollectionsystembefore consideringhowthesecanbesecurelyprotected.
- Otherforensicexpertsmayargueagainstsomeorallofthem:
  a. Forensicdatacollectionshouldbecompleteandnon-softwarespecific, thus avoidingsoftwaretrapsandhiddenpartitioning.
  b. Inoperation,itshouldbeasquickandassimpleaspossibletoavoiderrorordelay.

c. Itshouldbepossibleforanyonetouseaforensicdatacollectionsystemwiththeminimu mamountoftraining.

d. Necessarycostsand resourcesshouldbekeptto aminimum.

- Tomeettheconditionsspecifiedinitems2,3,and4,thedigitalintegrityverificationandauthentic ationprotocolmustbetailoredtosuit.
- Onlyinvestigatorsissuedwithavaliddigitalsignaturewouldbeabletocompletecopies.

PracticalImplementation

- ✓ A minimum amount of reliance is placed on the technical ability of theoperator/investigator.
- ✓ It mustbe understood thatduring the copying process,procedures areimplementedtotrapand handle hardwareerrors,mappingexceptions wherenecessary.
- ✓ Itmustalsobeunderstoodthatproceduresareimplementedtoverifythatinformationiscopiedco rrectly.
- ✓ Thisinformationisstoredoneachcartridgewithin acopyseries.
- ✓ Also stored on each cartridge is a reference area containing copy-specific informationsuchasCPUtypeandspeed,hardwareequipmentindicators,copyingdriveserialnu mber, cartridge sequence number, exhibit details and reference comments, operatorname together with a unique password, and the real date and time as entered by theoperator.
- ✓ The cartridge is divided into blocks of an arbitrary chosen size. Blocks may containreference, ROM, CMOS, or disk data depending on their location on the cartridge. Eachcartridge contains the information copied from the suspect drive on a sector by sectorbasis.

SafeBoxes andtheVault

→As each block is copied and verified, a hash value is generated such that a single bitchange anywhere within the block would produce a different hash. The result is stored inthe relevantsafeboxandcopyingtothenextblock.

→ Once all the blocks relevant to a particular cartridge have been copied and treated in thisway, the whole group of safe boxes, collectively referred to as the vault, are treated as anindividual block and a vault hash value is generated and stored in the final safe box. Thevaultisthencopiedtoanotherareaofthecartridgeandthissecondcopyisencrypted.

→The vault hash value for each cartridge is stored in a separate area in memory and theoperator is prompted to insert a new cartridge until the copy is completed. The finalcartridge will contain similar information to the others in the series and in addition willhavetheaccumulatedvaulthashvaluesfromallothercartridgesintheseries.

→Oncethefinalcartridgehasbeencopied,theoperatorispromptedtoinsertapreformattedfloppy diskintothedriveusedtostarttheDIBSprocess.All of theaccumulatedvaulthashvaluesarethenwrittentoafloppy disktogetherwiththereference details of the whole copy procedure. At least two identical floppy disks arecreatedinthismanner.

→The floppy disks are then sealed in numbered, tamperproof bags and both numbers arewritten on both envelops. The computer owner is given his or her chosen floppy and theotheris placedinsecurestorage.

SecurityConsiderations

→Computerforensicsinvestigatorsareconstantlydiscoveringnewvulnerabilitiesinoldimage verificationandauthenticationproducts.

→As aresultCIOs (Chief informationOfficers)are devotingmoremoney andtimetoimage verificationandauthenticationsecurity.

→Staff-membersaretheoneswhomakesurevirusesdon’tcomeinandholesaren’tcreatedinthefirewall.

→They have to understand that most business is built on trust, and their role in maintainingtrustis crucial.

→It’sdifficult, perhaps impossible,tomeasurethereturnoninvestmentinsecurity.

→Youhavetoprotectyourdata.Itonlytakesonetime---
onehackergettinginandhackingallyourfinancialdata.

→Itwouldbeirresponsibleon CIO's partnothave the toughestimage verification
andauthenticationsecuritypossible.

UNIT-III

COMPUTERFORENSICSANALYSISANDVALIDATION

DeterminingWhatDatatoCollectandAnalyze

Examining and analyzing digital evidence depend on the nature of the investigation and the amount ofdata to process. Criminal investigations are limited to finding data defined in the search warrant, and civilinvestigations are often limited by court orders for discovery. Corp.- rate investigators might be searchingfor company policy violations that require examining only specific items, such as e-mail. Therefore,investigations often involve locating and recovering a few specific items, which simplifies and speedsprocessing.

In the corporate environment, however, especially if litigation is involved, the company attar- nay oftendirects the investigator to recover as much information as possible. Satisfying this demand becomes amajor undertaking with many hours of tedious work. These types of invest- ligations can also result inscope creep, in which an investigation expands beyond the original description because of unexpectedevidence you find, prompting the attorney to ask you to examine other areas to recover more evidence.Scopecreepincreasesthetimeandresourcesneededtoextract,analyze,andpresentevidence.
Besuretodocument any requests for add- tonal investigation, in case you must explain why the investigation tooklongerthanplanned,whythescopewidenedduringthecourseoftheinvestigation,andsoforth.

One reason scope creep has become more common is that criminal investigations increasingly requiremore detailed examination of evidence just before trial to help prosecutors fend off attacks from defenseattorneys. Because defense attorneys typically have the right of full discovery of digital evidence usedagainst their clients, it's possible for new evidence to come to light while complying with the defenserequest for full discovery. However, this new evidence often isn't revealed to the prosecution; instead,the defense uses it to defend the accused. For this reason, it's become more important for prosecutionteams to ensure that they have analyzed the evidence exhaustively before trial. (It should be noted thatthe defense request for full discovery applies only to criminal cases in the however, depends on
whetherit'saninternalcorporateinvestigationoracivilorcriminalinvestigationcarriedoutbylawenforcement.
In an internal investigation, evidence collection tends to be fairly easy and straightforwardbecause

corporate investigators usually have ready access to the necessary records and files. In contrast,wheninvestigatingacriminalcyber-stalkingcase,youneedtocontacttheISPande-mailservice.

Some companies, such as AOL, have a system set up to handle these situations, but others do not. Manycompaniesdon'tkeepe-mailforlongerthan90days,andsomekeepitonly twoweeks.

An employee suspected of industrial espionage can require the most work. You might need to set up asmall camera to monitor his or her physical activities in the office. You might also need to plant asoftwareorhardwarekeylogger(forcapturingasuspect'skeystrokesremotely),andyouneedtoengagethe network administrator's services to monitor Internet and network activities. In this situation, you mightwant to do a remote acquisition of the employee's drive, and then use another tool to determine whatperipheraldeviceshavebeenaccessed.

1. For target drives, use only recently wiped media thathave been reformatted and inspected forcomputer viruses. For example, use ProDiscover Secure Wipe Disk, Digital Intelligence PDWipe, orWhiteCanyonSecureCleantocleanalldata fromthetargetdriveyouplantouse.

2. Inventory the hardware on the suspect's computer and note the condition of the computer whenseized.Documentallphysicalhardware componentsaspart ofyourevidence acquisitionprocess.

3. For static acquisitions, remove the original drive from the computer, if practical, and then check thedateandtimevaluesinthesystem'sCMOS.

4. Recordhowyouacquireddatafromthesuspectdrivenote,forexample,thatyoucreateda bit-stream image and which tool you used. The tool you use should also create an MD5 or SHA-1 or betterhashforvalidatingtheimage.

5. When examining the image of the drive's contents, process the data methodically and logically.List all folders and files on the image or drive. For example, FTK can generate a Microsoft Accessdatabase listing all files and folders on a suspect drive. Note where specific evidence is found, andindicatehowit'srelatedtotheinvestigation.

6. If possible, examine the contents of all data files in all folders, starting at the root directory of thevolume partition. The exception is for civil cases, in which you look for only specific items in theinvestigation.For all password-protected files that might be related to the investigation, make your best effort torecover file contents. You can use password recovery tools for this purpose, such as Access DataPassword RecoveryToolkit(PRTK),NTIPassword Recovery,orPassware KitEnterprise

1. Identify the function of every executable (binary or .exe) file that doesn't match known hashvalues. Make note of any system files or folders, such as the System32 folder or its content, that areout of place. If you can't find information on an executable file by using a disk editor, examine thefiletoseewhatitdoesandhowitworks.

1. Maintain control of all evidence and findings, and document everything as you progress throughyour examination. ps to locate specific message Refining and Modifying the Investigation Plan Incivil and criminal cases, the scope is often defined by search warrants or subpoenas, which specifywhat data you can recover. However, private sector cases, such as employee abuse investigations,might notspec-ify limitations in recovering data. For these cases,it's important to refine theinvestigation plan as much as possible by trying to determine what the case requires. Generally, youwant the investigation to be broad enough to encompass all relevant evidence, yet not so wide-rangingthatyou wastetimeandresourcesanalyzingdatathat'snotgoingto helpyourcase.

Of course, even if your initial plan is sound, at times you'll find that you need to deviate from theplanandfollowwheretheevidenceleadsyou.Eveninthesecases,havingaplanthatyoudeliberatelyrevise alongthe wayismuchbetterthansearchingforevidencehaphazardly.

Suppose, for example, an employee is accused of operating an Internet-based side business usingcompany resources during normal business hours. You use this timeframe to narrow the set of datayou're searching, and because you're looking for unauthorized Internet use, you focus the search ontemporary Internet files, Internet history, and e-mail communicate- ion. Knowing the types of datayou're looking for at the outset helps you make the best use of your time and prevents you fromcasting too wide a net. However, in the course of reviewing e-mails related to the case, you mightfind references to spreadsheets or Word documents containing financial information related to theside business. In this case, it makes sense to broaden the range of data you're looking for to includethese types of files. Again, the key is to start with a plan but remain flexible in the face of newevidence.

UsingAccessDataForensicToolkit toAnalyzeData

So far, you have used several different features of FTK; this section goes into more detail on itssearchand report functions.FTKcanperformforensicsanalysisonthe following filesystems:

- MicrosoftFAT12,FAT16, andFAT32

- MicrosoftNTFS(forWindowsNT,2000,XP,andVista)
- LinuxExt2fsandExt3fs

FTK can analyze data from several sources, including image files from other vendors. It can alsoread entire evidence drives or subsets of data, allowing you to consolidate large volumes of datafrom many sources when conducting a computer forensics analysis.With FTK, you can storeeverythingfromimagefilestorecoveredserverfoldersononeinvestigationdrive.

FTK also produces a case log file, where you can maintain a detailed record of all activities duringyourexamination,such as keywordsearches anddata extractions.Thislog is alsohandy forreporting errors to Access Data. At times, however, you might not want the log feature turned on. Ifyou're following a hunch, for example, but aren't sure the evidence you recover is applicable to theinvestigation, you might not want opposing counsel to see a record of this information because he orshe could use it to question your methods and perhaps discredit your testimony. (Chapter 15 coverstestimony issues in more detail.) Look through the evidence first before enabling the log feature torecord searches. This approach isn't meant to conceal evidence; it's a precaution to ensure that yourtestimonycanbeusedincourt.

FTK has two options for searching for keywords. One option is an indexed search, which catalogsall words on the evidence drive so that FTK can find them quickly. This option returns searchresults quickly, although it does have some shortcomings. For example, you can't search forhexadecimal string values, and depending on how data is stored on the eve- dense drive, indexingmight not catalog every word. If you do use this feature, keep in mind that indexing an image filecantakeseveralhours,soit'sbesttorunthisprocess overnight.

The other option is a live search, which can locate items such as text hidden in unallocated spacethatmightnotturnupinanindexedsearch.Youcanalsosearchforalphanumericandhexadecimal values on the evidence drive and search for specific items, such as phone numbers,credit card numbers, and Social Security numbers. Figure 9-1 shows the hits found during a livesearch of an image of a suspected arsonist's laptop. You can right-click a search hit to add ittoyourbookmarks,whichincludestheresultinyourfinalreport.

ValidatingForensicData

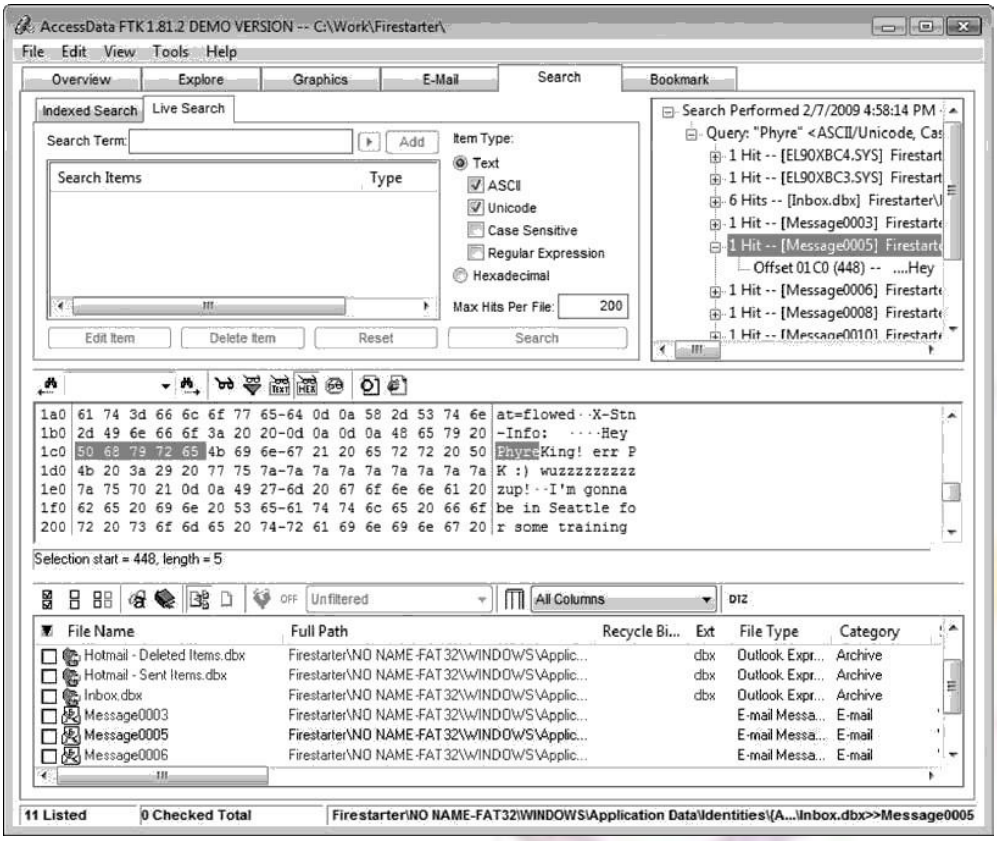


Fig:ValidatingForensicData

One of the most critical aspects of computerforensicsisvalidating digital evidence becauseensuring the integrity of data you collect is essential for presenting evidence in court. Chapter 5introduced forensic hashing algorithms, and in this section, you learn more about validating anacquiredimagebeforeyouanalyzeit.

Most computer forensic tools such as ProDiscover, X-Ways Forensics, FTK, and Encase provideautomated hashing of image files. For example, when ProDiscover loads an image file, it runs ahash and compares that value to the original hash calculated when the image was first acquired.You might remember seeing this feature when the AutoImage Checksum Verification messageboxopensafteryouloadanimagefileinProDiscover.Computerforen-sicstoolshavesome

limitations in performing hashing, however, so learning how to use advanced hexadecimal editorsisnecessarytoensuredataintegrity.

ValidatingwithHexadecimalEditors

Advanced hexadecimal editors offer many features not available incomputer forensics tools,such as hashing specific files or sectors. Learning how to use these tools is important, especiallywhen you need to find a particular file—for example, a known contraband image. With the hashvalue in hand, you can use a computer forensics tool to search for a suspicious file that mighthave had its name changed to look like an innocuous file. (Recall that two files with exactly thesame content have the same hash value, even if they have different names.) Getting a hash valuewith a full-featured hexadecimal editor is much faster and easier than with a computer forensicstool.

AddressingData-HidingTechniques

Datahidinginvolveschangingormanipulatingafiletoconcealinformation.Data-hidingtechniques include hiding entire partitions, changing file extensions, setting file attributes tohidden,bit-shifting,usingencryption,andsettinguppasswordprotection.Someofthesetechniques arediscussedinthefollowingsections.

HidingPartitions

One way to hide partitions is to create a partition and then use a disk editor, such as NortonDisk Edit, to delete any reference to it manually. To access the deleted partition, users can editthe partition table to re-create the links, and then the hidden partition reappears when thecomputer is restarted. Another way to hide partitions is with a disk-partitioning utility, such asGDisk,PartitionMagic,System Commander,orLinuxGrandUnifiedBootloader(GRUB), which provides a startup menu where you can select an OS. The system then ignoresotherbootablepartitions.

