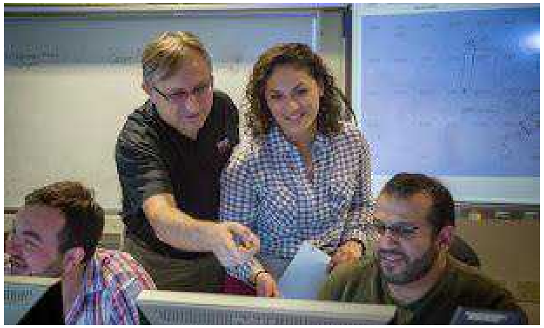
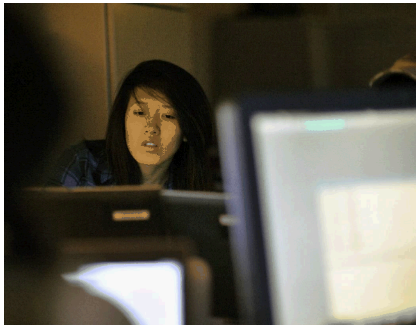
SAND2015-8947C

Exceptional service in the national interest

Sandia National Laboratories





Facilitation of Forensic Analysis Using a Narrative Template

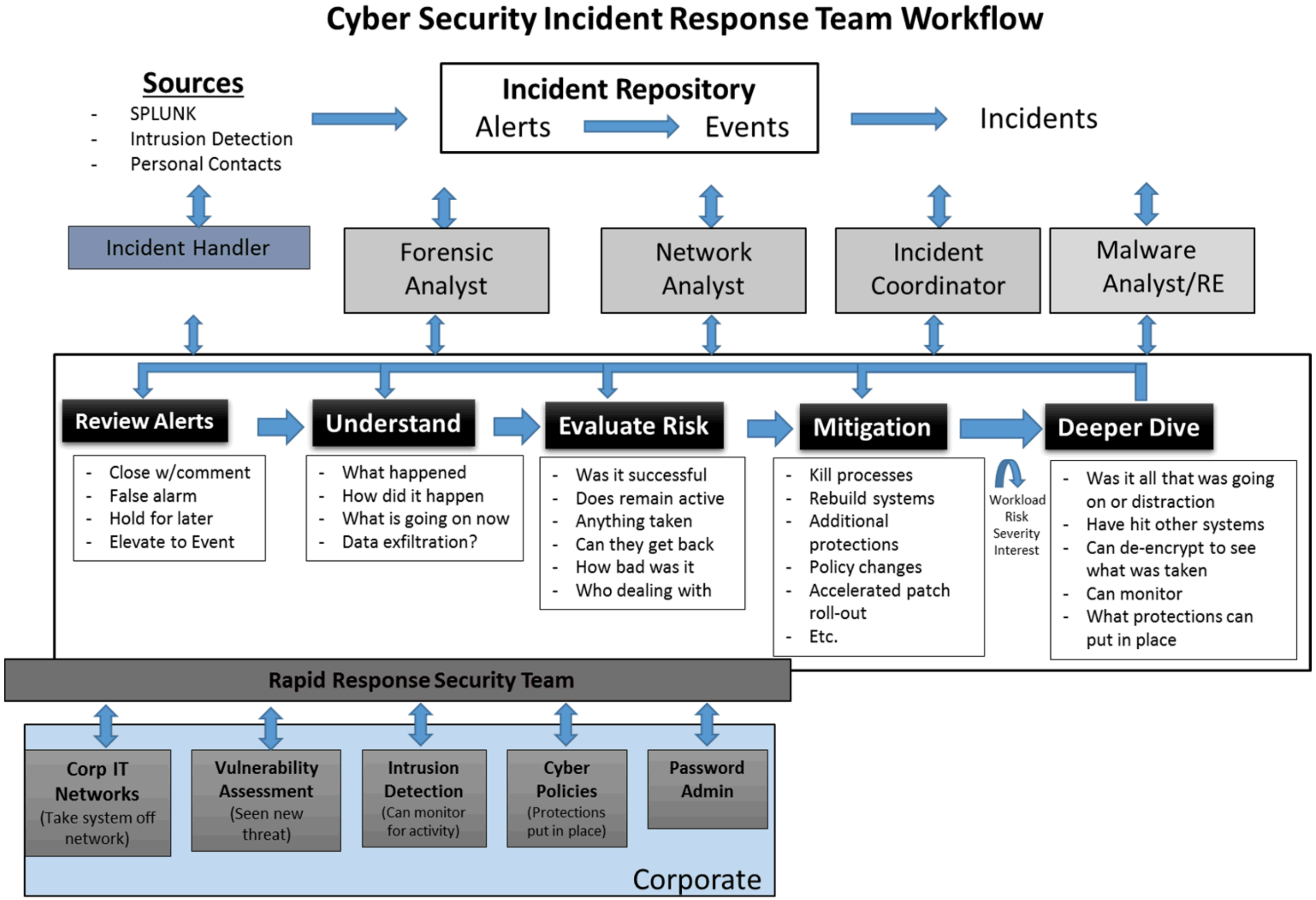
Shelby Hopkins, Andrew Wilson,
Austin Silva & Chris Forsythe

