Počítačová forenzní analýza

Informatika a počítačová věda

Pojem počítačová věda je v české a v celé kontinentálně-evropské literatuře velmi často významově ztotožňován s pojmem informatika. Důkazem může být citát nizozemského informatika Edsgera Wybe Dijkstra „Computer science is no more about computers than astronomy is about telescopes.“ tedy „Informatika se nezabývá počítači o nic více než astronomie dalekohledy.“2 V anglicky mluvících zemích je však pojem computer science chápán jen jako součást obecné informatiky – informatics.

Informatika a její vztah k počítačové vědě

Obecná informatika je věda o informaci samotné, praktikách a postupech užívaných při zpracování informace a navrhování informačních systémů (samozřejmě ne nutně na počítačích). Informatika studuje strukturu, algoritmy, chování a interakce přirozených a umělých systémů, které ukládají, zpracovávají, zpřístupňují a přenášejí informace. Dále rozvíjí svůj vlastní pojmový a teoretický aparát a využívá základů, rozvinutých v jiných oborech. Také rozvíjí vlastní koncepční a teoretické základy a schémata ale využívá k tomu i poznatky z jiných oblastí. Od doby vynalezení počítačů začali jednotlivci i organizace masově zpracovávat digitálně. To vede k dnešní představě o tom, že informatika má nutně něco společného s počítači.

Dá se říci, že dříve byla hlavní náplní informatiky informační věda. Nicméně, co se týče ztotožňování těchto pojmů a rozdílů mezi nimi, liší se evropská a americká literatura a mnohdy dochází k velkým rozdílům v jejich chápání i v rámci jednotlivých zemí. S nástupem počítačů však začala přibývat další a další subodvětví, jež zastřešuje informatika. Mezi ně patří například teorie informací, počítačová věda, kognitivní věda, umělá inteligence, didaktika informatiky či osobní informační management a mnoho dalších.

Informatika (informatics)

- informační věda (information science)
- teorie informace (information theory)
- umělá inteligence (artificial intelligence)
- kognitivní věda (cognitive science)
- počítačová věda (computer science)
- didaktika informatiky (didactics of informatics)
- informační managment (personal information managment)

Teorie informace (anglicky information theory) je věda spojující aplikovanou matematiku a elektrotechniku za účelem kvantitativního vyjádření informace. Zabývá se převážně přenosem, kódováním a měřením informace. Otcem teorie informací je americký matematik a elektrotechnik Claude Elwood Shannon. K rozvoji tohoto oboru po druhé světové válce přispěli také R. A. Fischer a N. Wiener4. Informací jako měřitelnou veličinou, kdy se míra opírá o redukci na určitý počet alternativ, se zabývá český filozof J. Patočka ve své stati5. V modernějším pojetí se pak teorie informace zabývá také například bezeztrátovou (např. ZIP) či ztrátovou kompresí (např. MP3), kapacitou přenosového kanálu či datových médií apod.

Informační věda bývá, jak je zmíněno výše, někdy nesprávně ztotožňována s informatikou. Je však pouze její součástí. Přestože je jen podmnožinou obecné informatiky, jde o obsáhlou interdisciplinární vědu zahrnující i aspekty na první pohled více či méně vzdálených vědních oblastí s velkou rozmanitostí. Má blízký vztah ke knihovnictví, managementu, matematice či sociálním vědám. Informační věda se zaměřuje na porozumění problematiky z pohledu zainteresovaných stran a následnou aplikaci informací a dalších potřebných technologií. Jinými slovy, primárně se pouští do systematických problémů spíše než do jednotlivých částí technologií v systému. V tomto ohledu může být vnímána jako odpověď na technologický determinismus, víra v to, že technologie rozvíjí své vlastní zákony, realizuje

vlastní potenciál a je omezována pouze materiálními zdroji, které jsou k dispozici, a musí být proto vnímána jako autonomní systém kontrolující a prostupující všechny podsystémy společnosti.

V rámci informační vědy byla poslední dobou věnována pozornost interakci člověka a počítače (human computer interaction), softwaru pro skupinovou práci (groupware), sémantickému webu, apod. Informační věda by neměla být zaměňována s obory jako teorie informace, či s knihovnictvím – oborem věnujícím se knihovnám, nebo studiem konkrétních matematických konceptů informatiky, tedy s obory, které používají jen některé z principů informační vědy. Někteří autoři používají pojem informatika jako synonymum pro informační vědu, zejména ve vztahu ke konceptu rozvinutému A. I. Mikhailovem a ostatními sovětskými autory poloviny šedesátých let, kteří zastávali názor, že informatika je vědní disciplína příbuzná studiu vědecké informace (informatiky).

Vzhledem k rychle se rozvíjející interdisciplinární povaze informatiky je dnes obtížné vysvětlit a definovat přesný význam pojmu „informatika“. Regionální odlišnosti a mezinárodní terminologie tento problém ještě více komplikují. Mnoho autorů poukazuje na fakt, že většina toho, čemu dnes říkáme informatika, bylo kdysi nazýváno informační vědou. Přesto, když knihovníci začali používat slovní spojení informační věda ve vztahu ke své práci, pojem informatika se začal v USA objevovat jako odpověď počítačových vědců k odlišení jejich práce od knihovnické vědy, a ve Velké Británii jako termín pro vědu o informacích, která studuje přirozené i umělé nebo konstruované systémy, které zpracovávají informace.

Informační věda se zabývá principy porozumění jak sbírat, třídit, ukládat, obnovovat (znovu získávat) a šířit jakýkoliv typ informace a jak s nimi zacházet. Informační věda má souvislost s forenzním subodvětvím nazývaným inforamation forensics.

Počítačová věda

Počítačové věda je studiem teoretických základů informatiky a aplikací praktických metod pro jejich realizaci a uplatnění v počítačových systémech. Často je charakterizována jako systematické studium algoritmických procesů, které popisují a transformují informace. Základní otázkou počítačové vědy je „Co může být (efektivně) automatizované?“7Počítačová věda má řadu subodvětví, z nichž některá, jako je počítačová grafika, kladou důraz na konkrétní výsledky, zatímco jiné, jako například teorie složitosti, studují vlastnosti výpočetních problémů obecně. Další se zaměřují na problémy při provádění výpočtů. Například teorie programovacích jazyků studuje přístupy popisující výpočet, zatím co při programování se aplikují konkrétní programovací jazyky na řešení konkrétních výpočetních problémů. Interakce člověk-počítač (HCI) se zaměřuje na to, aby počítače a výpočty realizované pomocí nich byly užitečné, použitelné, a univerzálně přístupné lidem.

Široká veřejnost si občas plete počítačovou vědu se souvisejícími oblastmi aplikace, které se zabývají počítači (např. obecně informační technologie), nebo si myslí, že souvisí s jejich vlastní zkušeností s počítači, která zpravidla zahrnuje činnosti, jako je hraní her, prohlížení webu či kancelářské aplikace. Nicméně počítačové věda je zaměřena na pochopení vlastností programů a algoritmů používaných k implementaci softwaru, jako jsou ony hry či webové prohlížeče, a na základě tohoto porozumění pomoci při tvorbě nových programů či zlepšení stávajících.

Jde tedy o aplikaci poznatků z obecné informatiky a jejich rozšiřování pro implementaci na počítačích. Aplikací počítačové vědy jsou potom oblasti jako:

- Operační systémy
- Počítačové sítě
- Počítačová grafika
- Databáze
- Bezpečnost IT
- HCI (human computer interaction)

Jako vědní disciplína zahrnuje počítačová věda celou řadu témat od teoretické studie algoritmů až po praktické otázky implementace výpočetních systémů v oblasti hardwaru a softwaru.9 The Computer Sciences Accreditation Board (CSAB)10, které se skládá ze zástupců Association for Computing Machinery (ACM)11, Institute of Electrical

and Electronics Engineers Computer Society (IEEE)12 a Association for Information Systems(AIS)13 vymezuje čtyři oblasti, které považuje za zásadní:

- teorie výpočtu,
- algoritmy a datové struktury,
- programovací jazyky a metody,
- architektury počítačů.

Kromě těchto čtyř hlavních oblastí, CSAB také vymezuje oblasti, jako je softwarové inženýrství, umělá inteligence, počítačové sítě a komunikace, databázové systémy, paralelní výpočty, distribuované výpočty, interakce člověka a počítače, počítačová grafika, operační systémy, a numerické a symbolické výpočty jako důležité oblasti počítačové vědy. Toto rozdělení oblastí a podoblastí počítačové vědy pak vypadá asi takto:

Počítačová věda (computer science)

- Teorie výpočtu (Theory of computation)

o Vyčíslitelnost (Computability theory)

o Složitost (Computational complexity theory)

- Teoretická počítačová věda (Theoretical computer science)

o Matematická logika (Mathematical logic)

o Teorie automatů (Automata theory)

o Teorie čísel (Number theory)

o Teorie grafů (Graph theory)

o Teorie typů (Type theory)

o Teorie kategorií (Category theory)

o Geometrické algoritmy (Computational geometry)

o Teorie kvantového počítání (Quantum computing theory)

- Algoritmy a datové struktury (Programming methodology and languages)

o Analýza algoritmů (Analysis of algorithms)

o Vlastní algoritmy (Alrgorithms)

o Datové struktury (Data structures)

- Metodika programovací jazyků

o Kompilátory (Compilers)

o Programovací jazyky (Programming languages)

- Architektury počítačů

o Logické obvody (Digital logic)

o Mikroarchitektury (Microarchitecture)

o Paralelizace (Multiprocessing)

Historie počítačové vědy

Když pomineme teoretické základy formulované před stovkami let, sloužící mimo jiné počítačové vědě, jako například použití nuly indickým matematikem Grahmaguptou, či práce On the Calculation with Hindu Numerals a Algoritmi de numero Indorum perského matematika Al-Khwarizmiho, ve kterých bylo poprvé použito pojmu algoritmus (jako systematické aplikace aritmetiky v algebře), je možno datovat počátky opravdové počítačové vědy do doby, kdy Charles Babbage navrhl svůj Difference Engine následovaný návrhem plně programovatelného Analytical Engine (který je z dnešního pohledu výpočetní silou ekvivalentní Turingovu stroji – podle Church-Turingovi teze14) a Augusta Ada King, známá jako Ada Lovelace, pro něj navrhla způsob programování pomocí děrných štítků a zavedla pojmy jako podmíněný a nepodmíněný skok, tedy někdy do přelomu poloviny 19. století. Nicméně ještě ve dvacátých letech 20. století byly počítači (computers, někdy téže computors) úředníci, kteří většinou pod vedením fyziků prováděli výpočty. Mnoho tisíc počítačů bylo zaměstnáno v obchodu, státních institucích a výzkumných zařízeních. Většina z těchto počítačů byly ženy. Prováděly výpočty například pro astronomické kalendáře. Po roce 1920 je již výrazu výpočetní stroj používáno pro stroj, který provádí práce lidského počítače, a ještě později zejména pro ty, které fungují v souladu s metodami z Church-Turingovy teze.

Když si uvědomíme, že vývoj k dnešnímu stavu, kdy máme přístupný veškerý obsah internetu ze zařízení velikosti krabičky od cigaret na téměř jakémkoli obydleném místě na světě, kdy drtivá většina objemu všech celosvětových finančních transakcí probíhá elektronickou cestou, netrval ani sto let, musíme dát za pravdu citátu jednoho slavného fyzika:„Computer science is not as old as physics; it lags by a couple of hundred years. However, this does not mean that there is significantly less on the computer scientist's plate than on the physicist's: younger it may be, but it has had a far more intense upbringing!“ tedy „Informatika není tak stará jako fyzika, pár set let za ní zaostává. To však neznamená, že si informatici naložili menší sousto než fyzici: informatika může být mladší, ale její vývoj byl mnohem intenzivnější.

Z těchto charakteristik počítačové vědy je mimo jiné zřejmé, že computer forensics vychází z významového smyslu anglického computer science a nikoli ze smyslu českého překladu, často ztotožňovaného s obecnou informatikou. Využívá poznatky a teoretická východiska počítačové vědy v kombinaci s výbornou znalostí oblastí její aplikace a zároveň užívá postupy vědy forenzní. Další forenzní vědou, odlišnou od computer forensics, související spíše s informační vědou, případně dalšími obory obecné informatiky (například informačním managementem), než s počítačovou vědou je pak information forensics.

Forenzní věda

Forenzní vědy (anglicky forensic science, často zkracováno na forensics) jsou aplikací širokého spektra vědních oborů ke zodpovídání otázek, jež jsou v zájmu právního systému. A to jak ve vztahu k právu trestnímu, tak i občanskému, či k jiným odvětvím práva. Při oproštění se od původního významu, souvisejícího s právním systémem, je možné forenzní vědy chápat obecně jako vědy, které se za pomoci přijatých teoretických či vědeckých metodik a norem snaží určit, zda fakta týkající se událostí nebo předmětů, jsou v širší představě o ověření pravosti tím, za co jsou ve skutečnosti označovány, nebo se jen snaží tak vypadat.16 Forenzní věda:

- je aplikací věd ve věcech právních (velmi často trestních, ale také občansko právních a dalších),
- podává nestranné, spolehlivé a definitivní informace,
- pomáhá identifikovat osoby, věci a látky,
- podává důkaz o vzájemném kontaktu osob či věcí,
- kvantifikuje, odhaluje časovou posloupnost dějů.

