KAUNO TECHNOLOGIJOS UNIVERSITETAS

KOMPIUTERIŲ KATEDRA

NUSIKALTIMAI ELEKTRONINĖJE ERDVĖJE IR JŲ TYRIMŲ METODIKOS

T120M152

Laboratorinio darbo Nr. 1 ataskaita

KOMPIUTERINĖS INFORMACIJOS IŠTYRIMAS

REGISTRAS

Atliko: IFM-1/3 gr.

Stud. Eligijus Kiudys

Patikrino:

Kaunas, 2022

# Laboratorinis darbas Nr. 1.

**Kompiuterinių įkalčių tyrimas ir bylos sudarymas**

## Darbo priemonės

1. Hyper-V, VMplayer, VirtualBox įkalčių OS;
2. Kompiuterio kietojo disko atvaizdas; NEE įkalčių atvaizdas; NEE įkalčių registras.
3. AccessData Registry Viewer;
4. Sysinternals paketas;
5. Microsoft File Checksum Integrity Verifier (kontrolinių sumų skaičiavimas);
6. Regripper;
7. FTP prieiga (įkalčių disko atvaizdai ir registrai – NEE katalogas; FCIV – TOOLS katalogas ) ftp://IP Prisijungimo vardas: anonymous; Naudoti KTU VPN (Klases) prisijungimą atliekant darbą namuose;
8. Galima naudoti ir šiame sąraše nepateiktą programinę įrangą (Programinės įrangos paketas yra pateiktas MS TEAMS TOOLS kataloge.

## Darbo scenarijus:

*Kompiuterio vartotojas Almantas Karvelis, buvo nužudytas, dėl galimo bendradarbiavimo su Valstybinėmis institucijomis arba dėl kibernetinių išpuolių prieš “KTU TELEKOM” organizaciją. Policijos skyrius atliko poėmio kratas ir sulaikė A. K. darbo (workstation) kompiuterį. DVI (pirmoji gr. – neporiniai; antroji gr. poriniai skaičiai tyrėjų-studentų grupės sąraše) grupės tirs įkalčių surinkimo tinkamumą ir bandys išsiaiškinti galimas nužudymo priežastis. Reikia atlikti kompiuterio kietojo disko tyrimą ieškant galimų vartotojo atliktų veiksmų įrodymų atliekant veiklos požymių.*

## Darbo tikslas

Atlikti kietojo disko atvaizdo kopijos analizę: registrų, istorijos, prisijungimo (login/password), el. pašto, debesų kompiuterijos paslaugų(“clouds computing”) analizę, ir pateikti išvadas, įvardinant įkalčių sąsajumą (neprivaloma).

Tyrimui pateikiama kompiuterio kietojo disko atvaizdo kopija, kuriame yra sekanti informacija: Windows registrai ir veiksmų istorija, esanti failuose NTUSER.DAT, SAM, SECURITY, SYSTEM, SOFTWARE, DEFAULT, naršyklės istorija, vartotojo profilio istorija, vartotojo paieškos istorija, prisijungimų duomenys, debesų kompiuterijos duomenų sinchronizacijos informacija). Kiekvienai **(viso 2)** grupei analizuojant pateiktą disko atvaizdą, naudojant elektroninių nusikaltimų tyrimo įrankius, reikės sugeneruoti HTML arba TXT tipo ataskaitas (“output”). Sugeneruotas ataskaitas reiks pateikti po užduoties klausimais. Toliau naudojant ( AutoPSY “The Sleuth Kit”) programinę įrangą, reikės sudaryti bylą, prie kurios reiks ridėti ankščiau sugeneruotas ataskaitas.

**UŽDUOTYS**

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

Naudojamos sistemos konfigūracijos numeris (Default konfiguracijos numeris atitinka naudojama ControlSet numerį, toliau pažymėtą kaip XXX)*SYSTEM\Select\Default*

|  |
| --- |
| 001 |

Kompiuterio operacinės sistemos pavadinimas (OS name)*SOFTWARE\Microsoft\Windows NT\CurrentVersion/ProductName*

|  |
| --- |
| Windows 8.1 Pro |

Įdiegto atnaujinimų rinkinio numeris (most recent service pack installed)*SOFTWARE\Microsoft\Windows NT\CurrentVersion/CSDVersion*

|  |
| --- |
| 6.3 |

OS įdiegimo katalogas (OS installation folder path)*SOFTWARE\Microsoft\Windows NT\CurrentVersion/PathName*

|  |
| --- |
| C:/Windows |

OS įdiegimo data (OS installation date)*SOFTWARE\Microsoft\Windows NT\CurrentVersion/InstallDate*

|  |
| --- |
| 2016-09-02 22:32:44 GMT+03:00 |

Registruotas kompiuterio savininkas (Registered Owner)*SOFTWARE\Microsoft\Windows NT\CurrentVersion/RegisteredOwner*

|  |
| --- |
| Almantas Karvelis |

Registruotas organizacijos pavadinimas (Registered Organization)*SOFTWARE\Microsoft\Windows NT\CurrentVersion/RegisteredOrganization*

|  |
| --- |
| Reikšmė nenustatyta |

Kompiuterio vardas (Computer Name)*SYSTEM\ControlSetXXX\Control\ComputerName/ComputerName*

|  |
| --- |
| KAUNAS |

Kompiuterio laiko juostos nustatymai (Computer Time Zone Information) *SYSTEM\ControlSetXXX\Control\TimeZoneInformation/StandardName*

|  |
| --- |
| Laiko juosta FLE Standard Time (UTC+02:00). Standartinis laikas įvedamas paskutinį spalio sekmadienį 4:00, vasaros laikas įvedamas paskutinį kovo sekmadienį 3:00. |