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Cyber Security Incident Response Teams (CSIRTs) serve as frontline defenders



Cyber Security Incident Response Team Workflow

CSIRT analysts assess alerts and conduct forensic analysis to identify, mitigate and defend against cyber threats

Narrative is intrinsic to cyber forensic analysis

- Analysts construct narratives in which events are organized on the basis of:
  - entities
  - entity motives and objectives
  - time
  - space
- The ability to infer narratives is essential to cyber forensic analysis and situation awareness/understanding

HYPOTHESIS: Tools facilitating the construction of narratives will result in better performance for cyber forensic analysis

Studying narrative in forensic analysis requires a suitable experimental protocol

- Given an operationally credible story and associated clues, can subjects reconstruct the crime(s)?
- Procedure
  - Subjects provided a collection of clues that would realistically be available to a forensic analyst
  - Clues consisted of legitimate clues reflecting the crime(s) of interest and other clues that served as red herrings
  - Subjects allowed a designated period of time to analyze the clues using alternative mediums
  - Subjects asked to construct a storyline based on their analysis
  - Subject-generated storylines evaluated based on whether subjects correctly assessed clues and organized them consistent with the experimenter-defined ground truth

The scenario asked subjects to assume the role of a forensic analyst

Pretense

> “You have been asked to look into a collection of suspicious events at Company Zirk. This company is a highly successful developer and manufacturer of vaccines distributed across many developing nations. You will be provided a collection of clues to one or more crimes that have been committed. Your task is to analyze the clues and determine what happened. Be aware, that some of the clues are red herrings and do not relate to the events you are investigating.”

Scenario involved multiple entities independently committing multiple crimes

- Hacktivist Thread

A Hacktivist group suspects Company Zirk's vaccine business is actually a cover for a secret government bioweapons program. Their objective is to expose Zirk. They **post their suspicions on social media** and **contact Zirk employees to ask about their work**. They also hang out at a local coffee shop that Zirk employees frequent hoping to overhear conversations. **An employee working in research leaves his laptop unattended and it is stolen** by a Hacktivist group member. The group finds various files on the computer regarding research activities at Zirk and contacts the media claiming they have proof that Zirk is developing biological weapons. The media is unwilling to report these claims, but instead, the **media reports that there is evidence of hazardous operations**. The Hacktivists decide that they must get onto the computer systems at Zirk to find the evidence they need to support their claims. Their next step is to **send Zirk employees a phishing email** disguised to be from a contractor who provides IT support. The phish claims that the annual license for Microsoft Office is about to expire and they must click the accompanying link to renew. Several employees click the link which downloads malware onto employees' computers that provides a backdoor for the Hactivists to remotely access their machines. While the hactivists are unable to access the research or manufacturing networks, they do **find the inventory database and perform a bulk download** of its contents. Based on this information, they return to the media and repeat their claims asserting that Company Zirk stocks all the materials they would need to create bioweapons. Instead of reporting these claims, the **media run a report about the safety of Zirk operations**.

NOTE: Red text signifies clues given to the subjects.