Význam slova forenzní pochází z latinského adjektiva forensis – před fórem. V době Římského impéria znamenalo obvinění z trestného činu nutnost prezentace případu před skupinou osob na veřejném fóru. Jak osoba obviněná z trestného činu, tak žalobce, pronesli proslov, založený na jejich pohledu na událost. Jedinec s nejlepšími argumenty a jejich podáním rozhodl výsledek procesu. Jednoduše řečeno osoba s nejlepším forenzní dovedností vyhrála proces. Tento původ slova forenzní je příčinou dvou jeho poněkud odlišných moderních použití:

- jako formy přípustného důkazu,

• jako kategorie veřejné prezentaci.

Nás bude přirozeně zajímat forenzní ve smyslu důkazu přípustného před soudem. Pokud budeme mluvit o forenzně čistém důkazu (například obraz datového nosiče) půjde o kopii získanou takovým způsobem, aby data na ní obsažená byla možno použít jako přípustný důkazní materiál při soudním sporu. Zjednodušeně řečeno, pojmem forenzní obvykle označujeme postupy a vědy související s vyšetřováním a soudním dokazováním skutečností, nejčastěji, a však ne pouze, v trestních záležitostech.

Používání termínu „forensics“ na místo „forenzní věda“ může být považováno za nesprávné stejně jako používání termínu „forensic“ jako synonymum pro „právní“ nebo „vztahující se k soudu“. Tento termín je v současné době tak úzce spjat s vědeckou oblastí, že většina slovníků ztotožnila pojmy forensic a forensics science. Forenzní vědy jsou tedy vědy, které se aplikují při vyšetřování a dokazování trestných činů, při ověřování identity osob, pravosti listin, dokazování skutečnosti, že proběhla jistá komunikace a podobně. Souhrn těchto věd se někdy zkráceně označuje jako forenzika (z anglického forensics).

Historie

Nejstarší zmínka o aplikaci vědy, konkrétně fyziky, pro odhalení podvodu, pochází z legendy „Heuréka“ ze třetího století př. n. l., kde Archimédes ze Syrakus zjistil specifickou hmotnost údajně zlaté koruny ponořením do vody a dokázal, že není zlatá, aniž by ji poškodil.18 Arabský příběh ze sedmého století vypráví o kupci Soleimanovi, který nechal na dlužní úpis otisknout prst dlužníka a ten byl pak jednoduše rozpoznán. Jde tak o první případ daktyloskopie. Čínskou příručku vyšetřovatele napsal roku 1248 Song Ci. Vyšetřovatel případu vraždy srpem nechal přinést všechny srpy ve vesnici a na ten, ze kterého byla nedokonale setřena krev, se slétly mouchy přitahované její vůní. Kniha dále nabízí rady, jak rozlišit mezi utonutím (voda v plicích) a uškrcením (poškození chrupavek v krku) i další postupy zkoumání mrtvého těla vedoucí ke zjištění, zda byla smrt způsobena vraždou, sebevraždou nebo nehodou.19 Mezi průkopníky forenzních věd v Evropě patřil francouzský dvorní lékař a chirurg Ambroise Paré (1510–1590), koncem 18. století vyšlo i několik pojednání o forenzním a policejním lékařství. Mezníkem v dalším vývoji forenzních věd byl objev mikroskopu, daktyloskopie a identifikace osob a stop z místa činu pomocí analýzy DNA.

Dělení forenzních věd

Existuje velká spousta odvětví forenzní vědy. Je jasné, že podskupinu forenzní vědy může tvořit téměř jakákoli věda, jejíž subjekt je spíše konkrétní než abstraktní. Pokud připustíme dělení věd na praktické a teoretické, budou právě ty praktické vědy mít s velkou pravděpodobností svého forenzního potomka. Existuje tak například forenzní psychologie, computer forensic, či forenzní inženýrství, avšak forenzní filozofie, forenzní matematika, či forenzní teoretická fyzika příliš smyslu nedávají. Mezi nejznámější forenzní vědy patří:

• Fyziologické vědy

o Forenzní patologie

o Forenzní stomatologie

o Forenzní antropologie

o Forenzní entomologie

o Forenzní archeologie

• Společenské vědy

o Forenzní psychologie

o Forenzní psychiatrie

• Ostatní obory

o Daktyloskopie

o Forenzní analýzy účetnictví

o Balistika

o Analýzy vzorů krevních skvrn o Identifikace těl

o DNA profilování o Forenzní toxikologie

- Související obory

o Forenzní inženýrství

o Forenzní materiálové inženýrství

o Forenzní inženýrství polymerů

o Rekonstrukce dopravní nehody

- Kybertechnologie ve forenzních vědách

o Information forensics

o Computer forensics

Computer forensics

Computer forensics je tedy syntézou dvou výše zmíněných věd – počítačové vědy a forenzní vědy. Je oborem forenzní vědy, zabývající se zajišťováním přípustných důkazů vyskytujících se v počítačích a na digitálních paměťových médiích. Computer forensics je známá také jako digital forensics. Cílem computer forensics je vysvětlit současný stav digitální stopy (potencionálního důkazu). Digitální stopou může být počítačový systém, paměťové médium (jako je pevný disk nebo CD-ROM), elektronický dokument (např. e-mailové zprávy, SMS zprávy nebo JPEG obrázek) nebo dokonce prostá posloupnost paketů v komunikaci přes počítačovou síť. Většinou jde o objasnění jednoduchých otázek jako například „jaká informace je zde skryta?“ nebo „jaký sled událostí je odpovědný za současnou situaci?“ V oblasti computer forensics existují například odvětví:

- Firewall Forensics
- Database Forensics
- Mobile Device Forensics
- Network forensics

Existuje mnoho důvodů, proč využívat technik computer forensics:

V právních případech jsou techniky computer forensics často používány k analýze počítačových systémů patřících obviněným (v trestních věcech) nebo některé ze stran sporu (v občansko-právních věcech).

- V případě potřeby obnovy dat po selhání hardwaru nebo softwaru.
- Při analýzy počítačových systémů po průniku útočníka, například k určení toho, jakým způsobem útočník získal přístup a jaké napáchal škody.
- Při shromažďování důkazů proti zaměstnancům organizace, kteří odcházejí, případně mají být propuštěni.
- Při získávání informací o tom, jak počítačový systém funguje, pro účely ladění, optimalizace výkonnosti, nebo reverzního inženýrství.

Při provádění forenzního šetření by měla být přijata zvláštní opatření, obzvláště máli být výsledek šetření použit u soudu. Jedním z nejdůležitějších opatření je zajistit, aby důkazy byly shromážděny korektně a dodržovat, aby od okamžiku, kdy je důkaz sebrán, byla každá transakce důkazu mezi osobami zdokumentována, a že je prokazatelné, že nikdo jiný nemohl mít k němu přístup (nejlepší je samozřejmě držet počet transakcí s důkazem na co nejnižší úrovni). Poté stačí jen prokázat, že existuje jasná vazba mezi obviněným a získaným důkazem. Za účelem dosažení souladu s potřebou zachování integrity digitálních důkazů je třeba dodržovat tyto zásady:

• Žádná opatření přijatá orgány činnými v trestním řízení nebo jejich zástupci by neměla změnit údaje uložené na počítači či paměťových médiích, které mohou být následně dovolávány u soudu.

• Ve výjimečných případech, kdy se zjistí, že je nutné přistoupit k původním údajům uloženým v počítači nebo na datových médiích, je příslušná osoba povinna být k tomu oprávněna a musí být schopna vysvětlit význam a důsledky svého jednání. Měly by být vytvořeny a uchovány revizní záznamy nebo jiné záznamy o všech procesech použitých při zkoumání digitálního důkazu. Nezávislá třetí strana, by měla být schopna zkoumat tyto procesy a dosáhnout stejného výsledku.

• Osoba, která má na starost vyšetřování (vyšetřovatel) má celkovou odpovědnost za dodržování těchto zásad.

Terminologie computer forensics

K objasnění základních pojmů z této oblasti či pochopení jejich vzájemných vztahů a hlavně porozumění dalšímu textu je třeba si vymezit některé z nich a ukázat mezi nimi rozdíly i shody. Vzhledem k tomu, že se jedná o vědu relativně novou, nejsou některé pojmy zcela ustálené a v průběhu času se poněkud mění, případně se mění jejich význam. Už samotný pojem computer forensics (někdy téže digital forensics) bývá významově ztotožňován s některými dalšími pojmy, které však nejsou vždy zcela ekvivalentní. Také elegantní, vystižný a logický český překlad ve zkrácené formě neexistuje. Nabízí se snad jen ona počítačová forenzika, jejímuž používání bych se spíše bránil. Některé další nepřesné překlady jako forenzní analýza nebo též soudní analýza bývají definovány jako druh zkoumání počítačů a počítačových systémů patřících do skupiny forenzních věd, což jsou vědy používané k řešení právních otázek. Právní moc se snaží zjistit pravdu v soudní při, forenzní zkoumání se snaží odhalit také pravdu, ale poněkud odlišnými metodami.

někud odlišnými metodami. Forenzní počítačová analýza má za cíl zajišťovat a získávat počítačová data pro účely případných soudních sporů. Informace takto získané mohou být:

• důkazem spáchání trestného činu

• mohou potvrzovat nebo vyvracet porušení interních předpisů

Hlavním principem forenzní počítačové expertizy je průkaznost a opakovatelnost důkazů, tedy veškeré činnosti znalce musí směřovat k plně dokumentovaným postupům za účelem přezkoumání činností.

• Vyhodnocování a zpřístupňování dokumentace datového obsahu osobních počítačů, notebooků primárně s OS MS Windows, méně pak Linux nebo Mac OS.

• Dokumentace datového obsahu mobilních telefonů, komunikátorů, karet SIM a paměťových karet.

• Forenzní bezpečnostní audit se zaměřením na nalezení mechanizmu provedení a dokumentaci formy bezpečnostního incidentu.

Forenzní analýza bývá občas chápána jako jediná náplň soudního znalectví v oboru počítačů, nicméně většina zdrojů se významově přiklání spíše k tomu, že jde pouze o tu část celého forenzního procesu, která zkoumá data získaná sběrem v terénu, a tedy nezahrnuje vlastní získávání dat pro analýzu. Forenzní analýzou tedy dále rozumíme forenzní analýzu digitálních důkazů. Nejpřesněji vystihujícím, avšak neprakticky dlouhým překladem, je pravděpodobně soudní znalectví v oboru počítačů. V angličtině se zase krom výrazů computer forensics a digital forensics setkáváme třeba s forensics IT jako ekvivalentním pojmem, od jehož používání se již ale spíše upouští, případně také pojmem forensic analysis, který bývá chápán spíše jako podmnožina computer/digital forensics.

Vymezení dalších pojmů

Digitální stopa a digitální důkaz jsou dalším příkladem pojmů, které jsou chápány jinak v odborné literatuře české a anglické. V zahraniční, ale i v české literatuře existuje několik definic vymezujících již běžně vžitý termín digitální důkaz (digital evidence). V češtině se ještě setkáváme s pojmem digitální stopa, který může být chápán poněkud odlišně. Slovo „evidence“ má však v angličtině primární význam „důkaz“. České slovo „stopa“ v souvislosti s moderními technologiemi v zahraniční literatuře nenalezneme (můžeme se setkat s významem potential digital evidence, který má smysl blízký českému pojmu „stopa“). Příčina je jednoduchá a vychází z praxe – zahraniční teorie i

praxe jsou silně orientovány na výsledek trestního procesu, tj. stopa musí být soudem akceptovatelná, a proto ve vnímání a následném používání termínů dochází k automatickému ztotožňování pojmů stopa a důkaz (angl. evidence).

Digitální stopa je jakákoliv informace s výpovědní hodnotou uložená nebo přenášená v digitální podobě.

Tato definice je otevřená jakékoliv digitální technologii. Tímto způsobem definovaná digitální stopa pokrývá jak oblast počítačů a počítačové komunikace, tak i oblast digitálních přenosů (mobilní telefony, ale do budoucna i digitální TV apod.), videa, audia, digitální fotografie, data kamerových systémů, data elektronických zabezpečovacích systémů a jakýchkoliv dalších technologií potenciálně spojených s hi-tech kriminalitou. V původním návrhu se hovořilo o binární podobě uložené nebo přenášené informace. Slovo binární bylo následně změněno na digitální, protože tento pojem je obecnější (binární forma je podmnožinou obecnější digitální formy). Na rozdíl od jiných definic je definice obecná i v tom smyslu, že digitální stopu nespojuje nutně s trestným činem, což je, jak uvidíme dále, velmi důležité. Digitální stopa musí být využitelná nejenom pro silové resorty, kriminalistiku, ale i pro obecné forenzní šetření prováděné jak státními orgány (občanskoprávní spory, obchodní zákony apod.), tak i na komerční bázi, pro potřeby nezávislých interních či externích auditů apod.

Vyšetřovatel je každý, kdo vyšetřuje případy, ve kterých je potřebné pracovat s digitálními důkazy, nezávisle na tom, zda vyšetřování probíhá v rámci trestního řízení nebo na základě jiných (např. vnitrofiremních) podnětů.

Znalec bude výraz pro všechny odborníky, kteří se zkoumáním digitálních důkazů zabývají nezávisle na tom, zda jsou oficiálně zapsáni v seznamu znalců ministerstva spravedlnosti, zda to jsou policejní experti a nebo jiní odborníci, kteří tuto činnost vykonávají pouze „ad-hoc“ nebo v rámci své pracovní náplně nebo se s ní setkávají pouze příležitostně.

