horizontal line

**Plus971 Cybersecurity**

Report on data Acquisition tools

**14th August 2023**

1. **FTK Imager:**
   1. Vendor Name: developed by - AccessData, sold by - Exterro
   2. Name and Version Number: FTK Imager 4.7.1
   3. Capabilities
      1. Full Disk Imaging: Capabilities: can do physical or logical imaging
      2. Custom Content Images: can collect necessary files or folders to reduce the amount of unnecessary data collected.
      3. Forensic Image Mounting: produces a read-only view that allows for analysts to examine the data in an image.
      4. Hash Reports: can generate hash reports for regular files and disk images that can be used to prove data integrity in a case.
      5. Preview Data: you can preview data in images located in your machine or on a network drive, CD’s, USB’s etc.
      6. Compatible Export Files: FTK Imager can work with various formats and can integrate into a pre-existing workflow.
      7. Ram Capture: it also allows for live acquisition as we can gather volatile data from RAM.
2. **Autopsy:**
   1. Vendor Name: maintained by - Basis Technology Corp, vendor - Sleuthkit.org
   2. Name and Version Number: Autopsy 4.20.0
   3. Capabilities
      1. Full Disk Imaging: Capabilities: can do physical or logical imaging
      2. Forensic Image Mounting: produces a read-only view that allows for analysts to examine the data in an image including
      3. file analysis which includes extracting metadata from many different file types.
      4. Keyword search allows you to narrow down a search.
      5. Hash Reports: can generate hash reports for regular files and disk images that can be used to prove data integrity in a case.
      6. Preview Data: you can preview data in images located in your machine or on a network drive, CD’s, USB’s etc.
      7. Timeline Analysis: a timeline displays when events took place that can give perspective to an analyst,
      8. Recover deleted data: this tool can identify and recover.
      9. Can analyze windows registry entries that can help uncover info about an attack or the user's actions.
      10. Communication analysis: can analyze emails, messages, etc.
      11. This platform can generate a detailed report and summarize the findings.
      12. Autopsy allows for easy integration with other tools
      13. Ram Capture: it also allows for live acquisition as we can gather volatile data from RAM.
3. **F-RAT:**
   1. Vendor Name: developed by - CDAC
   2. Name and Version Number: F-RAT 1.0
   3. Capabilities
      1. It extracts data from the live registry and raw registry in an understandable format and can also generate reports based on the data. It is also called F-RAN
4. **Elcomsoft Phone Viewer:**
   1. Vendor Name: developed by - Elcomsoft
   2. Name and Version Number: Elcomsoft Phone Viewer 5.40
   3. Capabilities
      1. It can analyze information extracted with ElcomSoft and third-party acquisition tools with a fast, lightweight viewer.
      2. Decrypt and view iOS backups and synced data, browse iOS file system images, analyze iCloud Photo Library
5. **WinHex:**
   1. Vendor Name: developed by - X-Ways
   2. Name and Version Number: WinHex 20.9
   3. Capabilities
      1. A tool used to recover damaged or fragmented data, mainly used for data recovery and low level data analysis
      2. Can work with RAID based solutions.
      3. Can wipe confidential files securely(hard drive cleansing)
      4. Device cloning
      5. Analyzing and comparing files
      6. etc..
6. **Regripper:**
   1. Vendor Name: developed by - keydet89
   2. Name and Version Number: RegRipper3.0
   3. Capabilities
      1. The main function of regripper is that it can recreate user activities using data from the registry.

**Which Tool would I prefer to use?**

FTK Imager: as it supports a number of forensic formats, can easily integrate into pre-existing workflows and it can do the job of multiple tools, such as creating a memory dump.

| **Vendors** | **Raw Format** | **Proprietary Format** | **AFF Format** | **Other Proprietary Formats** | **Compression of Image Files** | **Remote Network Acquisition** | **Validation Method** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **FTK Imager** | Yes | yes | yes | Encase(E01),smart | yes | yes | MD5, SHA-1 |
| **Autopsy** | Yes | Various | Yes, can analyze,can't capture an AFFimage | E01, FTK | Yes | Yes | MD5, SHA-1 |
| **F-RAT 1.0** | No | No | No | No | No | No | None |
| **Elcomsoft Phone Viewer** | No | Various | No | No | No | No | none |
| **WinHex** | Yes | Various | No | E01, SMART | no | No | MD5, SHA-1 |
| **RegRipper** | No | No | No | No | No | No | none |