Scenario involved multiple entities independently committing multiple crimes

- Criminal Thread

Through various mechanisms, a criminal organization has **thoroughly compromised the computer network at Supplier Q**, which is a major supplier to Zirk. The criminal organization sees that Supplier Q does business with Zirk and realizes that Zirk is a more lucrative target. All of the purchase orders and invoices between Zirk and Supplier Q are done electronically. Malware is attached to an electronic invoice that allows the criminal organization to get a foothold on the financial system at Zirk. **The malware sets off an alert**, but only after the criminal organization's hackers have inserted multiple backdoors to Zirk's financial system. When Zirk financial staff approve an invoice from a supplier, an electronic transaction is sent to the bank requesting funds be transferred from Zirk's account to the account of the supplier. The criminal organization installs malware that intercepts these transactions and alters the data fields so that funds are instead transferred into a bank account the criminal group controls. **Zirk financial staff recognizes that funds have been transferred into an unrecognized account** and soon thereafter, **suppliers begin to alert Zirk that their invoices have gone unpaid**.

NOTE: Red text signifies clues given to the subjects.

Scenario involved multiple entities independently committing multiple crimes

- Insider Thread

An employee for Company Zirk, Bob, is leaving the company to take a job with a competing company, Xeno. Zirk has a revolutionary manufacturing process and Bob knows that he will become a favorite at his new job if he knows how to reproduce Zirk's manufacturing capabilities. The manufacturing process is instantiated within the Numeric Control programs used to drive the machinery used in manufacturing the vaccines. Bob's objective is to acquire these programs and the data generated from several manufacturing runs. Bob is not a very good Insider and first **tries to send files to an off-site computer, but the firewall blocks this attempt**. Since this did not work, he decides he'll do it the hard way and transfer the information to flash drives while no one is around. However, he gets sloppy and **leaves one of the flash drives behind**. In the process, the access control system for the manufacturing facility detects and issues an alert concerning Bob's **entering and leaving at odd-hours**. Bob does get enough information that he is able to help **Xeno replicate the manufacturing processes of Zirk**, which is soon advertised by Xeno at a trade show attended by Zirk personnel.

NOTE: Red text signifies clues given to the subjects.

Other clues served as red herrings that were suspicious, but unrelated to the three threads

- Over a period of two weeks, security cameras on perimeter fence frequently malfunction
- Company Zirk scientists report email accusing them of putting drugs in the water to control people’s minds
- Trespasser is caught in the manufacturing facility locker room stealing valuables from lockers
- Unusual spike in outgoing email is traced to botnet on Company Zirk computer that was sending spam
- Employee Mary is disciplined for frequenting online gambling site from Company Zirk computer
- IT staff find that a CD with updates for software used in research is infected with a known virus
- The offsite backup of the Company Zirk Human Resources database is discovered to be corrupted
- A review of Company Zirk public external website reveals several instances of secret company information

Subjects were randomly assigned to one of three conditions to analyze clues

Narrative

- Worked at whiteboard
- Magnetic cards
  - Clues
  - Annotations
  - Context
- Entity cards
  - Identity
  - What trying to do
  - Why trying to do it
- Timeline
- Red Herring Corner
- Colored tags
- Dry-erase markers

Visuospatial elements to facilitate construction of a narrative

Association

- Worked at whiteboard
- Magnetic cards
  - Clues
- Colored tags
- Dry-erase markers

