IA 311: Network Forensics

Lecture 3: Network Based Evidence

Concepts in Digital Evidence

- What is evidence? (in broadest sense)
  - Refers to any observable and recordable event, or artifact of an event that can be used to establish a true understanding of the cause and nature of an observed occurrence.
    - Simply:
      - Observable and recordable event or artifact of an event.
        - It can be used to provide a true understanding of the cause and nature of an incident that occurred.

Concepts in Digital Evidence

- Categories of evidence (they have very specific meanings):
  - Real evidence
  - Best evidence
  - Direct evidence
  - Circumstantial evidence
  - Hearsay
  - Business Records
- As electronic communication systems are rising in popularity, the following categories of evidence are also included:
  - Digital evidence
  - Network-based Digital evidence

Real Evidence

- Refers to any physical, tangible object that played a relevant role in an event that is being adjudicated (judged/decided).
  - Refers to the physical, tangible object that played a role in an event and can be used in deciding a case.
  - Examples:
    - A murder weapon
      - A knife pulled from the victim's body.
      - A gun that fired the bullet.
    - The fingerprint or footprint
    - A signed paper contract
      - A physical contract that was signed by both parties.
    - In our case – digital forensics
      - The physical hard drive or USB device
        - » The hard drive from which data is to be recovered
      - The computer itself – chassis, keyboard and all.

Best Evidence

- Refers (roughly) to the best evidence that can be produced in a court of law.
  - In case an accident happens involving a train and a truck, a picture of the crime scene will suffice as the train and truck can not be taken to the court as evidence.
  - Examples:
    - A photo of the crime scene
    - A copy of the signed contract
    - A file recovered from the hard drive
    - A bit-for-bit snapshot of a network transaction

Direct Evidence

- Refers to the testimony offered by a direct witness of the act or acts in question.
  - Yes there is an approach to use video/audio recordings + … as evidence in a court, but reportable observation by a fellow human is also accommodated by the court.
    - The human testimony is classified as **direct evidence**.
      - Its is one of the most utilized evidence form though it is often disputed and unreliable.
      - It is usually utilized as long as it is relevant.
    - Examples:
      - “I saw him stab that guy.”
      - “I watched him crack passwords using John the Ripper and a password file he shouldn’t have.”
      - “I saw him with that USB device.”

Circumstantial Evidence

- Circumstantial evidence is evidence that does not directly support a specific conclusion.
  - This is evidence may be linked together with other evidence and used to deduce a conclusion.
  - This type of evidence is important in network forensics.
    - Why?
      - It is the primary mechanism used to link electronic evidence and its creator.
      - It is often used to establish the author of emails, chat logs or other digital evidence.
        - » Also, for evidence to be admissible in a court, authorship verification is necessary to establish authenticity.
  - Examples:
    - An email signature
    - A file containing password hashes on the defendant's (suspect's) computer
    - The serial number of the USB device

Hearsay

- Refers to the testimony offered second-hand by someone who was not a direct witness of the act or acts in question.
  - It includes comments from individuals with direct knowledge of an event but are unable or unwilling to deliver the comments directly to the court.
  - Digital evidence can be classified as hearsay if it contains assertions (statements/declarations) from people (**not computer generated content**).
  - Examples:
    - “The guy told me he did it.”
    - “He said he knew who did it, and could testify.”
    - “I saw a recording of the whole thing go down.”
    - A text file containing a personal letter

Business Records

- Refers to any documentation that an enterprise routinely generates and retains as a result of normal business processes, and that is deemed accurate enough to be used as a basis for managerial decisions.
  - Routinely generated and retained documentation by a business in its normal operations, which can be used in making its decisions.
    - Can include emails, memos, access logs and intrusion detection reports.
      - There may be legal requirements for retention periods for some of the data. **(What are the legal requirements in Tz??)**
    - NOTE:
      - As far as the business sees the records accurate and useful for decision making, the court sees them reliable for use in a case.

