Digitalna forenzika

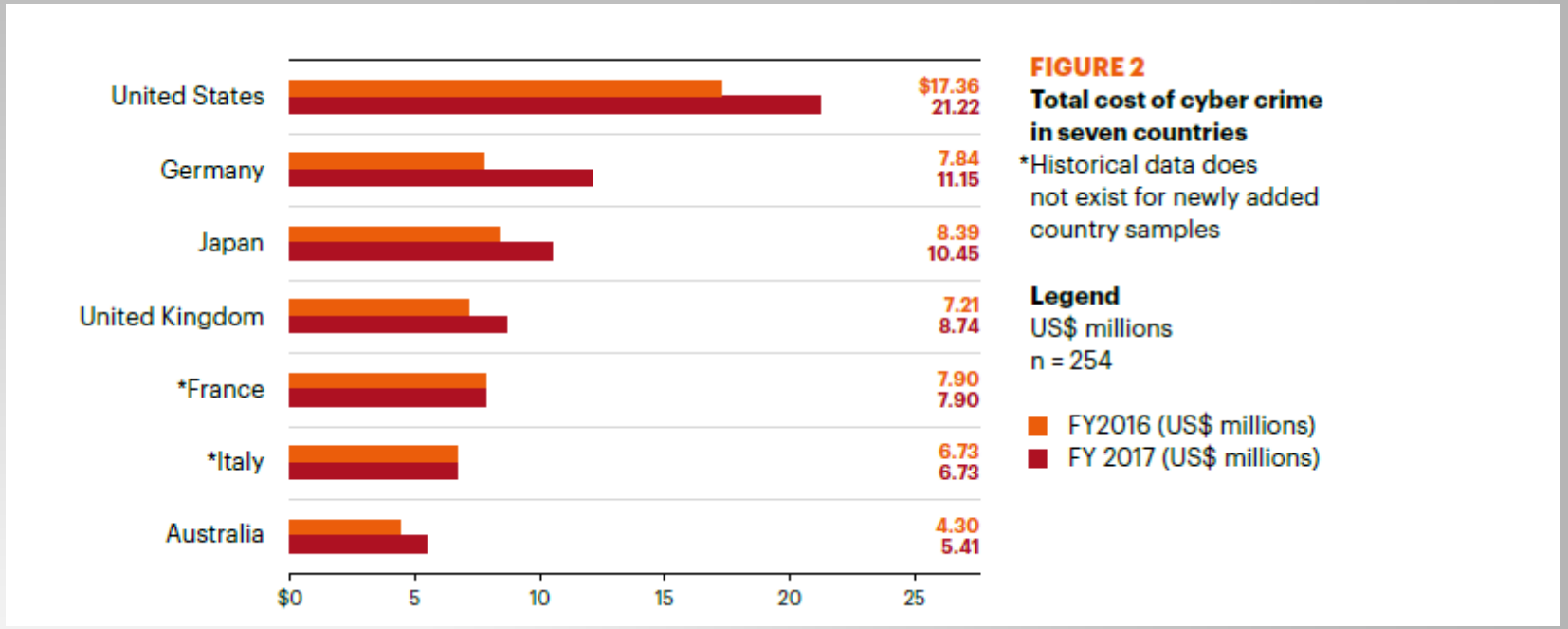
van.profesor dr Ana Kovačević,
Fakultet bezbednosti

kana@rcub.bg.ac.rs

Global State of Information Security Survey 2016

Izvor: Global State of Information Security Survey 2016, produced by PwC, *CIO* and CSO are based on over 10,000 world-wide respondents (http://www.idgenterprise.com/resource/research/2016-global-state-of-information-security-survey/)

Koliko košta sajber kriminal



Cost of Cyber Crime study, Ponemon institute 2017

Sajber kriminal serivisi

GCSP
Geneva Centre for Security Policy
Where knowledge meets experience

Cyber crime services

- Hacking a Facebook or Twitter account: $130
- Hacking a Gmail account: $162
- Hacking a corporate mailbox: $500
- Scans of legitimate passports: $5 each
- Windows rootkit (installing malicious drivers): $292
- Hiring a DDoS attack: $30-70 for a day, $1,200 for a month
- Winlocker ransomware: $10-20
- Unintelligent exploit bundle: $25
- Intelligent exploit bundle: $10-3,000
- Basic crypter: $10-30

** Ars Technica, Russian Underground 101, Trend Micro, Max Goncharov*

Izvor GCSP

Crv Slamer

- 2003. godine pušten je crv tzv. Slammer (poznati i kao Sapphire, Helkern or SQLExp), koji je u roku od deset minuta zarazio 90% računarskih sistema na planeti koji nisu imali (adekvatnu) zaštitu. Londonski Market intelligance (Mi2g) procenio je štetu koju je ovaj crv izazvao, na oko 1.2 milijarde dolara.