To circumvent these techniques, be sure to account for all disk space whenyou’re examiningan evidence drive. Analyze any disk areas containing space you can’t account for so that youcan determine whether they contain additional evidence. For example, in the following code,DiskManagerrecognizestheextendedpartition(labeledEXTDOS)asbeing5381.1MB

(listed as Mbytes). The LOG DOS labels for partitions E through F indicate that they'relogicalpartitions that make up the extended partition. However, if you add the sizes of drives Eand F, the result is only 5271.3 MB, which is your first clue to examine the disk more closely.The remaining 109.8 MB could be a previously deleted partition or a hidden partition. For thisexample,thefollowingcodeshows theletter–H‖toindicateahiddenpartition.DiskPartitions CylindersHeads SectorsMbytes Sectors 251116616635495.811255328

Partition	Status	Type	Volume Label	Mbytes	System	Usage
D:	1		PRIDOS	109.8	FAT16	2%
	2		EXTDOS	5381.1		98%
E:	3		LOGDOS	109.8	FAT16	2%
	4	H	LOGDOS	109.8	FAT16	2%
F:	5		LOGDOS	5161.5	FAT32	94%

Windows creates a partition gap between partitions automatically; however, you might find a gapthat's larger than it should be. For example, in Windows 2000/XP, the partition gap is only 63sectors, so 109.8 MB is too large to be a standard partition gap. In Windows Vista, the gap isapproximately128sectors.

In Figure,you can see ahidden partition in DiskManager, which shows itas anunknownpartition.In addition,the driveletters in the visible partitions are nonconsecutive (driveIisskipped), which can be another clue that a hidden partition exists. Most skilled users would makesurethisanomalydoesn'toccur,however.

Fig:Viewingahiddenpartitionin DiskManager

In ProDiscover, a hidden partition appears as the highest available drive letter set in the BIOS.Figure 9-9 shows four partitions, similar to Figure 9-8, except the hidden partition shows as thedrive letter Z. To carve (or salvage) data from the recovered partition gap, you can use othercomputerforensicstools,suchasFTKorWinHex.

Fig:ViewingahiddenpartitioninProDiscover

MarkingBadClusters

Anotherdata-hidingtechnique,morecommoninFATfilesystems,isplacingsensitiveorincriminating data in free or slack space on disk partition clusters. This technique involves using adisk editor, such as Norton Disk Edit, tomarkgood clusters as bad clusters. The OSthenconsiders these clusters unusable. The only way they can be accessed from the OS is by changingthemtogoodclusters withadiskeditor.

Bit-Shifting

Some home computer users developed the skill of programming in the computer manufacturer'sassembly language and learned how to create a low-level encryption program that changes theorder of binary data, making the altered data unreadable when accessed with a text editor orwordprocessor.Theseprogramsrearrangebitsforeachbyteinafile.Tosecureafilecontaining sensitive or incriminating information, these users run an assembler program (alsocalledamacro)on thefiletoscramblethebits.Toaccessthefile,theyrunanotherprogramthat

restores the scrambled bits to their original order. Some of these pro- grams are still used todayandcanmakeitdifficultforinvestigatorstoanalyzedataona suspectdrive.

Start Notepad, and in a text document, type TEST FILE. Test file is to see how shifting bits willalterthedatainafile.

SavethefileasBit_shift.txt inyour workfolder,andexitNotepad.

Fig:Hexworkshop

Start Hex Workshop. Click File, Open from the menu. Navigate to your work folder, and thendouble-clickBit_shift.txt.Bit_shift.txtopeninHexWorkshop.

To set up Hex Workshop for the bit-shifting exercise, click Options, Toolbars from the menu.IntheCustomizedialogbox,clicktheDataOperations checkbox,andthenclickOK.

Click the Shift Left button (<< icon) on the Data Operations toolbar. The Shift Left Operationdialog box opens, where you specify how you want to treat the data, the ordering scheme to useforbytes,andwhetheryoushiftbitsforselectedtextortheentirefile.

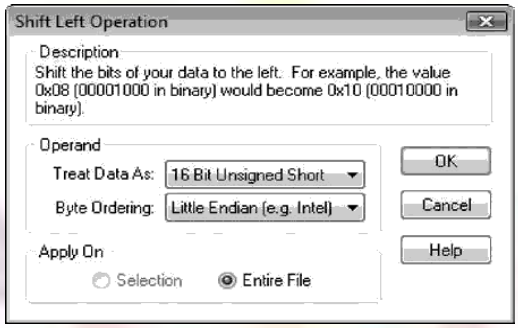


Fig:TheShiftLeftOperationdialogbox

1. ClickOKtoacceptthedefaultsettingsandshiftthebitsinBit_shift.txttotheleft.

2.Save the file as Bit_shift_left.txt in your work folder. above Figure shows the fileinHexWorkshop,withthe@symbolsindicatingshiftedbits.

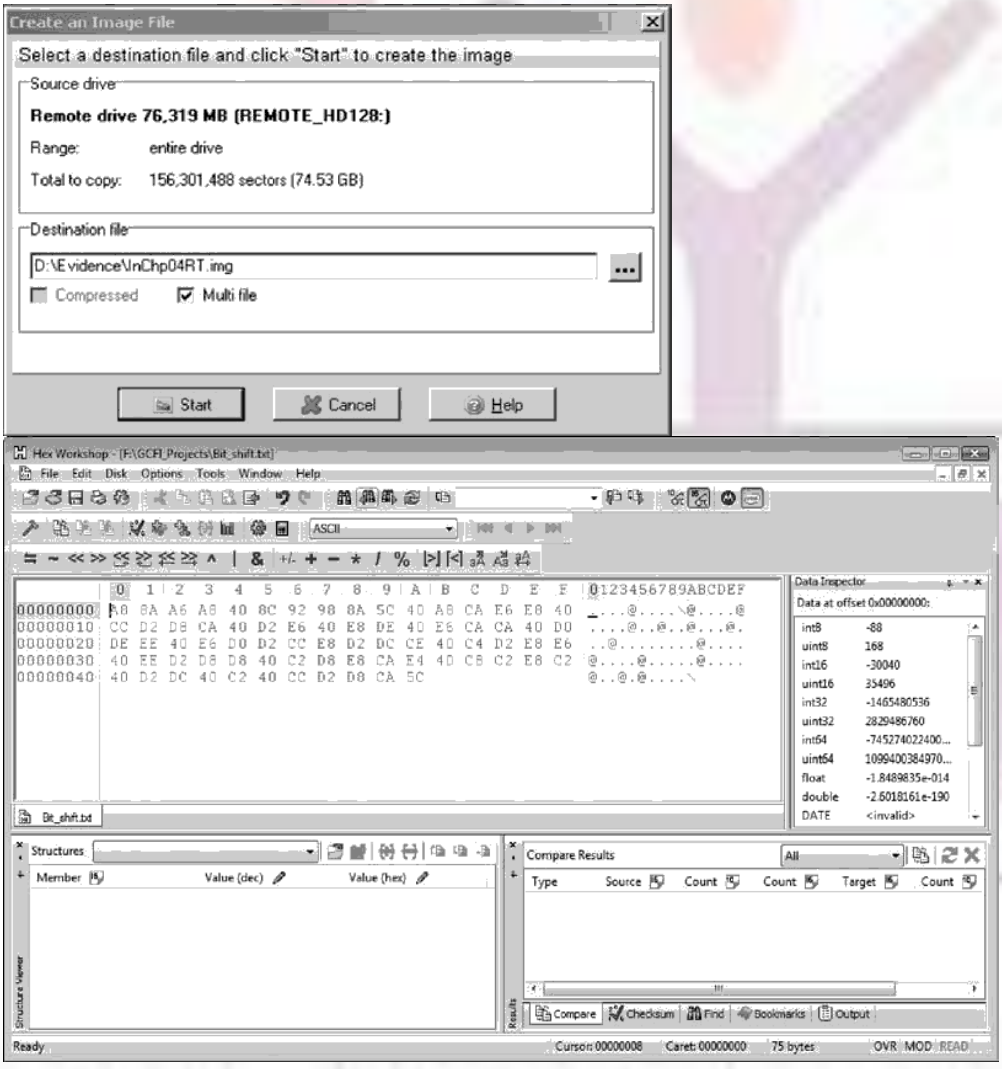


Fig:Viewing theshiftedbits

1. To return the file to its original configuration, shift the bits back to the right by clicking theShift Right button (>> icon) on the Data Operations toolbar. Click Ok to accept the defaultsettingsintheShiftRightOperationdialog box. Thefileisdisplayedinitsoriginalformat.

2. Save the file as Bit_shift_right.txt in your work folder, and leave Hex Workshop open for thenext activity. Now you can use Hex Workshop to find the MD5 hash values for these three files anddetermine whether Bit_shift.txt is different from Bit_shift_right.txt andBit_shift_left.txt. (Youcould also use FTK or ProDiscover to find the MD5 hash values.) To check the MD5 values in HexWorkshop,followthesesteps:

1. With Bit_shift_right.txtopen in Hex Workshop, click File,Open to open Bit_shift.txt, andthenrepeattoopenBit_shift_left.txt.

2. ClicktheBit_shift.txttabintheupperpanetomakeittheactivefile.

3. Click Tools, Generate Checksum from the menu to open the Generate Checksum dialog box. Inthe Select Algorithms list box, click MD5, and then click the Generate button. Copy theMD5hash value of Bit_shift.txt, shown in the lower-right pane, and paste it in a new text document inNotepad.

4. Repeat Steps 2 and 3 for Bit_shift_left.txt and Bit_shift_right.txt, pasting their hash values inthesametextfileinNotepad.

5. Compare the MD5 hash values to determine whether the files are different. When you'refinished,exitNotepadandHexWorkshop.

Typically, antivirus tools run hashes on potential malware files, but some advanced malwareuses bit-shifting as a way to hide its malicious code from antivirus tools. With the bit-shiftingfunctions in Hex Workshop, however, you can inspect potential malicious code manually. Inaddition, some malware that attacks Microsoft Office files consists of executable code that'sembedded at the end of document files, such as Word documents, and hidden with bit- shifting.When an Office document is opened, the malware reverses the bit-shifting on the executablecodeandthenrunsit.

PerformingRemoteAcquisitions

Remote acquisitions are handy when you need to image the drive of a computer far away fromyour location or when you don't want a suspect to be aware of an ongoing investiga- tion. Thismethod can save time and money, too. Many tools are available for remote acquisi- tions; in thefollowing sections,youuseRuntimeSoftwaretolearnhowremote acquisitionsaremade.

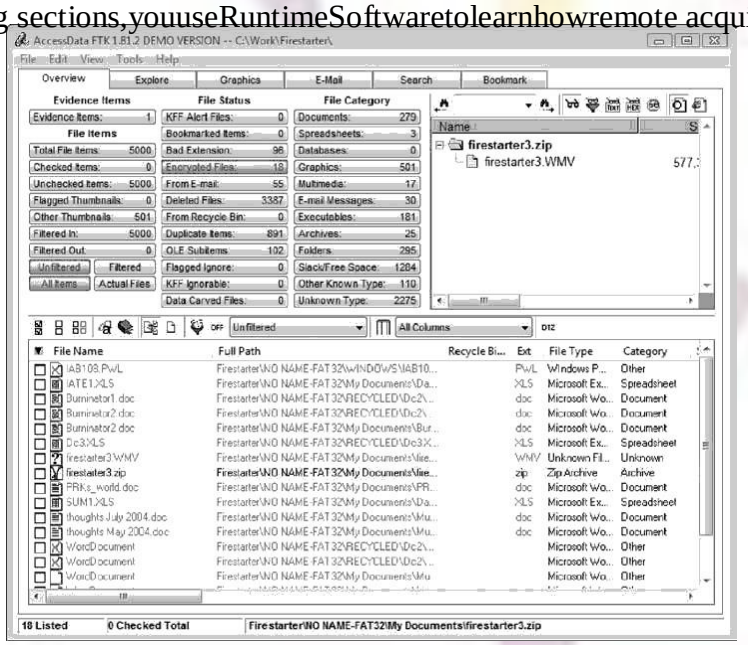


Fig:FTKdisplayingencryptedfiles

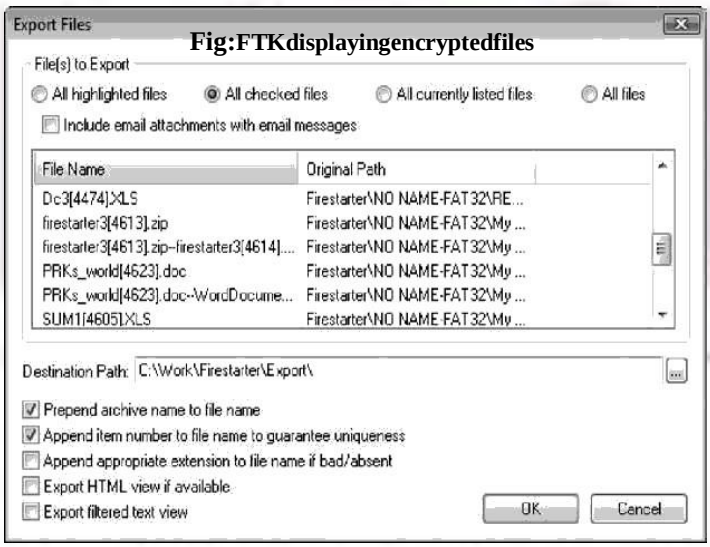


Fig:Exportingencryptedfiles

RemoteAcquisitionswithRuntimeSoftware

RuntimeSoftware(*www.runtime.org*)offersthefollowingsharewareprogramsforremotea cquisitions:

DiskExplorerforFAT

- DiskExplorerforNTFS
- HDHOST

Chapter 4 introduced these tools; remember that they're designed to be file system specific, sothere are DiskExplorer versions for both FAT and NTFS that you can use to create raw for-matimagefilesorsegmentedimagefilesforarchivingpurposes.

HDHOSTisaremoteaccessprogramforcommunicationbetweentwocomputers.Theconnection is establishedby using the DiskExplorer program (FAT or NTFS) correspondingto the suspect (remote) computer's file system. The following sections show how to make alive remote acquisition of another computer over a network. To use these tools, it's best tohave computersconnectedonthesamelocalhuborrouterwithminimalnetworktraffic.

NetworkForensicsOverview

Network forensics is the process of collecting and analyzing raw network data and trackingnetwork traffic systematically to ascertain how an attack was carried out or how an eventoccurred on a network. Because network attacks are on the rise, there's more focus on thisfield and an increasing demand for skilled technicians. Labor forecasts predict a shortfall of50,000 network forensics specialists in law enforcement, legal firms, corporations, anduniversities.

Network forensics can also help you determine whether a network is truly under attack or a userhas inadvertently installed an untested patch or custom program, for example. A lot of time andresources can be wasted determining that a bug in a custom program or an untested open-sourceprogramcausedthe–attack.‖

Networkforensicsexaminersmust establishstandardproceduresforhowtoacquiredataafteranattack orintrusionincident.Typically,networkadministratorswanttofindcompromised.

SecuringaNetwork

Network forensics is used to determine how a security breach occurred; however, steps must betaken to harden networks before a security breach happens, particularly with recent increases innetwork attacks, viruses, and other security incidents. Hardening includes a range of tasks, fromapplying the latest patches to using a layered network defense strategy, which sets up layers ofprotection to hide the mostvaluable data at the innermostpart of the network. It alsoensuresthat the deeper into the network an attacker gets, the more difficult accessbecomes and

themoresafeguardsareinplace.TheNationalSecurityAgency(NSA)developedasimilarapproach,called thedefenseindepth(DiD)strategy.DiDhave threemodesofprotection:

- People
- Technology
- Operations

If one mode of protection fails, the others can be used to thwart the attack. Listing people as amode of protection means organizations must hire well-qualified people and treat them well sothat they have no reason to seek revenge. In addition, organizations should make sure employeesare trained adequately in security procedures and are familiar with the organize- tion's securitypolicy. Physical and personnel security measures are included in this mode of protection. Thetechnology mode includes choosing strong network architecture and using tested tools, such asintrusion detection systems (IDSs) and firewalls. Regular penetration testing coupled with riskassessment can help improve network security, too. Having systems in place that allow quick andthoroughanalysiswhenasecuritybreachoccursisalsopartofthetechnologymodeofprotection.

PerformingLiveAcquisitions

The problem investigators face is the order of volatility (OOV), meaning how long a piece ofinformation lasts on a system. Data such as RAM and running processes might exist for onlymilliseconds; other data, such as files stored on the hard drive, might last for years. The following steps show the general procedure for a live acquisition, although investigators differ onexactsteps:

- Createordownloadabootableforensic CD,andtestitbeforeusingitona suspect drive. If the suspect system is on your network and you can access itremotely, add the appropriate network forensics tools to your workstation. If not,insertthebootableforensicsCDinthesuspectsystem.
- Make sure you keep a log of all your actions; documenting your actionsandreasonsforthese actionsiscritical.
- A network drive is ideal as a place tosend the informationyou collect.If you don't have one available, connect a USB thumb drive to the suspect systemforcollectingdata.Besuretonotethisstepinyourlog.
- Next, copy the physical memory (RAM). Microsoft has built-in tools forthistask,oryoucanuseavailablefreewaretools,suchasmemfetch(*www.freshports.org/sysutils/memfetch*)andBackTrack(discussedinthefollowingsection).
- Thenextstepvaries,dependingon theincident you're investigating. With an intrusion, for example, you might want toseewhetherarootkitispresentby using a toolsuchasRootKitRevealer(*www.microsoft.com/technet/sysinternals/Utilities/RootkitRevealer.mspx*).Youcan also access the system's firmware to see whether it has changed, create animage of the drive over the network, or shut the system down and make a staticacquisitionlater.
- Be sure to get a forensically sound digital hash value of all files yourecoverduringtheliveacquisitiontomakesuretheyaren't alteredlater.