Business Records

- Examples:
  - Contracts and other employment agreements
  - Invoices and records of payments received
  - Routinely kept access logs
  - /var/log/messages

Digital Evidence

- Is any documentation that satisfies the requirements of evidence in a proceeding, but that exists in electronic digital form.
  - Simply:
    - Digital evidence is an evidence that can be used in a case/proceeding but exists in electronic digital form.
      - It usually poses challenges to investigators seeking to preserve it and attorneys seeking to admit it in a court.
        - » To be used in a court – it has to be relevant to the case and authentic.
    - Examples:
      - Emails and IM sessions
      - Invoices and records of payment received
      - Routinely kept access logs
      - /var/log/messages

Network-Based Digital Evidence

- Is digital evidence that is produced as a result of communications over a network.
  - NOTE:
    - As opposed to primary and secondary storage which are also used in forensics analysis; Network-based digital evidence is very volatile.
      - Packets move pass through the wires in milliseconds.
      - Packets vanish from switches in the blink of an eye.
      - Also websites' content change depending on where they are viewed from and when.
        - » The case on the contents of the apps, especially social media apps – IG, FB, Tiktok, Twitter, …

Network-Based Digital Evidence

- NOTE: Continued
  - Also, admissibility requirements of network-based digital evidence are murky (not clear).
    - Often the source that generated the evidence is not obtainable or can not be identified.
      - If a recording of a chat log, blog posting or email is the evidence – proving the identity of the parties in the conversation (that is the authors of the statements) may be difficult to prove.
      - If the evidence is a website – it may be needed to provide supporting evidence to prove that the presented image in the court is what was actually viewed at the given time and location.
        - » In this case, courts usually require the testimony of a person with knowledge of the website's appearance to authenticate images of that website.
      - As a result, (depending on the method of capture and the details of the case,) packet captures of network traffic may be treated as *recordings of events*, similar to a taped conversation.

Network-Based Digital Evidence

- Examples of network-based digital evidence can include:
  - Emails and IM sessions
  - Browser activity, including web-based email
  - Routinely kept packet logs
    - Application logs
    - OS logs
    - Router logs
    - Firewall logs
    - Proxy logs
  - /var/log/messages

Network-Based Digital Evidence

- Application Logs
  - When someone defaces web servers, they usually view them shortly before and after defacement.
  - The web logs might contain evidence of someone checking for vulnerabilities before defacement.
    - With the IP address that they used.

Network-Based Digital Evidence

- Application Logs
  - Mail servers log details of message.
    - Example: An email spoofer makes a typo.
      - Logs contains entries with backspaces, …
  - OS log connections.
  - Network devices log.

Challenges Relating to Network Evidence

- Network-based digital evidence poses special challenges in several areas, including:
  - Acquisition
  - Content
  - Privacy
  - Seizure
  - Storage
  - Admissibility

Challenges Relating to Network Evidence

- Acquisition
  - It can be difficult to locate specific evidence in a network environment.
    - This is because networks contain so many possible sources of evidence.
      - From wireless access points, to web proxies, to central web servers – therefore it becomes tricky to locate the correct evidence location.
      - Though one might know where a specific piece of evidence is located, gaining it might be difficult due to political or technical reasons.
- Content
  - As opposed to file systems (which are designed to contain all files' contents and their metadata), network devices may or may not store evidence with the desired level of granularity.
    - This is because network devices usually have very limited storage capacity.
      - Usually, only selected metadata of a transaction or transferred data is kept (instead of complete records of the transaction/transmitted data).

Challenges Relating to Network Evidence

- Storage
  - Network devices do not use secondary (non-volatile/permanent) storage.
    - As a result the data they contain may be so volatile.
- Privacy
  - Depending on the laws of a given state/country, there may be legal issues involving personal privacy, that are specific to acquisition techniques of network-based digital evidence.
    - **What are the legal issues concerning personal privacy in TZ?**

Challenges Relating to Network Evidence

- Seizure
  - In creating a copy of an original hard drive, this can be achieved with limited disruption to business operations.
    - On the other hand, seizure of a network device can be more disruptive.
      - In a serious case, an entire network segment can be brought down.
        - » However, in most cases investigators can minimize the impact on network operations.

Challenges Relating to Network Evidence

- Admissibility
  - As opposed to file system-based evidence (which has clear standards and is currently used in a court of law – in USA, what about Tz?), network forensics is a newer approach to digital forensics.
    - Sometimes, there are conflicting or even non-existent legal standards specific to network-based digital evidence use in a court.
      - However, over time, legal standards specific to network-based digital evidence will be established and used in the court.
        - » Advice:
          - Let us push for these legal standards/issues whenever we get the chance to do so.