Tinklo plokščių informacija (NetworkCards information)*SOFTWARE\Microsoft\Windows NT\CurrentVersion\ NetworkCards\#*

|  |  |
| --- | --- |
| Pavadinimas/  Description | Identifikatorius/  ServiceName |
| (1) Realtek PCIe GBE Family Controler | {7BDB37D7-DF90-4E3A-95E0-FA85D8CB7009} |
| (2) Realtek RTL8191SE Wireless LAN 802.11n PCI-E NIC | {16BF4516-0C45-4EC9-AE24-1CF55DA247B2} |

Kompiuterio tinklo plokščių nustatymai „Default“ sistemos konfigūracijos rinkinyje (Networks adapter‘s configuration in the Default configuration profile) *SYSTEM\ControlSetXXX\Services\Tcpip\Parameters\Interfaces*

|  |  |  |
| --- | --- | --- |
| Pavadinimas/  Description | Tinklo plokštės konfigūracija/ Network adapter configuration | |
| (3) Realtek RTL8191SE Wireless LAN 802.11n PCI-E NIC | EnableDHCP | 1 |
| DhcpIPAddress | 192.168.0.200 |
| IPAddress | - |
| DhcpSubnetMask | 255.255.255.0 |
| SubnetMask | - |
| DhcpServer | 192.168.0.1 |
| DefaultGateway | - |
| DefaultGatewayMetric | - |
| NameServer | Reikšmė nenustatyta (value not set) |
|  |  |
| (1) Realtek PCIe GBE Family Controler | EnableDHCP | 1 |
| DhcpIPAddress | - |
| IPAddress | - |
| DhcpSubnetMask | - |
| SubnetMask | - |
| DhcpServer | - |
| DefaultGateway | - |
| DefaultGatewayMetric | - |
| NameServer | Reikšmė nenustatyta (value not set) |
|  |  |

Kokios USB atminties talpyklos buvo prijungtos prie kompiuterio *SYSTEM\ControlSetXXX\Enum\USBSTOR*

|  |  |
| --- | --- |
| Registro šakos pavadinimas | Pavadinmas/FriendlyName |
| Disk&Ven\_ADATA&Prod\_USB\_Flash\_Drive&Rev\_1.00 | ADATA USB Flash Drive USB device |
| Disk&Ven\_SanDisk&Prod\_Cruzer\_Fit&Rev\_1.00 | SanDisk Cruzer Fit USB device |

Kompiuterio vartotojų informacija (vartotojai, vartotojų prisijungimo laikai ir kartai, SID) *SAM\Domains\Account\Users*

|  |  |  |  |
| --- | --- | --- | --- |
| Vartotojas/  User Name | SID | Paskutinis prisijungimo laikas/  Last Logon Time | Prisijungimų kiekis/  Logon Count |
| Administrator | 000001F4 | 2013 – 08 – 22 14:47:09 UTC | 1 |
| Almantas Karvelis | 000001F5 | 2016 – 09 – 02 10:33:30 UTC | 4 |
| Guest | 000003E9 | Niekada | 0 |

Vėliausiai (paskutinis) prisijungęs vartotojas ir jo prisijungimo laikas *SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon* (DefaultUserName, Last Written Time)

|  |
| --- |
| (Value not set) 2016 – 09 – 07 14:16:51 |

Kokia programinė įranga buvo įdiegta kompiuteryje *SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*

|  |  |  |
| --- | --- | --- |
| Pavadinimas/  DisplayName | Įdiegimo katalogas/  Install Location | Įdiegimo data/  Last written time |
| LibreOffice 5.2.0.4 | C:\ProgramFiles (x86)\ LibreOffice 5\ | 9/5/2016 13:36:33 UTC |
| Gpg4win (2.3.3) | C:\ ProgramFiles (x86)\GNU\GnuPG | 9/2/2016 10:08:40 UTC |
| Mozilla Firefox 48.0.2 (x86 en-US) | C:\Program Files (x86)\Mozilla Firefox | 9/2/2016 10:02:09 UTC |
| Mozilla Thunderbird 45.3.0 (x86 en-US) | C:\Program Files (x86)\Mozilla Thunderbird | 9/2/2016 10:04:57 UTC |
| Google Drive | C:\ProgramFiles (x86)\ Google | 9/2/2016 10:28:00 UTC |

Podėlyje (angl. cache) rastas BoxSync diegimo failas (2016 – 09 – 02 13:48:50)

Ar kompiuteryje buvo įdiegta antivirusinė programa, kokia ji (pagal įdiegtos programinės įrangos sąrašą) ir jos įdiegimo data

|  |
| --- |
| Windows Defender 9/7/2016 14:16:51 UTC |

Kokia programinė įranga buvo naudojama kompiuteryje dažniausiai *NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\750...*

|  |  |  |  |
| --- | --- | --- | --- |
| Vykdytos programos pavadinimas/  Value Name ROT13 | Paskutinis vykdymo laikas/  Time | Vykdymų kiekis/  Times Executed | Trumpas programos aprašymas |
| {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Mozilla Thunderbird.lnk | 9/7/2016 14:19:08 UTC | 9 | El. pašto skaitymo PĮ „Thunderbird“ |

Kokia programine įranga vartotojas naudojosi paskutinio prisijungimo metu?

|  |
| --- |
|  |
|  |
|  |

Operacinės sistemos įkrovos metu vykdomos programos (Nurodytos registro šakos gali būti tuščios, arba šakų gali visiškai nebūti )

*SOFTWARE \Software\Microsoft\Windows\CurrentVersion\Runonce*

*SOFTWARE \Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run*

*SOFTWARE \Software\Microsoft\Windows\CurrentVersion\Run*

*NTUSER.DAT \Software\Microsoft\Windows NT\CurrentVersion\Windows\Run*

*NTUSER.DAT \Software\Microsoft\Windows\CurrentVersion\Run*

*NTUSER.DAT \Software\Microsoft\Windows\CurrentVersion\RunOnce*

|  |
| --- |
| "C:\Program Files\Box\Box Sync\BoxSync.exe" -m |
| "C:\Program Files (x86)\Google\Drive\googledrivesync.exe" /autostart |