PerformingaLiveAcquisitioninWindows

Live acquisitions are becoming more necessary, and several tools are available for capturingRAM. ManTech Memory DD(*www.mantech.com/msma/MDD.asp*)can access up to4 GBRAM in standard did format. Another freeware tool, Win32dd (*http://win32dd.msuiche.net*),runs from the command line to perform a memory dump in Windows. In addition, comer- coaltools,suchasGuidanceSoftwareWinen.exe,canbeused.

Another popular tool is Backtrack (*www.remote-exploit.org/backtrack.html*),which combinestools from the White Hat Hackers CD and The Auditor CD (see Figure 11-3). More than 300tools are available, including password crackers, network sniffers, and freeware forenticestools.Backtrackhasbecomepopularwithpenetrationtestersandisusedattheannual Collegiate CyberDefenseCompetitions.

Fig:SomeofthetoolsavailableinBackTrack

DevelopingStandardProceduresforNetworkForensics

Network forensics is a long, tedious process, and unfortunately, the trail can go coldquickly.Astandardprocedureoftenusedinnetworkforensicsisasfollows:

- Alwaysuseastandardinstallationimageforsystemsonanetwork. Thisimageisn't abit-streamimagebutanimagecontaining all the standard applications used. You should alsohave the MD5 and SHA-1 hash values of all application and OSfiles. Whenanintrusionincidenthappens,makesurethevulnerabilityhasbeenfixedtopreventotherattacksfromtakingadvantageoftheopening.
- Attempt to retrieve all volatile data, such as RAM and runningprocesses, by doing a live acquisition before turning the systemoff.Acquirethecompromiseddriveandmakeaforensicimageofit.

- Compare files on the forensic image to the original installationimage. Compare hash values of common files, such as Win.exeand standard DLLs,andascertainwhethertheyhave changed.

In computer forensics, you can work from the image to find most of the deleted or hidden filesandpartitions.Sometimesyourestore theimagetoaphysical drivesothatyoucanrunprograms on the drive. In network forensics, you have to restore the drive to see how mal- wareattackers have installed on the system works. For example, intruders might have trans- mitted aTrojan program that gives them access to the system and then installed a root kit, which is acollection of tools thatcan perform network reconnaissance tasks (using thels or netstatcommandtocollectinformation,forinstance),keylogging,andotheractions.

UsingNetworkTools

Avariety of toolsareavailablefornetworkadministratorstoperform remoteshutdowns,monitor device use, and more. The tools covered in this chapter are freeware and work inWindows and UNIX. Sysinternals (*www.microsoft.com/technet/sysinternals/*)is a collection offree tools for examining Windows products. They were created by Mark Russinovich and BryceCogswellandacquiredbyMicrosoft.

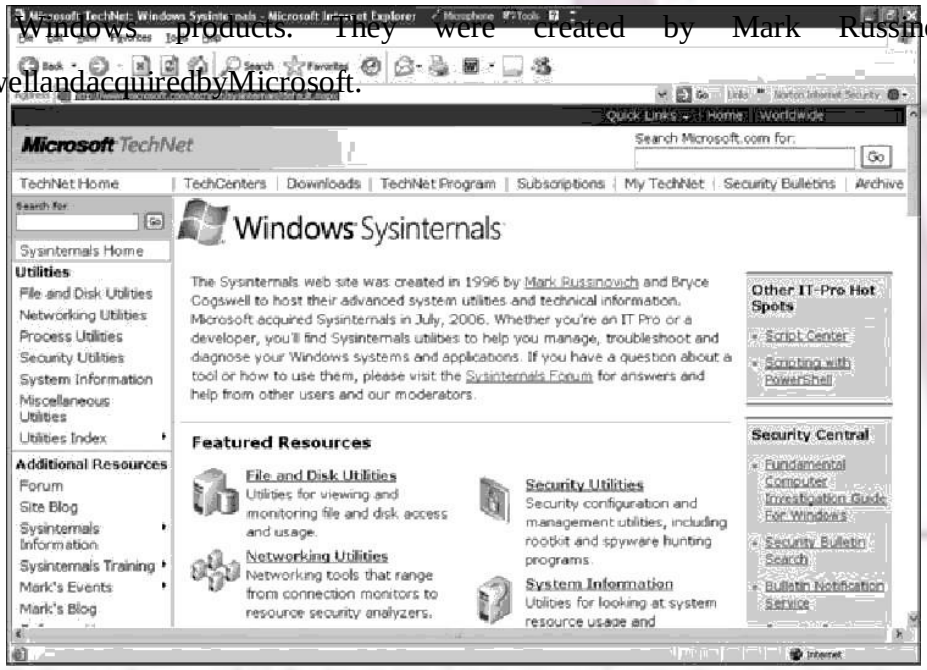


Fig:OpeningpageofSysinternals

As you can see in above Figure, you can choose from file and system, networking,process,andsecuritytools,amongothers.Thefollowinglistdescribesafewexampl esofthepowerfulWindows tools available atSysinternals:

- RegMonshowsallRegistrydatainrealtime.
- ProcessExplorershowswhatfiles,Registry keys,anddynamic linklibraries(DLLs)areloadedataspecifictime.
- Handleshowswhatfilesareopenandwhichprocessesareusingthesefiles.
- Filemonshowsfilesystemactivity.

Far too many tools are available to list here, but you should take some time to explore the siteand see what's available. One in particular that's worth investigating is PsTools, a suite createdbySysinternals thatincludes thefollowingtools:

- *PsExec*—Runsprocessesremotely
- *PsGetSid*—Displaysthesecurityidentifier(SID)ofacomputeroruser
- *PsKill*—KillsprocessesbynameorprocessID
- *PsList*—Listsdetailedinformationaboutprocesses
- *PsLoggedOn*—Displayswho'sloggedonlocally
- *PsPasswd*—Allowsyoutochangeaccountpasswords
- *PsService*—Enablesyoutoviewandcontrolservices
- *PsShutdown*—Shutsdownandoptionallyrestarts acomputer
- *PsSuspend*—Allowsyoutosuspendprocesses

UnderstandingRulesofEvidence

Consistent practices help verify your work and enhance your credibility, so you must handle allevidence consistently. Apply the same security and accountability controls for evidence in a civillawsuit asinamajorcrimetocomplywithyourstate'srulesofevidenceor

withtheFederalRulesofEvidence.Also,keepinmindthatevidenceadmittedinacriminalcasemightalso beusedinacivilsuit,andviceversa.Forexample,supposesomeoneischargedwithmurderandacquitteda t

thecriminaltrialbecausethejuryisn'tconvincedbeyondareasonabledoubtofthe person'sguilt.Ifenoughevidenceshowsthattheaccused'snegligencecontributedtoawrongfuldeath,however,thevictim'srelativescanusetheevidenceinacivillawsuitto recoverdamages.

Aspartofyourprofessionalgrowth,keepcurrentonthelatestrulingsanddirectivesoncollecting,processing, storing, and admitting digital evidence. The following sections discuss some keyconcepts of digital evidence. You can find additional information at the U.S. Department ofJustice Web site (*www.usdoj.gov*) and by searching the Internet for –digital evidence,‖–best evidencerule,‖–hearsay,‖andotherrelevantkeywords.Consultwithyourprosecutingattorney, Crown attorney, corporate general counsel, or the attorney who retained you to learn more aboutmanaging evidence for your investigation. DVD to your work folder. The work folderpathshowninscreenshotsmightdifferslightlyfromyours.

- Start Microsoft Word, and in a new document, type By creating a file,you can identify the author with file metadata. Save it in your work folder asInChp05-01.doc,andthenexitMicrosoftWord.
- To start FTK, click Start, point to All Programs, point to Access Data,point to Forensic Toolkit, and click Forensic Toolkit. If you're prompted witha warning dialog box and/or notification, click OK to continue, and click OK,ifnecessary,inthemessageboxthankingyouforevaluatingtheprogram.
- Click Go directly to working in program, and then click OK. ClickFile,AddEvidencefromthemenu.
- In the Add Evidence dialog box, enter your name as the investigator,and then click Next. In the Evidence Processing Options dialog box, acceptthedefaultsetting,andthenclickNext.
- In the main Add Evidence to Case dialog box, click the Add Evidencebutton. In the next Add Evidence to Case dialog box, click the Individual Fileoptionbutton,andthenclickContinue.
- In the Browse for Folder dialog box, navigatetoyour work folder,click

- InChp05-01.doc, click Open, and then click OK. Click Next, and thenclickFinish.
- In the main window, click the Overview tab, if necessary. Under theFile Category heading, click the Documents button. Click to select the InChp05-01.doc file in the bottom pane; its contents are then displayed in the upper-right pane. Figure shows an example (although the filename in this figure is different).

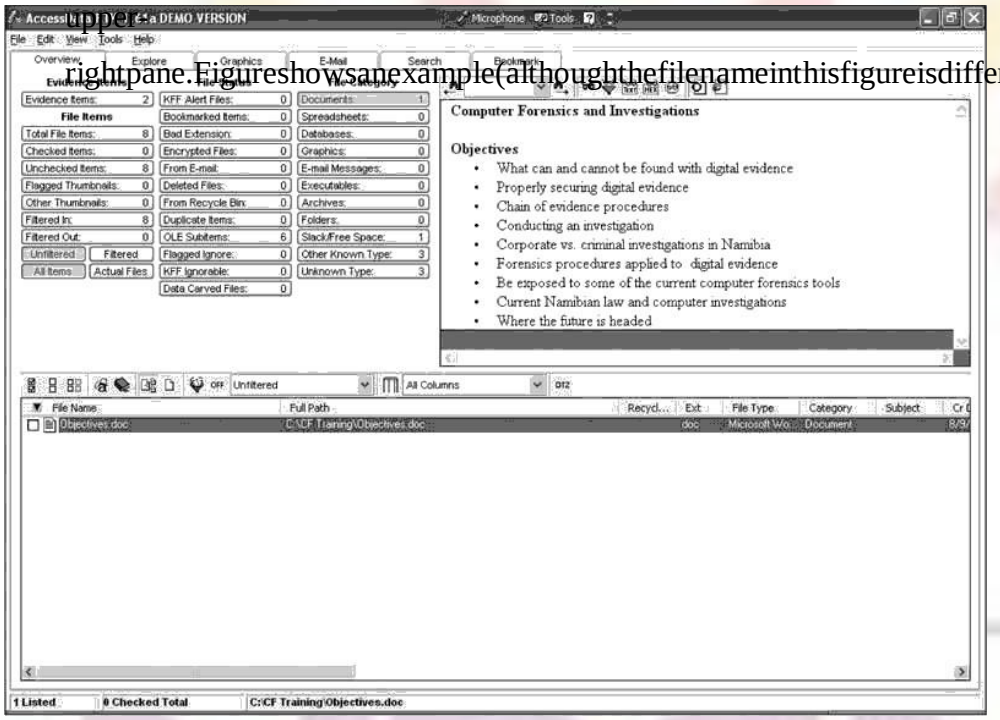


Fig:Selectingadocument

- On the File List toolbar at the upper right, click the View files innative format button, if the button isn't already selected. (*Hint*: Hover your mouseoverbuttons toseetheirnamesdisplayed.)
- Next,clicktheViewfilesinfilteredtext format button.Ifyouenteredyour username and organization when you installed Word, that information is displayed(see Figure5-2).

10. ExitFTK,clickingNoifpromptedtobackupyourwork.

Inadditiontorevealingtheauthor,computer-storedrecordsmustbeprovedauthentic, which is the most difficult requirement to prove when you're trying toqualify evidence as an exception to the hearsay rule. The process of establishingdigital evidence's trustworthiness originated with written documents and the bestevidence rule,which states that toprove the content of a written document,recording,orphotograph,ordinarilytheoriginalwriting,recording,orphoto graph is required (see Federal Rules of Evidence, 1002). In other words, theoriginal of a document is preferred to a duplicate. The best evidence, therefore, isthe documentcreatedandsavedonacomputer'sharddisk.

CollectingEvidenceinPrivate-SectorIncidentScenes

Private-sector organizationsincludebusinesses and governmentagencies thataren'tinvolved in law enforcement. In theUnited States, these agencies must comply withstate public disclo- sure and federal Freedom of Information Act (FOIA) laws and makecertain documents avail- able as public records. State public disclosure laws define statepublic records as open and available for inspection. For example, divorces recorded in apublic office, such as a court- house, become matter of public record unless a judgeorders the documents sealed. Anyone can request a copy of a public divorce decree.Figure5-3showsanexcerptofapublic disclosurelawforthestateofIdaho.

State public disclosure laws apply to state records, but the FOIA allows citizens torequestcopiesofpublicdocumentscreatedbyfederalagencies.TheFOIAwasoriginally enacted in the 1960s, and several subsequent amendments have broadened itslaws.SomeWebsitesnow providecopiesofpubliclyaccessible recordsforafee.

A special category of private-sector businesses includes ISPs and other communicationcompanies. ISPs can investigate computer abuse committed by their employees, but notbycustomers.ISPsmustpreservecustomerprivacy,especiallywhendealingwithe-mail.However, federal regulations related to the Homeland Security Actand the PatriotActof2001hasredefinedhowISPsandlargecorporateInternetusersoperateandmaintai

ntheirrecords.

ISPs and other communication companies now can investigate customers' activities that aredeemed to create an emergency situation. An emergency situation under the Patriot Act is theimmediate risk of death or personal injury, such as finding a bomb threat in an e-mail message.Some provisions of those laws have been revised over the past few years, so you should stayabreastoftheirimplications.

ProcessingLawEnforcementCrimeScenes

To process a crime scene properly, you must be familiar with criminal rules of search and seizure. You should also understand how a search warrant works and what to do when you processone. For all criminal investigations in the United States, the Fourth Amendment limits howgovernments search and seize evidence. A law enforcement officer can search for and seizecriminal evidence only with probable cause. Probable cause refers to the standard specifyingwhether a police officer has the right to make an arrest, conduct a personal or property search, orobtain a warrant for arrest. With probable cause, a police officer can obtain a search warrantfrom a judge that authorizes a search and the seizure of specific evidence related to the criminalcomplaint. Although several court cases have allowedlatitude whensearching and seizingcomputerevidence,makingyourwarrantas specific as possible toavoid challengesfromdefense attorneys is a good practice.Often a warrantis written andissuedin haste because ofthe nature of the investigation. Law enforcement officers might not have the time to research thecorrect language for stating the nature of the complaint to meet probable cause requirements.However, because a judge can exclude evidence obtained from a poorly worded warrant, youshouldreview theseissueswithyourlocalprosecutorbeforeinvestigatinga case.

PreparingforaSearch

Preparingfora computersearch and seizureisprobably themostimportantstep in computinginvestigations.Thebetteryouprepare,thesmootheryourinvestigationwillbe.Thefollowingsections discuss the tasks you should complete beforeyou search for evidence. To perform thesetasks, you might need to get answers from the victim (the complainant) and an informant, who couldbe a police detective assigned to the case, a law enforcement witness, or a manager or co-worker ofthe personof interesttotheinvestigation.

SecuringaComputerIncidentorCrimeScene

Investigators secure an incident or crime scene to preserve the evidence and to keep informationabouttheincidentorcrimeconfidential.Informationmadepubliccouldjeopardizetheinvestigation. If you're in charge of securing a computer incident or crime scene, use yellowbarrier tape to prevent bystanders from accidentally entering the scene. Use police officers orsecurity guards to prevent others from entering the scene. Legal authority for a corporate incidentscene includes trespassing violations; for a crime scene, it includes obstructing justice or failingtocomply with a police officer.Access to the scene shouldbe restricted to only those peoplewho have a specific reason to be there. The reason for the standard practice of securing anincidentorcrime sceneisto expandtheareaofcontrolbeyondthe scene'simmediatelocation.Inthis way, you avoid overlooking an area that might be part of the scene. Shrinking the scene'sperimeteris easierthanexpandingit.

For major crime scenes, computer investigators aren't usually responsible for defining a scene'ssecurityperimeter.Thesecasesinvolveotherspecialistsanddetectiveswhoarecollectingphysicalevidence and recording the scene. For incidents primarily involving computers, the computerscanbeacrimescenewithinacrimescene,containingevidencetobeprocessed.

SeizingDigitalEvidenceattheScene

With proper search warrants, law enforcement can seize all computing systems and peripherals.In corporate investigations, you might have similar authority; however, you might have theauthority only tomakeanimageof thesuspect'sdrive.Dependingon company policies,corporateinvestigatorsrarelyhavetheauthoritytoseizeallcomputersandperipherals.

