|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2022/23) Semester 4/6 | Week 13 |
| Tutorial 9 |
| **Live Response** | |

**OBJECTIVES**

After completing this topic, you should be able to

1. Describe how volatile data help in an investigation.
2. Explain what type of data can be collected from live response.
3. Describe the process involved in live response.

Q1. What is volatile data and why is it important in forensic investigation?

It is information that describes the current state of the system. This incudes network connections, running processes and registry keys. Imporatnat to understand the current state as it serves as evidence as to what the suspect was most recently viewing and can better understand where the train of thought of the suspect is.

Q2. Explain the purposes of gathering system date and time from victim’s machine.

Q3. In what situation would collecting an image of memory be most useful to the investigation?

Contains critical information, does not take too long to load, impacts mininal external systems, minimal changes to the target system

Q4. The following table shows some of the HKLM keys that are useful in live response investigations. From your own computer, start the Registry Editor (Start 🡪 regedit), access the following keys and enter the values and data.

|  |  |  |  |
| --- | --- | --- | --- |
| **Key** | **Value(s)** | **Data** | **Description** |
| HKLM\System\ CurrentControlSet\ Control\ Computername\ | (Default) | *(value not set)* | Computername contains configured machine name. This may be different from ActiveComputername if machine name has changed but not yet rebooted. |
| HKLM\Software\ Microsoft\ Windows NT\ CurrentVersion\ NetworkList\ Profiles\ {GUID} |  |  | Profiles for each networks to which the system has previously connected. For wireless networks, ProfileName and/or Description typically match SSID. |
| HKLM\Software\Microsoft\ Windows NT\ Currentversion\ ProfileList\ {SID}\ |  |  | Subkeys for each user SID that has logged on to the system. The value will indicate the path to the user’s profile folder, which can help to translate SID to username. |

- End -