KAUNO TECHNOLOGIJOS UNIVERSITETAS

KOMPIUTERIŲ KATEDRA

NUSIKALTIMAI ELEKTRONINĖJE ERDVĖJE IR JŲ TYRIMŲ METODIKOS

T120M152

Laboratorinio darbo Nr. 3 ataskaita

INFORMACIJOS IŠTYRIMAS ĮRENGINIO DARBINĖJE ATMINTYJE

Atliko: IFM-1/3 gr.

Stud. Eligijus Kiudys

Patikrino:

Kaunas, 2022

Laboratorinis darbas Nr. 3.

Elektroninių pėdsakų darbinėje atmintyje ištyrimas ir bylos sudarymas

Darbo priemonės

1. Darbinės atminties atvaizdas – įkalčiai – Prieinamas MS Teams: **General > Darbinis > RAM**;
2. Darbinės atminties analizės įrankis – Volatility;
3. AutoPSY (http://www.sleuthkit.org/autopsy/) ftp:// Prisijungimo vardas: anonymous; Naudoti KTU VPN (Klases) prisijungimą atliekant darbą namuose;
4. Galima naudoti ir šiame sąraše nepateiktą programinę įrangą.

Darbo scenarijus:

Kompiuterio naudotojas Almantas Karvelis, buvo nužudytas, dėl galimo bendradarbiavimo su Valstybinėmis institucijomis arba, dėl kibernetinių išpuolių prieš “KTU TELEKOM” organizaciją. Policijos skyrius kompiuterio poėmio metu atliko visus reikiamus veiksmus ir prieš išjungiant kompiuterį padarė darbinės atminties atvaizdą. Tačiau nepadarė kontrolės sumos pateikdami kartu su visais įkalčiais, todėl aponentai ginčija darbinės atminties tinkamumui pridėti prie bendros bylos. Policijos skyrius prašo pagalbos ir užduoda klausimus į kuriuos prašo atsakymų ir paaiškinimų tam, kad galėtų darbinės pateiktą atminties atvaizdą (ne-) susieti su Almantu Karveliu.

Darbo tikslas

Atlikti darbinės atminties atvaizdo kopijos analizę ir atsakyti į tyrėjų pateiktus klausimus. Parengti tyrimo ataskaitą su atsakytais klausimai ir padarytomis išvadomis. Vėliau papildyti ir pateikti AutoPSY programine įranga sudarytą Almanto Karvelio bylą.

Darbo uždaviniai

1. Naudojant Volatility surinkti informaciją iš darbinės atminties atvaizdo.
2. Pateikti darbo rezultatų išvadas.
3. Papildyti jau suformuotą ataskaitą.

UŽDUOTYS

Naudojantis elektroninių nusikaltimų ištyrimų priemonėmis, atsakyti į žemiau pateiktus klausimus:

1 Ar galite nustatyti tiksle datą ir laiką (laikas turi būti nurodytas pagal Jūsų laiko juostą) kada buvo atliktas darbinės atminties poėmis?

Pavadinimas (atvaizdo)	Data	Laikas
KAUNAS-20160907-142601.raw	2016-09-07	16:26:21

2. Ar galite nustatyti darbinės atminties atvaizde pateiktos operacinę sistemą arba jos šeima?

Pavadinimas (atvaizdo)	Operacinė sistema arba jos šeima
KAUNAS-20160907-142601.raw	Windows 8 SP1 x64

3. Ar galite nustatyti darbinės atminties atvaizde procesorių ar branduolių (CPU Core) kiekį?

Pavadinimas (atvaizdo)	CPU Core
KAUNAS-20160907-142601.raw	4

4. Ar galite nustatyti darbinės atminties atvaizde paleistų programų kurios siejamos su debesų paslaugomis (duomenų talpyklos) paleidimo datą ir laiką (laikas turi būti nurodytas pagal Jūsų laiko juostą)?

Pavadinimas (programos)	Paleidimo data	Paleidimo laikas
BoxSync.exe	2016-09-07	16:17:34
googledrivesyn	2016-09-07	16:17:50

5. Ar galite nustatyti darbinės atminties atvaizde paleistų programų, kuri buvo naudojama el. paštui, paleidimo datą ir laiką (laikas turi būti nurodytas pagal Jūsų laiko juostą)?