Kokios internetinės naršyklės buvo įdiegtos kompiuteryje *SOFTWARE\Clients\StartMenuInternet*

|  |
| --- |
| FIREFOX.EXE |
| IEXPLORE.EXE |

Kokia naršyklė naudojama kaip numatytoji

*SOFTWARE\Classes\http\shell\open\command*

*SOFTWARE\Clients\StartMenuInternet / default*

|  |
| --- |
| IExplore.exe |

Kokie URL adresai buvo įvesti Internet Explorer naršyklėje *NTUSER.DAT\Software\Microsoft\Internet Explorer\Typed URLs*

|  |  |
| --- | --- |
| Numeris | URL adresas |
| 1 | http://google.com/ |
| 2 | http://live.com/ |
| 3 | http://hotmail.com/ |
| 4 | http://www.mozila.org/en-US/thunderbird |
| 5 | http://www.mozila.org/ |
| 6 | http://go.microsoft.com/fwlink/p/?LinkId=255141 |

Kokie URL adresai buvo įvesti kituose naršyklėse

Kita naršyklė buvo naudota tik Mozila firedox

|  |  |
| --- | --- |
| 1 | https://www.mozilla.org/en-US/firefox/central/ |
| 2 | https://www.mozilla.org/en-US/firefox/help/ |
| 3 | https://www.mozilla.org/en-US/firefox/customize/ |
| 4 | https://www.mozilla.org/en-US/contribute/ |
| 5 | https://www.mozilla.org/en-US/about/ |
| 6 | http://go.microsoft.com/fwlink/p/?LinkId=255142 |
| 7 | place:sort=8&maxResults=10 |
| 8 | http://www.bing.com/search?q=7-zip&src=IE-TopResult&FORM=IETR02&conversationid= |
| 9 | http://www.bing.com/search?q=thunderbird&FORM=IE8SRC |
| 10 | http://www.bing.com/search?q=almantas+karveis&src=IE-TopResult&FORM=IETR02&conversationid= |
| 11 | http://www.bing.com/search?q=gnupg&src=IE-TopResult&FORM=IETR02&conversationid= |
| 12 | http://www.msn.com/?ocid=iehp |
| 13 | https://www.gpg4win.org/get-gpg4win.html |
| 14 | https://www.gpg4win.org/thanks.html |
| 15 | https://www.gpg4win.org/download.html |
| 16 | http://www.7-zip.org/ |
| 17 | https://www.mozilla.org/en-US/thunderbird/ |
| 18 | https://www.mozilla.org/en-US/firefox/products/ |
| 19 | https://www.mozilla.org/en-US/firefox/new/?scene=2 |
| 20 | https://www.mozilla.org/fr/thunderbird/ |
| 21 | https://www.mozilla.org/en-US/firefox/desktop/ |
| 22 | https://www.mozilla.org/en-US/ |
| 23 | place:type=6&sort=14&maxResults=10 |
| 24 | https://www.mozilla.org/en-US/firefox/48.0.2/firstrun/ |
| 25 | https://www.mozilla.org/en-US/firefox/48.0.2/firstrun/learnmore/ |
| 26 | https://www.google.com/search?q=gnupg&ie=utf-8&oe=utf-8 |
| 27 | https://www.google.com/search?q=gnupg&ie=utf-8&oe=utf-8#q=win4pgp |
| 28 | https://www.gpg4win.org/ |
| 29 | https://files.gpg4win.org/gpg4win-2.3.3.exe |
| 30 | https://www.google.com/search?q=gdrive&ie=utf-8&oe=utf-8&client=firefox-b-ab |
| 31 | https://www.google.lt/search?q=gdrive&ie=utf-8&oe=utf-8&client=firefox-b-ab&gfe\_rd=cr&ei=RFDJV5T7C4Sr8weG-J7ACA |
| 32 | https://www.google.com/search?q=gdrive&ie=utf-8&oe=utf-8&client=firefox-b-ab&gfe\_rd=cr&ei=RFDJV5T7C4Sr8weG-J7ACA |
| 33 | https://www.google.com/drive/ |
| 34 | https://accounts.google.com/ServiceLogin?service=wise&passive=true&continue=http%3A%2F%2Fdrive.google.com%2F%3Futm\_source%3Den%26utm\_medium%3Dbutton%26utm\_campaign%3Dweb%26utm\_content%3Dgotodrive%26usp%3Dgtd%26ltmpl%3Ddrive&urp=https%3A%2F%2Fwww.google.com%2F |
| 35 | https://accounts.google.com/ServiceLogin?service=wise&passive=true&continue=http%3A%2F%2Fdrive.google.com%2F%3Futm\_source%3Den%26utm\_medium%3Dbutton%26utm\_campaign%3Dweb%26utm\_content%3Dgotodrive%26usp%3Dgtd%26ltmpl%3Ddrive&urp=https%3A%2F%2Fwww.google.com%2F#identifier |
| 36 | https://accounts.google.com/ServiceLogin?service=wise&passive=true&continue=http%3A%2F%2Fdrive.google.com%2F%3Futm\_source%3Den%26utm\_medium%3Dbutton%26utm\_campaign%3Dweb%26utm\_content%3Dgotodrive%26usp%3Dgtd%26ltmpl%3Ddrive&urp=https%3A%2F%2Fwww.google.com%2F#password |
| 37 | https://accounts.google.com/signin/challenge/sl/password#password |
| 38 | https://www.google.lt/search?q=gdrive&ie=utf-8&oe=utf-8&client=firefox-b-ab&gfe\_rd=cr&ei=hFLJV-rjMIeA8Qfuv5CgBg |
| 39 | https://www.google.com/search?q=gdrive&ie=utf-8&oe=utf-8&client=firefox-b-ab&gfe\_rd=cr&ei=hFLJV-rjMIeA8Qfuv5CgBg |