Forenzní laboratoř je pak specializované pracoviště pro provádění znaleckého zkoumání digitálních důkazů

Motivace vzniku a historie

Motivací pro vznik tohoto odvětví forenzních věd je již zmíněné masové rozšíření informačních technologií, jejich snadná dostupnost a použitelnost, a tím zneužívání k trestné činnosti i páchání přestupků vůči právu. Bezprostřední motivací však byl narůstající počet incidentů, jimž se nedaří předcházet, ale je nutné je dodatečně odhalovat, objasňovat a cíleně postihovat.

Incidenty a reakce na ně

Incident je jakákoli událost, jež mění plánovaný chod, funkci nebo význam systému. Každý takový průnik, ale automaticky nemusí znamenat narušení chodu systému. Metodologie reakce na incident bývá popisována následujícími kroky:

- Příprava na incident
- Detekce incidentu
- Počáteční reakce
- Formulace strategie reakce na incidenty
- Forenzní duplikace kritických dat
- Pátrání
- Implementace bezpečnostních opatření
- Monitorování sítě
- Obnova
- Protokolování
- Poučení

Jedná se o obecně platné principy, jejichž zcela striktní dodržování nemusí být vždy možné, například z důvodů finančních omezení.

Příprava na incident a detekce bývají velmi složité. Detekovat incident se většinou povede až po relativně dlouhém časovém úseku, protože útočník se snaží nechávat minimum stop za svým počínáním v systému, a ten tak nemusí jevit žádné vnější rozpoznatelné známky změněné funkčnosti. Usnadněním detekce může být příprava na incident. Toto počínání vede ke zvýšení pravděpodobnosti odhalení incidentu, kterému však nebylo možné předcházet. Jedná se v podstatě o kontrolní mechanismy funkčnosti systému. Každý, kdo je zodpovědný za bezpečnost systému, by měl počítat s tím, že ani při nejlepší snaze nedokáže všem potenciálním problémům preventivně zabránit a k incidentu přece jen dojde. Proto je potřeba věnovat čas nejen vlastnímu zabezpečení, ale také přípravě na případný incident. Takovým opatřením je vytvoření kontrolních součtů všech souborů pro budoucí přezkoumávání, dále je vhodné logovat co nejvíce událostí systému. Samozřejmostí je použití firewallů, application gateway opět včetně logování apod. Toto je však spíše úkolem tvorby bezpečnostní politiky organizace a nad rámec této práce.

Počáteční reakce na incident se odvíjí od jeho typu. Je možné jej ignorovat, zabránit jeho pokračování, či vyčkávat a získávat cenná data o útočníkovi vedoucí k jeho dopadení. Důvody zvoleného postupu se mohou různit případ od případu, nemusí být vždy cílem dostat útočníka před soud a potrestat ho. Organizace může například chránit své dobré jméno a bude se snažit, aby informace o incidentu nebyly zveřejněny.

Formulace strategie reakce na incidenty zahrnuje způsob chování následující po odhalení incidentu, vedoucí k nápravě škod při zachování maximálního objemu potencionálních důkazních materiálů. Jde tedy o rozhodnutí, zda systém odpojit od sítě, či nechat připojený, které služby nechat přístupné a které nikoli apod. Je potřeba zvážit dopad na uživatele a zároveň zohlednit vyšetření incidentu.

Forenzní duplikace kritických dat je již součástí forenzního procesu. V tomto kroku je velmi důležité se rozhodnout, zda bude pořízena forenzní kopie důkazních datových médií (typicky pevný disk), nebo budou důkazy zkoumány přímo. Bývá doporučováno provádět zkoumání na kopiích, avšak v praxi se ukazuje, že velmi často je vhodnější získat důkazy přímo. Než bude vytvářena forenzní kopie měla by být zkoumána a zohledněna dočasná data Zkoumaný systém by mělo zůstat po zaznamenání incidentu zapnutý. Vypnutím, či restartováním systému o tato data a o případné potencionální důkazy nenávratně přicházíme. Jde ovšem o práci na živém systému kdy je možné v pozici vyšetřovatele či experta potencionální důkazy velmi snadno znehodnotit a je tedy třeba velké obezřetnosti.

Pátrání je v podstatě analýzou získaných dat v prostředí forenzní laboratoře a druhou částí forenzního procesu.

Implementace bezpečnostních opatření jako úprava bezpečnostní politiky a její zavedení do praxe, **monitorování sítě** jako předcházení dalším, potencionálním incidentům, **obnova systému** do původního stavu, **protokolování** jako součást dokumentování sledu události po vzniku incidentu (nikoli jen tvorba reportu forenzního procesu) a **poučení** se ze situace pro příště již nesouvisí příliš úzce s oblastí computer forensics.

Nejen incidenty

Postupem času však přestala být oblast computer forensics jen něčím co reagovalo na rostoucí počet bezpečnostních incidentů. V dnešní době je využíváno služeb expertů z této oblasti pro získávání důkazů ve všech myslitelných případech. Nejde už pouze o soudní spory, ale i případy auditování v rámci organizace, či šetření probíhajících v rámci správních řízení.

Computer forensics vs. physical forensics

Existuje mnoho základních rozdílů mezi computer a ostatními "physical forensics" odvětvími forenzní vědy.30 Na nejvyšší úrovni jsou fyzické forenzní vědy zaměřené na identifikaci a individualizaci. Oba tyto procesy porovnávají předmět z místa činu s jinými látkami kvůli identifikaci třídy předmětu (tj. je červená tekutina ovocné šťáva nebo krev?) nebo zdroje předmětu (pochází tato krev od osoby X?). Na straně druhé computer forensics se zaměřuje na hledání důkazů a jejich analýzu. Proto jde spíše o vyšetřování než o forenzní proces.31 Někteří autoři dávají přednost výrazu digitální forenzní vyšetřování (digital forensic investigation) před digital forensics právě proto, že práce, která je spojena s digital forensics je mnohem více podobná práci vyšetřovatele na místě činu než práci forenzního znalce z jiné oblasti forezních věd a jejich aplikací.

Computer fornesics vs. information forensics

Information Forensics je věda, zabývající se šetřením systémových procesů, které produkují informace. Systémové procesy primárně využívají počítače a komunikační technologie k zachycení, zacházení, ukládání a přenosu dat. Manuální procesy doplňují systémy technologické na všech úrovních systémových procesů od správy komunikace až k zálohování informačních reportů. Technologické i manuální systémy, které jsou buď cíleně chráněny duševním vlastnictvím či vyvinuty zcela nezamýšleně, tvoří firemní informační systém. Komplexní firemní informační systémy jsou často náchylné k podvodům, zneužití, omylům a napadání.

Information forensic se zabývá povahou vzniku, fungování a vývojem IS podniku. Výzkum se především zaměřuje na kauzální faktory a procesy, které řídí životní cyklus implementace takovýchto systémů. Forenzní vyšetřování bývá zahájeno, když je systém podezřelý nebo oslabený. Obecně začíná vyšetřování tehdy, když systém či jeho součást selže. Vyšetřování se obvykle soustřeďuje na specificky problematické oblasti nebo komponenty systému. Spletitosti systému, náklady a zdroje, které jsou k dispozici, často znemožňují podrobné šetření celého IS. Přesto uskutečnění vědeckého posouzení faktů, když se objeví problém, není jen rozumné, ale přímo nezbytné pro soud.

Je tedy patrné, že se jedná spíše o forenzní zkoumaní toku informací, postupů jejich zpracování a zkoumání procesů probíhajících v organizacích. Spíše než využívání teoretických základů počítačové vědy a prostředků, které vzešly z její aplikace, jde o zhodnocování poznatků informační vědy, obecné informatiky a také informačního managementu. Je zde kladen menší důraz na znalost a používaní pokročilých technologií, větší na zkoumání procesů a znalosti managementu. Je tu také jistá podobnost a provázanost s auditorskou prací.

Forenzní proces

Forenzní proces je posloupnost úkonů, na jejichž vstupu je vytipovaný šetřený a na jeho konci důkazní materiál, který jej pomůže usvědčit u soudu. Forenzní proces je možné v první fázi dělit na práci v terénu a práci se získanými daty ve forenzní laboratoři. Jde a použití metod a postupů popsaných v následující kapitole (viz. 5) při šetření na místě i pozdější laboratorní analýze.

Práce v terénu

Práce v terénu je, něčím co práci experta v oblasti computer forensics odlišuje od práce mnohých ostatních, výhradně laboratorně zaměřených expertů z jiných oblastí (viz. 3.4). Jde o vyšetřování na místě, ze kterého byl veden nějaký útok a také na místě, na něž bylo útočeno v rámci incidentu, ve firemních i soukromých prostorách šetřených subjektů. Veškeré tyto postupy musí vždy probíhat v souladu s platnými právními předpisy. Vystává tak například problém, zda se bude řídit šetření právními předpisy země, kde je sídlo šetřené organizace, nebo předpisy země, ve které je fyzicky umístěno datové úložiště s šetřenými daty apod. Zkoumání těchto souvislostí je však opět nad rámec rozsahu diplomové práce.

Shromažďování digitálních důkazů

Digitální důkazy lze shromažďovat z mnoha zdrojů. Mezi nejběžnější zdroje patří počítače, mobilní telefony, digitální fotoaparáty, pevné disky, CD-ROM, USB paměťové zařízení, atd. Mezi méně běžné zdroje může patřit nastavení všemožných embedded systémů (drtivá většina spotřební elektroniky od herních konzolí, přes multimediální přehrávače po kuchyňské spotřebiče dnes obsahuje nějaký jednoúčelový systém), černá skříňka automobilů, RFID identifikátor (nálepky sloužící k identifikaci zboží v obchodech) nebo webové stránky.

Manipulaci s digitálními důkazy v počítačích je třeba věnovat zvláštní péči. Tak jak je na jednu stranu velmi jednoduché změnit většinu digitálních informací, tak může být velmi složité zjistit, že ke změně došlo, nebo vrátit data do původního stavu. Z tohoto důvodu je běžnou praxí co nejčastější a nejdůkladnější tvorba kryptografických hashí a kontrolních součtu důkazních souborů a jejich uchovávání mimo šetřené médium (například v notebooku vyšetřovatele). Takže je pak kdykoli v budoucnu možné prokázat, že nedošlo k žádným změnám důkazů. Jedná se o jeden ze základních principů práce vyšetřovatelů a forenzních expertů. Další velmi užitečné metody a praktiky uplatňující se ve forenzním procesu.

Live vs. dead analýza

V počátcích computer science bývala šetření prováděna výhradně na datech v klidu – typicky obsah pevného disku PC. To lze pokládat za mrtvou analýzu (dead nalysis – analýzu mrtvého systému). Vyšetřovatelé v minulosti vypínali systémy z obavy, že by mohly obsahovat digitální time-bomby, které mohou způsobit vymazání dat po určitém čase. Analýza takového vypnutého zabaveného systémů v klidu laboratoře navíc v méně složitých případech přinese maximální výsledek, co se týče objemu získaných informací.

V posledních letech se stále více klade důraz na analýzu živých systémů (live anlysis). Jedním z důvodů je, že mnoho současných útoků na počítačové systémy nenechá žádné stopy na pevném disku počítače – útočník pouze získává informace z paměti počítače. Dalším důvodem je rostoucí využívání ke skladování kryptografických klíčů. Může se stát, že jediná kopie klíčů k dešifrování uložených dat je uchována v paměti počítače. Vypnutí počítače v takovém případě způsobí, že informace budou ztraceny. Také dead analýza (občas bývá používán výraz off-line analýza) clusteru s několika desítkami jader a připojeným diskovým polem nepřipadá většinou v úvahu. Na druhou stranu je to již vcelku běžné vybavení středně velké organizace, se kterým je možné se velmi často setkávat. Live analýzu od dead analýzy odlišuje hlavně přítomnost nestálých dat a snaha o jejich získání.

Sběr nestálých dat

Mezi tato data patří hlavně obsah vyrovnávacích pamětí, obsah operační paměti a odkládacího souboru (zde je možné dostat s ve speciálních případech k datům i po vypnutí systému , výpis spuštěných procesů, či informace o aktivních síťových připojeních. Při analýze „živého“ systému je potřeba jej co nejméně modifikovat. Je tedy vhodné používat nástroje, které podávají informace, ale modifikují minimum dat.

Tvorba obrazů digitálních médií

Pokud to podmínky dovolují je možné, a pro pozdější analýzu v laboratoři dokonce nezbytné vytvořit forenzně čistý obraz dat uložených na digitálním médiu. Možnost tohoto úkonu souvisí jednak s objemem času, který má expert k dispozici – tvorba obrazu o velikosti desítek či stovek GB je časově poměrně náročná, ale také s tím, zda je za použití dostupných HW a SW prostředků vůbec možné takovou kopii vytvořit. V situaci kdy jsou tato data uložena například na redundantním diskovém poli SAN připojeném přes fiber channel rozhraní jde o úkol daleko náročnější (časově i použitými finančními prostředky) než pokud vytváříme obraz pevného disku obyčejného PC. Tento postup je používán proto, aby docházelo k co možná nejmenším změnám (v ideálním případě při použití write blockeru žádným) a tím případnému znehodnocení původního systému.

