Analyzing and Attributing Cyber-Attacks: Digital Investigation Process Model

446H - Applied Network Security

Erisa Karafili

Imperial College London

February 8, 2019

Agenda

1. Introduction
2. Evidence
3. Digital Investigation Process Models
4. Project 3

1 Introduction

2 Evidence

3 Digital Investigation Process Models

4 Project 3

Imperial College London

The Future is Interconnected

In 2020 there is an expectation of more than 20 billions of IoT devices connected. (McAfee labs)

- The growing of connectivity increases the security challenges

"Every minute, we are seeing about half a million attack attempts that are happening in Cyber Space"(Fortinet)

- The cost of Cyber Crime Damage by 2021 will reach $6 Trillion (Cybersecurity Ventures)

Imperial College London

The Problem

The forensics investigator needs to

- collect the evidence
- check the sources of the evidence for evaluating their reliability
- deal with enormous amount of pieces of evidence
- analyse incomplete and/or conflicting evidence
- put in act preventive and mitigative actions
- discover who performed the attack

Imperial College
London

1. Introduction

2. Evidence

3. Digital Investigation Process Models

4. Project 3

Imperial College London

Evidence

Definition (Evidence)

Evidence is any observable and recordable event, or artifact of an event, that can be used to establish a true understanding of the cause of an observed occurrence.

Different types of evidence:

- *Digital Evidence* e.g., email, logs, invoices, /var/log/messages;
- *Network-Based Digital Evidence* e.g., chat log, emails, browser activities, logs.

Imperial College London

Challenges of Network-Based Evidence

- **Acquisition**: it is difficult to locate the evidence inside a network given the big number of possible sources of evidence, e.g., wireless access points, web proxies, central log servers;
- **Content**: the network devices are not designed to contain all the file, or not with a high level of granularity;
- **Storage**: network devices do not employ secondary or persistent storage, thus, it is difficult to keep the network data that are volatile and do not survive a reset of the device;
- **Privacy**: depending on the jurisdiction, there might be legal issues involving personal privacy that apply to network-based acquisition techniques;
- **Seizure**: it is difficult to seizure a network, sometimes an entire network segment may be brought down;
- **Admissibility**: the evidence should be admissible in court.

Forensics Tools for Recovering Network-Based Evidence (I)

- Tcpdump: Is a powerful command-line packet analyzer. It prints out a description of the contents of packets on a network interface that match the boolean expression; the description is preceded by a time stamp. `https://www.tcpdump.org/`
- Wireshark: Is a network protocol analyzer. It lets you see what's happening on your network at a microscopic level. `https://www.wireshark.org/`
- SNORT: Is an intrusion detection and prevention system capable of real-time traffic analysis and packet logging. `https://www.snort.org/`

Forensics Tools for Recovering Network-based Evidence (II)

- Autopsy from the Sleuth Kit: Is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools. `https://www.sleuthkit.org/autopsy/`
- Redline of FireEye: Provides host investigative capabilities to users to find signs of malicious activity through memory and file analysis and the development of a threat assessment profile.

  `https://www.fireeye.com/services/freeware/redline.html`
- SIFT workstation from SANS DFIR: Is a group of free open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings.

  `https://digital-forensics.sans.org/community/downloads`

Imperial College London

1. Introduction

2. Evidence

3. Digital Investigation Process Models

4. Project 3

Why Process Models for Digital Investigation?

- After or during an attack the digital evidence needs to be recovered and analyzed.
- The results of recovering and analyzing evidence from network sources should be reproducible and accurate.
- Thus, there is a need of process models that describe the investigations process followed during a digital investigation.

The process models are used:

- as a point of reference for reflecting on the state and nature of the field;
- for training and directing research;
- benchmarking performance against generally accepted practice.

Digital Investigation Process Models

- The process models define what is required to complete a comprehensive and successful investigation.
- An effective process model identifies the steps to achieve the goals, is general, and can be applied to new technologies.
- The process models permits to:
  - have a complete and rigorous investigation,
  - have a proper evidence handling,
  - reduce the chances of mistakes due to time pressure, or preconceived theories.
- The process models can be useful in certain cases, but can also have limitations.

Starting Activities of a Digital Investigation

Accusation or Incident Alert

- It is the starting point of an investigation;
- The alarm can be given by an IDS, system administrator reviewing firewall logs, log entries on a server, etc;
- Citizen reporting possible criminal activity.

Authorization

- Be sure to do not violate any law when performing the investigation;
- Not having the appropriate authorization or violating any law, could weakened or even suppress some of the collected evidence;
- Obtain if necessary written authorization from an attorney.