| 40 | https://accounts.google.com/CheckCookie?checkedDomains=youtube&checkConnection=youtube%3A1188%3A1&pstMsg=1&chtml=LoginDoneHtml&service=wise&continue=https%3A%2F%2Fdrive.google.com%2F%3Futm\_source%3Den%26utm\_medium%3Dbutton%26utm\_campaign%3Dweb%26utm\_content%3Dgotodrive%26usp%3Dgtd%26ltmpl%3Ddrive&gidl=CAwSAggM |
| 41 | https://security.google.com/settings/security/interstitials/recoveryoptions?authuser=0&hl=en&service=wise&continue=https%3A%2F%2Faccounts.google.com%2FServiceLogin%3Fcontinue%3Dhttps%253A%252F%252Fdrive.google.com%252F%253Futm\_source%253Den%2526utm\_medium%253Dbutton%2526utm\_campaign%253Dweb%2526utm\_content%253Dgotodrive%2526usp%253Dgtd%2526ltmpl%253Ddrive%26service%3Dwise%26hl%3Den%26authuser%3D0%26passive%3Dtrue%26ncpl%3D1%26sarp%3D1%26aodrpl%3D1%26checkedDomains%3Dyoutube%26checkConnection%3Dyoutube%253A1188%253A1%26pstMsg%3D1 |
| 42 | https://accounts.google.com/ServiceLogin?service=accountsettings&passive=1209600&osid=1&continue=https://security.google.com/settings/security/interstitials/recoveryoptions?authuser%3D0%26hl%3Den%26service%3Dwise%26continue%3Dhttps://accounts.google.com/ServiceLogin?continue%253Dhttps%25253A%25252F%25252Fdrive.google.com%25252F%25253Futm\_source%25253Den%252526utm\_medium%25253Dbutton%252526utm\_campaign%25253Dweb%252526utm\_content%25253Dgotodrive%252526usp%25253Dgtd%252526ltmpl%25253Ddrive%2526service%253Dwise%2526hl%253Den%2526authuser%253D0%2526passive%253Dtrue%2526ncpl%253D1%2526sarp%253D1%2526aodrpl%253D1%2526checkedDomains%253Dyoutube%2526checkConnection%253Dyoutube%25253A1188%25253A1%2526pstMsg%253D1&followup=https://security.google.com/settings/security/interstitials/recoveryoptions?authuser%3D0%26hl%3Den%26service%3Dwise%26continue%3Dhttps://accounts.google.com/ServiceLogin?continue%253Dhttps%25253A%25252F%25252Fdrive.google.com%25252F%25253Futm\_source%25253Den%252526utm\_medium%25253Dbutton%252526utm\_campaign%25253Dweb%252526utm\_content%25253Dgotodrive%252526usp%25253Dgtd%252526ltmpl%25253Ddrive%2526service%253Dwise%2526hl%253Den%2526authuser%253D0%2526passive%253Dtrue%2526ncpl%253D1%2526sarp%253D1%2526aodrpl%253D1%2526checkedDomains%253Dyoutube%2526checkConnection%253Dyoutube%25253A1188%25253A1%2526pstMsg%253D1&hl=en |
| 43 | https://security.google.com/accounts/SetOSID?continue=https%3A%2F%2Fsecurity.google.com%2Fsettings%2Fsecurity%2Finterstitials%2Frecoveryoptions%3Fhl%3Den%26service%3Dwise%26continue%3Dhttps%253A%252F%252Faccounts.google.com%252FServiceLogin%253Fcontinue%253Dhttps%25253A%25252F%25252Fdrive.google.com%25252F%25253Futm\_source%25253Den%252526utm\_medium%25253Dbutton%252526utm\_campaign%25253Dweb%252526utm\_content%25253Dgotodrive%252526usp%25253Dgtd%252526ltmpl%25253Ddrive%2526service%253Dwise%2526hl%253Den%2526authuser%253D0%2526passive%253Dtrue%2526ncpl%253D1%2526sarp%253D1%2526aodrpl%253D1%2526checkedDomains%253Dyoutube%2526checkConnection%253Dyoutube%25253A1188%25253A1%2526pstMsg%253D1%26pli%3D1&osidt=ALWU2cvOlKeESuA42CliASozItJQZunh26xqLOCKLRYuymoWEqmS1XD41pVR9cNrxM6aoTqWYOpTcdpeC-s\_xTp2f0jfqflEeS3npUzZzGuaxzAY0ItbWnB3F7JFRxAiGezWBl9Z4Qmv |
| 44 | https://security.google.com/settings/security/interstitials/recoveryoptions?hl=en&service=wise&continue=https%3A%2F%2Faccounts.google.com%2FServiceLogin%3Fcontinue%3Dhttps%253A%252F%252Fdrive.google.com%252F%253Futm\_source%253Den%2526utm\_medium%253Dbutton%2526utm\_campaign%253Dweb%2526utm\_content%253Dgotodrive%2526usp%253Dgtd%2526ltmpl%253Ddrive%26service%3Dwise%26hl%3Den%26authuser%3D0%26passive%3Dtrue%26ncpl%3D1%26sarp%3D1%26aodrpl%3D1%26checkedDomains%3Dyoutube%26checkConnection%3Dyoutube%253A1188%253A1%26pstMsg%3D1&pli=1 |
| 45 | https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2Fdrive.google.com%2F%3Futm\_source%3Den%26utm\_medium%3Dbutton%26utm\_campaign%3Dweb%26utm\_content%3Dgotodrive%26usp%3Dgtd%26ltmpl%3Ddrive&service=wise&hl=en&authuser=0&passive=true&ncpl=1&sarp=1&aodrpl=1&checkedDomains=youtube&checkConnection=youtube%3A1188%3A1&pstMsg=1 |