Dalšími důvody je fakt, že v laboratorních podmínkách mohou být dlouhodobějším zkoumáním objevena data, která by bylo možno na místě v časovém presu či při vyhrocenějších situacích přehlednout. Praktické zkušenosti zde ale ukazují, že velká část důkazů je nalezena přímo na místě a obrovské objemy dat předané do laboratoře jsou spíše kontraproduktivní. Dlouhý čas strávený jejich další analýzou nepřináší často kýžený výsledek a také mohou způsobovat další komplikace a zdržení, protože se může jednat osobní údaje šetřených, nesouvisející s případem, případne legal privilege (jakýsi závazek mlčenlivosti neumožňující nahlížet do komunikace šetřeného s jeho právníkem; v poslední době existuje dokonce tlak na to, aby se tato zásada aplikovala i na komunikaci s firemním právníkem35).

K takovýmto datům by neměl mít nikdo přístup a musí byt odfiltrována. K forenzní duplikaci digitálních médií se používá celá řada komerčních i nekomerčních softwarových i hardwarových nástrojů. Mezi nejvýznamnější patří produkty firmy Logicube36. Jedná se o propracované kity obsahující veškeré potřebné nástroje pro práci v terénu. Včetně systému pro kopírování pevných disků a vlastně jakýchkoli myslitelných datových nosičů, připojitelných přes všechna myslitelná rozhraní. Tato zařízení dovolují i takové věci jako vytvořit tištěné zprávy o zkopírovaných datech a to včetně souřadnic z GPS. Další význačným výrobcem systémů pro forenzní analýzu a kopírování dat je Acme Portable Machines37. Tato firma produkuje výkonné, ale přesto přenosné pracovní stanice. Veškerá hardwarová i softwarová zařízení musí používat postupů a technologií, které prokazatelně nemodifikují vytvořený obraz proti originálu. Jedná se tedy vždy o přesnou bitovou kopii.

Práce v laboratoři

Práce ve forenzní laboratoři zahrnuje převážně zkoumání digitální důkazů shromážděných v terénu. Jde o práci dosti časově náročnou a zdlouhavou. Ani za použití moderních nástrojů a výkonných serverů není možné analyzovat

stovky GB dat v řádu minut či jednotek hodin. Tato část procesu je velmi závislá na tom, jak relevantní data byla sebrána.

Analýza

Všechny digitální důkaz bývají analyzovány za účelem určení typu informací, které jsou na nich uloženy. Pro tento účel se používají speciální nástroje, které mohou zobrazovat informace ve formátu užitečné a čitelném pro vyšetřovatele a ne jen pro něj. Mezi nejznámější z nich patří

- AccessData FTK
- Guidance Software EnCase
- Brian Carrier's Sleuth Kit

První dva jsou heavy-weight aplikace s vysokými pořizovacími náklady zahrnujícími výkonný hardware. Třetí pak open source projekt, který je k dispozici zdarma. Výhoda drahých robustních aplikací je ta, že jsou relativně uživatelsky přívětivé a jejich obsluhu dokáže do jisté úrovně zvládnout i laik, který nepracuje primárně v oboru IT. Může jím být například case handler, či jiný právník řešící případ, nebo dokonce v jednom čase i jejich skupina. Pro práci se získanými a obnovenými daty pak není potřeba přílišné účasti technicky vzdělané obsluhy. Heavy-weight aplikace v sobě zakomponovávají i nástroje které jsou dostupné v rámci operačního systému a vytváří jednotné a přehledné rozhraní pro analýzu. Ve některých případech bývají k analýze specifických typů dat využívány i četné další nástroje. Typické forenzní analýza zahrnuje manuální přezkoumání materiálu dat na médiu, přezkoumání registru systému Windows, hledání a prolomení hesel, hledání klíčových slov souvisejících s případem, a exrahovaní e-mailů z datových souborů.

Tvorba reportu

Jakmile je analýza kompletní vyhotovuje se zpráva. Tato zpráva může být formou písemného dokumentu, či ústního svědectví, nebo kombinací obou.

Metody a postupy

Následující kapitola se bude zabývat postupy a nástroji, které výrazně usnadňují forenzní šetření na místě i analýzu sebraných dat. Rozdělení je zvoleno podle typu šetřených systémů. Jsou zde osvětleny principy fungování konkrétního systému s přihlédnutím k tématu a ukázáno kde a jakým způsobem bývají ukládána potencionálně zajímavá data. Mnoho mocných nástrojů je k dispozici přímo v konkrétních operačních systémech, avšak uživatelsky příjemnější a přehlednější bývá využití některých dalších, ať komerčních, či nekomerčních nástrojů. Největší prostor je věnován analýze systémům s OS Microsoft Windows. Stejně tak příklady analýzy sítí a komunikačních prostředků jsou zaměřeny na tyto operační systémy. Praxe ukazuje, že tyto systémy mají mezi šetřenými majoritní podíl a reflektují tak rozdělení trhu. Profesionální kyberzločinec sice zvolí sofistikovanější řešení, nicméně těchto případů není mnoho. Metody a postupy zde popsané tak najdou uplatnění daleko častěji.

Analýza Windowsových systémů

Tato část se bude zabývat forenzní analýzou systémů Windows. V dnešní době již v podstatě nemá cenu zabývat se systémy, které nejsou postaveny na technologii NT – tedy starší verze jako Windows 95, Windows 98 a Windows Millenium Edition. Ve většině případů se používají právě NT systémy jako desktopové Windows XP, Windows Vista či nové Windows Seven a serverové Windows 2000 Server, Windows 2003 Server a Windows 2008 Server. Většina postupů a nástrojů důležitých pro forenzní analýzu je shodná a použitelná pro všechny verze tohoto operačního systému.

Mezi tři základní pilíře kvalitní forenzní analýzy systému Windows patří:

- chápání principů souborových systému (hlavně NTFS),
- pochopení Windows artefaktů (většinou metasoubory vytvářené operačním systémem), včetně toho, jak je najít a interpretovat jejich vlastnosti,

- využití zdokumentovaného dostupného SW i HW vybavení.

Windows NT a vyšší (verze postavené na „New technology“) jsou značně odlišné od předchozích verzí operačních systémů společnosti Microsoft. Jednou z nejdůležitějších změn byl přechod z FAT na souborový systém NTFS.

FAT – File Allocation Table je názvem souborového systému a zároveň tabulkou alokace souborů, která popisuje přiřazení každého clusteru v oddílu (1 záznam odpovídá 1 clusteru). Obvykle existují 2 kopie (obě jsou uloženy bezprostředně za sebou) – ta druhá je použita v momentě, kdy se první stane nečitelnou. Přiřazení clusteru může nabývat různých specifických hodnot jako např. volný (0x0000), vadný (0xFFFE), cluster indikující konec souboru (0xFFFF) nebo obsahuje číslo následujícího clusteru souboru.

Jedná se sice o starší souborový systém, avšak pro svoji jednoduchost je stále velmi často používaný. Podporují jej OS MS-DOS, FreeDOS, OS/2, Linux, FreeBSD a BeOS.

Kvůli jednoduchosti a rozšíření je velmi často používán na výměnných médiích jako je disketa (zde se používá verze FAT12) nebo IOMEGA ZIP disk. Nejdůležitější však je, že se používá pro USB flash disky. K ukládání dat na optická média jako CD a DVD se však nepoužívá – zde je použit CDFS.

NTFS používá na rozdíl od FAT mnoho metadat. Pro NTFS je vše soubor, jak soubor tak složka. NTFS byl navržen jako nativní souborový systém pro Windows NT a (zejména oproti zastaralému souborovému sytému FAT) obsahuje spoustu novinek:

- Žurnálování – všechny zápisy na disk se zároveň zaznamenávají do speciálního souboru, tzv. žurnálu. Pokud uprostřed zápisu systém havaruje, je následně možné podle záznamů všechny rozpracované operace dokončit nebo anulovat a tím systém souborů opět uvést do konzistentního stavu.
- Access control list – podpora pro přidělování práv k souborům.
- Kompresi na úrovni souborového systému.
- Šifrování (EFS – Encrypting File System) umožňuje chránit data uživatele na úrovni souborového systému a je transparentní.
- Diskové kvóty umožňují nastavit pro konkrétního uživatele maximálně využitelné místo na diskovém oddíle. Do diskové kvóty se nezapočítávají komprimované soubory, ale jejich reálná velikost.
- Dlouhá jména souborů (ve FAT původně nebyla a ve Windows 95 je bylo třeba doplňovat značně komplikovaným způsobem).
- Pevné a symbolické linky – odkazy na soubory na úrovni filesystémů, známé z operačních systému UNIX. Windows pro editaci tohoto typu odkazů nemají standardní uživatelské rozhraní, ale umí je interpretovat a také

(Distribuovaný systém souborů na Windows server 2003 apod.). NTFS je flexibilní – všechny jeho soubory (včetně speciálních, s výjimkou boot sektoru) se dají přesunout. K indexování souborů se zde používá B+ stromů. FAT používá 8bit ASCII/ANSI. Naproti tomu NTFS používá Unicode kódování. Pro soubor pojmenovaný Document.doc pak vypadá

ASCII reprezentace:

44 6F 63 75 6D 65 6E 74 2E 64 6F 63

Unicode reprezentace:

0044 006F 0063 0075 006D 0065 006E 0074 002E 0064 006F 0063

Vzhledem k tomu, že systémy Intel jsou little endian, byty každého Unicode znaku se zobrazí při prohlížení v hexadecimálním editoru reverzně. Tak se bude 006B zobrazovat jako 6B00 v hexadecimální zobrazení. Naštěstí Windows NT má mnoho vlastností zděděných z předchozích verzí Windows. Je stále možné obnovovat smazaná data, která nebyla přepsána, odkládací soubor i volné místo stále obsahují užitečná data a registry a koš jsou stále bohatými zdroji informací. Navíc Windows NT a novější udržují mnohem více informací o systému a uživatelských akcích než předchozí verze Windows (logy apod.).

Časová razítka – MAC times

Windows zaznamenávají časová razítka (time stamps), tedy datum a čas vytvoření souboru (Created), poslední modifikace (Modified) a také datum a čas, kdy byl soubor naposledy zpřístupněn (Accessed). U data a času vytvoření je třeba mít na paměti, že jde o datum a čas vytvoření na aktuálním svazku. Při přesunu v rámci svazku se nemění, avšak při přesunu mezi svazky ano. Datum a čas posledního zpřístupnění souboru jsou pak měněny v závislosti na aplikaci. Některé aplikace změnu provádí, některé ne. Pro výpis MAC časů slouží v systémech Windows příkaz dir s přepínači Vytvoření (Created)

dir /tc

Poslední modifikace (Modified)

dir /tw

Posední zpřístupnění (Accessed)

dir /ta

Prošetření MAC časů souborů může poskytnout dobrou představu o historii souborů na počítači a o rozsahu povědomí uživatele o souborech, jejich existenci a obsahu. Využití nástrojů pro seřazení těchto časových razítek může být velmi užitečné pro vytváření časových os, čímž je možné získat mnohem lepší náhled na aktivity uživatele v systému. Tato data mohou být mnohem smysluplnější v kombinaci s informací o době smazání souboru.

```
F:\Case>dir /tc
Svazek v jednotce F je hda0.
Sériové číslo svazku je 8020-F610.
Výpis adresáře F:\Case
02.05.2009 23:20 .
02.05.2009 23:20 ..
02.05.2009 23:22       1 287 712 Animation.gif
02.05.2009 23:23         794 624 Audio.mp3
02.05.2009 23:23          33 792 Document.doc
02.05.2009 23:22         134 675 Index.htm
02.05.2009 23:22         592 709 Picture.jpg
02.05.2009 23:25       1 445 068 Video.avi
02.05.2009 23:22         189 247 Video.swf
               7 souborů,      4 477 827 bajtů
                     Adresářů: 2, Volných bajtů: 36 544 294 912


F:\Case>dir /ta
Svazek v jednotce F je hda0.
Sériové číslo svazku je 8020-F610.

Výpis adresáře F:\Case

02.05.2009 23:26 .
02.05.2009 23:26 ..
02.05.2009 23:22       1 287 712 Animation.gif
02.05.2009 23:23         794 624 Audio.mp3
02.05.2009 23:23          33 792 Document.doc
02.05.2009 23:22         134 675 Index.htm
02.05.2009 23:22         592 709 Picture.jpg
02.05.2009 23:25       1 445 068 Video.avi
02.05.2009 23:22         189 247 Video.swf
               7 souborů,      4 477 827 bajtů
```

Adresářů: 2, Volných bajtů: 36 544 294 912

F:\Case>dir /tw
Svazek v jednotce F je hda0.
Sériové číslo svazku je 8020-F610.

Výpis adresáře F:\Case
02.05.2009 23:25 .
02.05.2009 23:25 ..
02.05.2009 11:29 1 287 712 Animation.gif
15.12.2008 01:33 794 624 Audio.mp3
30.04.2009 00:46 33 792 Document.doc
02.05.2009 22:57 134 675 Index.htm
02.05.2009 12:33 592 709 Picture.jpg
02.05.2009 23:25 1 445 068 Video.avi
02.05.2009 10:51 189 247 Video.swf
7 souborů, 4 477 827 bajtů
Adresářů: 2, Volných bajtů: 36 544 294 912

Možnosti obnovení smazaných souborů

K pochopení toho, jak mohou být na NTFS smazané soubory obnoveny, je nutné porozumět několik aspektů NTFS. NTFS používá 64bitové adresy clusterů, takže diskový oddíl může být větší než u FAT (která ve své poslední verzi používala efektivně 28bitové adresování) a to konkrétně až 16 EB. Celý systém je řešen jako obří databáze, jejíž jeden záznam odpovídá souboru. Základ tvoří 12 systémových souborů, tzv. metadat, které vznikají bezprostředně po naformátování svazku.

