TS SURUGI Linux project
the right DFIR tools in the “wrong time”...

Giovanni 'sug4r' Rattaro
@tsurugi_linux

tsurugi-linux.org

European summit 2019
WHOAMI

GIOVANNI 'sug4r' RATTARO

• IT SECURITY CONSULTANT AND MANAGER @ OpenMinded

• Italian staff member old <<back|track Linux project

• Ex developer DEFT Linux

• Passionate DFIR instructor

• TSURUGI Linux core developer and project team leader
$CAT TSURUGI_LINUX.TEAM

- Marco 'Blackmoon' Giorgi
- Davide 'Rebus' Gabrini

NEW STAFF 2019:

- Francesco 'dfirfpi' Picasso
- Massimiliano 'YattaMax' Dal Cero
- Antonio 'Visi@n' Broi

tsurugi-linux.org
TSURUGI LINUX
PROJECT

the right DFIR tools in the “wrong time”...

tsurugi-linux.org
TSURUGI LINUX
OPEN SOURCE PROJECT
tsurugi-linux.org
TSURUGI LINUX project
TSURUGI LINUX [LAB]

- 64 bits Linux distribution
- Based on UBUNTU LTS version
- Patched kernel 5.1.15
- DFIR
- OSINT / Malware Analysis / Computer vision
- For educational and/or professional use
SPECIALS FEATURES?

tsurugi-linux.org
Custom Boot options

1. TSURUGI Linux Live (GUI mode)
   TSURUGI Linux Live (GUI mode, RAM preload)
2. TSURUGI Linux Live (Text mode)
   TSURUGI Linux Live (Text mode, RAM preload)
3. TSURUGI Linux Live (GUI mode) - Blacklist nVidia driver
   TSURUGI Linux Live (GUI mode) - Blacklist ATI driver
   Check disc for defects
Our idea based on investigation 6 phases

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation
TSURUGI Linux main menu & tools classification

- Imaging
- Hashing
- Mount
- Timeline
- Artifacts Analysis
- Data Recovery
- Memory Forensics
- Malware Analysis
- Password Recovery
- Network Analysis
- Picture Analysis
- Mobile Forensics
- OSINT
- Cloud Analysis
- Virtual Forensics
- Crypto Currency
- Other Tools
- Reporting
Artifacts analysis
Malware analysis
Network analysis
Computer vision
Mobile forensics

OSINT
Crypto currency

Other tools
KERNEL WRITE BLOCKER
KERNEL WRITE BLOCKER

All connected devices by default are in READ ONLY mode

tsurugi-linux.org
KERNEL WRITE BLOCKER

WHY A DEVICE WRITE BLOCKER AT KERNEL LEVEL?

tsurugi-linux.org
The /mnt DIRECTORY

tsurugi-linux.org
OSINT PROFILE
SWITCHER
WE CARE ABOUT DETAILS...

**TSURUGI LINUX [LAB]**

- Device automount/autoexec disabled
- System hibernation disabled
- After each session starts the defaults custom values are set
- Automatic set HI-DPI
- Mouse keys switch
- Boot cleaner script
- RAM saturation workaround
BENTO TOOLKIT

Bento
your forensic launcher box

TSURUGI
the sharpest weapon in your DFIR arsenal

tsurugi-linux.org
BENTO

- Live forensics analysis toolkit
- About 300 tools (Windows, Linux, macOS)
BENTO TOOLKIT