| 46 | https://accounts.youtube.com/accounts/SetSID?ssdc=1&sidt=ALWU2cvbawdYlTyZ3cK6FptOhKCJDvu7Lg2d3LMetb6RgY4%2FH%2BeQpIoGE0nHxFXXNIhQignZOsxO3jJHwUjWHacIEPihaCymN%2BS0zJXJwaS6%2BfcYChUv0TLnWk6sjeLM2ooJ6435xNoYZ08F%2BlRnPJllDj0IKwGAlJBKiAtyjMy1DaO75ZaGKFvwDlORlrRlzXsnZ%2BYJA0B0T16H93MHzzdvlTaE8ilTkmbg77CKM2KznkOfGnDMCGPb2qc604MioqODGYcd8spMbswCLDPMfJ%2BJeQvhnzlPCMCRi2dlqUlj1Wny8U%2FLy8o%3D&continue=https%3A%2F%2Fdrive.google.com%2F%3Futm\_source%3Den%26utm\_medium%3Dbutton%26utm\_campaign%3Dweb%26utm\_content%3Dgotodrive%26usp%3Dgtd%26ltmpl%3Ddrive%26pli%3D1%26auth%3DtgNKKFO0nH-MqdYH-HVDypHWSuD5SRRonGObRv2QwuhRh6vgOmcr8WoNPqKcqLD5KA2Deg.%26authuser%3D0&dbus=LT |
| 47 | https://accounts.google.lt/accounts/SetSID?ssdc=1&sidt=ALWU2ctZkOezKhKdWgB8N0pLlr4sGW7dABwsxqjpfXzi3ZIwkA0wLDOxtBiw5OaeVExUfcc5u0QZL6QWKcAljsrNWhPtU4nRPpNOhnPZd4OFWcnfHDy69%2Bq9XbTcQtn4RaypM6BkVCgo18UtC6crOD3TJBM6WxJbDV%2F59if052HfPFjcJMNUSKY5JkxMpWdRAPh2qlqICwXcb65zX0TPi1SfachtBu3mSGNCoFChDSDisP0c2lqdAD8GDex3mKKASLc7m2jljsT2g7yXMdn1%2FTxvC5gRca%2B4MaGej22Ktj6x6298W03fVAA%3D&continue=https%3A%2F%2Fdrive.google.com%2F%3Futm\_source%3Den%26utm\_medium%3Dbutton%26utm\_campaign%3Dweb%26utm\_content%3Dgotodrive%26usp%3Dgtd%26ltmpl%3Ddrive%26pli%3D1%26auth%3DtgNKKFO0nH-MqdYH-HVDypHWSuD5SRRonGObRv2QwuhRh6vgOmcr8WoNPqKcqLD5KA2Deg.%26authuser%3D0 |
| 48 | https://drive.google.com/?utm\_source=en&utm\_medium=button&utm\_campaign=web&utm\_content=gotodrive&usp=gtd&ltmpl=drive&pli=1&auth=tgNKKFO0nH-MqdYH-HVDypHWSuD5SRRonGObRv2QwuhRh6vgOmcr8WoNPqKcqLD5KA2Deg.&authuser=0 |
| 49 | https://drive.google.com/?utm\_source=en&utm\_medium=button&utm\_campaign=web&utm\_content=gotodrive&usp=gtd&ltmpl=drive&pli=1&authuser=0# |
| 50 | https://drive.google.com/drive/?ltmpl=drive&usp=gtd&utm\_campaign=web&utm\_content=gotodrive&utm\_medium=button&utm\_source=en# |
| 51 | https://drive.google.com/drive/# |
| 52 | https://drive.google.com/drive/my-drive |
| 53 | https://g.co/getdrive |
| 54 | https://www.google.com/drive/download/ |
| 55 | https://tools.google.com/dlpage/drive/index.html?hl=en#eula |
| 56 | http://dl.google.com/tag/s/appguid%3D%7B3C122445-AECE-4309-90B7-85A6AEF42AC0%7D%26iid%3D%7B8E58D411-11FA-F460-B5DD-B97F14806756%7D%26lang%3Den%26browser%3D3%26usagestats%3D0%26appname%3DGoogle%2520Drive%26needsadmin%3Dtrue/drive/googledrivesync.exe |
| 57 | https://tools.google.com/dlpage/drive/thankyou.html?hl=en |
| 58 | https://dl.google.com/tag/s/appguid%3D%7B3C122445-AECE-4309-90B7-85A6AEF42AC0%7D%26iid%3D%7B8E58D411-11FA-F460-B5DD-B97F14806756%7D%26lang%3Den%26browser%3D3%26usagestats%3D0%26appname%3DGoogle%2520Drive%26needsadmin%3Dtrue/drive/googledrivesync.exe |
| 59 | http://hotmail.com/ |
| 60 | https://mail.live.com/default.aspx |
| 61 | https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1472812134&rver=6.4.6456.0&wp=MBI\_SSL\_SHARED&wreply=https:%2F%2Fmail.live.com%2Fdefault.aspx%3Frru%3Dinbox&lc=1033&id=64855&mkt=en-us&cbcxt=mai |
| 62 | https://login.live.com/login.srf?lc=1033&sf=1&id=64855&tw=18000&fs=0&ts=-1&cbcxt=mai&sec=&mspp\_shared=1&seclog=10&claims=&wa=wsignin1.0&wp=MBI\_SSL\_SHARED&ru=https://mail.live.com/default.aspx%3frru%3dinbox |
| 63 | https://mail.live.com/default.aspx?rru=inbox |
| 64 | https://bay175.mail.live.com/default.aspx?rru=inbox |
| 65 | https://bay175.mail.live.com/?tid=cm6M444V8e5RGPjQAhWtfWyA2&fid=flinbox |
| 66 | https://bay175.mail.live.com/?fid=flinbox |
| 67 | https://bay175.mail.live.com/?tid=cmK7FyIAle5hG7q9idZ1x5wg2&fid=flinbox |
| 68 | https://bay175.mail.live.com/?tid=cm5SqY1BwI5hGPCxBgS7LiYA2&fid=flinbox |
| 69 | http://gmail.com/ |
| 70 | https://gmail.com/ |
| 71 | https://mail.google.com/mail/ |
| 72 | https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&scc=1&ltmpl=default&ltmplcache=2&emr=1&osid=1 |
| 73 | https://mail.google.com/accounts/SetOSID?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F%3Fpli%3D1%26auth%3DtgNKKNUKJrpWOeMBSbsM-gHn761usmQ3Beu-WxUgfSobJCtIZ6MgCfAFmRZAGWUdZSVR1Q.&osidt=ALWU2ct74pS9cZ0UpZ45AXfEHx65xDtFABYNE4pay-cjgZRV3RclPby2NZBTPOKbKLSyQBOhAMD4hQaZQrXPww\_8NyFXBpeHBriMHFPLPVriEWvHWj6Z4BbKGTahCCmY2ltx-SHZnrNY |
| 74 | https://mail.google.com/mail/?pli=1&auth=tgNKKNUKJrpWOeMBSbsM-gHn761usmQ3Beu-WxUgfSobJCtIZ6MgCfAFmRZAGWUdZSVR1Q. |