Tabulka 1 – NTFS metadata

Číslo záznamu	**Jméno**	**Popis**
1	$MFT	(Master File Table) – tabulka obsahující záznamy o všech souborech, adresářích a metadatech (jelikož $MFT je soubor, je i informace o něm v této tabulce); Nachází se hned za boot sektorem; jelikož se jedná o soubor, lze jej teoreticky fragmentovat (prakticky je tomu zamezeno), avšak aby se tomu předešlo, systém kolem něj udržuje zónu volného místa
2	$MFTMIRR	soubor, zajišťující bezpečnost dat; nachází se uprostřed disku, obsahuje prvních 16 záznamů $MFT; pokud je $MFT z nějakédo důvodu poškozená, použije se tato kopie
3	$LOGFILE	žurnálování – File system transactions
4	$VOLUME	obsahuje informace o svazku, tj. identifikátor svazku, název svazku, verze souborového systému apod.
5	$ATTRDEF	tabulka MFT atributů která asociuje numerické atributy se jmény kořenový adresář disku
6	$BITMAP	jednorozměrné pole bitů, které slouží ke sledování volného místa, když je bit 0, je volný a v opačném případě použitý
7	$BOOT	je vždy v prvním clusteru svazku a obsahuje bootloader (NTLDR či BOOTMGR)
8	$BADCLUS	drží seznam známých vadných clusterů, které znovu nebudou použity; pokud nastane chyba při čtení dat, systém označí clustery za špatné a $Badclus se aktualizuje
9	$SECURE	obsahuje Access control list
10	$UPCASE	obsahuje tabulku Unicode znaků zajišťující case sensitivity
11	$EXTEND	rozšíření souborového systému – kvóty apod.

$MFT jeden ze souborů, které jsou vytvořeny při formátování NTFS svazku, obsahuje MFT záznam pro každý soubor na svazku a jejich rezidentní a nerezidentní atributy. $BITMAP, další ze souborů, které jsou vytvořeny při formátování NTFS svazku, eviduje využití clusterů v NTFS. Využívá jeden bit k zaznamenávání stavu každého clusteru na svazku. Pokud je cluster na NTFS svazku používán, je odpovídající bit v souboru $BITMAP změněn na 1. Když je cluster k dispozici, odpovídající bit je změněn na 0. Pro alokování souboru na svazku musí být tedy splněno následující:

- $BITMAP soubor je upraven tak, aby zohlednil skutečnost, že používané clustery jsou alokovány,
- je vytvořen alokovaný MFT záznam pro soubor,
- je vytvořen záznam indexu pro název souboru v mateřské složce MFT záznamu,
- cluster rozsahu je vytvořen v souboru MFT záznamu pokud je nerezidentní.

Když je soubor smazán, jsou záznamy o clusterech, které využíval v souboru $BITMAP změněny na nulu. MFT záznam pro tento soubor je označen pro smazání a jeho index je smazán. Pokud je záznam zrušen, záznamy níže jsou přesunuty nahoru, čímž se zruší původní záznam. Jediný případ, kdy záznam zůstane viditelný po smazání, nastane tehdy, když jde o poslední položku v seznamu. V takovém případě je soubor smazán, ale data jsou stále na disku a jeho MFT záznam stále existuje. Pokud lze nalézt MFT záznam, je možné obnovit rezidentní atributy souborů včetně jména a časových razítek. Za předpokladu, že nejsou přepsány, je možno obnovit i nerezidentní atributy.

Při vytváření MFT záznamu NTFS přepisuje smazané MFT záznamy před tím než vytvoří nové. Proto s prodlužováním času uplynulého od smazání po obnovení výrazně klesá pravděpodobnost plného obnovení (včetně jména souboru a všech metadat) souboru. Nicméně i údaje, týkající se starších (dříve smazaných) souborů, mohou být ještě nalezeny v nepřiděleném místě. MFT záznamy jsou přepisovány daleko rychleji než volné místo (nealokované clustery), tedy nerezidentní atributy mohou zůstat na disku ještě velmi dlouho. Stejně tak jako vlastní obsah souborů. Těchto vlastností souborového systému NTFS lze úspěšně využívat při sběru dat a tyto pak využít znalcem při analýze ve forenzní laboratoři. Takto získaná data mohou dále posloužit jako digitální důkaz.

Koš

Pochopení, jak funguje Koš (Recycle Bin), je pro forenzní znalce kriticky důležité. Typický systém obsahuje velké množství důležitých dat přesunutých do koše a roztroušených po celém disku. Znalec může často určit, kdy uživatel mazal jednotlivé soubory, četnost operací mazání, či další důležitá metadata, a to i v případě, že tyto soubory byly zcela odstraněny – koš byl vyprázdněn. Koš je skrytá systémová složka systému Windows, pro kterou platí mírně odlišná pravidla než pro ostatní složky. Je vytvořena na každém svazku. Soubory odstraněné do koše se nachází v

.\Recycler

Když uživatel nebo aplikace smaže soubor, je jeho záznam v původní složce smazán a vytvořen nový ve složce koše. Krom toho jsou přidány informace o smazaném souboru do souboru INFO (nebo INFO2). Přestože systém Windows neuchovává datum a čas smazání souboru, je tato informace zaznamenána při přesunu souboru do koše právě v souboru INFO. V tomto souboru je uchováno krom informace o datu a čase smazání také umístění souboru a jeho jméno. Soubory jsou po přesunutí do koše přejmenovány do formátu D[písmeno svazku][číslo indexu].[originální přípona], tedy například soubor smlouva.doc původně uložená na svazku D: přesunutá do prázdného koše je v něm přejmenována na Dd0.doc. Indexy určují pořadí přesunu souborů do koše. Po vysypání koše se čítač nuluje, původní INFO soubor je smazán a je vytvořen nový. Platí pro něj všechna pravidla obnovitelnosti jako pro jiné soubory (viz. 5.1.2). Mnohdy může být velmi cenný i fragment tohoto souboru. Důležitým faktem je, že soubory mazané operačním systémem nejsou přesouvány do koše a zaznamenávány do INFO souboru. Je tedy průkazné, že soubory, které se nacházejí v koši, mazal uživatel, a že se tedy jedná o projev jeho vůle.

Registry

Registry jsou databází, do které si Windows ukládají všechna svá nastavení. V registrech najdeme nastavení týkající se veškerého používaného hardwaru a softwaru, dále pak nastavení týkající se vzhledu plochy, konkrétních uživatelů atd. Jakmile uživatel provede jakoukoliv změnu v systému prostřednictvím Ovládacích panelů, změnu v asociování

souborů, systémových politikách nebo v instalovaném softwaru, promítnou se všechny změny do registrů. Windows registry mají tedy pro chod systému zcela zásadní význam.

Registry jsou jako databáze fyzicky uloženy na pevném disku v několika souborech. Z těchto souborů se jejich obsah načítá při startu operačního systému do paměti. Drtivá většina těchto souborů je uložena v

%SYSTEMROOT%\system32\config\

Jen soubory Ntuser.dat a UsrClass.dat jsou uloženy v

%SYSTEMDRIVE%\Documents and Settings\%USERNAME%\

tedy

%USERPROFILE%

Registry se dělí na sedm „podregistrů" – registry hives. Jde o logickou skupinu klíčů, podklíčů a hodnot v registru mající řadu podpůrných souborů obsahujících i zálohu dat.

Tabulka 2 – přípony souborů registrů

Přípona	**Popis**
žádná	kompletní data
.alt	záloha kritického podregistru HKEY_LOCAL_MACHINE\System; pouze klíč System má .alt soubor
.log	transakční log změn klíčů a hodnot
.sav	Kopie dat pro případ, že by nastala neočekávaná chyba při užití editoru

Pokaždé, když se přihlásí k počítači nový uživatel, je pro něj vytvořen nový registry hive v souboru v příslušném profilu. Tento obsahuje konkrétní informace týkající se živatele, nastavení aplikací, desktopu, prostředí, síťových připojení a tiskárny. Tento registry hive je umístěn pod klíčem HKEY_USERS.

Nejen běžní uživatelé, ale i LocalService a NetworService mají svůj registry hive, který je opět uložen v

%SYSTEMDRIVE%\Documents and Settings\%USERNAME%\

Tabulka 3 – soubory registrů

Registry hive	**Soubory**
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav
HKEY_CURRENT_USER	Ntuser.dat, Ntuser.dat.log
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav H
KEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_USERS\.DEFAULT Default,	Default.log, Default.sav

Ve forenzním procesu mohou být zajímavé obzvláště některé větve registrů

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

MRU je zkratka pro most-recently-used. Tento klíč uchovává seznam nedávno otevřených nebo uložených souborů pomocí klasických dialogových oken průzkumníku (např. dialogové okno Uložit). Soubory, které jsou uloženy pomocí webového prohlížeče (včetně IE a Firefoxu) jsou zachovány. Avšak dokumenty, které jsou otevřeny nebo uloženy pomocí aplikace Microsoft Office zachovány nejsou

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU

Tento klíč rozšiřuje OpenSaveMRU klíč a poskytuje další informace. Pokud je přidána nová položka do klíče OpenSaveMRU, je vytvořena nebo aktualizována hodnota registru v tomto klíči. Každá binární hodnota registru tohoto klíče obsahuje nedávno použitý program, jeho spustitelný soubor, složku, cestu k souboru, na které byl program použit k otevření či uložení.

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Tento klíč také udržuje seznam naposledy otevřených souborů. Odpovídá %USERPROFILE%\Recent (Start>Poslední dokumenty). Obsahuje seznam souborů na lokálním stroji nebo síti, které byly nedávno otevřeny. Uložena jsou pouze jména souborů a cesta.

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Obsahuje seznam aplikací a příkazů spouštěných pomocí Start>Spustit... MRUList pak obsahuje záznam pořadí, ve kterém byly naposledy spouštěny.

HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Memory Management

Obsahuje informace o stránkovacím souboru Windows, jeho umístění, velikosti a chování. Stránkovací soubor (obvykle %systemdrive%\pagefile.sys) může obsahovat důkazní informace, které by mohly být odstraněny, jakmile je šetřený počítač vypnut. Tento klíč registru obsahuje hodnotu s názvem ClearPagefileAtShutdown, která určuje, zda by měly Windows vymazat obsah stránkovacího souboru v případě, že je počítač vypnut. Ve výchozím nastavení systému Windows není nastaveno vymazání obsahu stránkovacího souboru. Nicméně šetřený může změnit tuto hodnotu registru na 1 a tím vynutit smazání obsahu stránkovacího souboru. Forenzní vyšetřovatel by měl ověřit tuto hodnotu před vypnutím počítače šetřeného během procesu shromažďování důkazů.

HKCU\Software\Microsoft\Search Assistant\ACMru

Obsahuje poslední výrazy hledané pomocí výchozího vyhledávače. Podklíč 5603 obsahuje klíčová slova pro nalezení složky či souboru, zatímco podklíč 5604 obsahuje hledané výrazy pro hledání slov nebo fráze v souboru.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

Každý podklíč v tomto klíči představuje nainstalovaný program v počítači. Všechny programy, kterou jsou uvedeny v Ovládací panely>Přidat nebo odebrat programy odpovídají jednomu z uvedených podklíčů. Jsou však i další nainstalované programy (například ovladač zařízení, aktualizace), které nejsou uvedeny v Přidat nebo odebrat programy. Každý podklíč obvykle obsahuje mimo jiné i hodnoty registru – DisplayName (název programu) a UninstallString (instalátor a cesta k němu). Může obsahovat i další užitečné informace, například o času instalace či použité verzi.

HKLM\SYSTEM\MountedDevices

Obsahuje seznam všech namontovaných svazků, kterým je přiřazené písmeno jednotky, včetně zařízení USB a externí DVD/CD-ROM mechaniky.

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume

Z hodnot zde uvedených je možné zjistit informace o konkrétním namontovaném zařízení. Například v případě, že hodnoty obsahují Storage#RemoveableMedia, znamená, že jde o USB vyměnitelný disk, který byl připojen do systému. LastWrite zase obsahuje informace o čase posledního připojení.

HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR

Tento klíč obsahuje informace o namontovaných USB paměťových zařízeních, včetně externích paměťových karet. Tento klíč, pokud je použit ve spojení se dvěma předchozím klíči, může poskytnout důležité důkazní informace.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce

Tyto klíče obsahují informace o programech, které se spouštějí automaticky bez interakce s uživatelem.

HKLM\SOFTWARE\Microsoft\Command Processor

HKCU\Software\Microsoft\Command Processor

Tento klíč má hodnotu registru s názvem Autorun, která může obsahovat příkaz, který je automaticky proveden pokaždé, když je spuštěn cmd.exe.50 Nicméně změna tohoto klíče vyžaduje administrátorská práva. Malware může využívat tuto funkci, aby nahrál sám sebe bez vědomí uživatele

HKLM\SYSTEM\CurrentControlSet\Services

Tento klíč obsahuje seznam služeb Windows. Každý podklíč představuje službu a služba obsahuje informace jako je konfigurace spouštění a cesta spustitelného souboru. I některé malware se mohou nainstalovat jako služba.52 Další důležité klíče registrů související se sítěmi.