When seizing computer evidence in criminal investigations, follow the U.S. DOJ standards forseizing digital data (described later in this chapter, or see *www.usdoj.gov/criminal/cybercrime/searching.html*).Forcivil investigations,followthe samerules of evidenceasforcriminalinvestigation. You might be looking for specific evidence, such a particular e-mail message orspreadsheet.Inacriminalmatter,investigatorsseizeentiredrivestopreserveasmuchinformationas possible and ensure that no evidence is overlooked. If you have any questions, doubts,

orconcerns,consultwithyourattorneyforadditionalguidance.

StoringDigitalEvidence

With digital evidence, you need to consider how and on what type of media to save it and whattype ofstorage deviceisrecommended to secureit.Themediayou useto storedigital

Evidence usually depends on how long you need to keep it. If you investigate criminal matters,store the evidence as long as you can. The ideal media on which to store digital data are CD- Rsor DVDs. These media have long lives, but copying data to them takes a long time. Older CDshad lives up to five years. Research is currently being done on CD-Rs and CD-RWs with lifespans of only one or two years. Today's larger drives demand more storage capacity; 200 GBdrives arecommon,andDVDs canstoreuptoonly17GBofdata.

You can also use magnetic tape to preserve evidence data. The 4-mm DAT magnetic tapes storebetween 40 to 72 GB or more of data, but like CD-Rs, they are slow at reading and writing data.If you're using these tapes, test your data by copying the contents from the tape back to a diskdrive. Then verify that the data is good by examining it with your computer forensics tools ordoinganMD5 hashcomparisonoftheoriginaldata setandthenewlyrestoreddataset.

If a 30-yearlifespan for data storage is acceptable foryour digital evidence, older DLTmagnetic tape cartridge systems are a good choice. Keep in mind that you never know howlong it will take for a case to go to trial. Figure shows a 4-mm DATdriveand tape andaDLTtapedrive.

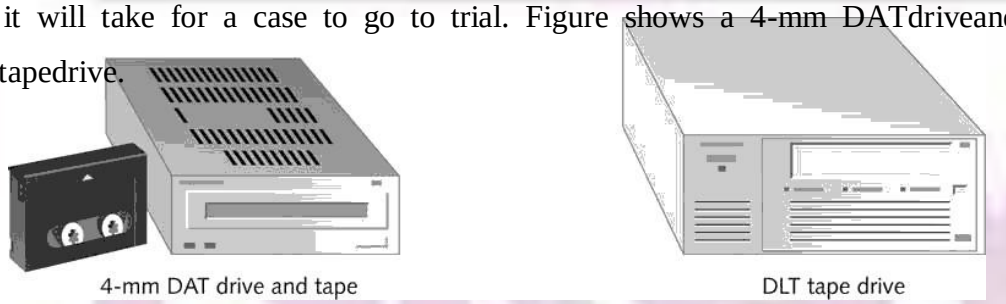


Fig:4-mmDATandDLTtapedrives

DLT systems have been used with mainframe computers for several decades and are reliable data-archiving systems. Depending on the size of the DLT cartridge, one cartridgecan store up to

80GBofdatain compressedmode.SpeedofdatatransferfromyourharddrivetoaDLTtapeisalso

faster than transferring data to a CD-R or DVD. The only major drawbackof a DLT drive andtapes is cost. A drive can cost from $400 to $800, and each tape is about $40. However, with thecurrent large disk drives, the DLT system does offer significant labor savings over other systems.Recently, manufacturers such as Quantum Corp. have introduced a high-speed, high-capacity tapecartridge drive system called Super Digital Linear Tape (Super-DLT or SLDT). These systems arespecifically designed for large RAID data backups and can store more than 1 TB of data. SmallerexternalSuper-DLTdrivescanconnecttoaworkstationthroughaSCSIcard.

However, don't rely on one media storage method to preserve your evidence—be sure to maketwo copies of every image to prevent data loss. Also, if practical, use different tools to create thetwo images. For example, you can use the Linux dd command to create the first image andProDiscovertocreatethesecondimage.

ObtainingaDigitalHash

To verify data integrity, different methods of obtaining a unique identity for file data have beendeveloped. One of the first methods, the Cyclic Redundancy Check (CRC) is a mathematicalalgorithm that determines whether a file's contents have changed. The most recent version isCRC-32. CRC, however, is not considered a forensic hashing algorithm. The first algorithm forcomputer forensics use was Message Digest 5 (MD5). Like CRC, MD5 is a mathematicalformulathattranslatesafileintoahexadecimalcodevalue,orahashvalue.Ifabitorbyteint hefile changes, it alters the hash value, a unique hexadecimal value that identifies a file or drive.(Before you process or analyze a file, you can use a software tool to calculate its hash value.)After you process the file, you produce another digital hash. If it's the same as the original one,you can verify the integrity of your digital evidence with mathematical proof that the file didn'tchange.

ReviewingaCase

Some of which are repeated in the following list. Later in this section, you apply each task to ahypothetical investigation to create a preparation plan for searching an incident or crime scene.Thefollowingarethe generaltasksyouperforminanycomputerforensics case:

- Identifythecaserequirements.
- Planyourinvestigation.
- Conducttheinvestigation.
- Complete thecasereport.
- Critiquethecase.

UNIT-4

CURRENTCOMPUTERFORENSICTOOLS

TypesofComputerForensicsTools

Computer forensics tools are divided into two major categories: hardware and software. Eachcategory has additional subcategories discussed in more depth later in this chapter. The followingsectionsoutlinebasicfeaturesrequiredandexpectedofmostcomputerforensicstools.

HardwareForensicsToolsHardwareforensicstoolsrangefromsimple,singlepurposecomponentstocompletecomputersystemsandservers.Single-purposecomponentscanbedevices, such as the ACARD AEC-7720WP Ultra Wide SCSI-to-IDE Bridge, which is designed towrite-blockanIDEdriveconnectedtoaSCSIcable.

Some examples of complete systems are Digital Intelligence F.R.E.D. systems, DIBS AdvancedForensicWorkstations,andForensicComputersForensicExaminationStationsandportable units.

Software Forensics Tools Software forensics tools are grouped into command-line applicationsand GUI applications. Some tools are specialized to perform one task, such as Safe Back, acommand-line disk acquisition tool from New Technologies, Inc. (NTI). Other tools are designedto perform many different tasks. For example, Technology Pathways Pro- Discover, X-WaysForensics, Guidance Software En Case, and Access Data FTK are GUI tools designed to performmostcomputerforensicsacquisitionandanalysisfunctions.

Software forensics tools are commonly used to copy data from a suspect's drive to an image file.Many GUI acquisition tools can read all structures in an image file as though the image were theoriginal drive. Many analysis tools, such as ProDiscover, En Case, FTK, X-Ways Forensics,ILook, and others, have the capability to analyze image files. In Chapter 4, you learned how someofthesetools are usedtoacquiredata fromsuspects'drives.

TasksPerformedbyComputer ForensicsTools

All computer forensics tools, both hardware and software, perform specific functions. Thesefunctions are grouped into five major categories, each with sub functions for further

refining dataanalysis andrecovery:

- Acquisition
- Validationanddiscrimination
- Extraction
- Reconstruction
- Reporting

In the following sections, you learn how these five functionsand associated sub functionsapplytocomputinginvestigations.

Acquisition, the first task in computer forensics investigations, is making a copy of the originaldrive. As described in Chapter 4, this procedure preserves the original drive to make sure itdoesn't become corrupt and damage the digital evidence. Sub functions in the acquisition categoryincludethefollowing:

- Physicaldatacopy
- Logicaldatacopy
- Dataacquisitionformat
- Command-lineacquisition
- GUIacquisition
- Remoteacquisition
- Verification

Some computer forensics software suites, such as Access Data FTK and En Case, provide separatetools for acquiring an image. However, some investigators opt to use hardware devices, such as theLogic be Talon, VOOM Hard Copy 3, or Image MASSter Solo III Forensic unit from IntelligentComputer Solutions, Inc., for acquiring an image. These hardware devices have their own built-insoftware for data acquisition. No other device or program is needed to make a duplicate drive;however,youstillneedforensicssoftwaretoanalyzethedata.

ValidationandDiscrimination

Two issues in dealing with computer evidence are critical. First is ensuring the integrity of databeing copied—the validation process. Second is the discrimination of data, which involves sortingandsearchingthroughallinvestigationdata.Theprocessofvalidatingdataiswhatallows

discrimination of data. Many forensics software vendors offer three methods for discriminating datavalues.Thesearethesubfunctionsofthevalidationanddiscriminationfunction:

- Hashing
- Filtering
- Analyzingfileheaders

Validating data is done by obtaining hash values. As a standard feature, most forensics tools andmany disk editors have one or more types of data hashing. How data hashing is used depends on theinvestigation, but using a hashing algorithm on the entire suspect drive and all its files is a goodidea. This method produces a unique hexadecimal value for data, usedto make sure the originaldatahasn't changed.

This unique value has other potential uses. For example, in the corporate environment, you couldcreate a known good hash value list of a fresh installation of an OS, all applications, and allknown good images and documents (spreadsheets, text files, and so on). With this information, aninvestigator could ignore all files on this known goodlistandfocusonother files on the diskthat aren't on this list. This process isknown as filtering.Filteringcan also be used to find dataforevidenceincriminalinvestigationsortobuild acaseforterminatingan employee.

The primary purpose of data discrimination is to remove good data from suspicious data. Good dataconsistsofknownfiles,suchasOS filesand commonprograms (MicrosoftWord,forexample).

Several computer forensics programs can integrate known good file hash sets, such as the ones fromthe NSRL, and compare them to file hashes from a suspect drive to see whether they match. Withthis process, you can eliminate large amounts of data quickly so that you can focus your evidenceanalysis.Youcanalsobeginbuildingyourownhashsets.

Another feature to consider for hashing functions is hashing and comparing sectors of data. Thisfeature is useful for identifying fragments of data in slack and free disk space thatmight bepartiallyoverwritten.

An additional method of discriminating data is analyzing and verifying header values for known filetypes. Similar to the hash values of known files, many computer forensics pro- grams include a

listofcommonheadervalues.Withthisinformation,youcanseewhetherafileextensionisincorrect

for thefiletype.Renamingfileextensionsisacommonwaytotrytohidedata,andyoucouldmisspertinentdata ifyoudon’tcheckfileheaders.

Extraction

Theextractionfunctionistherecoverytaskinacomputinginvestigationandisthemostchallengingofalltaskst omaster.

Recoveringdataisthefirststepinanalyzinganinvestigation’sdata.Thefollowingsubfunctionsofextractio nareusedininvestigations:

- Dataviewing
- Keywordsearching
- Decompressing
- Carving
- Decrypting
- Bookmarking

Many computer forensics tools include a data-viewing mechanism for digital evidence. How data isvieweddependsonthetool.ToolssuchasProDiscover,X-WaysForensics,FTK,EnCase,SMART, ILook, and others offer several ways to view data, including logical drive structures, suchas folders and files. These tools also display allocated file data and unallocated disk areas withspecial file and disk viewers. Being able to view this data in its normal form makes analyzing andcollectingcluesfortheinvestigationeasier

.4.2ComputerForensicsSoftwareTools

Whether you use a suite of tools or a task-specific tool, you have the option of selecting one thatenables you to analyze digital evidence through the command line or in a GUI. The followingsectionsexploresomeoptionsfor command-lineandGUItoolsinbothWindowsandUNIX/Linux.

Command-LineForensicsTools

Computers used several OSs before MS-DOS dominated the market. During this time, computerforensics wasn’ta majorconcern.After people started using PCs, however, they figured outhowtousethemforillegalanddestructivepurposesandtocommitcrimesandcivilinfractions.

Software developers began releasing computer forensics tools to help private- and public-sectorinvestigators examine PCs. The first tools that analyzed and extracted data from floppy disks andharddisks wereMS-DOStoolsforIBM PCfilesystems.

One of the first MS-DOS tools used for computer investigations was Norton Disk Edit. This toolused manual processes thatrequiredinvestigators tospend considerable time on a typical 500MB drive. Eventually, programs designed for computer forensics were developed for DOS,Windows, Apple, NetWare, and UNIX systems. Some of these early programs could extract datafrom slack and free disk space; others were capable only of retrieving deleted files. Currentprograms are more robust and can search for specific words or characters, import a keyword listtosearch,calculatehashvalues,recoverdeleted items,conductphysicaland logicalanalyses,andmore.

One advantage of using command-line tools for an investigation is that they require few sys-temresources because they're designed to run in minimal configurations. In fact, most tools fit onbootablemedia(floppy disk,USBdrive,CD,orDVD).Conductinganinitialinquiry oracomplete investigation with bootable media can save time and effort. Most tools also produce atextreportsmallenoughtofitonafloppydisk.

ForensicWorkstations

Many computer vendors offer a wide range of forensic workstations that you can tailor to meetyour investigation needs. The more diverse yourinvestigationenvironment,themore optionsyouneed.Ingeneral,forensicworkstationscanbedividedintothe followingcategories:

• *Stationaryworkstation*—Atowerwithseveralbaysandmanyperipheraldevices

• *Portableworkstation*—Alaptopcomputerwithabuilt-inLCDmonitorandalmostasmanybays andperipheralsas astationaryworkstation

• *Lightweightworkstation*—usuallyalaptopcomputerbuiltintoacarryingcasewitha smallselectionofperipheraloptions

When considering options to add to a basic workstation, keep in mind thatPCs have limitationson how many peripherals they can handle. The more peripherals you add, the more potentialproblems you might have, especially if you're using an older version of Windows. You must learntobalancewhatyouactuallyneedwithwhatyoursystemcanhandle.

ValidatingandTestingForensicsSoftware

Now that you have selected some tools to use, you need to make sure the evidence you recover andanalyze can be admitted in court. To do this, you must test and validate your software. Thefollowing sections discuss validation tools available at the time of this writing and how to developyourownvalidationprotocols.

Using National Institute of Standards and Technology(NIST)Tools

The National Institute of Standards and Technology publishes articles, provides tools, and createsprocedures for testing and validating computer forensics software. Software should be verified toimprove evidence admissibility in judicial proceedings. NIST sponsors the Computer ForensicsToolTesting(CFTT)projecttomanage researchoncomputerforensicstools.

- Establishcategoriesforcomputerforensicstools—Groupcomputerforensicssoftwareaccordingtocategories,suchasforensicstoolsdesignedtoretrieveandtracee-mail.
- Identify computer forensics category requirements—For each category,describethetechnicalfeaturesorfunctionsaforensicstoolmusthave.
- Develop test assertions—Based on the requirements, create tests thatproveordiSprovethetool'scapabilitytomeettherequirements.
- Identify test cases—Find or create types of cases to investigate with theforensics tool, and identify information to retrieve from a sample drive orothermedia.Forexample,usetheimageofaclosedcasefilecreatedwithatrusteddforensicstooltotestanewtoolinthesamecategoryandseewhetheritproducesthesameresults.
- Establishatestmethod—Consideringthetool'spurposeanddesign,specifyhowtotestit.
- Reporttest results—Describethetest resultsinareportthatcomplieswithISO 17025,whichrequiresaccurate,clear,unambiguous,andobjectivetestre

ports.

Another standards document, ISO 5725, demands accuracy for all aspects of the testing pro- cess, so resultsmustberepeatableandreproducible.–Repeatableresults‖meansthatifyouworkinthesamelab onthesame machine, yougeneratethesameresults. –Reproducibleresults‖meansthat ifyou're in a differentlabworkingonadifferentmachine,thetoolstillretrieves the sameinformation.

ExploringtheRoleofE-mailinInvestigations

E-mailevidencehasbecomeanimportantpartofmanycomputinginvestigations,socomputerforensicsinvestigators mustknowhowe-mailisprocessedtocollectthisessential evidence.Inaddition, with the increase in e-mail scams and fraud attempts with phishing or spoofing, investigatorsneedtoknow howtoexamineandinterprettheunique contentofe-mailmessages.

As a computing investigator, you might be called on to examine a phishing e-mail to see whether it'sauthentic.Later,in–Tracingan E-mailMessage,‖youlearnaboutresourcesforlookingupe-mail and Webaddressestoverifywhetherthey'reassociatedwithaspoofedmessage.

One of the most noteworthy e-mail scams was 419, or the Nigerian Scam, which originated as a chainletter from Nigeria, Africa. Fraudsters now need only access to Internet e-mail to solicit victims, thussaving postage costs of international mail. Unlike newer, more sophisticated phishing e-mail frauds,419messageshavecertaincharacteristicploysandatypicalwritingstyle.Forexample,thesenderasksfor access to your bank account so that he can transfer his money to it as a way to prevent corruptgovernment officials in his homeland from confiscating it. The sender often promises to reward youfinancially if you make a minor payment or allow access to your bank account. The messages areusuallyinuppercaseletters andusepoorgrammar

ExploringtheRolesoftheClientandServerinE-mail

You can send and receive e-mail in two environments: via the Internet or an intranet (an internalnetwork).In both e-mail environments,messagesaredistributedfrom acentral servertomanyconnectedclient computers,aconfigurationcalled client/serverarchitecture.Theserverrunsane-mailserver program, such as Microsoft Exchange Server, Novell GroupWise, or UNIX Send mail, toprovide e-mail services. Client computers use e-mail programs (also called e-mail clients), such asNovell Evolution or Microsoft Outlook, to contact the e-

mail server and send and retrieve e-mailmessages.