Crv Stuxnet

- **Stuxnet** koji je instalian u elektronske delove uređaja, pogodio postrojenja za obogaćivanje uranijuma u Iranu,
- Stuxnet je otkriven u junu 2010: prvi maliciozni program napravljen da napadne industrijske sisteme kao što su elektrane i nuklearni reaktori.
- Crv je napravljen sa ciljem da usporava i ubrzava centrifuge koje su veoma osetljivi uređaji, i ukoliko se pojavi problem u kontroli frekvenicje -→ uništenje uređaja i katastrofa.
- Izvor: http://www.informacija.rs/Vesti/Iran-optuzio-Zapad-i-Izrael-za-napad-kompjuterskim-crvom-Stuxnet-i-napad-na-naucnike.html

Kompjuterski kriminalitet

- **Kompjuterski kriminalitet** predstavlja oblik kriminalnog ponašanja, kod koga se korišćenje **kompjuterske tehnologije** ispoljava kao **način** izvršenja krivičnih dela, ili se kompjuter upotrebljava kao **sredstvo** ili **cilj** izvršenja, čime se ostvaruje neka u krivično pravnom smislu relevantna posledica.
- Definicija kompjuterskog kriminaliteta mora se zasnivati na tri elementa:
  - način izvršenja (modus operandi)
  - sredstvo izvršenja
  - posledice kriminalnog delovanja

Bezbednosni izazov

- Primena računara u svim oblastima života => veliki broj podataka.
- Eksplozivni razvoj Interneta i servisa za plaćanje putem Interneta.
- **Računari kao oružje, kao podrška poslu, ali i za kršenje zakona.**
- Bezbednosni proboj preko Interneta su u porastu, i računarski kriminal je u porastu.
- **Računarski kriminal (**ili visokotehnološki kriminal, *sajber kriminal*) obuhvata aktivnosti tokom kojih se računari, računarske mreže ili računarski podaci koriste kao izvori, sredstva, objekat ili mesta izvršenja krivičnog dela" (Milosavljević i dr., 2009)

Cybersecurity (ISO 27032)

- **Cybersecurity**
- **Cyberspace security**
- preservation of confidentiality, integrity and availability of information in the Cyberspace
- NOTE 1 In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
- NOTE 2 Adapted from the definition for information security in ISO/IEC 27000:2009.

CIA vs DAD

- Tri fundamnetalna principa **bezbednosti informacija:**
  - Poverljivost (engl. Confidentality) informacija je dostupna samo onima koji su ovlašćeni da joj pristupe.
  - Integritet, celovitost (engl. Integrity) podatke ne smeju da menjaju neovlašćenja lica ili procesi;
  - Raspoloživost (engl. Availability) ovlašćeni korisnici mogu pravovremeno da prisutupe podacima ili računarskim resursima.
- SUPROTNO:
  - DAD Disclosure (otkrivanje), Alteration (izmena), Destruction (uništenje).

Sajber kriminal

- Podela u zavisnosti od tipa počinjenih dela:
  - Politički: cyber špijunaža, haking, cyber sabotaža, cyber terorizam i cyber ratovanje.
  - Ekonomski: cyber prevare, haking, krađa Internet usluga i vremena, piratstvo softvera, mikročipova, cyber industrijska špijunaža i spam.
  - Proizvodnja i distribucija nedozvoljenih i štetnih sadržaja – dečja pornografija, pedofilija, verske sekte, širenje rasističkih, nacističkih i sl. ideja i stavova, i zloupotreba dece i žene.
  - Manipulacija zabranjenim proizvodima, supstancama i robama – drogom, ljudskim organima, oružjem.
  - Povrede cyber privatnosti – nadgledanje e-pošte, prisluškivanje, snimanje pričaonica, praćenje e-konferencija, i analiza “cookies”.

DIGITALNA FOREZNIKA

autor: dr Ana Kovačević, FB

Digitalna foreznika

Digitalna forenzika kao relativno nova naučna disciplina (uspostavljena 1999. godine od strane IECO - International Organization on Digital Evidence) obezbeđuje jedini pouzdani alat za istragu računarskog kriminala.

Digitalna forenzika

- Digitalna forenzička istraga predstavlja **proces** koji korišćenjem naučnih metoda i tehnologije,

  razvija i testira teorije kroz hipoteze,

  analizirajući digitalne uređaje, koji predstavljaju relevantan dokaz u sudskom postupku.
- DIGITALNI **DOKAZ- digitalni objekat koji sadrži pouzdane informacije koje podržavaju hipotezu ili je opovrgavaju.**
- Cilj takve istrage je da se utvrdi istina o protivpravnoj aktivnosti i svih okolnosti u vezi sa počiniocem i načinom izvršenja krivičnog (prekršajnog dela).

Digitalna forenzika

- U slučaju da je došlo do zloupotrebe IKT sistema, odnosno računarskog kriminala ili potrebe za upravljanjem računarskim incidentom, administrativnih zahteva ili civilne parnice, odgovore će dati digitalna forenzika koja podrazumeva:
  - otkrivanje (pretraga, istraga) i sakupljanje (akviziciju),
  - čuvanje (upravljanje),
  - dokazivanje (analizu) i
  - ekspertsko svedočenje/veštačenje (prezentaciju) digitalnih dokaza pred sudom [Milosavljević &Grubor *2009.*].
  - **Milosavljević M., Grubor G., *Digitalna forenzika računarskog sistema, Univerzitet Singidunum, Beograd 2009.*

Cilj istrage visokotehnološkog kriminala

- Glavni cilj istrage visokotehnolškog kriminala je, kao i u slučaju klasičnog kriminala, izgraditi za pravosudne organe neoboriv, ili čvrst dokaz, i/ili dokaz za oslobađanje osumnjičenog, i/ili pravedno sankcionisanje učinjenog dela (Milosavljević&Grubor, 2008).
- Da bi se obezbedio takav dokaz, u slučaju visokotehnološkog kriminala, neophodno je, uz pomoć niza posrednih dokaza, pronaći informacije u digitalnom obliku koje imaju verodostojnu vrednost, a koja je uskladištena ili prenešena u takvom obliku.
- Takve informacije su digitalni dokazi.

Digitalna forenzika

- Forenzika računara (računarskih sistema)
- Forenzika telefona
- Forenzika mreže
- Virtualna forenzika (i forenzika u oblaku)
- **Forenzika baza podataka.