| 75 | https://mail.google.com/mail/?pli=1 |
| 76 | https://mail.google.com/mail/#inbox |
| 77 | https://mail.google.com/mail/#inbox/156ea6f278f8a595 |
| 78 | https://mail.google.com/mail/#inbox/156ea744fbcb4be8 |
| 79 | https://www.google.com/search?q=box+sync&ie=utf-8&oe=utf-8&client=firefox-b |
| 80 | https://www.google.lt/search?q=box+sync&ie=utf-8&oe=utf-8&client=firefox-b&gfe\_rd=cr&ei=hFbJV5G1Lo2r8wepj57YDg |
| 81 | https://www.google.com/search?q=box+sync&ie=utf-8&oe=utf-8&client=firefox-b&gfe\_rd=cr&ei=hFbJV5G1Lo2r8wepj57YDg |
| 82 | https://www.google.com/?client=firefox-b#q=box+sync&gfe\_rd=cr |
| 83 | https://www.box.com/file-sharing |
| 84 | https://www.box.com/en-gb/file-sharing |
| 85 | https://account.box.com/login |
| 86 | https://mail.google.com/mail/#inbox/15180d07d50f81ff |
| 87 | https://mail.google.com/mail/#inbox/1517b9bdd8652cf2 |
| 88 | https://mail.google.com/mail/#inbox/1508c43c8f999573 |
| 89 | https://mail.google.com/mail/#inbox/1504954b67c77d19 |
| 90 | https://mail.google.com/mail/#inbox/14e963584f96ab42 |
| 91 | https://mail.google.com/mail/#inbox/14e530ec6daeb348 |
| 92 | https://mail.google.com/mail/#inbox/14d09e11ae067dad |
| 93 | https://onedrive.live.com/ |
| 94 | https://onedrive.live.com/?id=root&cid=60AB0CCA314CE2E0 |
| 95 | https://g.live.com/8SESkyDrive/SkyDriveApps?biciid=lhnlink |
| 96 | https://onedrive.live.com/about/?page=download&biciid=lhnlink |
| 97 | https://onedrive.live.com/about/en-gb/download |
| 98 | https://onedrive.live.com/about/en-gb/download/ |
| 99 | https://go.microsoft.com/fwlink/p/?LinkId=248256 |
| 100 | http://g.live.com/1rewlive5skydrive/skydrivesetup |
| 101 | https://oneclient.sfx.ms/Win/Direct/17.3.6517.0809/OneDriveSetup.exe |
| 102 | https://app.box.com/login/assertion?a=lacLiveV1%21ET7cOvCOfEQAZDGlM6ypDuWvYvDUcjrnIU5urlnAt8P6SvncyHuHuuDh\_sdohDZpC\_5ecbj00qD27ohlIaaZIVglL05GeX9fIJOtTzs-QYYKrshhSN05GjxOaCbF-x-HmgQ2YDLCfgb0hDT2bj2s9mL3&redirect\_url=%2F |
| 103 | https://app.box.com/ |
| 104 | https://app.box.com/files |
| 105 | http://plus.google.com/ |
| 106 | https://plus.google.com/ |
| 107 | https://app.box.com/settings/sync |
| 108 | https://e3.boxcdn.net/box-installers/sync/Sync+4+External/BoxSyncSetup.exe |
| 109 | https://app.box.com/settings/account |
| 110 | https://app.box.com/files/0/f/0 |
| 111 | https://plus.google.com/collections/ |
| 112 | https://plus.google.com/s |
| 113 | https://plus.google.com/communities/104313824247294134329 |
| 114 | http://kaunas.lt/ |
| 115 | http://www.kaunas.lt/ |
| 116 | http://www.kaunas.lt/wp-admin |
| 117 | http://www.kaunas.lt/meras/apie-mera/ |
| 118 | http://www.kaunas.lt/meras/mero-komanda/ |
| 119 | http://ktu.edu/ |
| 120 | http://ktu.edu/lt |
| 121 | https://dvs.ktu.lt/ |
| 122 | http://pastas.ktu.lt/ |
| 123 | https://pastas.ktu.lt/ |
| 124 | https://pastas.ktu.lt/horde |
| 125 | https://login.ktu.lt/simplesaml/saml2/idp/SSOService.php?SAMLRequest=fVJNb4IwGP4rpHdpQRFthITpYSZuksF22GUpWKVZaTveso9%2FPxDdXLJ46aXPd94FsFoamrS2Ug%2F8reVgnc9aKqDHjwi1jaKagQCqWM2B2pJmyd2G%2Bi6hptFWl1oiJwHgjRVaLbWCtuZNxpt3UfLHh02EKmsNUIwNA8vAfbWtKy3OKlEUWnJbuQAa96I%2BTrdZjpxVl0Io1uv9sqU%2BCHUmg6iN5H1E3D8%2BFjuDs2x7snVNZZCzXkXoZT4bByWfkjCYzEi5nwXMC6ehvydeEczD%2BbiDAbR8rbpsykbIJ950ROYj4uceoYFPx5Nn5KSnpjdC7YQ6XJ%2BlGEBAb%2FM8HQ2VnngDxzodAMWLPjQ9GjcXc1%2BXZeeNUfz%2FovCz6AJfGAxuht53iutVqqUov5xESv2xbDizPEIewvFA%2BXsJ8Tc%3D&RelayState=ss%3Amem%3A9645000f5ceedbbf7811565b8db249d1 |
| 126 | https://login.ktu.lt/simplesaml/module.php/core/loginuserpass.php?AuthState=\_7d31e015dbcaafae7b90cd2ad70ee6b80fe0ed1905%3Ahttps%3A%2F%2Flogin.ktu.lt%2Fsimplesaml%2Fsaml2%2Fidp%2FSSOService.php%3Fspentityid%3Dhttps%253A%252F%252Fpastas.ktu.lt%252Fshibboleth%26cookieTime%3D1472813555%26RelayState%3Dss%253Amem%253A9645000f5ceedbbf7811565b8db249d1 |
| 127 | https://uais.cr.ktu.lt/ktuis/ |
| 128 | https://uais.cr.ktu.lt/ktuis/stp\_prisijungimas |
| 129 | https://uais.cr.ktu.lt/ktuis/auth.autologin |