Main Steps in Digital Investigation Process Models

- **Preparation**: Creating a plan of actions
- **Identification**: Finding potential sources of evidence
- **Preservation**: Collecting and storing the evidence
- **Examination and Analysis**: Extracting and viewing information from the evidence, and analyzing it, and answering different questions (who, what, where, when, how and why)
- **Presentation**: Reporting the findings in a satisfiable way (legal, corporate, military, etc.)

Examination

Examination is the process of extracting evidence and preparing them for the analysis.
As it is usually time consuming it is useful to use an examination composed of three levels:

- Triage forensics inspection: finds the most useful evidence;
- Preliminary forensics examination: finds the most useful that can be quickly provided to the investigator;
- In-depth forensics examination: analyses the other part of the evidence to have a broader understanding of the incident.

After the information is recovered, some evidence will be harvested for later analysis, other will be immediately analysed.
The information is going to be organized, and the irrelevant items will be eliminated from the investigations.

Analysis

Answers the following questions: Who, What, Where, How, and Why.

- The content and context of the evidence can have information that is used to reconstruct the attack and to determine factors such as motivations and means.
- A hypothesis that can explain the evidence is developed.
- Check if the collected evidence applies to the hypothesis.
- Each incident has a chronological component where events/actions fill the time slices. This answers to questions like, where, when, and sometimes how.

Formation and Evaluation of Hypothesis

- Based on the observed facts and evidence the investigators will form a theory/hypothesis of what may have occurred.
- Based on the hypothesis the investigator will predict where the evidence are located.
- The available evidence will be analyzed in order to test the hypothesis.
- The investigator can find that the hypotheses were confirmed, denied or there weren't enough evidence.

Process Models in Reality

- Usually digital investigations are not linear and the steps are not neatly separated.
- Some steps need to be revisit.
- Preparation is needed in every step, and not only for the overall investigation.
- The examination and analysis process tend to consume the most resources in terms of time, intellectual effort and creativity.

References

1. Sherri Davidoff, Jonathan Ham. *Network Forensics: Tracking Hackers Through Cyberspace*. 2012.
2. Eoghan Casey. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 3rd Edition, 2011.
3. tcpdump `https://www.tcpdump.org/`
4. Wireshark `https://www.wireshark.org/`
5. SNORT `https://www.snort.org/`
6. Autopsy `https://www.sleuthkit.org/autopsy/`
7. Redline `https://www.fireeye.com/services/freeware/redline.html`
8. Sift workstation `https://digital-forensics.sans.org/community/downloads`

Imperial College
London

1. Introduction
2. Evidence
3. Digital Investigation Process Models
4. Project 3

Project 3

- Two network forensics challenges.
  1. Operation Hermes
  2. Operation Ares
- Goal: Perform a network forensic investigations on simulated but realistic security-intelligence assignments.
- You are given on CATE a pdf with your briefing and a zipped pcap file with the data to analyse.
- Your task is to analyse the data to achieve the objectives detailed in the briefing, and write a comprehensive forensic report.
- In the forensics report you need to describe the followed steps and how you arrived at the conclusions.

The forensics challenges are provided by B. Jordan.
The project details are given by S.Maffeis and E.Karafili.

Info about the Projec

- Each group member should aim to spend about 12 hours on the project.
- Do not search online for the solutions.
- **Deadline**: 22/2/19 at 2pm.
- **Submission**: one member of the group should submit one or two pdf reports.

Report

Each forensic report should comment on all the assignment objectives, solved, attempted, or not. In particular, include in your report the following:

- A time line of events.
- A description of the investigation process model you followed.
- All the preparation steps you took before the analysis, or before any step, if applicable.
- How did you identify, collect and store the evidence?
- How did you examine and analyze the evidence?
- A list of all the tools, software and scripts you used, where did you get them from, what did you use them for. Provide additional details if you have created any bespoke tool or script.

Report

- Estimate the cost of your investigation, assuming all team members were forensics analysts. Report the time spent in the overall project, how it was divided in the various phases (find quotes for the cost of a Junior Cyber Forensics Analyst in London).
- The report should be between 10 and 30 pages long. It is expected that most of the content will be relevant listings, screenshots, tables, etc.
- An example report for a different kind of forensic investigation is also provided on CATE.

Tips

- Forensics bridges the gap between technical aspects and human aspects. Thinking about human behaviour, motivations, objectives, and linking different sources of information is as important to a forensic investigation as the technical analysis of network packets. You will need to do both to achieve the operation objectives.
- The information in the pcap files alone may not be sufficient to reach all of the objectives. You may need other tools, data or information available online.
- Don't expect to be able to reach all the objectives at first. Formulate different hypotheses, and when you move on with your analysis, some hypotheses will be confirmed and others will be falsified.