Pavadinimas (programos)	Paleidimo data	Paleidimo laikas
Thunderbird	2016-09-07	16:18:07

6. Ar galite nustatyti darbinės atminties atvaizde paleistų programų, kur ar kokį (galimai) elektroninė paštą skaito naudotojas?

Pavadinimas (programos)	IP adresas, prievadas	Pastaba (kokiam el. pašto paslaugos tiekėjui galite priskirti)
Thunderbird	74.125.133.109:993	Gmail

7. Ar galite nustatyti kokie yra disko skirsniai ir / ar buvo prijungti šifruoti (kokie) disko skirsniai (“partitions”)

symlinkscan

Pavadinimas (skirsnio)	Prijungta iš...	Prijungta į	Pastaba (jei reikia paaiškinti skirsnio pavadinimą)
	Harddisk0Partition1	\Device\HarddiskVolume1	
C:	Harddisk0Partition2	\Device\HarddiskVolume2	
E:	Harddisk0Partition3	\Device\HarddiskVolume3	
X:	Harddisk0Partition4	\Device\HarddiskVolume4	
F:	Harddisk1Partition1	\Device\HarddiskVolume5	Tai diskas žmogaus, dariusio poėmį
D:		\Device\CdRom0	

8. Ar galite išvardinti kokią programinę įrangą (bent 5), naudojantis paleistų failų išvedimu, galimai naudojo kompiuterio naudotojas?

Eil. Nr.	Pavadinimas (programinės įrangos)	Įkaltis	Pastaba (jei reikia paaiškinti pasirinkimą)
1	Box sync	C:\Program Files\Box\Box Sync\SQLite.Interop.dll	
2	Google drive sync	\Device\HarddiskVolume2\Users \ALMANT~1\AppData\Local\Google\Drive\ user_default\snapshot.db	
3	Thunder Bird	\Device\HarddiskVolume2\Users\Almantas Karvelis\AppData\ Roaming\Thunderbird\Profiles\luhl9gdo.default\cert8.db	
4	Internet Explorer	\Device\HarddiskVolume2\Users\Almantas Karvelis\AppData \Local\Packages\windows_ie_ac_001\ AC\InetCache	

		\GA9UG1HG\erotinesprekes_125x125_b[1].png	
5	7-zip	\Device\HarddiskVolume2\Program Files\7-Zip\7-zip.dll	

9 Ar galite nustatyti kompiuteriui priskirtą IP adresą (parašyti pastabą iš kur daroma tokia prielaida)?

IP adresas	Pastaba
192.168.0.200	Komanda „volatility.exe py.h -f F:\RAM\KAUNAS-20160907-142601.raw --profile=Win8SP0x64 netscan“

10. Ar galite nustatyti atvaizde pateiktų bibliotekų (1-3) informaciją?

Pavadinimas (failas)	Pavadinimas (Kompanijos sukūrusios biblioteką)	Failo versiją	Produkto versiją
sqlite3.dll	Robert Simpson, et al.	1.0.94.0	1.0.94.0
python27.dll	Python Software Foundation	2.7.9	2.7.9

2832 BoxSync.exe 0x000000001e000000 True True True \PROGRA~1\Box\BOXSYN~1\python27.dll

2832 BoxSync.exe 0x00007ff9827a0000 True True True \PROGRA~1\Box\BOXSYN~1\sqlite3.dll

11. Ar galite nustatyti kokia ir kada (laikas turi būti nurodytas pagal Jūsų laiko juostą) programine įranga padarytas darbinės atminties atvaizdas?

Pavadinimas (programos)	Data	Laikas
DumpIt.exe	2016-09-07	16:26:21

IŠVADA

Išanalizuoti visko puikiai neišėjo, bet pagrindiniai procesai ir failai buvo išnagrinėti. Poėmis priklauso tam pačiam asmeniui, kadangi analizės metu apalnaklų pavadinimai buvo jo vardas ir pavardė. Naudojamos programos taip pat sutampa. Padarius laboratorinį darbą buvo išmokta naudotis naujai įrankiais.