Dipanshu Pandey

Dipanshu Pandey Sep 6 · 3 min read

Best Practices To Be Maintained as a Digital Forensic Investigator

Hi, I am Dipanshu Pandey and this is my third article. This is a complete non-technical article and here we would be discussing some best practices you should follow as a investigator to avoid any harm to the evidence and ruin the case…

. . .

1. Never Ever Try To Change the State of Compromised Machine -> whenever you counter a system that may be suspect of malicious activity then never try to to browse that computer and make changes to it. Like you found a PC in a enterprise that is suspect to attack then do not allow anyone to touch that system, because it can destroy some evidence.Like if anyone would browse some files or internet from the suspected computer then it would lead to some changes in the logs and database of the browser which person is browsing, and these kinds of things will mis-lead the evidence and cause false postivies.

2. Maintain Complete Documentation and Chain of Custody -> Whenever you arrive at a crime scene and you want to collect the evidence (PC, server for investigation) then always document what all systems you are taking along with you and their full information, like model no. and time of acquisition and also the owner of the system. The chain of custody is the most critical process of evidence documentation. It is a must to assure the court of law that the evidence is authentic. The chain of custody proves the integrity of a piece of evidence. A paper trail is maintained so that the persons who had charge of the evidence at any given time can be known quickly and summoned to testify during the trial if required.(source https://www.ncbi.nlm.nih.gov/books/NBK551677/).

3. Never Ever Work with Original Evidence -> Never ever try to work with Original Evidence because it is most sensitive and if damage is caused to it then case would be ruined and also the company's data stored in it would be gone. So always use a write-blocker to open HDD in read only mode and then make a forensic image of it and work with it keeping the original evidence safe.

4. Never Go Out of Scope -> Before every investigation the scope of the investigation is decided that what areas to investigate and then you need to investigate only areas where their is possibility of evidence and you don't need to investigate anything else other than that.For eg. A company can specify only to investigate their web servers . Specially in government cases violating the scope can also create a problem for you.

5. Focus on Quality Not on Quantity -> Whenever you will visit an organisation for investigation you will see 100's of computer and servers. And if you are planning to investigate all of them then you are nothing more than a silly…investigator. Investigation of 100's of these system properly would take years and you would surely not be able to reach to conclusion. A better approach would be to collect data only from those endpoint systems and servers which could be suspect of attack depending on the scenario.

. . .

So The above mentioned were some of the best practices which you should follow as a Forensic Investigator for a successful investigation without false positives.

My Other Articles:

1. How to get started in Digital Forensic- https://link.medium.com/Nv5UWnGSkjb

2. Digital Forensics Artifacts on Microsoft Windows- https://link.medium.com/uTxVjhASkjb

Thank You !!

Dfir Blue Team