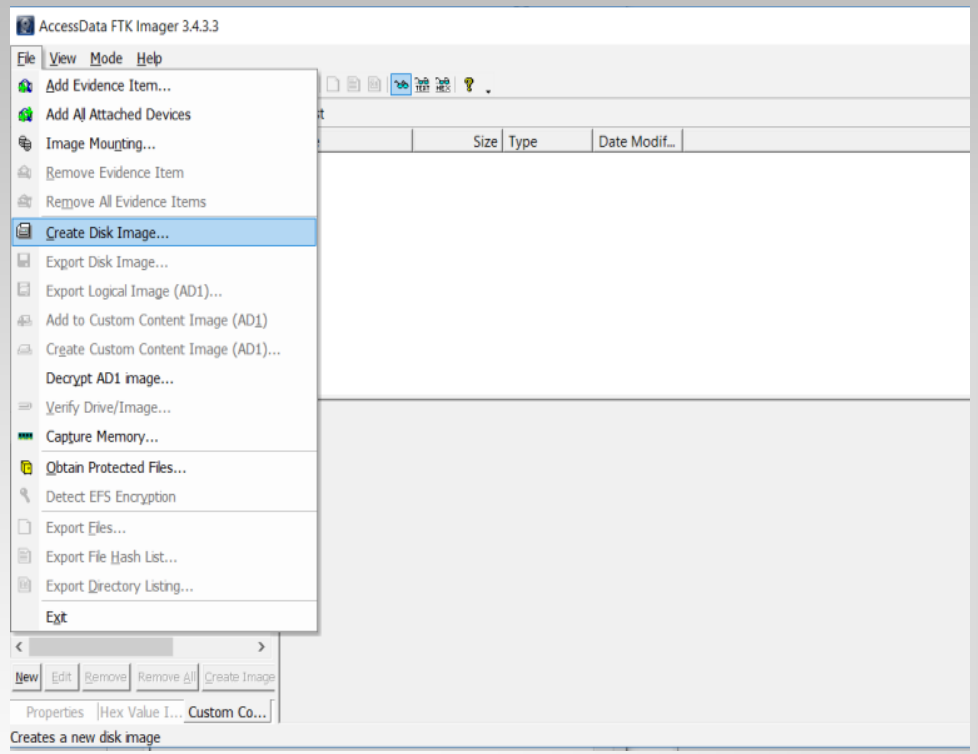
Forenzika računara

- Forenzika računara je relativno nova oblast, i razvija se u poslednjih 20-25 godina.
- Računari su više počeli da se koriste 70-tih godina prošlog veka, a računarski kriminalitet ima šire razmere od 90-tih god XX veka.
- Računarska forenzika istražuje računarske uređaje korišćenjem naučnih metoda za iznošenje dokaza tako da se oni mogu predstaviti na sudu.

Generalne smernice

- Što manje uticaja na dokaz što je moguće (ispitivati a ne menjati, imati jasan trag svega što je izmenjeno, obezbediti dokaz).
- **Ne "dirati" sumnjiv disk**
  - Ne menjati sistem u procesu istraživanja
  - Napraviti 1 (2) kopije originalnog drajva.
  - Kreiranje hash vrednosti sumnjivog drajva (da budemo sigurni da ništa nije menjano)
  - Pravljenje imidža drajva sa forenzičkim alatom

Forenzički alat



- FTK Imager (AccessData): jednostavan i besplatan, a poprilično pouzdan za kreiranje imidža drajva i “mountovanje” imidža koji su kreirani.

Da li se može obavljati forenzika na radnoj mašini?

- Opšta preporuka: kreiranja imidža drajva i analiza nad njim.
- Ali nekad je potrebno obaviti forenziku nad živim podacima. Potrebno je objasniti zašto je urađeno, i biti siguran da koraci koji su preuzeti imaju malo uticaja na sistem.
  - Analiza nad procesima koji se izvršavaju (pre isključivanja mašine).
  - Neophodno u oblaku i klasterima...

Trag dokumenta

- **Dokumentovati sve**
- Ako se otkrije kompjuterski kriminal, moraju se dokumentovi događaji koji su se otkrili:
  - Ko je aktivan, šta je radio
  - Koji uređaji su zakačeni za računar
  - Koje veze su postojale preko mreže/interneta
  - Koji harver/operativni sistem je korišćen

Dokumetovanje traga

- Ako se započne forenzička istraga mora se dokumentovati svaki korak:
  - Dokumentovanje procesa koji se koristi da se napravi forenzička kopija
  - Dokumentovanje svakog alata koji je korišćen, svakog testa koji je izvršen...
  - Potrebno je da se prikaže sve što je urađeno.

Obezbeđivanje dokaza

- Računar treba da se isključi da bi se izbeglo dalje ometanje.
- Postoje ograničene okolnosti kada mašina je online da bi pratila aktivni napad koji se odigrava, ali u opštem slučaju je treba isključiti
- Sledeći korak je da se ograniči pristup mašini, hard drajv treba zaključati na bezbedno mesto ili sobu. Analiza se obavlja u sobi sa ograničenim pristupom.
- Mora se dokumentovati ko ima pristup dokazima, kako se postupa sa njima i gde je sačuvana evidencija i to u svakom trenutku: **CHAIN OF CUSTODY: kontinuitet dokaznom materijala, lanac očuvanja integriteta dokaza.**

Lanac očuvanja integriteta dokaza (chain of custody)

- *Chain of custody:* ključni element forenzičke nauke, odnosi se na detaljnu dokumentaciju koja pokazuje status dokaza u svakom trenutku vremena od trenutka napada do momenta predstavljanja na sudu.
- Bilo kakav prekid u tom procesu će verovatno učiniti da je dokaz neprihvatljiv na sudu.
- **"The chain of custody must include a description of the evidence and a documented history of each evidence transfer" (Prema Scientific Working Group on Digital Evidence Model Standard Operation Procedures for Computer Forensics).**
- Ne postoji mogućnost da je predokumentovano!! Navesti detalje šta je rađeno, koji alati su korišćeni, ko je prisutan, ko je izvršio koje testove, screenshoots i dr.