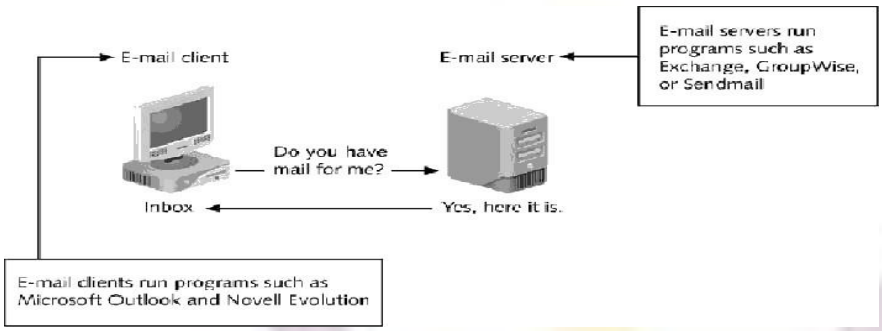


Fig:RoleofclientandserverinE-mail

Regardless of the OS or e-mail program, users access their e-mail based on permissions the e-mailserver administrator grants. These permissions prevent users from accessing each other's e-mail. Toretrieve messages from the e-mail server, users identify themselves to the server, as when loggingontothenetwork.Thene-mails aredeliveredtotheircomputers.

E-mail services on both the Internet and an intranet use a client/server architecture, but they differ inhow clientaccounts are assigned, used,andmanagedandinhowusersaccess their e-mail.Overall, an intranet e-mail system is for the privateuseofnetwork users, and Internet e-mailsystems are for public use. On an intranet, the e-mail server is generally part of thelocalnetwork,and an administrator manages the server and its services. In most cases, an intranet e-mail system isspecific to a company, used only by its employees, and regulated by its business practices, whichusually include strict security and acceptable use policies. For example, network users can't createtheirown e-mailaccounts,andusernamestendtofollowanamingconventionthatthee-mailadministrator determines.

InvestigatingE-mailCrimesandViolations

Investigating crimes or policy violations involving e-mail is similar to investigating other types ofcomputer abuse and crimes. Your goal is to find out who's behind the crime or policy violation,collecttheevidence,and presentyourfindingstobuildacaseforprosecutionorarbitration.

E-mail crimes and violations depend on the city, state, and sometimes country in which the e-mailoriginated. For example, in Washington State, sending unsolicited e-mail is illegal. However, in otherstates, it isn't considered a crime. Consult with an attorney for your organization to determine whatconstitutes ane-mailcrime.

Committing crimes with e-mail is becoming commonplace, and more investigators are findingcommunications that link suspects to a crime or policy violation through e-mail. For example, somepeopleusee-mailwhencommittingcrimessuchasnarcoticstrafficking,extortion,sexualharassment, stalking, fraud, child abductions, terrorism, child pornography, and so on. Because e-mailhasbecomea majorcommunicationmedium,anycrimeorpolicyviolationcan involvee-mail.

ExaminingE-mailMessages

After you have determined that a crime has been committed involving e-mail, first access the victim'scomputer to recover the evidence. Using the victim's e-mail client,find and copy any potentialevidence. It might be necessary to log on to the e-mail service and access any protected or encryptedfiles or folders. If you can't actually sit down at the victim's com- puter, you have to guide the victimon the phone to open and print a copy of an offending message, including the header. The headercontains unique identifying numbers, such as the IP address of the server that sent the message. Thisinformationhelpsyoutracethee-mailtothesuspect.

CopyinganE-mailMessage

Before you start ane-mailinvestigation,youneedto copy and print the e-mail involved in thecrime or policy violation. You might also want to forward the message as an attachment to another e-mailaddress,dependingonyourorganization'sguidelines.

The following activity shows you how to use Outlook 2007, included with Microsoft Office,to copyan e-mail message to a USB drive. (*Note*: Depending on the Outlook version you use, the stepsmight vary slightly.) You use a similar procedure to copy messages in other e-mail programs, such asOutlook Express and Evolution. If Outlook or Outlook Express is installed on your computer, followthesesteps:

- InsertaUSBdriveintoaUSBport.
- OpenWindowsExplorerortheComputerwindow,navigatetoth eUSBdrive,andleavethiswindowopen.
- Start Outlookbyclicking Start,pointingtoAllPrograms,pointingtoMicrosoftOffice,andcl ickingMicrosoftOfficeOutlook2007.

- In the Mail Folders pane (see Figure 12-2), click the foldercontaining the message you want to copy. For example, click theInbox folder. A list of messages in that folder is displayedin thepaneinthemiddle.Clickthemessageyouwanttocopy.
- ResizetheOutlookwindowsothatyoucanseethemessageyouwantt ocopyandtheUSBdriveiconinWindowsExplorerortheComputer window.
- Dragthemessagefromthe OutlookwindowtotheUSBdriveiconin WindowsExplorerorthe Computerwindow.
- Click File, Print from the Outlook menu to open the Print dialogbox.Afterprintingthee-mailsothatyouhaveacopytoincludeinyourfinalreport,exitOutlook.

ViewingE-mailHeaders

After you copy and print a message, use the e-mail program that created it to find the e-mail header.Thissectionincludesinstructionsforviewinge-mailheadersinavarietyofe-mailprograms,including Windows GUI clients, a UNIX command-line e-mail program, and some common Web-based e-mail providers. After you open e-mail headers, copy and paste them into a text document sothatyoucanreadthemwithatexteditor,suchasWindows.

ToretrieveanOutlooke-mailheader,followthesesteps:

- Start Outlook, and then select the original of the message youcopiedinthepreviussection.
- Right-click the message and click Message Options to open theMessage Options dia- log box. The Internet headers text box at thebottomcontains themessageheader.

Fig: AnOutlooke-mailheader

- Selectall themessageheader text,and then press Ctrl+Ctocopy itto theClipboard.
- Start Notepad,andthen pressCtrl+Vinanewdocumentwindowtopastethemessageheadertext.
- Save the document as Outlook Header.txt in your work folder.Then close the document and exit Outlook. To retrieve an OutlookExpresse-mailheader,follow thesesteps:
- StartOutlookExpress,andthendisplaythemessageyouwanttoexamine.
- Right-clickthemessageandclickPropertiestoopenadialogboxshowinggeneralinformationaboutthemessage.

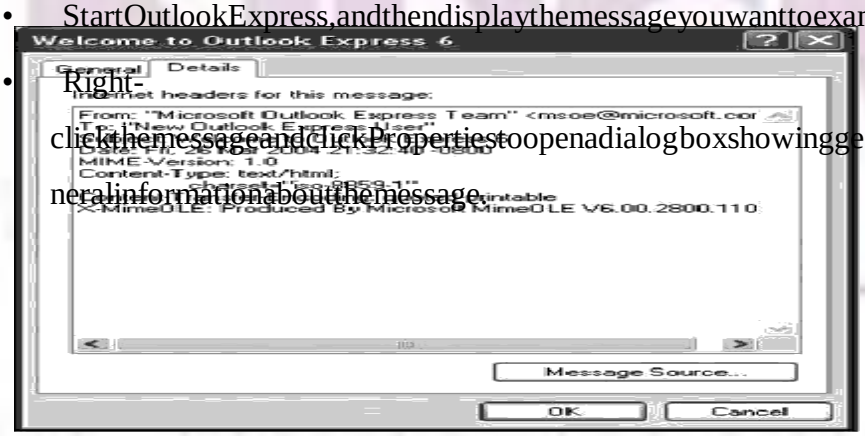


Fig:AnOutlookExpresse-mailheader

- ClicktheMessageSourcebuttontoviewthee-mail'sHTMLsourcecode,whichcanbehelpfulinexaminingpossiblephishingmessages.
- Selectall themessageheadertext,andthen pressCtrl+CtocopyittotheClipboard.
- StartNotepad,andthenpressCtrl+Vinanewdocumentwindowtopastethemessageheadertext.
- SavethedocumentasOutlookExpressHeader.txtinyourworkfolder,andthenexitNotepad.
- Closeallopenwindowsanddialogboxes,andthenexitOutlookExpress.

Fig:Viewingthemessage'sHTMLsourcecode

Toretrieveane-mailheaderinNovellEvolution,followthesesteps:

- StartEvolution,andopentheInbox.
- Double-clickthee-mailmessagetoopenit.
- Click View, All Message Headers from the menu to display thee-mailheader,showninFigure12-6.
- Select all the message header text, and then press Ctrl+C tocopy itto the Clipboard. Starta texteditor,such as KEditor gedit,andthenpressCtrl+Vinanewdocumentwindowtopastethemessage headertext.
- Save the document as Evolution Header.txt in your workfolder, closethefile, and thenexitthetexteditorandEvolution.

In the previous activities, you used a GUI program to find the header information. Now you see howto find this same information with a command-line e-mail program. If available, follow these steps toretrievee-mailheadersinUNIXPine:

- Start Pinebytypingpineatthecommandpromptandpressing Enter. The Pine e-mail screen appears with availableoptions atthebottom.
- Typestodisplaysetupoptions.

UnderstandingE-mailServers

An e-mail server is loaded with software that uses e-mail protocols for its services andmaintains logs you can examine and use in your investigation. As a computer forensics investigator,you can't know everything about e-mail servers. Your focus is not to learn how a particular e-mailserver works but how to retrieve information about e-mails for an investigation. Usually, you mustwork closely with the network administrator or e-mail administrator, who is often willing to help youfind the data or filesyou need and might even suggest new ways to find this information. Ifyoucan'tworkwithanadministrator,conductresearch ontheInternetorusetheforensicstoolsdiscussedlaterinthischaptertoinvestigatethee-mailserversoftwareandOS.

To investigate e-mail abuse, you should know how an e-mail server records and handles the e-mail itreceives. Some e-mail servers use databases that store users' e-mails, and others use a flat file system.All e-mail servers can maintain a log of e-mails that are processed. Some e-mail serversaresetuptologe-mailtransactionsbydefault;othersmustbeconfiguredtodoso.Moste-mailadministrators log system operations and message traffic to recover e-mails in case of a disaster, tomakesurethefirewallande-mail filtersareworkingcorrectly,andtoenforce companypolicy.

However, the e-mail administrator can disable logging or use circular logging, whichover- writes the log file when it reaches a specified size or at the end of a specified time frame.Circular logging saves valuable server space, but you can't recover a log after it's overwritten. Forexample, on Monday the e-mail server records traffic in the Mon.log file. For the next six days, thee-mail server uses a log for each day, such as Tues.log, Wed.log, and so forth. On Sunday atmidnight, the e-mail server starts recording e-mail traffic in Mon.log, overwriting the informationlogged the previous Monday. The only way to access the log file information is from a backup file,whichmanye-mailadministrators createbeforealogfileisoverwritten.

E-mail logs generally identify the e-mail messages an account received, the IP address from whichthey were sent, the time and date the e-mail server received them, the time and date the clientcomputeraccessedthee-mail,thee-mailcontents,system-specificinformation,andanyotherinformation the e-mail administrator wants to track. These e-mail logs are usually formatted in plaintextandcanbereadwitha basictexteditor,suchasNotepadorvi.

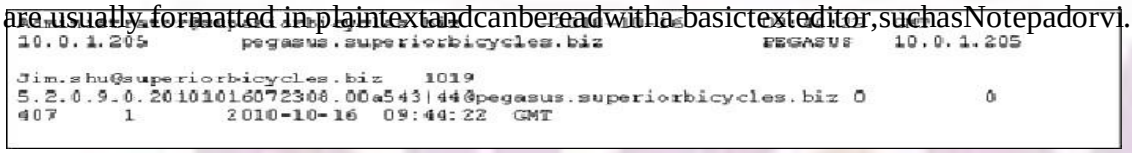


Fig:Ane-mailserverlogfile

UsingSpecializedE-mailForensicsTools

For many e-mail investigations, you can rely on e-mail message files, e-mail headers, and e-mailserverlogfiles.However,ifyoucan'tfindane-mailadministratorwillingtohelpwiththeinvestigation, or you encounter a highly customized e-mail environment, you can use data recoverytoolsandforensicstools designedtorecovere-mailfiles.

Astechnologyhasprogressedine-mailandotherservices,sohavethetools

forrecoveringinformationlostordeletedfromaharddrive.Inpreviouschapters,youhavereviewedmanytoolsf ordata

recovery, such as ProDiscover Basic and Access Data FTK. You can also use these tools to investigateand recover e-mail files. Other tools, such as the ones in the follow- ing list, are specifically created fore-mailrecovery,includingrecoveringdeletedattachments fromaharddrive:

- DataNumenforOutlookandOutlookExpress
- FINALeMAILforOutlookExpressand Eudora
- Sawmill-GroupWiseforloganalysisoffice_agent.html)
- DBXtractforOutlookExpress
- FookesAid4MailandMailBagAssistantforOutlook,Thunderbird,andEudora
- ParabenE-MailExaminer,configuredtorecoverseverale-mailformats
- AccessDataFTKforOutlookandOutlookExpress
- OntrackEasyRecoveryEmailRepairforOutlookand OutlookExpress
- R-ToolsR-MailforOutlookandOutlookExpress.
- Office Recovery's Mail Recovery for Outlook, Outlook Express, Exchange,ExchangeServer,andIBMLotusNotes

When you use a third-party tool to search for a .db file, for example, you can find where theadministrator stores .db files for the e-mail server. To find log files, use .log as the search criteria.You're likely to find at least two logs related to e-mail—one listing logged events for messages andtheotherlistingloggedeventsforaccounts accessinge-mail.

FTK, En Case, and other forensics tools enable you to find e-mail database files, personal e-mailfiles,offlinestoragefiles,andlogfiles.Sometoolsallowyoutoviewmessagesandotherfileswitha special viewer; others require using a text editor to compare information, such as the date and timestamp, username,domain, andmessage contents, to determine whetheritmatches whatwas foundonthevictim'scomputer.

One advantage of using data recovery tools is that you don't need to know how the e-mail serveror e-mail client operates to extract data from these computers. Data recovery tools do the workforyouandallowyoutoviewevidenceonthecomputer.

After you compare e-mail logs with the messages, you should verify the e-mail account, messageID, IP address, and date and time stamp to determine whether there's enough evidence for awarrant.Ifso,you canobtainandserveyourwarrantforthe suspect'scomputerequipment.

UnderstandingMobileDeviceForensics

People store a wealth of information on cell phones, and the thought of losing your cell phoneand, therefore, the information stored on it can be a frightening prospect.Despite this concern,not many people think about securing their cell phones, although they routinely lock and securelaptops or desktops. Depending on your phone's model, the following items mightbe stored onit:

- Incoming,outgoing,and missedcalls
- TextandShortMessageService(SMS)messages
- E-mail
- Instantmessaging(IM)logs
- Webpages
- Pictures
- Personalcalendars
- Addressbooks
- Musicfiles
- Voicerecordings

Many people store more information on their cell phones than they do on their computers andwith this variety of information, piecing together the facts of a case is possible. Recent cases,such as the rape allegations at Duke University and the Scott Peterson murder trial, showthatcell phone data is used increasingly in court as evidence. In some countries, cell phones are evenusedtologintobankaccountsandtransferfundsfromonecellphonetoanother,which

provides even more potential evidence. This handheld device is one of the most versatile piecesofequipmentinventedyet.

Despite the usefulness of these devices in providing clues for investigations, investigating cellphones and mobile devices is one of the most challenging tasks in digital forensics. No singlestandard exists for how and where cell phones store messages, although many phones use similarstorage schemes. In addition, new phones come out about every six months, and they're rarelycompatible with previous models. Therefore, the cables and accessories you have might becomeobsolete in a short time. Also, cell phones are often combined with PDAs, which can makeforensicsinvestigationsmorecomplex.

MobilePhoneBasics

Since the 1970s, when Motorola introduced cell phones, mobile phone technology has advancedrapidly. Gone are the days of two-pound cell phones that only the wealthy could afford. In thepast 40 years, mobile phone technology has developed far beyond what the inventors could haveimagined.

Up to the end of 2008, there have been three generations of mobile phones: analog, digitalpersonal communications service (PCS), and third-generation (3G). 3G offers increased band-width,comparedwiththeother technologies:

- 384Kbps forpedestrianuse
- 128Kbpsinamovingvehicle
- 2Mbpsinfixedlocations,suchasofficebuilding.

UnderstandingAcquisitionProceduresforCellPhonesandMobileDevices

All mobile devices have volatile memory, so making sure they don't lose power before you canretrieve RAM data is critical. At the investigation scene, determine whether the device is on oroff.Ifit'soff,leaveitoff,butfindtherechargerandattachitassoonaspossible.Note thisstepin your log if you can't determine whether the device was charged at the time of seizure. If thedeviceison,checktheLCDdisplayforthebattery'scurrentchargelevel.