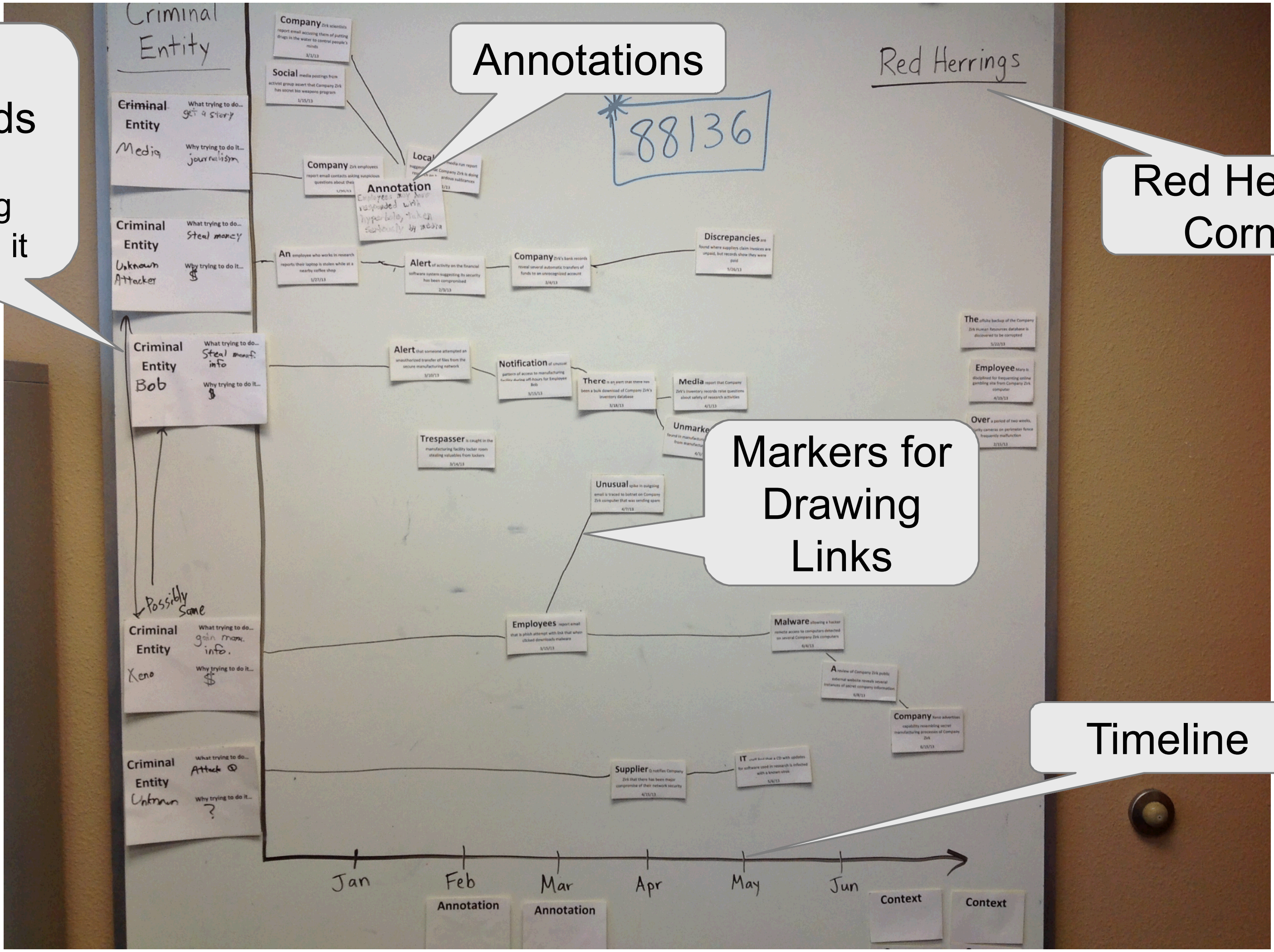
Visuospatial elements for organizing clues, without specific narrative components

Impoverished

- Worked at PC
- Excel spreadsheet
  - Clues
- MS Word
  - Recording notes

No visuospatial elements for organizing clues or elements to facilitate narrative construction

Narrative condition provided visuospatial elements to facilitate construction of a narrative