FBI smernice za forenziku

- Pored opštih, FBI navodi i neke specifične
- Prikupiti što više podataka o incidentu: uraditi backup kopiju logova, uništenih/izmenjenih fajlova,fajlove koje je ostavio napadač, ili ukoliko je napad u toku
- Dokumentovati specifične gubitke zbog napada kao i sam napad (cena: rada potrošenog na odgovoru i oporavku; uništene opreme, podatka…)
- Naglašena važnost očuvanja dokaza (ne može se ograničiti koncept računarske evidencije na PC i labtop, pa USB uređaji, ekst. diskovi, ipod, iPad, firewall..)
- Pravljene forenzičke kopije sumnjivog drajva/particije da bi se radilo sa kreiranjem hash vrednostima tog drajva.

U.S. Secret Service smernice za forenziku

- Zlatna pravila za započinjanje istraživanja:
  - Obezbediti scenu i učiniti je sigurnom
  - Ako smatrate da računar je uključen u kriminal koji istažjuje, preduzeti odmah korake da se sačuvaju dokazi.
  - Odrediti da li postoje legalne osnove za zaplenu računra
  - Izbeći pristupanje računarskim fajlovima. Ako je računar uključen, ići na odgovarajući deo kako da se propisno obori i spremi za prenošenje dokaza.
  - Ako smatrate da računar uništava dokaz, odmah oboriti računar izvlačenjem kabla sa zadnje strane računara.
  - Ako je kamera dostupna i računar je on, uzeti slike računarskog ekrana. Ako je računar off, uzeti sliku računara, lokacije računara i zakačenih elektronskih medija.

  Ovo su sve važni prvi koraci koji očuvaju *chain of custody* i obezbeđuju integrerit istraživanja.

Budipeštanksa konvencija za sajber kriminal

- EU ima 5 principa koji čine osnovu za elektronske dokaze:
  - Princip 1: Integritet podataka (dokaz da su podaci validni)
  - Princip 2: Revizorski trag (slično kao chain of cusdody)
  - Princip 3: Podrška specijaliste
  - Princip 4: Odgovarajući trening
  - Princip 5: Zakonitost (svi dokazi su sakupljeni i obrađeni na odgovarajući način u skladu sa zakonom)

SWGDE- Scientific Working Group on Digital Evidence

- SWGDE- www.swgde.org kreira brojne standarde za digitalnu forenziku; brojni dokumenti
- Prema SWDGE Model Standard Operation Procedures for Computer Forensics, postoje četiri koraka ispitivanja:
  1. Vizuelni pregled
  2. Forenzikčki duplikat (poželjno raditi sa kopijom ne sa originalnom)
  3. Ispitivanje medija (hard disk, RAM, SIM kartica..)
  4. Vraćanje dokaza na odgovarajuću lokaciju i njihovo obezbeđivanje (zaključavanje)

Lokardova prinicp razmene

- Dr Edmond Locard- forenzičar-naučnik
- Princip je prvo bio primenjen na fizičku forenziku, u suštini kaže da ne može se interagovati sa bilo kakvim okruženjem bez ostavljanja nečega iza sebe. Npr. Ako neko provali u kuću ostavlja nešto iza sebe.
- Može se primeniti i na računarsku forenziku→ zato se radi sa kopijom a ne sa originalom;
- Npr. Windows: svaki put nakon prijave, otvaranja fajla, dolazi do promene u Registry-ju→ istražitelji moraju da budu oprezni da ne ostave trag iza sebe.

ALATI

- FTK (AccessData http://accessdata.com: Forensic Toolkit): robustan kompjuterski forenzički alat koji omogućava oporavak obrisanih fajlova, ispitivanje Registry-ja, i izvođenje brojnih forenzičkih zadataka.
- Sam softver može biti skup al je popularan u sprovođenju zakona.
- FTK pretražuje i otkirva fajlove uključne u dečju pornografiju.

EnCase

- Popularan i direktna konkurencija FTK.
- Omogućava kreiranje imidža drajva, oporavak obrisanih fajlova, ispitivanje Registry-ja, i dr.
- Komercijalni proizvod, skuplji.
- https://www.guidancesoftware.com/encase-forensic

OSForensics

- Noviji alat, ali lepo prihvaćen u forenzičkom društvu.
- Komercijalan, jeftiniji i jednostavan za korišćenje.
- Ima puno funkcija, omogućava oporavak obrisanih fajlova, ispitivanje regisrtry-ja, i pretraživanje drajva.
- Ima i probna verzija: www.osforensics.com

Sleuth Kit (www.sleuthkit.org)

- Suit open source alata, malo komplikovaniji za korišćenje.
- Svaki od alata zahteva učenje skupa komandnih linija komandi za izvršavanje.

Oxygen (www.oxygen-forensic.com/en)

- Za forenziku telefona: posebno za iPhones.
- Nije (bar sada) toliko efikasan sa starijim verzijama Androida ili Windows telefona.

Cellebrite (cellebrite.com)

- Jedan od najpopularnijih forenzičkih alata za telefone.
- Veoma je efikasan sa brojnim telefonima.
- Mana izuzetno je skup.