Network Forensics Investigative Methodology (OSCAR)

- Recovery and analysis of evidence from network sources must be done in such a way that the results are reproducible and accurate.
  - To achieve this, network forensics tasks should be performed within a methodological framework.
  - One of the recommended step-by-step process has the following steps (referred to as **OSCAR**):
    - **O**btain information
    - **S**trategize
    - **C**ollect evidence
    - **A**nalyze
    - **R**eport

Network Forensics Investigative Methodology (OSCAR)

- **O**btain information
  - As a forensics investigator (be it in law enforcement, internal security staff or forensic consultant), you will need to do two things at the beginning of an investigation:
    - Obtain information about the **incident** itself, and
    - Obtain information about the **environment**.

Network Forensics Investigative Methodology (OSCAR)

- **O**btain information : Continued
  - The Incident:
    - As the investigator, you will usually want to know the following about the incident:
      - 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 management and processes
      - Legal issues
      - Time frame for investigation/recovery/resolution
      - Goals
    - NOTE:
      - This list is simply a starting point, and one might need to customize it for each incident.

Network Forensics Investigative Methodology (OSCAR)

- **O**btain information : Continued
  - The Environment
    - As an investigator, the information he/she gathers about the environment depends on his/her level of familiarity with the environment.
    - One should also note that, every environment is constantly changing, also social and political dynamics may occur during an incident.
      - Even if one is familiar with an organization, one is advised to take time to understand how the organization is responding to a particular incident, as well as clearly establish who needs to be investigated further/closely.

Network Forensics Investigative Methodology (OSCAR)

- **O**btain information : Continued
  - The Environment
    - An investigator will usually need to know the following about the environment:
      - Business model
      - Legal issues
      - Network topology (request a network map, etc. if you do not have one)
      - Available sources of network evidence
      - Organizational structure (request an organizational chart if you do not have one)
      - Incident response management processes/procedures (forensic investigators are part of the response process and should be at least basically familiar with it)
      - Communications systems (is there a central incident communication system/evidence repository?)
      - Resources available (staff, equipment, funding, time)

Network Forensics Investigative Methodology (OSCAR)

- **S**trategize
  - As an investigator, it is crucial that early on, one accurately assesses his/her resources and plans his/her investigation.
    - Though this is important in any investigation, it is very important in network forensics as there are many potential sources of evidence and some of which are also very volatile.
    - As an investigator, one must work efficiently.
      - From time to time, the investigator will have to collaborate with investigative/incident response team in planning and conducting the investigation as well as share important developments of a case.
    - Based on the number of potential sources of evidence, the required effort to obtain each, volatility and priority – the investigator will eventually have to come up with an evidence acquisition plan.

Network Forensics Investigative Methodology (OSCAR)

- **S**trategize: Continued
  - Some tips for developing an investigative strategy:
    - Understand the goals and time frame of the investigation.
    - List your resources, including personnel, time, and equipment.
    - Identify likely sources of evidence.
    - For each source of evidence, estimate the value and cost of obtaining it.
    - Prioritize your evidence acquisition.
    - Plan the initial acquisition/analysis.
    - Decide upon method and times of regular communication/updates.
    - Keep in mind that after conducting your initial analysis, you may decide to go back and acquire more evidence.
      - NOTE: Forensics is an iterative process.

Network Forensics Investigative Methodology (OSCAR)

- **C**ollect evidence
  - Based on the evidence acquisition plan created in the previous step, in this step, evidence is then collected from each source.
    - There are three components that an investigator must address every time he/she acquires evidence:
      - Document
      - Capture
      - Store/Transport

Network Forensics Investigative Methodology (OSCAR)

- **C**ollect evidence: Continued
  - There are three components that an investigator must address every time he/she acquires evidence:
    - Document
      - A log (record) of all systems accessed and actions taken during evidence collection should be carefully kept.
        - » These should be securely stored and may be referenced in a court.
        - » Even if the investigation might not go to court, the records might still be very helpful during analysis.
        - » Examples of details to record include: the date, time, source, method of acquisition, name of the investigator(s) and chain of custody (i.e. the documentation of the handling of the evidence from acquisition at the crime scene, transportation to the lab, …. until in the court).

Network Forensics Investigative Methodology (OSCAR)

- **C**ollect evidence: Continued
  - There are three components that an investigator must address every time he/she acquires evidence: Cont…
    - Capture
      - This is about capturing the evidence itself.
      - This may include:
        - » Capturing packets and writing them to a hard drive
        - » Copying logs to hard drive or CD, or
        - » Imaging hard drives of web proxies or logging servers
    - Store/Transport
      - This is about ensuring that the evidence is securely stored and the chain of custody is maintained.
        - » This includes keeping an accurate, signed, verifiable log of the persons who have accessed or possessed the evidence.

