OSACAR

Dr. Lokesh Chouhan

Associate Professor

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

राष्ट्रीय न्यायालयिक विज्ञान विश्वविद्यालय
(राष्ट्रीय महत्त्व का संस्थान, गृह मंत्रालय, भारत सरकार)

National Forensic Sciences University
(An Institution of National Importance under Ministry of Home Affairs,
Government of India)

E-Mail: Lokeshchouhan@gmail.com, Lokesh.chouhan_goa@nfsu.ac.in

Mob: +91-898924399, 9827235155

Network Forensics Investigative Methodology (OSCAR)

OSCAR

- Similar to other forensic task, discovering and analyzing evidence from network sources has to be done in steps so that the results can be accurate. Forensic investigators should perform our activities within a methodological framework. According to Sherri Davidoff and Jonathan Ham in Network Forensics : Tracking Hackers through Cyberspace, the recommended way to recover a digital evidence is:

OSCAR

1. **O**btain information
2. **S**trategize
3. **C**ollect evidence
4. **A**nalyze
5. **R**eport

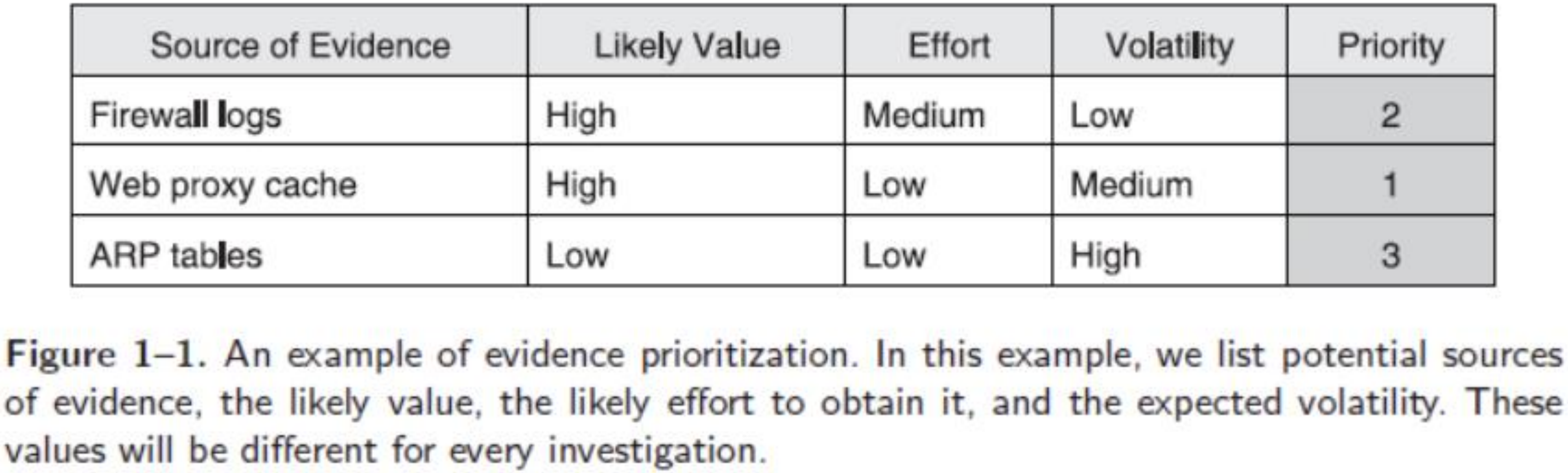
1.Obtain information

- Getting information related to the incident and gaining information about the environment when the incident occurs.
- Knowing the following things are important:
- • Description of what happened (as is currently known)
  • Date, time, and method of incident discovery
  • Persons involved
  • Systems and data involved
  • Actions taken since discovery
  • Summary of internal discussions
  • Incident manager and process
  • Legal issues
  • Time frame for investigation/recovery/resolution
  • Goals

2.Strategize

- Working efficiently and effectively is an important trait of an investigator. Communication is a must, so an investigator has to frequently communicate with other investigator regarding the case. Make sure everyone is working in concordance and that important developments are communicated. Prioritization of evidences is also needed. Here’s an example of evidence prioritization.

2.Strategize



Source of Evidence	Likely Value	Effort	Volatility	Priority
Firewall logs	High	Medium	Low	2
Web proxy cache	High	Low	Medium	1
ARP tables	Low	Low	High	3

Figure 1–1. An example of evidence prioritization. In this example, we list potential sources of evidence, the likely value, the likely effort to obtain it, and the expected volatility. These values will be different for every investigation.

3.Collect evidence

- The investigator came up with an acquisition plan based on the sources of evidence from the previous step. Then, based on the plan, collect evidences from each source. Here are 3 things an investigator must address in every evidence:
- Document -> Store the evidence securely, it may be referenced in court, and the notes might be helpful in the future
- Capture -> Capture each evidence
- Store/Transport -> Store the evidence securely and maintain the
  chain of custody. Keep eyes on who can access the evidence.

4.Analyze

- Usually, the analyzing process in nonlinear. But these following things should be essential:
- · Correlation
  · Timeline
  · Events of Interest
  · Corroboration
  · Recovery of additional
  · Interpretation

5.Report

- The report that the investigator produce must be:
- • Understandable by nontechnical laypeople, such as:
- – Legal teams
  – Managers
  – Human Resources personnel
  – Judges
  – Juries
- • Defensible in detail
  • Factual

Dr. Lokesh Chouhan
NFSU Goa
Lokesh.chouhan_goa@nfsu.ac.in