| 130 | https://login.ktu.lt/simplesaml/saml2/idp/SSOService.php?SAMLRequest=hVJNT4MwGP4rpPdRCg5HM0hwO7hkOiLowYspUEdjabFv8ePfC2PqvMxLL32%2B8y6BtbKjaW8bdcdfew7W%2BWilAnr4iFFvFNUMBFDFWg7UVjRPb7bUdz3aGW11pSVyUgBurNBqpRX0LTc5N2%2Bi4vd32xg11nZAMe6ZALcy7ovtXWkxNKIsteS2waOij7NdXiBnPUQQio1iv1Sp90L9EEXbST7mw%2BPjY1F3OM93R0%2B3azrkbNYxeqrLReRd8Es2fw5D4gXVooxISKLAm9cRC4IBBtDzjQLLlI2R75Fw5kUzzy%2BIR%2BcBJeQROdmx5pVQtVD785uUEwjodVFks6nSAzdwqDMAULIcQ9ODsTnZ%2Brws%2Bx4YJf%2FOucQnDpNdR28Hyc0601JUn04qpX5fGc4sjxFBOJkof%2B8g%2BQI%3D&RelayState=ss%3Amem%3Ab84ef170f51290351e1aaed269f532fcb8858a8c3b05597a4c2b9a4aa80a8c80 |
| 131 | https://login.ktu.lt/simplesaml/module.php/core/loginuserpass.php?AuthState=\_55a56ec70afb957b127cf5dcb38e5297cb05ca411e%3Ahttps%3A%2F%2Flogin.ktu.lt%2Fsimplesaml%2Fsaml2%2Fidp%2FSSOService.php%3Fspentityid%3Dhttps%253A%252F%252Fuais.cr.ktu.lt%252Fshibboleth%26cookieTime%3D1472813591%26RelayState%3Dss%253Amem%253Ab84ef170f51290351e1aaed269f532fcb8858a8c3b05597a4c2b9a4aa80a8c80 |
| 132 | https://bay175.mail.live.com/?page=Compose |
| 133 | https://plus.google.com/communities/recommended |
| 134 | http://delfi.lt/ |
| 135 | http://www.delfi.lt/ |
| 136 | http://www.delfi.lt/news/medijos-karas-propaganda/v-putinas-medaliu-apdovanojo-vsd-ataskaitoje-minima-lietuvos-politika.d?id=72197774 |
| 137 | http://www.delfi.lt/news/daily/world/v-putinas-bandymas-perziureti-antrojo-pasaulinio-karo-rezultatus-atvertu-pandoros-skrynia.d?id=72197002 |
| 138 | https://www.google.com/search?q=telekomo+saugumas&ie=utf-8&oe=utf-8&client=firefox-b |
| 139 | https://www.google.lt/search?q=telekomo+saugumas&ie=utf-8&oe=utf-8&client=firefox-b&gfe\_rd=cr&ei=UFTNV-mvO4er8wfKqqCICA |
| 140 | https://www.google.com/search?q=telekomo+saugumas&ie=utf-8&oe=utf-8&client=firefox-b&gfe\_rd=cr&ei=UFTNV-mvO4er8wfKqqCICA |
| 141 | https://www.google.com/?client=firefox-b#q=telekomo+saugumas&gfe\_rd=cr |
| 142 | https://www.google.com/search?q=openoffice&ie=utf-8&oe=utf-8&client=firefox-b |
| 143 | https://www.google.lt/search?q=openoffice&ie=utf-8&oe=utf-8&client=firefox-b&gfe\_rd=cr&ei=GXPNV9\_PMIOr8wemi56wCA |
| 144 | https://www.google.com/search?q=openoffice&ie=utf-8&oe=utf-8&client=firefox-b&gfe\_rd=cr&ei=GXPNV9\_PMIOr8wemi56wCA |
| 145 | https://www.google.com/?client=firefox-b#q=openoffice&gfe\_rd=cr |
| 146 | http://www.openoffice.org/download/ |
| 147 | http://sourceforge.net/projects/openofficeorg.mirror/files/4.1.2/binaries/en-US/Apache\_OpenOffice\_4.1.2\_Win\_x86\_install\_en-US.exe/download |
| 148 | https://sourceforge.net/projects/openofficeorg.mirror/files/4.1.2/binaries/en-US/Apache\_OpenOffice\_4.1.2\_Win\_x86\_install\_en-US.exe/download |
| 149 | http://downloads.sourceforge.net/project/openofficeorg.mirror/4.1.2/binaries/en-US/Apache\_OpenOffice\_4.1.2\_Win\_x86\_install\_en-US.exe?r=http%3A%2F%2Fwww.openoffice.org%2Fdownload%2F&ts=1473082149&use\_mirror=netassist |
| 150 | https://www.google.com/search?q=libreoffice&ie=utf-8&oe=utf-8&client=firefox-b |
| 151 | https://www.google.lt/search?q=libreoffice&ie=utf-8&oe=utf-8&client=firefox-b&gfe\_rd=cr&ei=N3PNV\_nwDIur8weuuJ3oBA |
| 152 | https://www.google.com/search?q=libreoffice&ie=utf-8&oe=utf-8&client=firefox-b&gfe\_rd=cr&ei=N3PNV\_nwDIur8weuuJ3oBA |
| 153 | https://www.google.com/?client=firefox-b#q=libreoffice&gfe\_rd=cr |
| 154 | https://www.libreoffice.org/download/ |
| 155 | https://www.libreoffice.org/download/libreoffice-fresh/ |
| 156 | http://donate.libreoffice.org/home/dl/win-x86/5.2.0/en-US/LibreOffice\_5.2.0\_Win\_x86.msi |
| 157 | http://download.documentfoundation.org/libreoffice/stable/5.2.0/win/x86/LibreOffice\_5.2.0\_Win\_x86.msi |
| 158 | http://ftp.byfly.by/pub/tdf/libreoffice/stable/5.2.0/win/x86/LibreOffice\_5.2.0\_Win\_x86.msi |
| 159 | https://addons.mozilla.org/thunderbird/addon/enigmail/ |
| 160 | https://addons.mozilla.org/en-US/thunderbird/addon/enigmail/ |
| 161 | https://addons.mozilla.org/thunderbird/downloads/latest/enigmail/addon-71-latest.xpi?src=dp-btn-primary |
| 162 | https://addons.cdn.mozilla.net/user-media/addons/\_attachments/71/enigmail-1.9.5-tb+sm.xpi?filehash=sha256%3A12b2dfa25cb0169fb55c0def1628feabb991a8c0c771374b16eab09bf3873ed2 |