NALAŽENJE DOKAZA NA PC

Nalaženje dokaza na PC

Nakon kreiranja forenzičke kopije, analiza:

- Nalaženje dokaza u Browseru (npr. izvor direktnog dokaza, posrednog ili podržava, npr. dečja pornografija, sajber zlostavljanje; za kreiranje virusa npr. pretraživanje oblasti kreiranja virusa (iako se izbriše istorija pretraživanja, informacije se čuvaju u index.dat: search queries..)
- Nalaženje dokaza u sistemskom logu
- Vraćanje obrisanih fajlova

Nalaženje dokaza u sistemskom logu

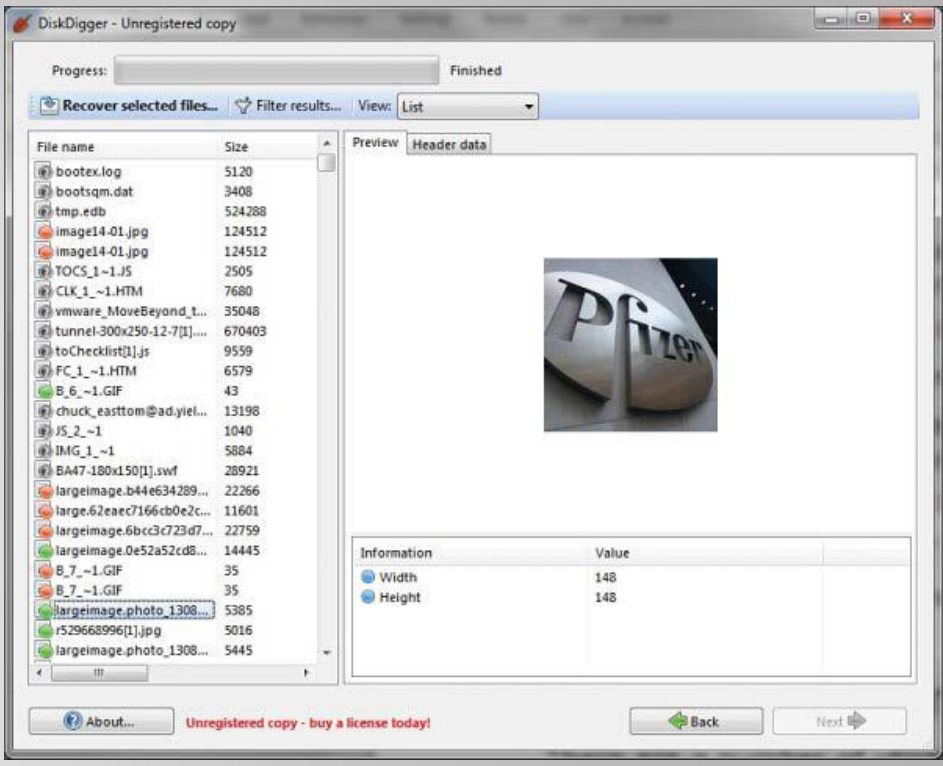
- Bez obzira koji se operativni sistem koristi, postoji njihov log i on je kritičan u svakoj forenzičkoj istrazi i treblo bi da se koristi.
- Windows logs
  - Windows 7/8/10: Start button→ControlPanel→Admistrative Tools→Event Viewer.
  - Podesiti logging on.

Windows logovi

- **Security log-** najznačajniji sa stanovišta forenzičara. Ima uspešne/neuspešne login događaje.
- **Application log-** Ovaj log sadrži različite događaje prijavljivanja aplikacije ili programa. Mnoge aplikacije će snimati svoje greške u logu aplikacije.
- **System log-** Sadrži događaje logovanja Windows sistemskih komponenti; uključuje događaje kao pad drajvera;
- **ForwardedEvents log:** The ForwardedEvents log se koristi da sačuva događaje od udaljenih (remote) računara. Imaće podatke u njima ako je prosleđivanje događaja konfigurisano**.**
- **Applications and Services logs:** koristi se da sačuva događaje od jedne aplikacije ili komponente pre nego događaji koji imaju uticaja na celi sistem.
- Napomena:
- 1. sve verzije Windowsa nemaju sve logove.
- 2. Mogućnost brisanja loga, uklanjanja određenih stavki, postavljanja on/off

