Dnevnik rada

Prije početka semestra (03.02.-02.03.2014.)

Kontaktiran mentor s preddiplomskog projekta mr.sc. Predrag Pale te dogovorena suradnja oko suradnje na predmetu Završni rad. Kao kontakt osoba za rad postavljen je asistent sa ZESOI-ja mag.ing. Kristian Skračić.

Na inicijalnom sastanku je raspravljano o temama iz područja informacijske sigurnosti, s posebnim naglaskom na socijalni inžinjering te računalnu forenziku. Kao moguća tema je predložen “Dumpster diving”, pretraga odbačenog poslovnog materijala u potrazi za korisnim informacijama.

Na kasnijim sastancima tema “Dumpster diving” je odbačena zbog manjka akademskih radova koji bi se koristili kao reference te potrebe da u sklopu Završnog rada bude implementirano neko programsko rješenje.

Na idućem sastanku je kao područje rada odabrana računalna forenzika, dok odabrana tema Završnog rada glasi “Programski alat za automatiziranu forenzičku analizu GPS uređaja”.

Daljnji koraci

Daljni koraci u ovoj fazi su bili općenito zadani te su se uglavnom odnosili na upoznavanje s temom.

1. tjedan (03.-09.03.2014.)

Održan sastanak u vezi razrade ideje programa. Aplikacija je koncipirana kao bitovni parser koji prolazi kroz trajnu memoriju GPS uređaja te pronalazi relevantne podatke. Zbog lakoće korištenja i prethodne izrade fakultetskih projekata u njemu, za jezik u kojem će se implementirati programsko rješenje je odabran Python.

Daljnji koraci

Kao daljni koraci su zadani pronalazak python biblioteke za učitavanje/čitanje FAT32 podatkovnog sustava, izrada demo inačice s USB memorijom, pokušati čitati podatkovni sustav u binarnom modu i pronaći obrisane datoteke te pronalazak datoteke koja automatski prepoznaje tip datoteke.

2. tjedan (10.-16.03.2014.)

Vezano uz traženje python biblioteka koje će se koristiti učitavanje i čitanje slike, nađena su dva koja prema opisima odgovaraju potrebana projekta: Hachoir (https://bitbucket.org/haypo/hachoir/wiki/Home) i Glance (http://docs.openstack.org/developer/python-glanceclient/). Nažalost, pobližim pregledom uočen je izuzetan manjak dokumentacije i primjera korištenja navedenih razreda te se odustalo od njihovog korištenja.

Daljnji koraci

Kao prioritet u daljnjim koracima je navedeno upoznavanje s datotečnim sustavima te osmišljavanje koncepta “ručnog” čitanja podataka, bez specijaliziranih biblioteka za takvu vrstu operacija.

3. tjedan (17.-23.03.2014.)

Upoznavanje s računalnim datotečnim sustavima, posebice sustavom FAT32. Kao službena literatura i materijal s posebno dobro objašnjenim elementima datotečnih sustava je uzeta knjiga:

“File System Forensic Analysis”, Brian Carrier, 2005

Osim navedene knjige, za službenu literaturu i reference su uzeti idući naslovi i poveznice:

“Recover data from corrupted drives”, SOFT_RAJAT (http://www.codeproject.com/Articles/696388/Recover-Data-From-Corrupted-Drives-File-Systems-FA)

“Partition Tables Explained”, Elias Bachaalany

“Grow Your Own Forensic Tools: A Taxonomy of Python Libraries Helpful for Forensic Analysis”, T.J.OConnor

http://www.datarescue.com/laboratory/partition.htm

Također, održan je tjedni sastanak na kojem su raspravljeni daljnji koraci i riješene administrativne obaveze vezane uz Završni rad. Preuzeta datoteka koja sadrži presliku podataka (engl. Image) GPS uređaja marke TomTom.

Daljnji koraci

Nastavak proučavanja datotečnih sustava, analiza slike uređaja s nekim od alata otvorenog koda te početak pisanja koda koji će čitati binarnu datoteku, prolaziti po istoj te vraćati podatke s njihovim odgovarajućim značenjem.

4. tjedan (24.-.30.03.2014.)

Upoznavanje s MBR (Master Boot Record) u sklopu datotečnih sustava. Upoznavanje s VBR (Volume Boot Record) u sklopu FAT32 datotečnog sustava. Detaljno proučena struktura MBR-a te dokumentiran svaki relevantan oktet unutar sektora koji sadrži MBR.

Daljnji koraci

Održan tjedni sastanak na kojem su razjašnjene neke nedoumice u vezi datotečnih sustava te dogovoren nastavak rada na prošlotjednim zadacima.

5. tjedan (31.03.-06.04.2014.)

Analiza utvrđenih činjenica vezanih uz datotečne sustave te provjera tih zaključaka na praktičnom primjeru, bitovno identičnoj slici USB memorije napravljenoj pomoću Windows alata ImageUSB. Ručna provjera ključnih vrijednosti sadržanih unutar okteta navedene slike pomoću alata HXD. Analiza slike GPS uređaja obavljena je Windows inačicom alata Autopsy.

Daljnji koraci

Zbog činjenice da slika memorije TomTom uređaja koristi Linuxov datotečni sustav, potrebno je fokus proučavanja preusmjeriti s FAT32 na Linux sustave. Također, krenuti s pisanjem koda koja “šeće” po slici te analizira podatke.

6. tjedan (07.-13.04.2014.)

Napisan kod u programskom jeziku Python koji čita, analizira te u datoteku upisuje MBR sektor dobivene slike diska, odnosno memorije.

Daljnji koraci

Nastaviti s učenjem o Linux datotečnom sustavu te napisati ostatak koda koji pronalazi relevantne podatke na dobivenoj slici.

7. tjedan (14.-20.04.2014.)

Pauza zbog učenja za međuispite te ostalih fakultetskih projekata i zadaća.