Because mobile devices are often designed to synchronize with applications on a user's PC, anymobile device attached to a PC via a cable or cradle/docking station should be disconnected fromthePCimmediately.Thisprecautionhelpspreventsynchronizationthatmightoccurautomatically on a preset schedule and overwrite data on the device. In addition, collect the PCand any peripheral devices to determine whether the hard drive contains any information that'snotonthemobiledevice.

Depending on the warrantor subpoena, the time of seizure mightbe relevant.In addition,messages might be received on the mobile device after seizure that may or may not be admissiblein court. If you determine that the device should be turned off to preserve battery power or apossible attack, note the time and date at which you take this step. The alternative is to isolate thedevicefromincomingsignalswithoneofthefollowingoptions:

- Placethedeviceinpaintcan,preferablyonethatpreviouslycontainedradiowave–blockingpaint.
- Use the Paraben Wireless Strong Hold Bag which conforms to Faradaywirecagestandards.
- Useeightlayersofantistaticbags(forexample,thebagsthatnewharddrivesare wrappedin)toblockthesignal.

The drawback of using these isolating options is that the mobile device is put into roaming mode,which accelerates battery drainage. NIST suggests supplying a portable means of power, such asa battery-powered charger, to prevent this problem. Newer mobile devices shut themselves off orentera‐sleepstate‖afterreachingacertainlowbatterylevel.

As mentioned, memory resides in the phone itself and in the SIM card, if the device is equippedwith one. The file system for a SIM card is a hierarchical structure. This file structure begins withthe root of the system (MF). The next level consists of directory files (DF), and under them arefilescontainingelementarydata(EF).EFsundertheGSMandDCS1800DFscontainnetworkdataondifferentfrequencybandsofoperation.TheEFsundertheTelecomDFcontainservice-relateddata.

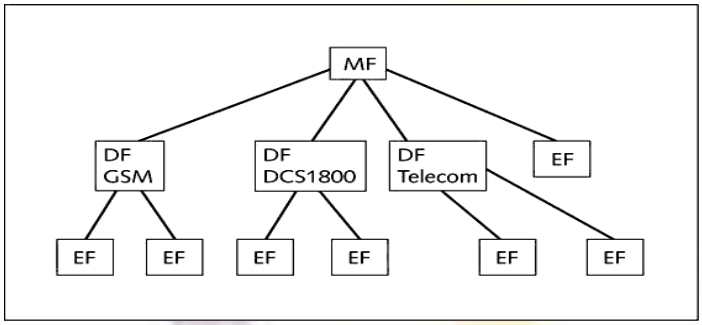


Fig:SIMfilestructure

Youcanretrievequiteabitofdatafromasimcard.Theinformationthatcanberetrievedfallsintofourcategories:

- Service-relateddata,suchasidentifiersfortheSIMcardandsubscriber
- Calldata,suchasnumbersdialed
- Messageinformation
- Locationinformation

If power has been lost, you might need PINs or other access codes to view files. Typically, userskeep the original PIN assigned to the SIM card, so when you're collecting evidence at he scene,look for users' manuals and other documentation that can help you access the SIM card. Withmost SIM cards, you have three attempts at entering an access code before the device is locked,which then requires calling the service provider or waiting a certain amount of time before tryingagain.Commoncodes totryare1-1-1-1or1-2-3-4.

SIM Card Readers With GSM phones and many newer models of mobile devices, the next stepis accessing the SIM card, which you can do by using a combination hardware/ software devicecalled a SIM card reader. To use this device, you should be in a forensics lab equipped withantistatic devices. In addition, biological agents, such as fingerprints, might be present on theinside of the case, so you should consult the lead investigator when you're ready to proceed tothisstep.Thegeneralprocedureisasfollows:

- Removethebackpanelofthedevice.
- Removethebattery.
- Underthebattery,removetheSIMcardfromitsholder.

- InserttheSIMcardintothecardreader,whichyouinsertintoyourforensicwork station'sUSB port.

A variety of SIM card readers are on the market. Some are forensically sound and some are not;make sure you note this feature of the device in your investigation log. Another problem withSIM card readers is dealing with text and SMS messages that haven't been read yet. After youview a message, the device shows the message as opened or read. For this reason, documentingmessages that haven't been read is critical. Using a tool that takes pictures of each screen can bevaluableinthissituation. Thesescreencaptures canprovide additionaldocumentation.

IPhone Forensics Because the iPhone is so popular, its features are copied inmanyothermobile devices. The wealth of information that can be stored on this device makes iPhoneforensicsparticularlychallenging.Atfirst,manyresearchersandhackerstriedtofindawayto –crack‖theiPhonebutwereunsuccessfulbecausethedeviceispracticallyimpenetrable.Amore fruitful approach was hacking backup files. However, this method doeshave limitations: Youcan access only files included in a standard backup, so deleted files,for example, can't beaccessed

UNIT–V

WORKINGWITHWINDOWSandDOSSYSTEMS

Understandingfilesystems

To investigate computer evidence effectively,you must understand how the most commonlyused OSs work and how they store files. In addition to this section on file systems, you shouldreview books on Computer Technology Industry Association. A file system gives an OS a roadmap to data on a disk. The type of file system an OS uses determines how data is stored on thedisk. A file system is usually directly related to an OS, although some vendors grandfather inprevious OSs so that newer ones can read them. For example, most current Linux releases canaccessdisksconfiguredintheolderLinuxExt2fsandExt3fsfilesystems.

No matter which platform you use, you need to know how to access and modify system settingswhen necessary. When you need to access a suspect's computer to acquire or inspect data relatedtoyourinvestigation,youshouldbefamiliarwiththecomputer'splat-form.

UnderstandingtheBootSequence:

To ensure that you don't contaminate or alter data on a suspect's Windows or DOS PC, youmust know how to access and modify a PC's Complementary Metal Oxide Semi-conductor(CMOS)andBasicInput/OutputSystem(BIOS)settings.Acomputerstoressystemconfigura tion and date and time information in the CMOS when power to the system is off. ThesystemBIOS contains programsthatperforminputandoutputat thehardware level.

When a subject's computer starts, you must make sure it boots to a forensic floppy disk orCD, becausebootingtotheharddiskoverwritesand changes evidentiary data. To do this,you access the CMOS setup by monitoring the subject's computer during the initial bootstrapprocess to identify the correct key or keys to use. The bootstrap process is contained in ROM andtells the computer how to proceed. As the computer starts, the screen usually displays the key orkeys, such as the Delete key; you press to open the CMOS setup screen. You can also tryunhooking the keyboard to force the system to tell you what keys to use. The key you press toaccess.

CMOS depends on the computer's BIOS. The popular BIOS manufacturers Award and AMI usethe Delete key to access CMOS; other manufacturers use Ctrl+Alt+Insert, Ctrl+A, Ctrl+A, orCtrl+F1,F2,andF10.

Figure shows a typical CMOS setup screen, where you check a computer's boot sequence. Ifnecessary, you can change the boot sequence so that the OS accesses the CD/ DVD drive or afloppydrive(ifavailable)beforeanyotherbootdevice.EachBIOSvendor'sscreenisdifferent,

but you can refer to the vendor's documentationor Web site for instructions on changing thebootsequence.

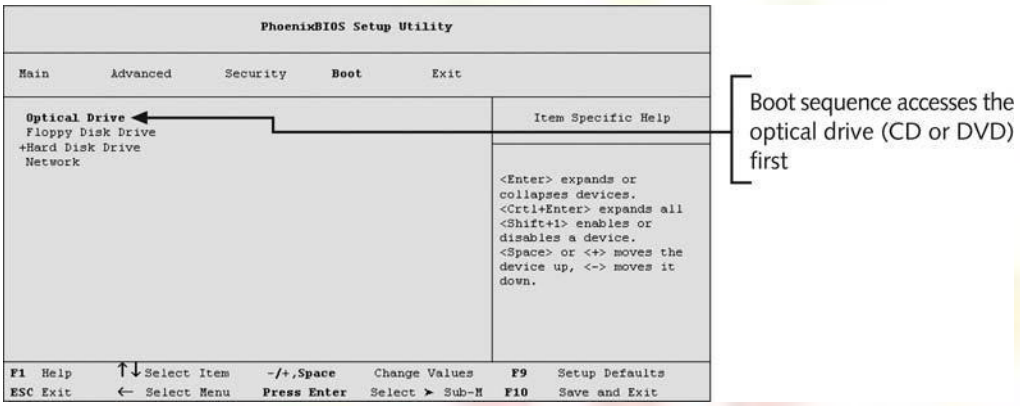


Fig:AtypicalCMOSsetupscreen

UnderstandingDiskDrives:

You should be familiar with disk drives and how data is organized on a disk so that you can finddata effectively. Disk drives are made up of one or more platters coated with magnetic material,and data is stored on platters in a particular way. For additional information ondisk driveconfigurations, see*www.storagereview.com/guide2000/ref/hdd/index.html*. Follow- ingis a listofdiskdrivecomponents:

- *Geometry*—Geometryrefers toadisk'sstructureofplatters,tracks,andsectors.
- *Head*—theheadisthedevicethatreadsandwritesdatatoadrive.There'soneheadperplatter.
- *Tracks*—Tracksareconcentriccirclesonadiskplatterwheredataislocated.
- *Cylinders*—acylinderisacolumnoftracksontwoormorediskplatters.Typically,eachplatterhas twosurfaces:topandbottom.
- *Sectors*—asectorisa sectiononatrack,usuallymadeupof512bytes.

The manufacturer engineers a disk to have a certain number of sectors per track, and a typicaldisk drive stores 512 bytes per sector. To determine the total number of addressable bytes on adisk, multiply the number of cylinders by the number of heads (actually tracks) and by thenumberofsectors (groupsof512ormorebytes).

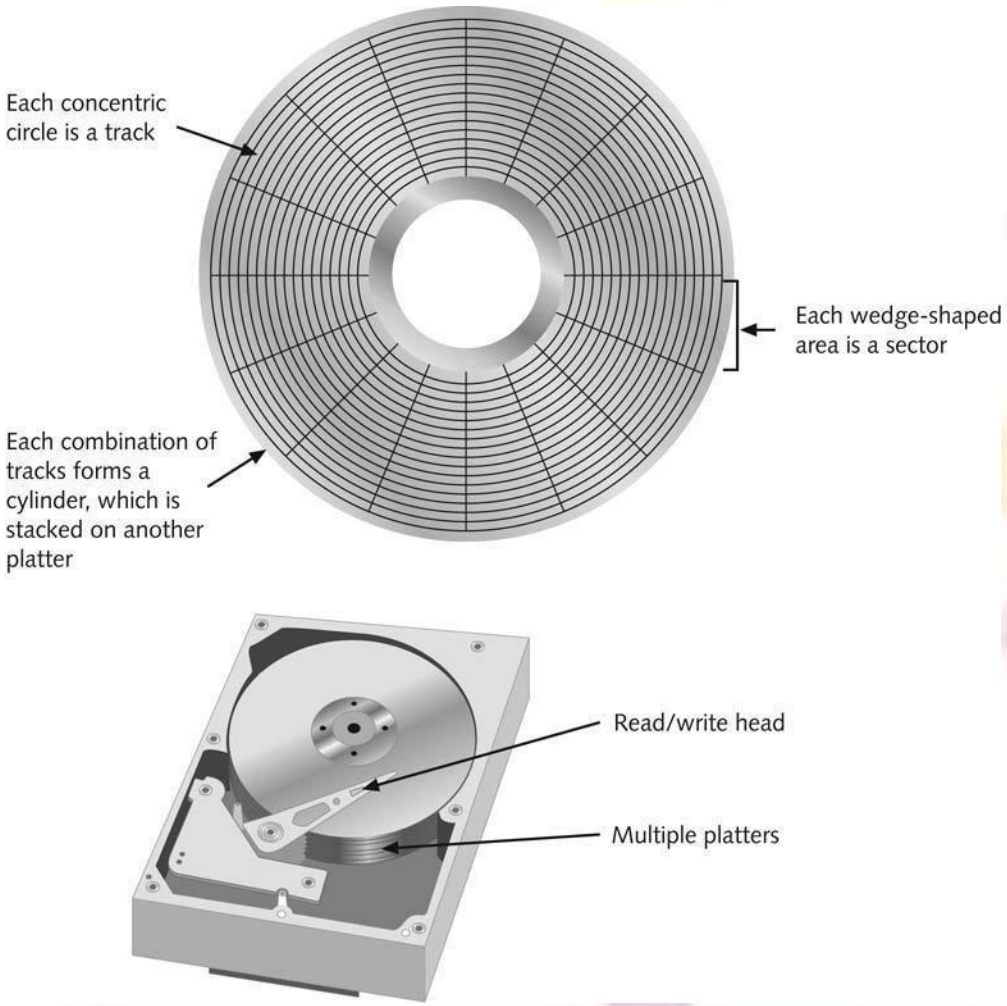


Fig :diskdrives

ExploringMicrosoftFileStructures

BecausemostPCsuseMicrosoftsoftwareproducts,youshouldunderstandMicrosoftfilesystems so that you know how Windows and DOS computers store files. In particular, you needto understand clusters, File Allocation Table (FAT), and New Technology File System (NTFS).The method an OS uses to store files determines where data can be hidden. When you examine acomputer for forensic evidence, you need to explore these hiding places to determine whethertheycontainfilesorpartsoffilesthatmightbeevidenceofa crime orpolicyviolation.

In Microsoft file structures, sectors are grouped to form clusters, which are storage allocationunits of one or more sectors. Clusters are typically 512, 1024, 2048, 4096, or more bytes each.Combining sectors minimizes the overhead of writing or reading files to a disk. The

OS groupsoneormoresectorsintoacluster.Thenumberofsectorsinaclustervariesaccordingtothedisk

size. For example, a double-sided floppy disk has one sector per cluster; a hard disk has four ormoresectors percluster.

Clusters are numbered sequentially starting at 2 because the first sector of all disks contains asystem area, the boot record, and a file structure database. The OS assigns these cluster numbers,which are referred to as logical addresses. These addresses point to relative cluster positions; forexample,clusteraddress100is 98clustersfromclusteraddress

Sectornumbers,however,arereferredtoasphysical addressesbecausethey resideatthehardware or firmware level and go from address 0 (the first sector on the disk) to the last sectoron the disk. Clusters and their addresses are specific to a logical disk drive, which is a diskpartition.

DiskPartitions

Many hard disks are partitioned, or divided, into two or more sections. A partition is a logi-caldrive. For example, an 8 GB hard disk mightcontain four partitions or logical drives. FAT16does not recognize disks larger than 2 MB, so these disks have to be partitioned into smallersections for FAT to recognize the additional space. Someone who wants to hide data on a harddisk can create hidden partitions or voids—large unused gaps between partitions on a disk drive.For example, partitions containing unused space (voids) can be created between the primarypartitionandthefirstlogical partition.Thisunusedspacebetweenpartitionsis calledthepartition gap. If data is hidden in a partition gap, a disk editor utility could also be used to alterinformation in the disk's partition table. Doing so removes all references to the hidden partition,concealingitfromthecomputer'sOS.Anothertechniqueistohideincriminatingdigitaleviden ce at the end of a disk by declaring a smaller number of bytes than the actual drive size.Withdisk-editing tools,however,you canaccessthesehid-denoremptyareasofthe disk.

One way to examine a partition's physical level is to use a disk editor, such as Norton Disk-Edit,WinHex, or Hex Workshop. These tools enable you to view file headers and othercritical partsof a file. Both tasks involve analyzing the key hexadecimal codes the OS uses to identify andmaintain the file system. Table 5-1 lists the hexadecimal codes in a partition table and identifiessomecommonfilesystemstructures.

Hexadecimalcode	Filesystem
01	DOS12-bitFAT
04	DOS16-bitFATforpartitionssmallerthan32MB
05	Extendedpartition

06	DOS16-bitFATforpartitions largerthan32MB
07	NTFS
08	AIXbootablepartition
09	AIXdatapartition
0B	DOS32-bitFAT
0C	DOS32-bitFATforinterrupt13support
17	HiddenNTFS partition(XPandearlier)
1B	HiddenFAT32partition
1E	HiddenVFATpartition
3C	PartitionMagic recoverypartition
66–69	Novellpartitions
81	Linux
82	Linuxswap partition(canalsobeassociatedwithSolarispartitions)
83	Linuxnativefilesystems(Ext2,Ext3,Reiser,Xiafs)
86	FAT16volume/stripeset(WindowsNT)
87	HighPerformanceFileSystem(HPFS)fault-tolerantmirroredpartitionorNTFSvolume/stripeset
A5	FreeBSDandBSD/386
A6	OpenBSD
A9	NetBSD
C7	Typicalofacorrupted NTFS volume/stripeset
EB	BeOS

Table5-1Hexadecimalcodes inthepartitiontable

1. Ifnecessary,downloadHexWorkshopfromBreakPointSoftwareandinstallit.Checkwith yourinstructoraboutwhereyou shouldinstallit on yourcomputer.