Nástrojem sloužícím pro prohlížení souborů registry hives je regedit

%SystemRoot%\regedit.exe

Event logs

Zaznamenávání (žurnálování) události v systému (event logging) poskytuje správcům systému důležité informace o stavu systému, ale také je pro forenzní znalce zdrojem mnoha užitečných informací a může být potencionálním důkazem. Soubory event logů jsou uloženy v:

%SystemRoot%\System32\Config

Desktopové systémy obsahují tři základní logy:

%SystemRoot%\System32\ConfigSysEvent.evt

- log systémových událostí

%SystemRoot%\System32\Config\AppEvent.evt

- log událostí aplikací

%SystemRoot%\System32\Config\SecEvent.evt

- log bezpečnostních událostí Serverové operační systémy pak přidávají

%SystemRoot%\System32\Config\Director.evt

- log adresářové služby – obsahuje události reportované Active Directory

%SystemRoot%\System32\Config\DNSEvent.evt

- log DNS Serveru – obsahuje události reportované Windows DNS Serverem

%SystemRoot%\System32\Config\NTFrs.evt

-log File Replication Service – obsahuje události reportované FRS Service.54 Windows Event event logs rozlišuje 5 typů událostí:

Upozornění (warning) – nemusí představovat závažný problém, ale jde o indikování potencionálního problému v budoucnosti.

Chyba (error) – upozorňuje na závažný problém, který může mít za následek ztrátu dat nebo funkčnosti systému. Příkladem může být například konflikt IP adres.

Informace (information) – popisuje úspěšné provedení operace aplikací nebo službou. Může jít například o protokolování úspěšného spuštění konkrétní služby. Dalším příkladem využití jsou informace print spooleru. Z těch je možné zjistit kdo, kdy a v jakém objemu tiskl na které tiskárně.

Auditovaná úspěšná operace (success audit) – přístup k auditovanému zdroji se zdařil. Záznam je vytvořen například tehdy, když uživatel úspěšně vstoupí do složky, pro niž má příslušná oprávnění a u níž je současně aktivováno auditování úspěšných pokusů o přístup.

Auditovaná neúspěšná operace (failure audit) – přístup k auditovanému selhal. Záznam je vytvořen například tehdy, jestliže se uživatel pokusí vstoupit do složky, do níž nemá přístup a u níž je současně zapnuto auditování neúspěšných pokusů o přístup. Všechny typy událostí najdou široké uplatnění v rámci computer forensics. Naučit se číst v těchto událostech tak, aby toto počínání vedlo ke zdárnému výsledku, však chce dlouhodobější zkušenost. První dva typy událostí najdou uplatnění hlavně při zkoumání napadených systémů. Poslední dva pak mohou pomoci při auditech a v rámci information forensics. K prohlížení těchto událostí ze souboru event logů je nejvhodnější použít snap-in modul Microsoft management konzole – event viewer.

%SystemRoot%\system32\eventvwr.msc

Nástroje pro analýzu

Jelikož operační systémy Microsoft Windows jsou ryze komerční, jsou i nástroje analýzy těchto systémů velmi často komerčními produkty. Mezi nejvýznamnější patří výše zmíněné **ForesicToolKit** a **Guidance Software EnCase**, výhodou je jejich komplexnost. Obsahují variaci na všechny zmíněné nástroje obsažené přímo v OS, přidávají prohlížeč všech možných typů souborů a indexované vyhledávání klíčových slov. Nespornou výhodou, jak už tomu na dané platformě bývá, je intuitivnost grafického uživatelského prostředí. To vše je však vyváženo vysokou cenou.

Analýza Unixových systémů

Stejně jako je tomu u operačních systému MS Windows, tak i u Unixových systému a hlavně u často používaných Linuxových distribucí, je potřeba pochopit jak funguje souborový systém.

Ext – Extended file system (rozšířený souborový systém) byl první souborový systém vytvořený speciálně pro operační systém Linux. Napsán byl Rémym Cardem a měl překonat omezení Minix file systemu (první Linuxový filesystem implementovalný Linusem Torvaldsem; podobný Unix V7 FS; používal bitmapy místo zřetězených seznamů; velikost omezena na 64MB; maximální délka jmen 14 znaků)

Ext2 – Second extended file system byl původně implementován pro jádro Linuxu, avšak je možné ho nalézt i v dalších operačních systémech. Navrhl ho opět Rémy Card jako nástupce souborového systému ext a je k dispozici jako open source software. Mezi jeho hlavní vylepšení proti ext patří:

- lze vytvářet adresáře,
- lze vytvářet různé typy souborů: obyčejný soubor, speciální soubor (reprezentuje zařízení, je typu blokový a znakový), pojmenované roury, societies,
- umožňuje používat pevné odkazy, symbolické odkazy,
- pro každý soubor a adresář se ukládají práva UGO – vlastníka (user), skupiny (group), ostatních (other) a rozšířené atributy.

Ext3 – ext3 je žurnálovací systém souborů vytvořený pro operační systém Linux a je přímým a zpětně kompatibilním následníkem souborového systému ext2. Ext3 je implicitním souborovým systémem mnoha populárních Linuxových distribucí. Ačkoli je výkon (rychlost) v některých specifických operacích nižší než u konkurentů jako je JFS2, ReiserFS a XFS, má tu významnou výhodu, že umožňuje jednoduchý přechod z původního ext2 na ext3 bez nutnosti kompletní zálohy a obnovy dat. Další výhodou je jeho dlouhá historie a široké nasazení, které zajišťuje dostatek aktivních vývojářů a vysokou úroveň jeho kódu. Souborový systém ext3 nabízí oproti svému předchůdci ext2:

- žurnálování (informace o dokončených operacích),
- indexy souborů v adresáři implementované pomocí stromových struktur (do té doby se používal pouze lineární seznam, v ext3 se používá jen na malé adresáře),
- možnost změnit velikost souborového systému za běhu (od listopadu 2004).

V Linuxové implementaci ext3 jsou dostupné tři způsoby žurnálování:

- Žurnál – metadata i obsah souborů se ukládají do žurnálu a teprve poté jsou zapsány na disk. Nejspolehlivější, ale zároveň nejpomalejší metoda, protože data jsou zapisována dvakrát.
- Writeback – metadata se žurnálují, ale obsah souborů ne. Toto je nejrychlejší způsob, ale přináší riziko, že při pádu budou data zapsána tam, kam nemají. Při dalším mountu se tedy může stát, že k souborům, se kterými systém v tu chvíli pracoval, budou na konec zapsány různé nesmysly.
- Ordered – podobné jako writeback, s tím rozdílem, že si vynucuje zapsání souboru, než jej v metadatech označí jako zapsaná. Tento způsob je dobrým kompromisem mezi výkonem a stabilitou, a z toho důvodu je použit jako výchozí.

Ext4 přináší mnoho novinek typických pro moderní souborové systémy, jako je odstranění limitů ext3 (velikost souborového systému, souborů, počtu souborů v adresáři), podporu extentů, prealokaci místa na disku, odloženou alokaci, kontrolní součet žurnálu, online defragmentaci, rychlejší kontrolu, multiblokový alokátor a zvýšenou přesnost uložených časových údajů a také samozřejmě zvýšení výkonu. Tento souborový systém se teprve rozšiřuje.

I-node (I-uzel) je datová struktura uchovávající metadata o souborech a adresářích (objektech) používaná v Unixových souborových systémech (např. ext2, ext3, UFS). Z důvodu zachování kompatibility ostatní souborové systémy I-uzly emulují. Jde tedy o pravděpodobně nejdůležitější vlastnost těchto souborových systémů z hlediska forenzní analýzy. I-node obsahuje metadata pro každý libovolně velký soubor i adresář. Například čas poslední změny, přístupová práva, seznam datových bloků a podobně. V adresářích jsou pak dvojice název souboru a I-node, které definují soubory a adresáře. I-node popisuje i některé systémové struktury, jako je kořenový adresář nebo žurnál. Počet I-uzlů je u klasických souborových systémů (ext2, ext3) určen při formátování systému souborů a později již nemůže být změněn. Jejich množství určuje maximální počet adresářů a souborů, které lze v souborovém systému vytvořit. I když může být na disku volné místo pro data, nemusí být možné z důvodu nedostatku volných i-uzlů vytvořit další soubory a adresáře.

Výpis obsazeného datového prostoru:

df

Výpis počtu obsazených I-uzlů:

df -i

Výpis názvů spolu s čísly I-uzlů v adresáři:

ls –i

Struktura I-uzlu je popsána standardem POSIX:

- MODE – druh souboru a přístupová práva
- OWNER – vlastník (ID vlastníka)
- GROUP – skupina (ID skupiny)
- TIME STAMPS – časové informace
    - atime: čas posledního přístupu (čtení ze souboru, výpis adresáře)
    - mtime: čas poslední změny objektu

- ctime: čas poslední změny informací o objektu

- SIZE – velikost objektu
- REFERENCE COUNT – počet odkazů mířicích na tento objekt
- DIRECT BLOCKS – přímé odkazy mířící na objekt
- SINGLE INDIRECT – odkazy na blok, který obsahuje odkaz na objekt

Časová razítka – MAC times

Stejně jako Windows (viz. 5.1.1) i Unixové systémy zaznamenávají MAC times. Časová razítka souborů jsou pro vyšetřovatele nejcennějším zdrojem informací v situaci, kdy se snaží o rekonstrukci událostí v čase. Většina souborových systémů používá nejméně tři časová razítka pro každý soubor, ale například Ext4 už používá modification time (mtime), attribute modification time (ctime), access time (atime), delete time (dtime), create time(crtime). MAC times se používají stejně jako v případě NTFS ve Windows, tedy čas vytvoření souboru (Created), poslední modifikace (Modified) a čas, kdy byl soubor naposledy zpřístupněn (Accessed). Linux používá také čas smazání. V raw formátu jsou informace uloženy jako čas v sekundách od počátku.

Historie shellu

Řádkový shell je v Unixových systémech ještě mocnějším (také díky propracovanějšímu skriptování a kvalitní dokumentaci v podobě manuálových stránek) a hlavně daleko používanějším nástrojem než příkazová řádka ve Windows, kde se často preferuje GUI (grafické uživatelské rozhraní). Výhodou při forenzním šetření je, že historie příkazů shellu bývá zaznamenávána. Historie záznamu shellu (příkazové řádky) je obvykle nastaven tak, že ukládá příkazy zadané v jeho prostředí. To může být velmi užitečné, neboť v podstatě umožňuje vyšetřovateli tímto způsobem sledovat přesně to, jaké příkazy vetřelec použil ke kompromitování daného systému a i v jakém pořadí. Ve výchozím nastavení je záznam historie uložen pro každého uživatele zvlášť v jeho domovském adresáři. Jméno souboru historie se liší pro každý použitý shell. Někdy, když je použito více shellů současně, bývá historie příkazů zapsána do nového souboru poté, co byl soubor historie smazán. Níže je uveden seznam výchozích umístění pro historii souborů v některých z nejpopulárnějších shellů:

C shell (CSH)

.history

Korn Shell(KSH)

.ksh_history

Bourne Again Shell(BASH)

.history

Bohužel, Bourne shell neudržuje soubor s historií příkazů. To je z hlediska forenzního šetření závažný problém, protože právě Bourne shell bývá výchozím shellem pro root uživatele a jiné systémové účty v mnoha Unixových systémech a Linuxových distribucích.

Nástroje pro analýzu

Stejně jako jistá část Unixových systémů a hlavně Linuxových distribucí, jsou nástroje pro forenzní analýzu pro tuto platformu vyvíjeny jako open source, případně GNU General Public License apod. Jedná se sice o kvalitní produkty, nicméně reflektují celou ideologii Unixových systémů se všemi pro i proti. Jedná se většinou o nástroje bez GUI, skládající se z mnoha jednoúčelových aplikací.

The Coroner's Toolkit (TCT) je sada nástrojů určených pro efektivní forenzní analýzu unixového systému. Autoři Dan Farmer a Wietse Venema o něm říkají, že toto softwarové vybavení nemá jednoznačně vytyčený jediný cíl, ale že s ním lze rekonstruovat události, které se v čase v systému staly – vytvářet snapshoty systému. Aplikace spadá pod

IBM Public Licence a její zdrojové kódy jsou plně k dispozici. Program je kompatibilní kromě Linuxu i se systémy FreeBSD, OpenBSD, SunOS a některými dalšími.