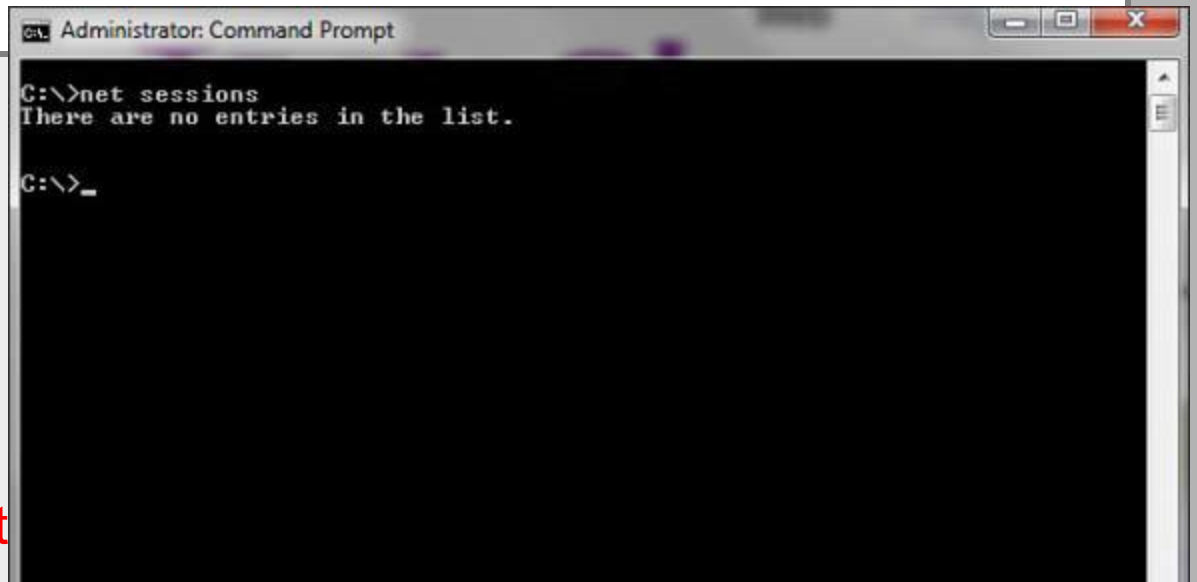
Oporavak izbrisanih fajlova

- Izbrisane fajlove je moguće povratiti pomoću aplikacija poput Disk Digger
- **DiskDigger**: jednostavan, besplatan alat.
- Ne mogu svi fajlovi da se oporave



Ostalo

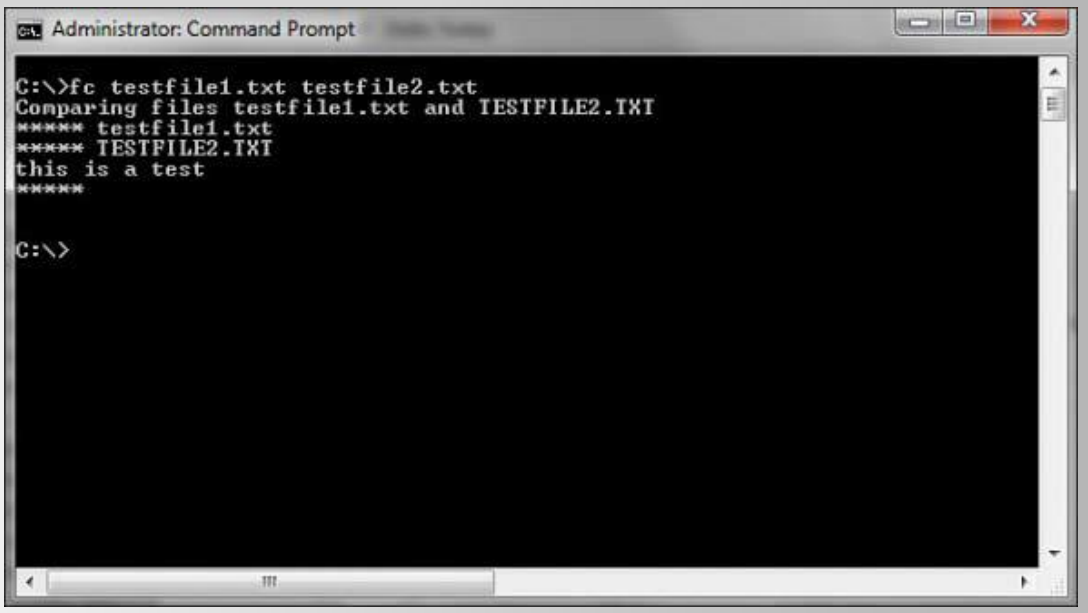
- Postoje brojne mogućnosti (alati) ugrađeni u operativni sistem, posebno za izvršavanje live da bi se uhvatio napad u progresu.
- Net sessions: prikazaće bilo koju aktivnu sesiju povezanu na računar na kojoj se izvršava.
- Openfiles – prikazuje deljenje fajlove koji su otvoreni, za prikazivanje aktivnog napada.
- Netstat –Izlistava sve trenutne mrežne konekcije- ulazne/izlazne, kao i tekući napad.



aut

FC komanda

Fc komanda proverava dva fajla i prikazuje razlike. Npr. Uporediti fajl za konfigurisanje sa poznatim back up om.



Windows Registry

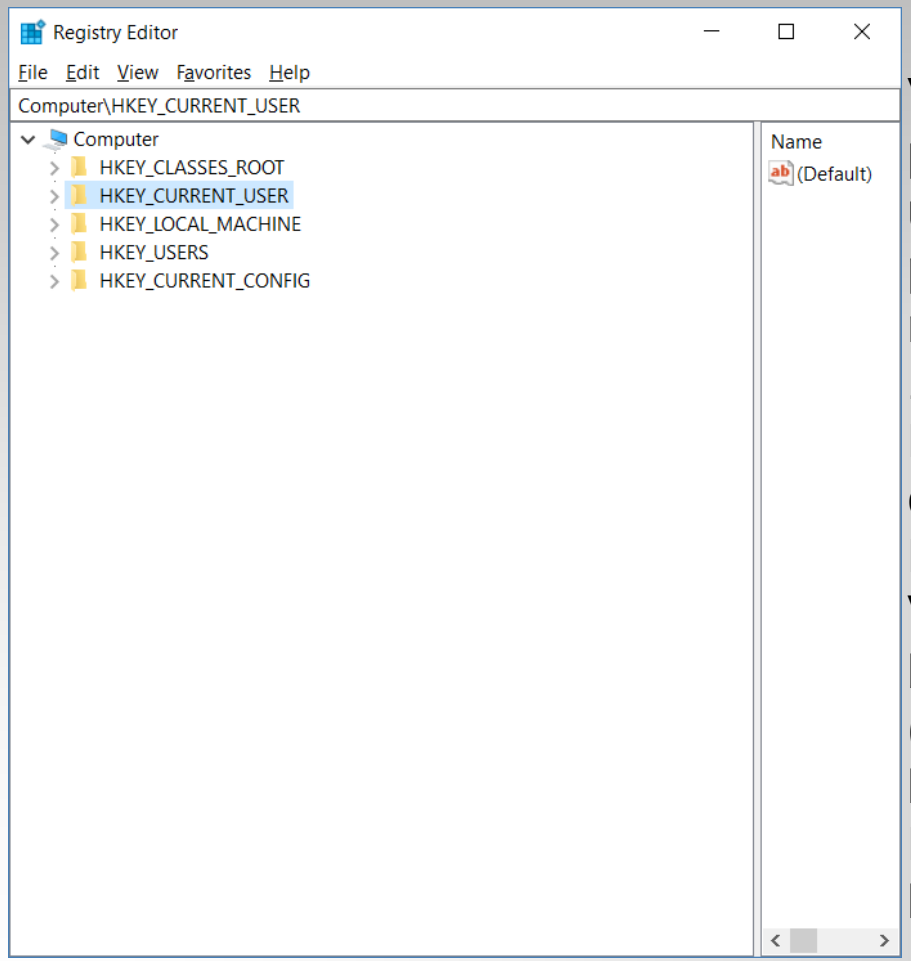
- Windows Registry je izvanredan izvor potenicajlno vrednih forenzičkih informacija. To je srce Windowsa.
- **Regedit tool** za inerakciju sa Registy (Windows +R)