2. InsertaUSBdriveintoaUSBport.
3. Start Hex Workshop by right-clicking the Hex Workshop desktop icon and clickingRun as administrator, andthen clicking the Continue button inthe UACmessagebox.
4. In Hex Workshop, click Disk, Open Drive from the menu to see a list of your logicaldrives.ClicktheC: drive(oryourworkingdrive),and clickOK.
5. Click Disk, Open Drive again, but this time, in the Open Drive drop-down list, clickyour USB drive, and then click OK. Compare the file system label for this drive to theoneyousawinStep 4.LeaveHexWorkshopopenforthenextactivity.

With tools such as Hex Workshop, you can also identify file headers to identify file types with orwithout an extension. Before performing the following steps in Hex Workshop, use WindowsExplorer or My Computer to find a folder on your system containing a bitmap (.bmp) file and afoldercontaininga Worddocument(.doc).Thenfollow thesesteps:

1. Toopenabitmapfileonyourcomputer,clickFile,OpenfromtheHexWorkshopmenu.Navigatetoafoldercontainingabitmap(.bmp)file,andthendouble-clickthe .bmpfile.(Ifyou'repromptedtoselectanybookmarks,clickCancelandcontinuewiththis activity.)
2. HexWorkshopwindowidentifiesthe file type forthegraphic.For.bmpfiles,itshows –BM6,‖-BM,‖or -BMF.‖Asshown in the figure, -42 4D‖isalso displayed to indicatea.bmpfile.
3. To open a Word document, click File, Open from the menu. Navigate to a foldercontaining a Word document (.doc) file, and then double-click the .doc file. As showninFigure6-6,thefirstlinecontainsarowof0sfollowedby-D0CF11E0A1B11A E1,‖ which identifies the file as a Microsoft Office document. The same file header isdisplayedforanExcelor aPowerPointfilebutdoesn'tapplytoAccessdatabases.
4. ExitHexWorkshop.

ExaminingNTFSDisks

New Technology File System (NTFS) was introduced when Microsoft created Windows NT andis theprimary filesystemforWindowsVista.Each generation of Windows sinceNThasincluded minor changes in NTFS configuration and features. The NTFS design was partiallybased on, and incorporated many features from, Microsoft's project for IBM with the OS/2operating system; in this OS, the file system was High Performance File System (HPFS). WhenMicrosoft created Windows NT, it provided backwardcompatibilitysothat NT could readOS/2 HPFS disk drives. Since the release of Windows 2000, this back- ward compatibility is nolongeravailable.

NTFS offers significant improvements over FAT file systems. It providesmore informationabout a file, including security features, file ownership, and other file attributes. With NTFS, youalsohavemorecontroloverfilesandfolders(directories) thanwithFATfilesystems.

In NTFS, everything written to the disk is considereda file. On an NTFS disk, the first datasetis the Partition Boot Sector, which starts at sector [0] of the disk and can expand to 16 sectors.Immediately after the Partition Boot Sector is the Master FileTable(MFT).The MFT, similarto FAT in earlier Microsoft OSs, is the first file on the disk. An MFT file is cre- ated at the sametime a disk partition is formatted as an NTFS volume and usually consumes about 12.5% of thedisk when it's created. As data is added, the MFT can expand to take up 50 % of the disk. Animportant advantage of NTFS over FAT is that it results in much less file slack space. Comparethe cluster sizes in Table 5-3 to Table 5-2, which showed FAT cluster sizes. Clusters are smallerforsmallerdiskdrives.ThisfeaturesavesmorespaceonalldisksusingNTFS.

Drivesize	Sectorspercluster	FAT16
0–32MB	1	512 bytes
33–64MB	2	1KB
65–128MB	4	2KB
129–255MB	8	4KB
256–511MB	16	8KB
512–1023MB	32	16KB
1024–2047MB	64	32KB
2048–4095MB	128	68KB

Table5-2Sectorsandbytes percluster

Drivesize	Sectorspercluster	Clustersize
0–512MB	1	512bytes
512 MB–1 GB	2	1024 bytes
1–2GB	4	2048 bytes
2–4GB	8	4096 bytes

4–8GB	16	8192 bytes
8–16GB	32	16,384bytes
16–32GB	64	32,768bytes
Morethan32GB	128	65,536bytes

Table5-3 Clustersizes inanNTFSdisk

NTFSSystemFiles

Because everything on an NTFS disk is a file, the first file, the MFT, contains information aboutall files on the disk, including the system files the OS uses. In the MFT, the first 15 records arereserved for system files. Records in the MFT arereferred toasmetadata.Table 6-4 lists thefirst16metadata recordsyoufindintheMFT.

Filename	Systemfile	Recordposition	Description
$Mft	MFT	0	BasefilerecordforeachfolderontheNTFSvolume;otherrecordpositionsintheMFTareallocatedifmore spaceisneeded.
$MftMirr	MFT2	1	The first four records of the MFT are saved in thisposition.If a single sector failsin the firstMFT,the records can be restored, allowing recovery ofthe MFT.
$LogFile	Logfile	2	PrevioustransactionsarestoredheretoallowrecoveryafterasystemfailureintheNTFSvolume.
$Volume	Volume	3	Informationspecifictothevolume,suchaslabelandversion,is storedhere.
$AttrDef	Attributedefinitions	4	Atablelistingattributenames,numbers,anddefinitions.
$	Root filename index	5	This istherootfolder ontheNTFS volume.
$Bitmap	Bootsector	6	AmapoftheNTFSvolumeshowingwhich

			clustersareinuseandwhichareavailable.
$Boot	Bootsector	7	UsedtomountheNTFSvolumeduringthebootstrap process; additional code is listed here ifit'sthebootdriveforthe system.
$BadClus	Badclusterfile	8	Forclustersthathaveunrecoverableerrors,anentr yofthecluster locationis madeinthis file.
$Secure	Securityfile	9	Uniquesecuritydescriptorsforthevolumearelisted in this file. It's where the access control list(ACL) is maintained for all files and folders on theNTFSvolume.
$Upcase	Upcasetable	10	Convertsalllowercasecharacterstouppercase UnicodecharactersfortheNTFS volume.
$Extend	NTFSextensionf ile	11	Optionalextensionsarelistedhere,suchasquotas,obje ctidentifiers,andreparse pointdata.
		12–15	Reservedfor futureuse.

Table5-2 MetadatarecordsintheMFT

MFTandFileAttributes

WhenMicrosoftintroducedNTFS,thewaytheOSstoresdataondiskschangedsignifi-

y.

IntheNTFSMFT,allfilesandfoldersarestoredinseparaterecordsof1024bytesea ch recordcontainsfileorfolderinformation.Thisinformationisdividedintorecordfieldscontaining metadata about the file or folder and the file's data or links to the file's data. Arecordfieldis referredtoas anattributeID.

File or folder information is typically stored in one of two ways in an MFT record: resident andnonresident. For very small files, about 512 bytes or less, all file metadata and data are stored inthe MFT record. These types of records are called resident files because all their information isstoredintheMFTrecord.

Fileslarger than 512 bytes are stored outside the MFT.The file orfolder's MFTrecord pro-vides cluster addresses where the file is stored on the drive's partition. Thesecluster addressesare referred to as data runs. This type of MFT record is called nonresident because the file's

dataisstoredinitsownseparatefileoutsidetheMFT.

MFTStructuresforFileData

When viewing an MFT record with a hexadecimal editor, such as WinHex, the data is displayedin little endian format, meaning it's read from right to left. For example, the hexadecimal value400 isdisplayedas 0004 0000,andthe number0x40000isdisplayedas00000400.

The first section of an MFT record is the header that defines the size and starting position of thefirst attribute. Following the header are the attributes that are specific for the file type, such as anapplication file or a data file. MFT records for directories and system files have additionalattributes that don't appear in a file MFT record. The following sections explain how data filesareconfiguredintheMFT.

MFTHeaderFields

FortheheaderofallMFTrecords,therecord fieldsofinterestareasfollows:

- *Atoffset0x00*—TheMFTrecordidentifierFILE;theletterFisatoffset0.
- *At offset 0x1C to 0x1F*—Size of the MFT record; the defaultis0x400 (1024)bytes,ortwosectors.
- *At offset 0x14*—Length of the header, which indicates where the next attribute starts;it'stypically0x38bytes.
- *Atoffset0x32and0x33*—Theupdatesequencearray,whichstoresthe2twobytesof the first sector of the MFT record. It's used only when MFT dataexceeds512bytes.Theupdatesequencearrayisusedasachecksumforrecordintegrityvalidation.

NTFSCompressedFiles

To improve data storage on disk drives, NTFS provides compression similar to FATDrive-Space 3, aWindows 98 compression utility. Under NTFS, files, folders, or entire volumescanbe compressed. With FAT16, you can compress only a volume. OnaWindows Vista,XP,2000, or NT system, compressed data is displayed normally when you view it in WindowsExplorerorapplications suchas MicrosoftWord.

During an investigation, typically you work from an image of a compressed disk, folder, or file.MostcomputerforensicstoolscanuncompressandanalyzecompressedWindowsdata,including data compressed with the Lempel-Ziv-Huffman (LZH) algorithm and in formats suchasPKZip,WinZip,andGNUgzip.Forensicstoolsmighthavedifficulty withthird-partycompression utilities, such as the RAR format. If you identify third-party compressed data, youneedtouncompressitwiththeutilitythatcreatedit.

NTFSEncryptingFileSystem(EFS)

WhenMicrosoftintroducedWindows2000,itaddedbuilt-inencryptiontoNTFScalledEncryptingFileSystem(EFS).EFSimplementsapublickeyandprivatekey methodofencrypting files, folders, or disk volumes (partitions). Only the owner or user who encrypted thedata can access encrypted files. The owner holds the private key, and the public key is held by acertificate authority,suchasaglobalregistry,networkserver,orcompanysuchasVeriSign.

When EFS is used in Windows Vista Business Edition or higher, XP Professional, or 2000, arecovery certificate isgeneratedandsenttothe local Windows administratoraccount. Thepurpose of the recovery certificate is to provide a mechanism for recoveringencrypted filesunder EFS if there's a problem with the user's original private key. The recovery key is stored inone of two places. When the user of a network workstation initiates EFS, the recovery key is sentto the local domain server's administrator account. If the workstation is standalone, the recoverykeyissenttotheworkstation'sadministratoraccount.

EFSRecoveryKeyAgent

TheRecoveryKeyAgentimplementstherecoverycertificate,whichisintheWindowsadministratoracc ount.Windowsadministratorscanrecoverakeyintwoways:throughWindows or from an MS-DOS command prompt. These three commands are available from theMS-DOScommandprompt:

- Cipher
- Copy
- Efsrecvr(usedtodecryptEFSfiles)

DeletingNTFSFiles

Typically, you use Windows Explorer to delete files from a disk. When a file is deleted inWindows NT and later, the OS renames it and moves it to the Recycle Bin. Another method isusing the Del (delete) MS-DOS command. This methoddoesn'trenameandmove the file totheRecycleBin,butiteliminatesthe filefromtheMFTlistinginthesamewayFATdoes.

When you delete a file in Windows Explorer, you can restore it from the Recycle Bin. The OStakesthe followingstepswhenyoudeleteafile ora folderinWindowsExplorer:

1. Windows changes the filename and moves the file to a subfolder with unique identity inthe RecycleBin.
2. Windows stores information about the original path and filename in the Info2 file, whichis the control file for the Recycle Bin. It contains ASCII data, Unicode data, and the

dateandtimeofdeletionforeachfileorfolder.

UnderstandingWholeDiskEncryption

In recent years, there has been more concern about loss of personal identity information (PII) andtrade secrets caused by computer theft. Company PII might consist of employees' full names,home addresses, and Social Security numbers.With this information, criminals could easilyapply for credit card accounts in these employees' names. Trade secrets are any information abusiness keeps confidential because it provides a competitive edge over other companies.
Theinadvertentpublicreleaseofthisinformationcoulddevastateabusiness'scompetitiveedge.

Of particular concern is the theft of laptop computers and other handheld devices, such as PDAs.If data on these devices isn't secured properly, the owners could be liable for any damagesincurred, such as stolen identities, credit card fraud, or loss of business caused by the release oftrade secrets to the competition. Because of the PII problem, many states have enacted lawsrequiring any person or business to notify potential victims of the loss as soon as possible. Tohelp prevent loss of information, software vendors, including Microsoft, now provide whole diskencryptionthisfeature createsnewchallengesinexamining and recovering datafromdrives.

Currentwholediskencryptiontoolsofferthefollowingfeaturesthatcomputerforensicsexaminersshoul dbeawareof:

- Prebootauthentication,such asasinglesign-on password,fingerprintscan,ortoken(USBdevice)
- Fullorpartialdiskencryptionwithsecurehibernation,suchasactivatingapassword-protectedscreensaver
- AdvancedencryptionalgorithMs,suchasAESandIDEA
- KeymanagementfunctionthatusesachallenGe-and-responsemethodtoresetpasswordsorpassphrases
- A TrustedPlatformModule(TPM)microchiptogenerate encryptionkeysandauthenticatelogins

ExaminingMicrosoftBitLocker

Microsoft'sutilityforprotectingdrivedataiscalledBitLocker,availableonlywithVistaEnterprise and Ultimate editions. BitLocker's current hardware and software requirements are asfollows:

- AcomputercapableofrunningWindowsVista

- TheTPMmicrochip,version1.2ornewer
- Acomputer BIOScompliantwithTrustedComputingGroup(TCG)
- TwoNTFSpartitionsfortheOSandanactivesystemvolumewith1.5GBavailablespace
- TheBIOSconfiguredsothattheharddrivebootsfirstbeforecheckingtheCD/DVDdrive orotherbootableperipherals

Windows Registry

When Microsoft created Windows 95, it consolidated initialization (.ini) files into the Registry,a database that stores hardware and software configuration information, network connections,user preferences (including usernames and passwords), and setup information. The Registry hasbeenupdatedandisstillusedinWindowsVista.

For investigative purposes,the Registry can contain valuable evidence.Toview the Registry,you can use the Regedit (Registry Editor) program for Windows 9x and Regedt32 for Windows2000,XP, and Vista.Formore information on how touseRegeditandRegedt32, see theMicrosoftWindowsResourceKitdocumentationfortheOS.

ExploringtheOrganizationoftheWindowsRegistry

The Windows Registry is organized in a specific way that has changed slightly with each newversion of Windows. However, the major Registry sections have been consistent, with someminorchanges,sinceWindows 2000;they'reslightly differentinWindows 9x/Me.Beforeproceeding,reviewthefollowinglistofRegistryterminology:

- *Registry*—Acollectionoffilescontainingsystemanduserinformation.
- *Registry Editor*—A Windows utility for viewing and modifying data in theRegistry.TherearetwoRegistryEditors:RegeditandRegedt32.
- *HKEY*—Windows splits the Registry into categories with the prefix HKEY_. Windows 9xsystems have six HKEY categories and Windows 2000 and later have five. Windowsprogrammersrefertothe-H‖asthehandleforthekey.
- *Key*—Each HKEY contains folders referred to as keys. Keys can contain other key foldersorvalues.
- *Sub key*—A key displayed under another key is a subkey, similar toa subfolderinWindowsExplorer.
- *Branch*—Akeyanditscontents, includingsubkeys,makeupabranchintheRegistry.

- *Value*—Anameandvalueinakey;it'ssimilar toafileanditsdatacontent.

- *Defaultvalue*—Allkeyshaveadefaultvaluethatmayormaynotcontaindata.
- *Hives*—Hives are specific branches in HKEY_USER and HKEY_LOCAL_MACHINE.HivebranchesinHKEY_LOCAL_MACHINE\SoftwareareSAM,Security,Components, and System. For HKEY_USER, each user account has its own hive link toNtuser.dat.

ExaminingtheWindowsRegistry

Some forensics tools, such as ProDiscover and FTK, have built-in Registry viewers. For this nextactivity, your company's Legal Department has asked you to search for any references to theSuperior Bicycles company and e-mail addresses containing the name Denise. A parale- gal tellsyouthehomepageforSuperiorBicycles(*www.superiorbicycles.biz*)andgivesyouaProDiscover .eve file containing the image of a Windows 98 computer belonging to a SuperiorBicycle employeenamedDeniseRobinson.

For this activity, you use ProDiscover Basic to extract System.dat and User.dat from the imagefile, and then use Access Data Registry Viewer to see what information you can find in thesefiles. If you find any items of interest, you copy the Registry path and name to a text file thatyou can give to the paralegal. Although the file is an image of a Windows 98 computer, you canuse Windows XP or Vista to run ProDiscover Basic and Access Data Registry Viewer in thefollowing activities. Registry Viewer can run in Windows 9x and later and analyze all WindowsRegistryversions.

ToextractRegistryfileswithProDiscover Basic,followthesesteps:

1. Start ProDiscover Basic with the Run as administrator option. If the Launch Dialog boxopens,clickCancel.
2. ClickFile, NewProjectfromthemenu.
3. In the New Project dialog box, type InChap06 in the Project Number text box and theProjectFileName textbox,andthenclickOK.
4. Inthetree viewofthemain window,clickto expandAdd andthenclickImageFile.
5. In the Open dialog box, navigate to your work folder, click the GCFI-Win98.eve imagefile, andclickOpen. ClickYes intheAutoImageChecksummessagebox,ifnecessary.
6. Click the Search toolbar button. In theSearch dialogbox, clickthe ContentSearchtab. Click the Search for files named option button, and in the Search text box, typesystem.dat and user.dat. Under Select the Disk(s)/Image(s) you want to search in, clickthe imagefile (seeFigure6-26),andthenclickOK.