Hlavní program grave-robber využívá podprogramů:

- file – rozeznávání typů souborů
- icat – kopíruje soubory podle čísla i-uzlu
- ils – vypíše informace o i-uzlu
- lastcomm – vypíše informace o zadaných příkazech
- mactime – vypíše atime, mtime a ctime
- md5 – vytváření MD5 hashí
- pcat – vypíše paměť procesu

TCT dále obsahuje programy:

- bdf – prochází rekurzivně textové i binární soubory a vyhledává
- ils2mac – konvertuje výstup programu ils, aby byl použitelný pro program mactime a tak bylo možné získat přístupové časy smazaných souborů
- realpath – získávání skutečných cest k souboru – včetně odkazů
- findkey – hledání kryptografických klíčů
- entropy – počítá entropii dat
- unrm – obnovení nealokovaných sektorů a program
- lazarus – obnovování smazaných souborů

The Sleuth Kit, jehož tvůrcem je Brian Carrier, je založen na TCT. Zdrojové kódy jsou volně ke stažení. The Sleuth Kit je podporován operačními systémy Linux, Mac OS X, OpenBSD, FreeBSD, Solaris, nebo jej lze spustit přes CYGWIN (v podstatě prostředí textového shellu s Linuxovými příkazy pod Windows). Mezi podporované souborové systémy patří NTFS, FAT, FFS, Ext2 a Ext3, UFS1/2. Lze však zpracovávat pouze obrazy jednotlivých oddílů, nikoli celého disku. Jednotlivé nástroje této aplikace lze rozčlenit do několika vrstev:

- File System Layer Tools
    - fsstat – vypisuje základní údaje o souborovém systému
- File Name Layer Tools
    - ffind – vypisuje alokovaná i nealokovaná jména souborů vážící se k zadanému i-uzlu
    - fls – vypisuje alokované a smazané soubory a adresáře
- Meta Data Layer Tools
    - icat – kopíruje soubory podle čísla i-uzlu
    - ils – vypíše informace
    - i-uzluDále o ifind – najde i-uzel k zadanému jménu souboru nebo jiné datové struktuře (block, cluster, apod.) a to i v nealokovaném prostoru
    - istat – zobrazuje informace o datové struktuře v uživatelsky přívětivějším formátu
- Data Unit Layer Tools

- dcat – extrahuje obsah zadané datové struktury

- dls – zobrazí informace o datové struktuře a také umí extrahovat nealokované prostory souborového systému

- dstat – zobrazí statistické informace o zadané datové struktuře ve snadno čitelném formátu o dcalc – počítá, kde data v nealokovaném prostoru jsou

- File System Journal Tools
  - jcat – který zobrazuje obsah určitého bloku
  - jls – vypisuje přístupy do žurnálu
- Media Management Tools
  - mmls – zobrazení struktury disku.
- Image File Tools o img_stat – zobrazuje informaceo obrazu.
- Disk Tools o disk_sreset – utilita kterou lze dočasně odstranit HPA (Host Protected Area) na discích ATA.
  - disk_stat – ukazuje, zdali HPA na disku existuje
- Další utility o hfind – práce s hashi vytvořenými programem md5sum
  - mactime – vytvoří časovou řadu s událostmi, které se s daným souborem děly, kdy jako vstup bere výstup programu fls a ils
  - sorter – třídí vyhledané soubory
  - sigfind – hledá binární hodnoty při zadaném offsetu, což je vhodné pro hledání ztracených datových struktur.

K dispozici je i grafický frontend k The Sleuth Kit s názvem Autopsy65. Výhoda GUI je zde však vykompenzována omezením spočívajícím v tom, že Autopsy vyžaduje pro svůj běh X Windows.

Analýza sítového prostředí a komunikačních nástrojů

Analýza síťového prostředí a nástrojů využívaných na nich ke komunikaci je díky množství možných použitých technologií a aplikací velmi rozmanitá. Předpokladem pro zvládnutí analýzy forenzní komunikace v prostředí počítačových sítí je nutná vynikající znalost komunikačních protokolů a principů jejich fungování. Následující subkapitola proto shrnuje jen ty opravdu nejpoužívanější metody a postupy aplikovatelné v prostředí nejrozšířenějších operačních systému, webových prohlížečů (dle Market Share66) či Instant Messaging klientů (dle Billions Connected67). Z velké části půjde o metody použitelné na serverových OS a aplikacích firmy Microsoft a klientech stejného výrobce. Krom následujících je možné použít.

Důležité klíče registrů a nástroje

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\GUID

Tento klíč obsahuje poslední nastavení síťových adaptérů, jako je IP adresa a výchozí brána pro dané síťové adaptéry. Každý GUID podklíč odkazuje na síťový adaptér68. Údaje jsou uchovávány i v případě, kdy je síťové připojení již odpojeno.

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

První klíč udržuje seznam namapovaných síťových disků, včetně serveru a sdílené složky. Hodnoty v tomto klíči zůstávají zachovány i v případě, kdy namapované síťové jednotky byly již trvale odstraněny nebo odpojeny. Kromě prvního podklíče bývají informace uchovány (za předpokladu, že by byly z prvního ručně smazány) i v druhém.

HKCU\Software\Microsoft\Internet Explorer\TypedURLs

Tento klíč obsahuje seznam 25 posledních URL adres (nebo cest k souboru), které byly naposledy napsány v adresním řádku Internet Exploreru nebo Průzkumníku Windows. Nicméně obsahuje pouze odkazy, které jsou plně napsané. Tedy adresy automaticky doplněné při psaní, nebo odkazy, které jsou vybrány ze seznamu historie navštívených adres, zobrazeny nebudou. Také webové stránky, které jsou přístupné přes oblíbené položky, nejsou zaznamenány. Tyto hodnoty je také jednoduše možno odstranit přímo v Internet Exploreru pomocí vymazání historie.

HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\GUID

Tento klíč obsahuje informace o bezdrátové síti a o adaptérech využívajících Windows Wireless Zero Configuration Service. Pod GUID podklíči jsou binární hodnoty registru pojmenované Static#0000, Static#0001 atd. (v závislosti na počtu registrovaných SSID), které odpovídají příslušné SSID v seznamu preferovaných sítí v konfiguraci bezdrátového připojení k síti71. Hodnota registru obsahuje název SSID v binární podobě. Pokud hodnota registru ActiveSettings obsahuje SSID jméno, jde o poslední připojenou síť. Nevýhodou je ovšem to, že pokud na šetřeném PC není bezdrátové připojení spravováno systémem Windows, ale správcem připojení, například od výrobce síťové karty (např. Intel), či správcem připojení zajišťujícím bezpečné připojení do firemní sítě (např. Cisco), nebudou tyto klíče registru obsahovat hledané informace. Další důležité klíče registrů, které se vztahují nejen k forenzní analýze sítí, ale OS Windows.

Velmi užitečnými nástroji pro forenzní analýzu stavu sítě je několik příkazů dostupných přímo v systému Windows. Patří mezi ně:

- ipconfig.exe
- nbtstat.exe
- netstat.exe
- nslookup.exe
- route.exe
- tracert.exe

Všechny jsou dostupné v

%SystemRoot%\system32

ipconfig.exe zobrazí všechny aktuální hodnoty konfigurace sítě TCP/IP a aktualizuje nastavení protokolu DHCP (Dynamic Host Configuration Protocol) a služby DNS (Domain Name System). Při použití bez parametrů zobrazí příkaz ipconfig pro všechny adaptéry adresu IP, masku podsítě a výchozí bránu

```
C:\>ipconfig /all

Konfigurace protokolu IP systému Windows

        Název hostitele . . . . . : COMPUTER
        Primární přípona DNS. . . . . : SUBDOMAIN.DOMAIN.CZ
        Typ uzlu  . . . . . : hybridní
        Povoleno směrování IP . . . . . : Ne
        WINS Proxy povoleno . . . . . : Ne
        Prohledávací seznam přípon DNS. . : SUBDOMAIN.DOMAIN.CZ
                                            DOMAIN.CZ

Adaptér sítě Ethernet Připojení k místní síti:

        Stav média  . . . . . : odpojeno
        Popis . . . . . : Broadcom NetXtreme 57xx Gigabit
Controller
        Fyzická Adresa. . . . . : 00-21-70-95-0A-B2

Adaptér sítě Ethernet Bezdrátové připojení k síti:

        Přípona DNS podle připojení . . . :
        Popis . . . . . : Intel(R) Wireless WiFi Link
4965AGN
        Fyzická Adresa. . . . . : 00-21-5C-43-8C-7B
```

```
        Protokol DHCP povolen . . . . . : Ano
        Automatická konfigurace povolena  : Ano
        Adresa IP . . . . . : 10.0.0.100
        Maska podsítě . . . . . : 255.255.255.0
        Výchozí brána . . . . . : 10.0.0.1
        Server DHCP . . . . . : 10.0.0.1
        Servery DNS . . . . . : 10.0.0.1
        Zapůjčeno . . . . . : 19. ledna 2009 16:58:22
        Zápůjčka vyprší . . . . . : 19. září 2037 5:14:07
```

nbtstat.exe mimo jiné zobrazí statistické údaje o protokolu NetBIOS přes TCP/IP (NetBT), tabulky názvů NetBIOS místních i vzdálených počítačů a mezipaměť systému NetBIOS pro názvy

```
C:\>nbtstat -A 10.0.0.103
Bezdrátové připojení k síti:
Adresa IP uzlu: [10.0.0.103] ID oboru: []
       Tabulka názvů vzdálených počítačů NetBIOS
         Název                Typ            Stav
    ---------------------------------------------
    COMPUTER        <00>  JEDINEČNÁ   Registrovaný
    COMPUTER        <20>  JEDINEČNÁ   Registrovaný
    DOMAIN          <00>  SKUPINA     Registrovaný
    DOMAIN          <1E>  SKUPINA     Registrovaný
    DOMAIN          <1D>  JEDINEČNÁ   Registrovaný
    ..__MSBROWSE__.<01>  SKUPINA     Registrovaný
    Adresa MAC = 00-c1-5C-43-8C-7B
```

netstat.exe zobrazí aktivní připojení TCP, porty, přes které počítač přijímá požadavky, statistické údaje systému Ethernet, směrovací tabulku protokolu IP, statistické údaje IPv4 (pro protokoly IP, ICMP, TCP a UDP) a IPv6 (pro protokoly IPv6, ICMPv6, TCP přes IPv6 a UDP přes IPv6).

```
C:\>netstat

Aktivní připojení

  Proto  Místní adresa          Cizí adresa            Stav
```

```
  TCP    COMPUTER:1068          www.meebo.com:https    CLOSE_WAIT
  TCP    COMPUTER:1070          www.meebo.com:https    CLOSE_WAIT
  TCP    COMPUTER:1076          messenger.live.com:1863NAVÁZÁNO
  TCP    COMPUTER:1219          213.199.141.141:http   CLOSE_WAIT
  TCP    COMPUTER:1272          63.111.74.129:http     NAVÁZÁNO
  TCP    COMPUTER:1309          10.0.0.102:3549        NAVÁZÁNO
  TCP    COMPUTER:1320          www.meebo.com:http     NAVÁZÁNO
  TCP    COMPUTER:1079          localhost:1084         NAVÁZÁNO
  TCP    COMPUTER:1084          localhost:1079         NAVÁZÁNO
```

nslookup.exe zobrazí informace, které lze využít k diagnostice infrastruktury systému DNS (Domain Name System). Před použitím tohoto nástroje je třeba znát, jakým způsobem systém názvů domén (DNS) funguje. Příkaz nslookup je k dispozici pouze v případě, že je nainstalován protokol TCP/IP.

```
C:\>nslookup
Výchozí server:
Address:  10.0.0.1

> set q=mx
> fi.muni.cz
Server:
Address:  10.0.0.1

DNS request timed out.
    timeout was 2 seconds.
Neautorizovaná odpověď:
fi.muni.cz       MX preference = 50, mail exchanger = relay.muni.cz

fi.muni.cz       nameserver = ns.muni.cz
fi.muni.cz       nameserver = aisa.fi.muni.cz
fi.muni.cz       nameserver = anxur.fi.muni.cz
ns.muni.cz       internet address = 147.251.4.33
>
```

```
C:\>route print
===========================================================================
Seznam rozhraní
0x1 ........................... MS TCP Loopback interface
0x2 ...00 21 70 95 0a b2 ...... Broadcom NetXtreme 57xx Gigabit Controller -
Packet Scheduler Miniport
0x3 ...00 21 5c 43 8c 7b ...... Intel(R) Wireless WiFi Link 4965AGN - Packet
Scheduler Miniport
===========================================================================
===========================================================================
Aktivní směrování:
       Cíl v síti      Síťová maska            Brána       Rozhraní  Metrika
         0.0.0.0          0.0.0.0         10.0.0.1      10.0.0.100       25
        10.0.0.0    255.255.255.0       10.0.0.100      10.0.0.100       25
      10.0.0.100  255.255.255.255        127.0.0.1       127.0.0.1       25
   10.255.255.255  255.255.255.255       10.0.0.100      10.0.0.100       25
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1        1
        224.0.0.0        240.0.0.0       10.0.0.100      10.0.0.100       25
  255.255.255.255  255.255.255.255       10.0.0.100               2        1
  255.255.255.255  255.255.255.255       10.0.0.100      10.0.0.100       1
Výchozí brána:          10.0.0.1
===========================================================================
Trvalé trasy:
  Žádné
```

tracert.exe určuje trasu k cíli tím, že do cíle odešle zprávy protokolu ICMP (Internet Control Message Protocol) s požadavkem na odezvu se zvyšujícími se hodnotami polí TTL (Time-To-Live). Zobrazenou cestu představuje seznam bližších rozhraní směrovačů na trase mezi zdrojovým hostitelem a cílem. Bližší rozhraní je rozhraní směrovače, které je k odesílajícímu hostiteli z hlediska cesty nejblíže.

```
C:\>tracert fi.muni.cz

Výpis trasy k fi.muni.cz [147.251.48.1]
s nejvýše 30 směrováními:

  1     1 ms     1 ms     1 ms  . [10.0.0.1]
  2    24 ms     2 ms     1 ms  192.168.139.1
  3     6 ms     3 ms     4 ms  gate.mohnet.rtr.rps.cz [88.103.228.57]
  4     8 ms     9 ms     9 ms  88.103.236.234
  5    18 ms    16 ms    19 ms  201.9.broadband16.iol.cz [90.183.9.201]
```

```
  6    51 ms    51 ms    51 ms  198.18.96.137
  7    52 ms    53 ms    51 ms  198.18.10.49
  8    51 ms    53 ms   274 ms  80.188.33.239q
  9   295 ms   204 ms   140 ms  80.188.33.238
 10    46 ms    52 ms     *     194.228.190.165
 11    28 ms    26 ms    25 ms  nix4-10ge.cesnet.cz [194.50.100.191]
 12    28 ms    30 ms    29 ms  c-cps.bb.muni.cz [195.178.87.10]
 13    30 ms    31 ms    30 ms  c-sci.bb.muni.cz [147.251.241.210]
 14    30 ms    28 ms    30 ms  ics-1.bb.muni.cz [147.251.241.78]
 15    27 ms    30 ms    29 ms  ares1-240.fi.muni.cz [147.251.240.12]
 16    58 ms    55 ms    55 ms  fi.muni.cz [147.251.48.1]

Trasování bylo dokončeno.
```

Internet Explorer

Internet Explorer vytváří ve výchozím nastavení cache navštívených stránek. Když uživatel navštíví stránku, Internet Explorer zkontroluje, zda je soubor již nacacheován. Pokud je ve vyrovnávací paměti, Internet Explorer používá nacacheovaný soubor namísto stahování souboru z Internetu. Tyto dočasné soubory jsou uchovávány spolu s indexačním souborem INDEX.DAT v adresáři.