- Microsoft opisuje Registry: “A central hierarchical database used in the Microsoft Windows family of Operating Systems to store information necessary to configure the system for one or more users, applications and hardware devices. The registry contains information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents that each can create, property sheet settings for folders and application icons, what hardware exists on the system and the ports that are being used.”

Windows Registry
organizovan u 5 delova (hives):

- HKEY_CLASSES_ROOT (HKCR)- drag&drop pravila, prečice za program, korisnički intefejs, ...
- HKEY_CURRENT_USER (HKCU): !! Info o trenuntom korisniku, i njegova podešavanja
- HKEY_LOCAL_MACHINE (HKLM)!: sadrži podešavanja za mašinu
- HKEY_USERS (HKU)!!: sadrži profile za sve korisnike i odgovajuća podešavanja
- HKEY_CURRENT_CONFIG (HCU): sadrži trenutnu konfiguraciju sistema.

Regedit (Windows+R)



Vrednosti u Registry-ju kad je poslednji put rađena izmena, u FILETIME strukturi koji predstavlja brpj od 100-nanosekudi intervalu od 1.1.1601.

MS retko korisiti jaku enkripciju da sakrije stavke u Registy-ju

Većina je sačuvana kao 16-bitni Unicode karakteri (2bajta, max 65536 karaktera)

EXPORT podataka: desni klik Export

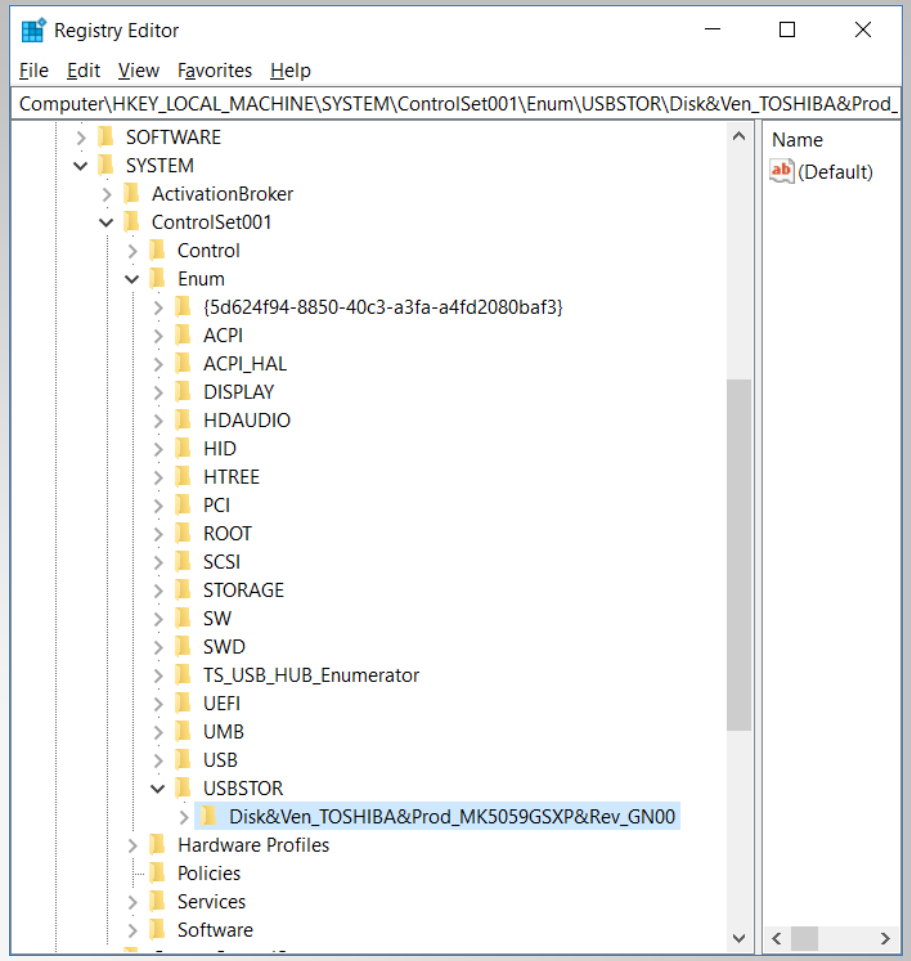
Specifični ulazi

- Često se uzimaju podaci na eksterne uređaji,kao USB
- HKEY_LOCAL_MACHINE\System\ControlSet\Enum\USBSTOR
  - prikazuje USB uređaje koji su bili povezani na računar.
- ID proizvođača i proizvoda može se naći ovde:

  SYSTEM\CurrentControlSet\Enum\USB

  …
- Svi relevantni USB Registry key trebaju da se pretraže da bi se dobila kompletna i tačna slika šta se desilo korišćenjem specifičnog USB uređaja.