Network Forensics Investigative Methodology (OSCAR)

- **C**ollect evidence: Continued
  - NOTE:
    - Evidence admissibility is dependent on its relevance and reliability.
      - To achieve admissibility – the investigator should carefully track the source, method of acquisition and chain of custody.
        - » When in doubt (not sure), one is advised to take careful notes and seek legal counsel.
    - Tips for evidence collection (best practices for evidence collection):
      - Acquire as soon as possible, and lawfully
      - Make cryptographically verifiable copies
      - Sequester (seize) the originals under restricted custody and access (or [do the same for] your earliest copy, when the originals are not available)
      - Analyze only the copies
      - Use tools that are reputable and reliable
      - Document everything you do.

Network Forensics Investigative Methodology (OSCAR)

- **A**nalyze
  - Though this step is usually non-linear, certain elements should be considered essential. These include:
    - Correlation
    - Timeline
    - Events of Interest
    - Corroboration
    - Recovery of additional evidence
    - Interpretation

Network Forensics Investigative Methodology (OSCAR)

- **A**nalyze: Continued
  - Though this step is usually non-linear, certain elements should be considered essential. These include: Cont…
    - Correlation
      - One should consider what data should be compiled, from which sources, and how can it be correlated.
        - » This can be done manually or in an automated way.
    - Timeline
      - After data from various sources is compiled and correlated, a timeline of activities should be built (who did what and when, …)
    - Events of Interest
      - Some of the events will stand out as more relevant than others.
        - » These need to be isolated and further carefully investigated.

Network Forensics Investigative Methodology (OSCAR)

- **A**nalyze: Continued
  - Though this step is usually non-linear, certain elements should be considered essential. These include: Cont...
    - Corroboration
      - This refers to verification/justification/rationale.
      - Here, as data is from various sources, there might be a need to verify some of the events.
        - » This can be achieved using evidence from multiple sources.
          - It might also mean seeking out data that had not previously been compiled, from sources not previously consulted.
    - Recovery of additional evidence
      - Usually, the above steps lead to the need to expand the evidence acquisition and analysis areas.
        - » An investigator should be prepared for such a situation – to repeat the process until the events of interest are well understood.

Network Forensics Investigative Methodology (OSCAR)

- **A**nalyze: Continued
  - Though this step is usually non-linear, certain elements should be considered essential. These include: Cont...
    - Interpretation
      - Throughout the analysis step, the investigator might need to develop working theories of the case.
        - » This refers to the ideas of what might actually have happened in the incident as supported by the evidence that has been compiled and analyzed.
        - » It is very important that the investigator separates his/her interpretation of the evidence from fact.
          - The investigators interpretation of the evidence is always a hypothesis which may be proved or disapproved.

Network Forensics Investigative Methodology (OSCAR)

- **R**eport
  - The investigator should be able to eventually convey the results of the investigation to others.
    - Failure to be able to do this means, what the investigator has done (in all the previous steps) does not matter.
    - As a result, reporting might be the most important aspect of the investigation.
    - Most commercial tools handle this step, but not in a way that is most useful to a lay (non-tech) audience, which is generally necessary.

Network Forensics Investigative Methodology (OSCAR)

- **R**eport: Continued
  - The produced report must be:
    - Understandable by non-technical lay people, such as:
      - Legal teams
      - Managers
      - Human Resources personnel
      - Judges
      - Juries
    - Defensible in detail
    - Factual
  - NOTE:
    - The results of the investigation should be explained in such a way that makes sense to non-technical people.
      - The descriptions should still be backed by details that can easily be defended.

Network Forensics Investigative Methodology (OSCAR)

- Conclusion
  - As challenges associated with network forensics are concerned, investigators are advised to:
    - Carefully assess each investigation.
    - Develop a realistic strategy that takes into account both:
      - The investigative goals and
      - The available resources
  - 2,500 years ago, **Sun Tsu** wrote:
    - "**A victorious army first wins and then seeks battle; a defeated army first battles and then seeks victory**."
      - Take away message:
        - » Strategize first, then collect your evidence and do your analysis & report.
          - By considering the challenges unique to your investigation up front, you will meet your investigative goals most efficiently and effectively.