Kokie failai ir kokiuose kataloguose buvo išsaugoti kompiuteryje *NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU*

|  |
| --- |
| Asc, txt |

Ar buvo naudojami prijungti tinkliniai diskai (Mapped Network Drives) *Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU*

|  |
| --- |
| Ne |

Kokia programine įranga duomenų sinchronizavimui vartotojas naudojosi paskutinio prisijungimo metu?

SkyDrive, GoogleDrive

Kokie yra vartotojo prisijungimo vardai ir slaptažodžiai (login/password) ir su kokia programine įranga naudojami?

|  |  |  |  |
| --- | --- | --- | --- |
| Vartotojas | Slaptažodis | Naudojama programinė įranga | Pastabos |
| ALarvelis@gmail.com | 1/eFg5BbQAfdEK1npd8awAjK56OPUchveNYn-\_Z016CFY | Thunder Bird |  |
|  |  |  |  |

Kokias el. pašto susirašinėjimo programines įrangas A. K. naudojo?

|  |  |  |  |
| --- | --- | --- | --- |
| Programinė įranga | El. pašto dėžutė (tikslus kelias iki el. pašto dėžutės diske) | Antraštės (svarbių el. laiškų antraštės) | Tarp kokių subjektų susirašinėjimas buvo vykdomas) |
| Mozilla Thunderbird | C:\Program Files (x86)\Mozilla Thunderbird | Derybos | [alarvelis@gmail.com](mailto:alarvelis@gmail.com) ir skaitmeninis.legionas@gmail.com |
| Mozilla Thunderbird | C:\Program Files (x86)\Mozilla Thunderbird | drobox decryptor | [alarvelis@gmail.com](mailto:alarvelis@gmail.com) ir linas@bruzas.lt |
| Mozilla Thunderbird | C:\Program Files (x86)\Mozilla Thunderbird | ataskaitos | [alarvelis@gmail.com](mailto:alarvelis@gmail.com) ir karolis.steikunas@ekt.lt |

Kokią programine įranga vartotojas naudojo elektroniniam dokumentams (e. parašas) apsikeisti

|  |  |  |  |
| --- | --- | --- | --- |
| Vartotojas | El. paštas | Naudojama programinė įranga | Pastabos (Private/Public keys) |
| Almantas Karvelis | [alarvelis@gmail.com](mailto:alarvelis@gmail.com) | Enigmail |  |

***Kokius svarbius (bendrai kiekvienos grupės) dokumentus radote ir naudosite grupės laboratorinio gynime?***

(išvardinti pasiimtus dokumentus, kurie vėliau bus įtraukti į galutinę ataskaitą, atsakant į klausymą: “Ar tinkamai yra surinkti įkalčiai ir ar galima šį dokumentą pridėti, kaip svarbu nagrinėjant A. K. nužudymo bylą?”)

|  |  |  |  |
| --- | --- | --- | --- |
| Numeris | Dokumento pavadinimas | Kur rastas dokumentas (tikslus kelias iki dokumento ar registro įrašo) | Kontrolinė suma |
|  |  |  |  |
|  |  |  |  |

**Išvados**

Išanalizavus įkalčius matoma, su kuo žmogus bendravo, kuom jis naudojosi ir kokiose svetainėse jis lankėsi.

**Darbo rezultatų vertinimas**

|  |  |  |  |
| --- | --- | --- | --- |
| Vertinimas  (balais) | Galimas maksimalus vertinimo balas | Vertinimo objektas | Pastabos |
|  | 5 | Surinkta pagrindinė informacija iš vartotojo registrų | Tik bendra informacija apie vartotoją |
|  | 1 | Surinkta informacija apie vartotojo veiksmų istoriją | Veiksmų istorijos informaciją |
|  | 1 | Surinkta informacija apie debesų paslaugų naudojimą | Vartotojo vardai, prisijungimai, debesų programinė įranga |
|  | 3 | Pateikta informacija apie surinktus įkalčius | Tinkamas dokumentų (įkalčių) sąrašas |
|  | 10 |  | |