HKEY_LOCAL_MACHINE\System\ControlSet\Enum\USBSTOR



Primer: autostart

- Prikazuje programe koji su konfigurisani da pokrenu se kada se pokrene i Windows, ukoliko se tu pojavljuje neki neuobičajeni može da upućuje na virus:
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Primer: Poslednja poseta

- Poslednja poseta: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
- Ovaj ključ pokazuje skore sajtove koji su posećeni. Podaci su u hex formatu (prevod uz regedit)
- Skorašnji dokument: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU

Deinstaliranje softvera

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
- Važan forenzički ključ
- Instaliranje softvera za različite svrhe kao brisanje fajlova ili kreiranje zadnjih vrata. On bi, obrisao softver koji se koristi.
- Steganografija.

Mobilna mreža

- Mobilna mreža je zasnovana na radio stanicama a svaka stanica se sastoji od antene i radio opreme.
- Global System for Mobile Communication GSM, 2G; prvenstevno samo za glas.
- **UMTS:** Universal Mobile Telecommunications Systems: 3G, omogućava prenos tekst, video, glas i multimediju 2Mb/s.
- LTE: **Long Term Evolution (4G)** omogućava Internet, multimediu i glas. Zasnovano na GSM/EDGE tehnologiji. Teoretski dostiže brzine od 300Mb/s. Za razliku od GSM-sličnih mreža, LTE je zasnovano na IP adresi kao i klasičan računar.

Šta se traži?

- Detalji samog telefona (br.modela, serijski br SIM kartice, operativni si…)
- Istorija poziva
- Slike i video
- GPS informacije
- Informacije mreže (npr. ako je tel. Povezan na kafić bizu mesta zločina→indikacija)

Forenzička sertifikacija

- Čemu sertifikacija?
  - Ispunjavanje min. standarda
- Sajber forenzika:
  - Sertifikacija proizvođača (najčešće povezana za jedan ili više proizvoda proizvođača): AccessData ima brojne sertifikacije za svoj proizvod; Gidance Software: EnCase.
  - Konceptualna sertifikacija: za forenzičke koncepte, ne specifičan alat.
- EC-Council: Certified Hacking Forensics Investigator test.

Forenzička sertifikacija

- ISC2: Certified Cyber Forensics Investigator (CCFP)
- SANS Instut: Certified Forensics Analyst (GCFA) i Certified Forensics Examiner (GCFE) $$$

Svedok ekspert

- Forenzičar ispitivač može biti pozvan na potvrdi na sudu.
- Federal Rule 702:
  - Ekspert mora biti ekspert u toj specifičnoj oblasti ili polju.
  - Svedočenje te osobe mora biti korisno sudiji/poroti da bi razumeli tehničke/specijalizovane činjenice o slučaju.
  - Svedočenje mora da se zasniva na pouzdanim naučnim metodama.

Daubert-ov standard

- Daubert standard se koristi u U.S. federalnom sudu da odredi da li ili ne ekspertska naučna metoda je zasnovana na rasuđivanju ili metodologiji koja je naučno validna i može se adekvatno primeniti na činjenice.
- Da li je metodologija validna:
  - Teorije ili tehnike u pitanjima su testirane
  - Ili su objavljene
  - Poznata je potencijalna greška
  - Postojanje i održavanje standarda kontroliše operaciju
  - Ili je prihvaćeno u okviru relevantne naučne zajednice.

Forenzika mreže

- Forenzika mreže podrazumeva presretanje mrežnih paketa koji putuju preko mreže i istraživanje za dokaze, kao npr. odakle dolaze *paketi*, koji protokol se koristi, koji se port koristi i da li je enkripitovan ili ne.

Forenzika mreže

- Wireshark: www.wireshark.org
- CommView: www.tamos.com/products/commview/
- Softperfect Network Protocol Analyzer: www.softperfect.com
- HTTP Sniffer: www.effetech.com/sniffer/
- ngrep: http://sourceforge.net/projects/ngrep/

Virtualna forenzika

- Virtualizacija je način da se obezbede različiti IT resursi koji su nezavisni od fizičke mašine korisnika, tj. čine logičke IT resurse koje mogu da mogu da budu nezavisni od krajnjeg korisnika OS kao i hardvera.
- Osnovna zahtev za forenziku je situacija gde sumnjiva mašina ima virtualnu mašinu koja se izvršava na njoj.

Literatura

- Easttom II, W. C. (2016). *Computer security fundamentals*. Pearson IT Certification; ch 14. (354-387)

Dodatna literatura

- Korać, V. (2014). DIGITALNA FORENZIKA U FUNKCIJI ZAŠTITE INFORMACIONOG SISTEMA BAZIRANOG NA LINUX I WINDOWS PLATFORMAMA, doktorska disertacija
- Milosavljević M., Grubor G., *Digitalna forenzika računarskog sistema, Univerzitet Singidunum, Beograd 2009.*
- Filipić, K., & Protrka, N. (2016). Uloga forenzičkog softvera EnCase pri radu s elektroničkim tragovima. *Kriminalistička teorija i praksa*, *3*(2/2016.), 121-134.
- NIST - Computer Forensics Tool Catalog: https://toolcatalog.nist.gov/index.php