tsurugi-linux.org
<table>
<thead>
<tr>
<th>Name</th>
<th>Category</th>
<th>Released on</th>
<th>Version</th>
<th>Size</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdapterWatch</td>
<td>Internet</td>
<td>2009/05/18</td>
<td>1.05</td>
<td>37 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>AdvancedRun</td>
<td>Utilities</td>
<td>2018/09/11</td>
<td>1.06</td>
<td>59 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>AdvancedRun x64</td>
<td>Utilities</td>
<td>2018/09/11</td>
<td>1.06</td>
<td>71 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>AllThreadsView</td>
<td>Utilities</td>
<td>2018/04/01</td>
<td>1.00</td>
<td>53 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>AllThreadsView x64</td>
<td>Utilities</td>
<td>2018/04/01</td>
<td>1.00</td>
<td>63 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>AlternateStreamView</td>
<td>Utilities</td>
<td>2018/09/29</td>
<td>1.54-1.55</td>
<td>52 Kb</td>
<td>Update</td>
</tr>
<tr>
<td>AlternateStreamView x64</td>
<td>Utilities</td>
<td>2018/09/29</td>
<td>1.54-1.55</td>
<td>67 Kb</td>
<td>Update</td>
</tr>
<tr>
<td>AltStreamDump</td>
<td>Utilities</td>
<td>2012/02/19</td>
<td>1.05</td>
<td>10 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>AppNetworkCounter</td>
<td>Internet</td>
<td>2018/10/11</td>
<td>1.05</td>
<td>58 Kb</td>
<td>Update</td>
</tr>
<tr>
<td>AppNetworkCounter x64</td>
<td>Internet</td>
<td>2018/10/11</td>
<td>1.05</td>
<td>68 Kb</td>
<td>Update</td>
</tr>
<tr>
<td>AppReadWriteCounter</td>
<td>Utilities</td>
<td>2018/07/18</td>
<td>1.05</td>
<td>58 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>AppReadWriteCounter x64</td>
<td>Utilities</td>
<td>2018/07/18</td>
<td>1.05</td>
<td>68 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>BatteryInfoView</td>
<td>Utilities</td>
<td>2017/08/11</td>
<td>1.23</td>
<td>115 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>BluetoothCL</td>
<td>Internet</td>
<td>2014/02/16</td>
<td>1.07</td>
<td>13 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>BluetoothLogView</td>
<td>Internet</td>
<td>2016/10/20</td>
<td>1.12</td>
<td>269 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>BluetoothView</td>
<td>Internet</td>
<td>2013/02/17</td>
<td>1.66</td>
<td>52 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>BrowsingHistoryView</td>
<td>Internet</td>
<td>2018/07/16</td>
<td>2.17</td>
<td>248 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>BrowsingHistoryView x64</td>
<td>Internet</td>
<td>2018/07/16</td>
<td>2.17</td>
<td>255 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>BulletsPassView</td>
<td>Utilities</td>
<td>2015/03/01</td>
<td>1.32</td>
<td>59 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>BulletsPassView x64</td>
<td>Utilities</td>
<td>2015/03/01</td>
<td>1.32</td>
<td>69 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>ChromeCacheView</td>
<td>Internet</td>
<td>2018/09/25</td>
<td>1.80</td>
<td>71 Kb</td>
<td>Update</td>
</tr>
<tr>
<td>ChromeCookiesView</td>
<td>Internet</td>
<td>2018/05/08</td>
<td>1.47</td>
<td>180 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>ChromeHistoryView</td>
<td>Internet</td>
<td>2018/03/20</td>
<td>1.35</td>
<td>181 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>ChromePass</td>
<td>Utilities</td>
<td>2018/01/27</td>
<td>1.46</td>
<td>153 Kb</td>
<td>Added</td>
</tr>
<tr>
<td>CredentialsView</td>
<td>Utilities</td>
<td>2017/10/29</td>
<td>1.07</td>
<td>74 Kb</td>
<td>Added</td>
</tr>
</tbody>
</table>
### BENTO PACKAGE MANAGER

<table>
<thead>
<tr>
<th>Name</th>
<th>Category</th>
<th>Released on</th>
<th>Version</th>
<th>Size</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrowdInspect</td>
<td>Security - Forensics</td>
<td>2017/02/14</td>
<td>1.5</td>
<td>530Kb</td>
<td>Available</td>
</tr>
<tr>
<td>CrowdResponse</td>
<td>Security - Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CyLR</td>
<td>Security - Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DFIRTriage</td>
<td>Security - Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DMDE (x64)</td>
<td>Security - Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DMDE (x86)</td>
<td>Security - Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FastIR Collector (x64)</td>
<td>Security - Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FastIR Collector (x86)</td>
<td>Security - Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>glogg</td>
<td>Text - Viewers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HDD Raw Copy</td>
<td>Security - Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPEC Free</td>
<td>Security - Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KAPE</td>
<td>Security - Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LaZagne</td>
<td>Security - Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Live Response Collection</td>
<td>Security - Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**KAPE 0.8.1.0**

KAPE is an efficient and highly configurable triage program that will target essentially any device or storage location, find forensically useful artifacts, and parse them within a few minutes.

- **App publisher**
- **Contact reviewer**

**Installation completed**

**License**: [https://learn.duffandhelps.com/kapec-license-agreement](https://learn.duffandhelps.com/kapec-license-agreement)

**Free space on F: 19.0/1001.7GB**
TSURUGI ACQUIRE

tsurugi-linux.org
TSURUGI ACQUIRE

- 32 bits Linux distribution
- Live minimal version
- Only for “disk acquisition”
- KERNEL WRITE BLOCKER
TSURUGI ACQUIRE

tsurugi-linux.org
OUR GOALS?

SHARE KNOWLEDGE
&
GIVE BACK TO THE COMMUNITY

tsurugi-linux.org
NEXT STEPS & OUR ROADMAP

• System upgrade to new 20 LTS version [Q2 2020]

• New Amazing feature! (Use Tsurugi Linux and try to find the hint...) [Q3 2020]

• Create free basic DFIR trainings [Q4 2020]

• Don’t forget to sleep... 😊 [Q4 2021]

tsurugi-linux.org
NEXT STEPS & OUR ROADMAP

[Updates Q4 2019!]

BENTO toolkit

Tsurugi Acquire

Tsurugi LAB 2019.2

tsurugi-linux.org
A problem has been detected and Windows has been shut down to prevent damage to your computer.

If this is the first time you've seen this stop error screen, restart your computer. If this error persists after following these steps:

Check to be sure you have adequate disk space. If a driver is identified in the Stop message, disable the driver or check with the manufacturer for driver updates. Try changing video adapters.

Check with your hardware vendor for any BIOS updates. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced boot options, and then select Safe Mode.

Technical information:

*** STOP: 0x0000007E, ffffff8800000000, 0x00200C592B, 0xFFFFF880032839F8, 0xFFFFF88003283250

*** srv2.sys, 80000000, FFFF880020A1000, DateStamp 494319e9

Collecting data for
Initializing disk for dump
Beginning dump of physical memory
Dumping physical memory to disk...
THANK YOU

@tsurugi_linux
@Sug4r7

www.linkedin.com/in/giovannirattaro

info [at] tsurugi-linux [dot] org
giovanni [at] tsurugi-linux [dot] org

tsurugi-linux.org