7. In the search results, click the check box nextto theSYSTEM.DATfile.WhentheAdd Comment dialog box opens, type Registry files to extract, click the Apply to allitemscheckbox,andthenclickOK (seeFigure6-27).

8. Click the check box next to the USER.DAT file, and then click Tools, Copy SelectedFiles from the menu. In the Choose Destination dialog box, click Browse. In the Browsefor Folder dialog box, navigate to and click your work folder, and then click OK. ClickOKagaininthe ChooseDestinationdialogbox.

9. ExitProDiscoverBasic,savingtheprojectifprompted.

MicrosoftStartupTasks

Youshouldhaveagoodunderstandingofwhathappenstodiskdataatstartup.Insomeinvestigations, you must preserve data on the disk exactly as the suspect last used it. Any accessto a computer system after it was used for illicit purposes alters your disk evidence. As youlearned in Chapter 4, altering disk data lessens its evidentiary quality considerably. In someinstances, accessing a suspect computer incorrectly could make the digital evidence corrupt andlesscredibleforanylitigation.

Inthefollowingsections,youlearnwhatfilesareaccessedwhenWindowsstarts.Thisinformationhelpsy oudeterminewhenasuspect'scomputerwaslastaccessed,whichisparticularlyimportantwithcomputer sthatmighthavebeenusedafteranincidentwasreported.

StartupinWindowsNTandLater

Although Windows NT is much different from Windows 95 and 98, the startup method for theNT OSs—NT, 2000, XP, and Vista—is about the same. There are some minordifferences inhowcertainsystemstartfilesfunction,butbasically,theyaccomplishthesameorderlystartup.

AllNTFScomputersperformthefollowingstepswhenthecomputeristurnedon:

- Power-onselftest(POST)
- Initialstartup
- Bootloader
- Hardwaredetectionandconfiguration
- Kernelloading
- Userlogon

Windows OSs use the files discussed in the following sections to start. These files can be locatedonthesystempartitionorbootpartition.

Startup Files forWindows VistaWhenMicrosoftdevelopedVista,itupdatedthe bootprocess to use the new Extensible Firmware Interface (EFI) as well as the older BIOS sys- tem.The EFI boot firmware is designed to provide better protection against malware than BIOS does.EFIVista'sbootprocesseshavealsochangedsinceWindowsXP.TheNtldrprograminWindowsX PusedtoloadtheOShasbeenreplacedwiththesethreebootutilities:

- *Bootmgr.exe*—
  TheWindowsBootManagerprogramcontrolsbootflowandallowsbootingmultiple OSs,suchasbootingVistaalongwithXP.
- *Winload.exe*—
  TheWindowsVistaOSloaderinstallsthekernelandtheHardwareAbstractionLayer(H AL)andloadsmemorywiththenecessarybootdrivers.
- *Winresume.exe*—ThistoolrestartsVista aftertheOS goesintohibernation mode.

Startup Files for Windows XP unless otherwise specified, most startup files for Windows XP arelocated in the root folder of the system partition. The NT Loader(Ntldr) file loads the OS.When the system is powered on,Ntldr reads the Boot.ini file,which dis- plays aboot menu.After you select the mode to boot to, Boot.ini runs Ntoskrnl.exe and reads Bootvid.dll, Hal.dll,and startup device drivers. Boot.ini specifies the Windows XP path installation and containsoptionsforselectingtheWindowsversion.

IfasystemhasmultiplebootOSs,includingolderonessuchasWindows9xor DOS,Ntldr readsBootSect.dos(ahidden file),whichcontainsthe address(bootsectorlocation)ofeachOS.

When the boot selection is made, Ntldr runs NTDetect.com, a 16-bit real-mode program thatqueries the system for device and configuration data, and then passes its findings to Ntldr. Thisprogramidentifiescomponentsandvaluesonthecomputer system,suchasthefollowing:

- CMOStimeanddatevalue
- BusesattachedtothemotherboardsuchasIndustryStandardArchitecture(ISA)orPeripheralC omponentInterconnect(PCI)
- Disk drives connectedtothe system
- Mouseinputdevicesconnected tothesystem

ContaminationConcernswithWindowsXPWhenyoustartaWindowsXPNTFSworkstation, several files are accessed immediately. When any of these or other related OS filesare accessed at startup, the last access date and time stamp for the files change to the current dateandtime.ThischangedestroysanypotentialevidencethatshowswhenaWindowsXPworkstation was last used. For this reason, you should have a strong working knowledge of thestartupprocess.

Startup inWindows9x/Me

Like Windows XP, system files in Windows 9x/Me containing valuable information can bealtered easily during startup, which affects their evidentiary value and integrity. Windows9xOSs have similar boot processes. Windows Me is similar, too, with one importantexception:You can't boot to a true MS-DOS mode. When you're conducting a computing investigation,being able to boot to MS-DOS is preferred, especially ifyou're running a later version ofWindows 95 OEM SR2 (version 4.00.1111) or a newer oneinwhichthe MS-DOS bootmodecanreadandwritetoaFAT32disk.

Windows 9x OSs has two modes: DOS protected-mode interface (DPMI) and protected-modeGUI (serves the same purpose as Config.sys in MS-DOS). Many older computer forensics toolsuse DPMI mode and can't be run from a Windows command prompt window because they usecertaindiskaccesses thatconflictwiththe GUI.

The system files Windows 9x uses have their origin in MS-DOS. The Io.sys file communicatesbetween a computer's BIOS, the hardware, and the OS kernel. During the boot phase of aWindows 9x system, Io.sys monitors the keyboard for an F8 keystroke. If F8 is pressed duringstartup, Io.sys loads the Windows Startup menu, which has options such as booting to Windowsnormallyandrunning inSafemodetoperformmaintenance.

```
Windows 98 Startup Menu
1. Normal
2. Logged (\BOOTLOG.TXT)
3. Safe mode
4. Step-by-step confirmation
5. Command prompt only
6. Save mode command prompt only

Enter a choice: 1
```

MS-DOSStartupTasks

MS-DOS uses three files when starting, with the same names as in Windows 9x/Me: Io.sys,Msdos.sys, and Command.com. Two other files are then used to configure MS-DOS at startup:Config.sys and Autoexec.bat. Although MS-DOS and Windows 9x use some of the same startupfilenames,there aresomeimportantdifferencesbetweenthefilesintheseOSs.

Io.sys is the first file loaded after the ROM bootstrap loader finds the disk drive. Io.sys thenresidesinRAMandprovidesthebasicinputandoutput serviceforallMS-DOS functions.

Msdos.sys is the second program to load into RAM immediately after Io.sys. As mentioned, thisfile is the actual OS kernel, not a text file as in Windows 9x and Me. After Msdos.sys finishessettingupDOSservices,itlooksfortheConfig.sysfiletoconfiguredevicedriversandother

settings.Config.sysisatextfilecontaining commandsthattypicallyrunonlyatsystemstartuptoenhancethecomputer'sDOSconfiguration.

Msdos.sys then loads Command.com,which contains the sameinternal DOS commandsinWindows 9x. As the loading of Command.com nears completion, Msdos.sys looks for and loadsAutoexec.bat, a batch file containing customized settingsfor MS-DOSthat runs automatically.In this batch file,you can define the defaultpath and setenvironmental variables, such astemporary directories. MS-DOS then accesses and resets the last access dates and times on fileswhenpoweredup.

OtherDiskOperatingSystems

Years ago, other microcomputer OSs, such as Control Program for Microprocessors (CP/M),Digital Research Disk Operating System (DR-DOS), and Personal Computer Disk OperatingSystem (PC-DOS) were used. Of these OSs, only DR-DOS is still available. As mentioned inChapter 1, if you encounter an old computer running one of these OSs, you might need to callon your network of experts to research, explore, and test the OS. This section summarizes somefeaturesoftheseOSs.

In the 1970s, Digital Research created the first nonspecific microcomputer OS, CP/M, which hada unique file system. Computers using CP/M had 8-inch floppy drives and didn't support harddrives. The CPU was the Zilog Z-80, which could access up to 64KBRAM.Inthe early1980s, IBM supplied an expansion card with abuilt-inZ-80CPU thatalloweduserstoprocess applications availableforCP/M.

After Microsoft developed MS-DOS, Digital Research created DR-DOS in 1988 to compete withthat OS; it used FAT12 and FAT16 and had a richer command environment than MS-DOS. DR-DOS isnowsold primarilyasanembedded OSforout-of-the-boxROMorFlashROMsystems.

When IBM created the first PC using the Intel 8088 processor, it contracted with Microsoft, thenastartupcompany,tocreateanOS.In1981,Microsoftpurchased86-DOSfromSeattleComputing; it could run on the Intel 8088 16-bit processor and was a modification of CP/M.Microsoftsupplied 86-DOStoIBMforuse onits PCs,andIBM calleditPC-DOS.IBMmaintainedupgradestoPC-DOSuntilMicrosoftreleasedWindows95.

PC-DOS works much like MS-DOS, although its OS files are slightly different. For example,Io.sys is called Ibmio.sys, and Msdos.sys is called Ibmdos.sys. However, PC-DOS uses FAT12and FAT16,soaccessingdata isnodifferentfromworkingwithMS-DOS.

VirtualMachines

New versions of OSs and applications are released frequently, but older versions are still widelyused. As an investigator, you'll be faced with the challenge of having enough resourcestosupportthevariety of softwareyou'relikely toencounter.Morecompaniesareturningtovirtualization to reduce the cost of hardware purchases, so the number of investigations involvingvirtualmachines willincreaseas this practicecontinues.

As an investigator, you might need a virtual server to view legacy systems, and you mightneedto forensically examine suspects' virtual machines. Virtual machines enable you run another OSon an existing physical computer (known as the host computer) by emulating a computer'shardware environment VMware Servervirtual machine running Windows XP Professional onthe desktop of a host computer. Typically, a virtual machine consists of several files. The twomain files are the configuration file containing hard- ware settings, such as RAM,networkconfigurations, port settings, and so on, and the virtual hard disk file, which contains the bootloaderprogram,OSfiles,andusers'data files.

A virtual machine acts like any other file but with a twist:It performs all the tasks the OSrunning on the physical computer can, up to a certain point. The virtual machine recognizeshardware components of the host computer it's loaded on, such as the mouse, keyboard, andCD/DVD drive. However, the guest OS (the one running on a virtual machine) is limited by thehost computer's OS, which might block certain operations. For example, most virtual machinesrecognize a CD/DVD drive because the host computer defaults to auto-detect. Some virtualmachines don't recognize a USB drive; this capability varies with the virtualization software.Althoughnetworkingcapabilitiesarebeyondthescopeof thisbook,beawarethatvirtualmachines can use bridged, Network Address Translation (NAT), or other network configurationstodetermine howtheyaccesstheInternetand communicatewithsystems onthelocalnetwork.

Creating aVirtualMachine

Some common applications for creating virtual machines are VMware Server and VMwareWorkstation, Sun Microsystems Virtual Box, and Microsoft Virtual PC, although othersareavailable.VirtualBoxisanopen-sourceprogramthatcanbedownloadedat*www.virtualbox.org*.

Consult with your instructor before doing the following activity. You must download and installVirtual PC first, and you need an ISO image of an OS becauseno OSs areprovidedwithVirtualPC.Follow thesesteps tocreateavirtualmachine:

1. Ifyouhaven'talreadydoneso,installMicrosoftVirtualPC.
2. StartVirtual PC.InVirtual PC2007,theNewVirtual MachineWizardstartsautomatically.

(Ifitdoesn’t,clickFile,NewVirtualMachine Wizardfromthemenu.)

3. InthewelcomewindowoftheNewVirtualMachineWizard,click Next.
4. IntheOptionswindow,click theCreateavirtualmachineoptionbutton,andclickNext.

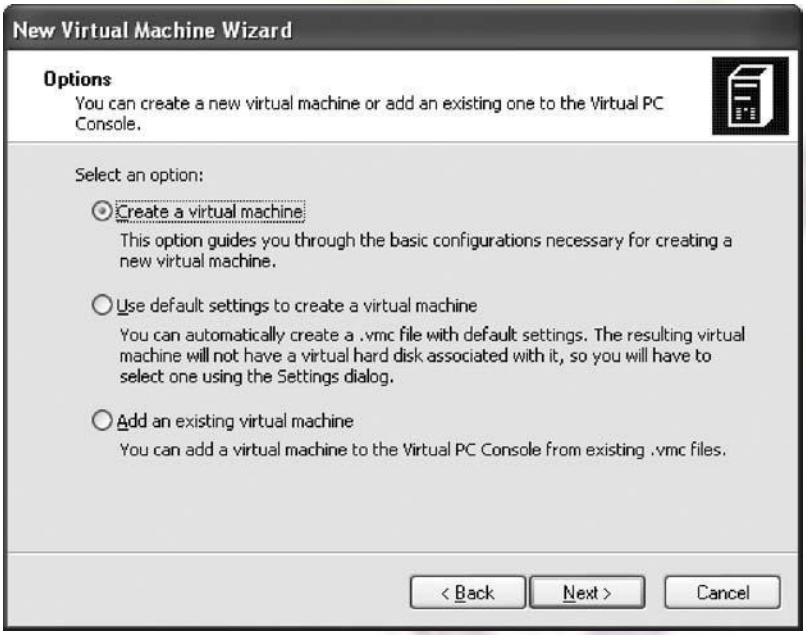


Fig:creatinganewvirtualmachine

5. In the Virtual Machine Name and Location window, type Windows Server 2003 for thevirtual machine name. Note that the default location for Vista is Documents\ VirtualMachines.Yourinstructormighttell youtouseadifferentlocation.ClickNext.
6. In the Operating System window,click WindowsServer 2003 in the Operating systemlistbox,andthenclickNext.
7. In the Memory window, you allocate the amount of RAM. You can increase the amountofRAM ifneeded, butfornow,leaveitattherecommendedlevel, and thenclickNext.
8. In the VirtualHard Disk Options window, click the A new virtual hard disk optionbutton,andthenclickNext.
9. In the Virtual Hard Disk Location window, accept the default location and then clickNext.
10. ClickFinish.

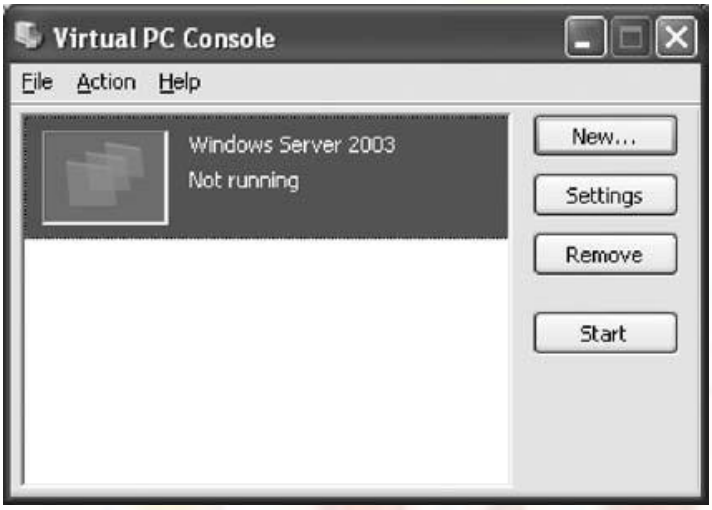


Fig:TheVirtualPCConsolewithavirtualmachineavailable

In the following activity, you use an ISO image that your instructor will provide on the net-workor a CD for installing a guest OS. For any guest OS, you must have a valid product key toinstallit.Youcangettheproductkeyfromyourinstructor.

1. In the Virtual PC Console,makesure the Windows Server 2003 virtual machineisselected,andthenclicktheStartbutton.
2. The Virtual PC user console opens, similar to the window you see when a physicalcomputerstarts,andVirtualPCexamines the hostcomputer'shardware.
3. This book assumes you know how to install an OS, sodetailedstepsaren't given.Virtual PCtreatsanISOimagethesameasaninstallationCD,sowhenyou'reprompted for the source disk, enter the location of the ISO image. For the name oftheowner,typeSallyFreidman,andfor thecompanyname,typeABCCorporation.
4. Create adomainnameofMainHost.
5. Createanadministratorpasswordand makeanoteofit.
6. After the OS is installed, log on. Note that pressing Ctrl+Alt+Delete activates the hostcomputer. To log on to the virtual machine, press right Alt+Delete. (You can also useAlt+Enterforfullscreen.)
7. You should be able to navigate through the contents of the Windows Server 2003 virtualserverasthoughitwereareal computer.Toswitch between thevirtual machinewindowandthe desktop,pressrightAltandmovethe cursor.
8. To exit Virtual PC, click File, Close from the menu, and then click Turn off in the drop-

downlist.