%USERPROFILE%\Temporary Internet Files\Content.IE5

Dalším zdrojem potencionálních důkazů můžou být soubory cookie. Jako cookie se v protokolu HTTP označuje malé množství dat, která WWW server pošle prohlížeči, a ten je uloží na počítači uživatele. Při každé další návštěvě téhož serveru pak prohlížeč tato data posílá zpět serveru. Cookies běžně slouží k rozlišování jednotlivých uživatelů, ukládá se do nich obsah „nákupního košíku“ v elektronických obchodech, uživatelské předvolby apod. Jedná se o jedinou výjimku, kdy může webová stránka ukládat data na klientský počítač. Cookies jsou uloženy v

%USERPROFILE%\Cookies

Cookies jsou podobně jako dočasné soubory internetu idexovány. Sobor je uložen ve stejné lokaci jako cookies pod názvem INDEX.DAT.

Exchange server

Jelikož je Microsoft Exchange, přesto že se jedná o samostatně prodejný produkt, silně integrován s platformou Windows NT, není možné jednoduše obnovit soubory a databáze Exchange a zkoumat ji přímo. Pro zkoumání obsahu databáze Exchange existují jen dvě možnosti. Tou náročnější je vytvoření serveru pokud možno co nejshodnějšího s původním a překopírování databáze. Tento zdlouhavý postup je možné ve speciálních případech výrazně urychlit (například když server běží ve virtuálním prostředí), nicméně nejde o univerzální postup. Veškerá data databáze Exchange jsou ve výchozím nastavení uložena v adresáři

%Program Files%\Exchsrvr\Mdbdata

Tabulka 4 – soubory databáze exchange

Název	**Popis**
Priv1.ebd	rich-textový databázový soubor, který obsahuje e-mailové zprávy, textové přílohy a hlavičky pro uživatele e-mailu
Priv1.stm	streaming soubor, který obsahuje multi-mediální údaje, které jsou ve formátu MIME dat
Pub1.ebd	rich-textový databázový soubor, který obsahuje zprávy, text a přílohy záhlaví pro soubory uložené ve veřejné složce stromu.
Pub1.stm	streaming soubor, který obsahuje multi-mediální údaje, které jsou ve formátu MIME dat
E##.log	aktuální transakční log databáze; jakmile dosáhne soubor velikosti 5MB je přejmenována na E########.log je vytvořen a nový E##.log soubor; stejně jako u kontrolního souboru ## reprezentuje identifikátor

datové skupiny. Zatímco je vytvářen nový E##.log soubor je vidět soubor s názvem Edbtmp.log což je šablona log souborů Exchange Server

E#######.log jsou sekundárním transakční logy; jsou číslovány hexadecimální posloupností začínající E0000001.log a opět mají velikost 5MB.

Res1.log soubor rezervovaný pro případ nedostatku místa na disku

Res2.log další rezervovaný log se stejnou funkci jako Res1.log

Lokace databázových souborů však může být změněna administrátorem serveru. Informaci o tom, kde je aktuálně úložiště, nalezneme v registrech Windows

HKLM\SYSTEM\CurrentControlSet\Services\MSExchangeIS\ParametersSystem\Working Directory

Druhou možností, jak získat data z databáze Microsoft Exchange server, je pomocí utility exmerge.exe. Tu je možné získat zdarma na stránkach Microsoftu nebo z instalačního CD Exchange serveru. Soubor je vhodné překopírovat ze složky na CD

Support\Utils\I386\Exmerge

do

%PROGRAMFILES%\Exchsrvr\bin

Exmerge umožňuje za pomoci GUI vyexportovat libovolnou poštovní schránku z databáze Exchange do souboru osobních složek *.pst. Tento databázový soubor je pak možné připojit a prohlížet v poštovním klientu Outlook, nebo otevřít v některém ze specializovaných nástrojů pro forenzní analýzu. Nevýhodou tohoto postupu je, že jsou získána pouze data z konkrétního mailboxy (případně všech mailboxů na serveru), ale nejsou získány informace z transakčních logů.

Grafické uživatelské rozhraní pro práci s Exchange serverem je opět řešeno jako snap-in modul do Microsoft management Konsole

%PROGRAMFILES%\Exchsrvr\bin\Exchange System Manager.msc

Active Directory

Adresářová služba je jednou z core komponent serverových operačních systému firmy Microsoft, která funguje jako centrální úložiště pro velké množství kritických dat včetně uživatelských účtů, hesel, e-mailových adres a dalších osobních údajů. Active Directory také ukládá nastavení zabezpečení objektu oprávnění NTFS a nastavení a kontrolu nastavení jednotlivých objektů. Informace v AD jsou uloženy na řadičích domény v databázi s názvem Ntds.dit

%Program Files%\NTDS\Ntds.dit

Jako database engine je použit Extensible Storage Engine (ESE) postavený na Jet database používané také pro MS Exchange Server. Vzhledem k množství dat, které Active Directory obsahuje, může být bohatým zdrojem důkazů. Souboru Ntds.dit lze prohlížet pomocí Active Directory snap-in modulu v Microsoft Management Console.

%SystemRoot%\system32\dsa.msc

Typické otázky, které mohou být zodpovězeny za pomoci AD, jsou: „Kdo má oprávnění číst data konkrétního uživatel?“ či „Kdo může měnit přístupová práva pro danou organizační jednotku?“

Analýza embedded systémů

Téměř libovolné digitální zařízení v dnešní době obsahuje nějaký jednoúčelový vestavný počítač. Embedded systémy jsou například mobilní i pevné telefony, kopírky, faxy, přijímače pozemního i satelitního digitálního vysílaní, MP3, DVD, BD, DivX i HD přehrávače a rekordéry, HUBy, routery, switche či GPS. Dále pak monitorovací systémy, systémy řídící dopravu, prodejní automaty, řídící jednotky klimatizací a vytápění a domovní alarmy, výtahy a eskalátory, digitální fotoaparáty a kamery, systémy pro kontrolu výroby a řízení v energetice apod. V podstatě každé

elektronické zařízení je dnes řízeno jednoúčelovým procesorem. Jakékoli z těchto zařízení, disponující pamětí, je možné podrobit forenzní analýze a je z něj možné získat potenciální důkaz. Rozmanitost těchto zařízení však nedovoluje formulovat mnoho obecně platných postupů při jejich analýze, kromě těch pro práci s pamětí (například nevhodnost odpojení napájení u zařízení s energeticky závislou pamětí). Velmi často je nutné paměť vyjmout ze zařízení a podrobit ji zkoumání ve forenzní laboratoři.

Zajímavým zdrojem informací pro analýzu jsou digitální fotoaparáty. Přestože se jedná o embedded systémy, ukládají data na masově rozšířená média a přidávají k nim spoustu metadat použitelných ve forenzním procesu ve formě EXIF. Z EXIF dat je možno zjistit kromě méně důležitých expozičních údajů také jméno majitele fotoaparátu (pokud jej zadal), jeho výrobní číslo, čas, datum a v poslední době i souřadnice pořízení snímku (u fotoaparátů vybavených GPS).

Analýza mobilních zařízení

Vzhledem k masovému rozšiřování mobilních technologií (nikoli jen laptopy, či tablet PC, ale spíše menší zařízení) je potřeba zlepšovat znalosti těchto zařízení v rámci computer forensics. V dnešní době již téměř neexistuje trh PDA (personal digital assistant – osobní digitální pomocník) zařízení. Tato byla nahrazena chytrými telefony – smatphone. V mnoha případech jde vlastně o PDA s telefonním GSM modulem umožňujícím připojení do WWAN datové sítě. Takové zařízení v závislosti na zvoleném operačním systému a rychlosti datového připojení dokáže plně nahradit, alespoň co se týče komunikace, laptop či PC. Hlavní problém v šetření mobilních zařízení je zapříčiněn velkou roztříštěností trhu použitých operačních systému. Mezi dnes nejpoužívanější, případně ty s potenciálem masově se rozšířit, patří:

- Windows Mobile
- Symbian
- Linux
- Blackberry OS
- Google Android
- iPhone OS X
- WebOS

Forenzní analýza mobilních zařízení patří společně s analýzou embedded systémů k obtížnějším a hlavně méně prozkoumaným subodvětvím computer forensics. Každý mobilní operační systém je zcela odlišný. Navíc tato zařízení jsou vysoce multifunkční a spojují mnoho přístrojů technologií. Dokáží komunikovat v rámci WWAN – GSM modul (včetně vysokorychlostních přenosů GPRS, EDGE, 3G, HSDPA, HSUPA) i WLAN (Wi-Fi 802.11a/b/g/n) či PAN (IrDA, BlueTooth). Dále nabízí spojení PDA, GPS, digitálního fotoaparátu a kamery a přehrávače médií. Existují pro ně plnohodnotné webové prohlížeče, kancelářské aplikace, emailové klienty s přímým připojením na firemní emailový server (například díky technologii DirectPush ve Windows Mobile je možné přijímat v telefonu emaily ihned poté, co jsou přijaty Exchange serverem). Veškeré instant messaging sítě disponují i mobilní nebo webovou verzí svých klientů. Všechny tyto komunikační soubory mohou zanechávat informace o své činnosti. Je tedy zřejmé, že takové zařízení bude zdrojem velmi užitečných informací, které se mohou stát cennými důkazy.

Nástroje pro analýzu

Nástroje pro forenzní analýzu SIM karet a mobilních zařízení jako PDA, smartphone i klasické mobilní telefony vyvíjí firma Paraben80. Její nástroje PDA Seizure a Cell Seizure byly prvními komerčními forenzní nástroje pro mobilní telefony. Současný produkt Device Seizure je kombinací těchto dvou programů a má širokou podporu mobilních telefonů a PDA, dalším nástrojem je pak například Oxygen Forensic Suite.

Praktické poznatky

Uvedené metody a postupy umožňují zkušenému znalci či vyšetřovateli zjistit nejen obsah, pro případ důležitých souborů, ale také, což je neméně důležité, si udělat (nejen za pomoci získaných metadat) velmi přesný obrázek o

chování a zvycích uživatele a sestavit přesnou časovou osu jeho počínání. Je zřejmé, že jinak bude probíhat šetření, kde na straně šetřeného je IT profesionál s letitou zkušeností v oboru, a jinak v situaci, kde na straně šetřených je vrcholový management podniku či běžný administrativní pracovník nebo odborník v oboru mimo informační technologie, který nemá o technickém řešení ani zdání. Sběr dat je vždy podobný u šetřených se stejným technickým řešením. Technické řešení se typicky odvíjí od počtu zaměstnanců a případně také oboru podnikání. Je možné se naučit správné a vyzkoušené postupy – algoritmy pro sběr a analýzu dat. K efektivní práci je však potřeba uplatnit jistou mazanost a schopnosti – skilly nabyté dlouhodobou praxí a založené na přehledu a znalosti systémů „z druhé strany“. Forenzní znalec v oboru IT bývá většinou velmi zdatný administrátor konkrétního počítačového systému s letitou praxí v oboru a širokým přehledem o informačních technologiích jako celku a také systematik se znalostí principů teoretické informatiky. Od určité velikosti organizace dle počtu zaměstnanců je relativně málo kombinací a možností komplexních řešení IT zázemí. Je pravděpodobné, že například podnik využívající přístup ke kontaktům, emailům či kalendářům z mobilních zařízení bude zároveň využívat MS Exchange server a MS Outlook (ať na mobilní či desktopový) na straně klienta. Podobně je tomu třeba i na trhu IP telefonie, či security appliance. Určité skupiny produktů fungují ideálně jen s některými dalšími.

Praxe ukazuje, že nejcennější informace bývají získávány z počítačů uživatelů v jejich přítomnosti. Ti občas vůbec netuší, co se na jejich HDD skrývá. Rozhovor s uživatelem velmi často přináší informace o tom, jaké má postupy on a jaké se aplikují v rámci organizace, co je v ní zvykem. Na základě těchto informací je pak daleko snadnější např. seznámení se s nestandardním informačním systémem či toky informací v organizaci a vypátrání důkazů v něm obsažených. Analýza systému se také výrazně zjednoduší, pokud má expert k dispozici heslo pro přístup do systému a k šifrovaným souborům. Toto je vhodné zajistit například za pomoci právníka poučením, včetně důsledků odmítnutí. Velmi kvalitním elektronickým zdrojem dalších informací může být webová stránka Forensics Wiki na adrese: http://www.forensicswiki.org/wiki/Main_Page.