Criminal Entity Cards
- Identity
- What doing
- Why doing it

Annotations

Red Herring Corner

Markers for Drawing Links

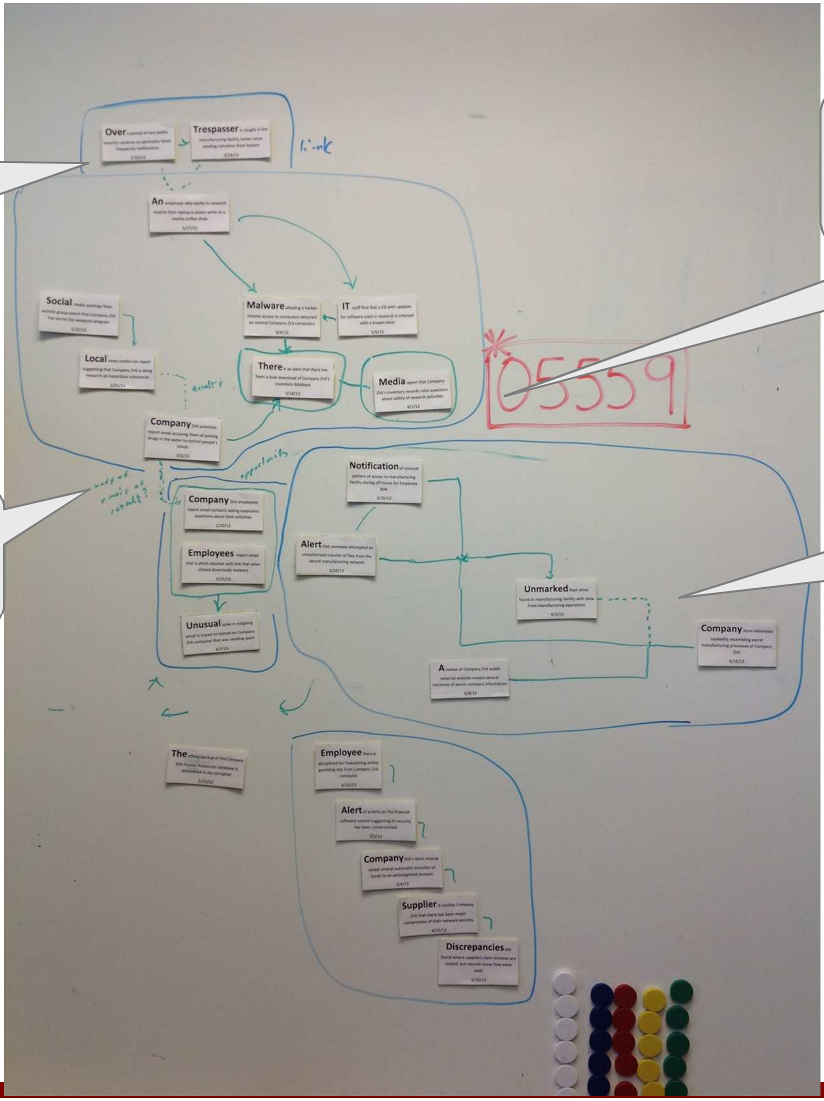
Timeline

NOTE: Subjects were also given colored magnets that they could use as tags

Association condition provided *visuospatial organization*, *<u>without</u> narrative components*

Could organize and group clues

Could insert notes as annotations

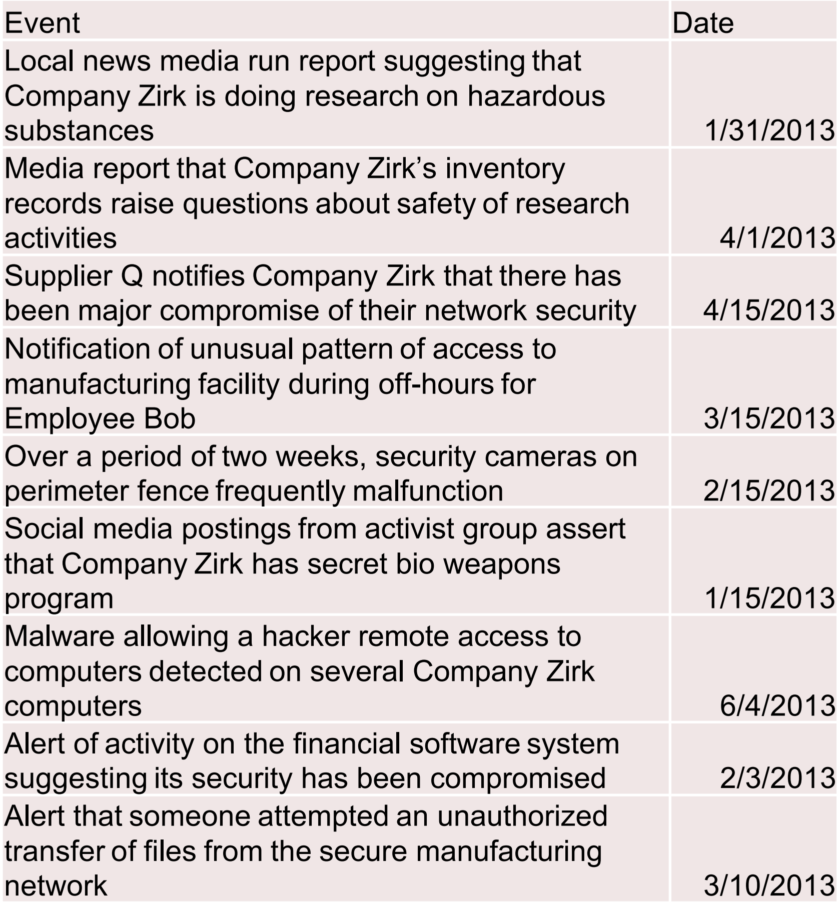


Could draw boundaries around groups of clues

Could draw connections between clues

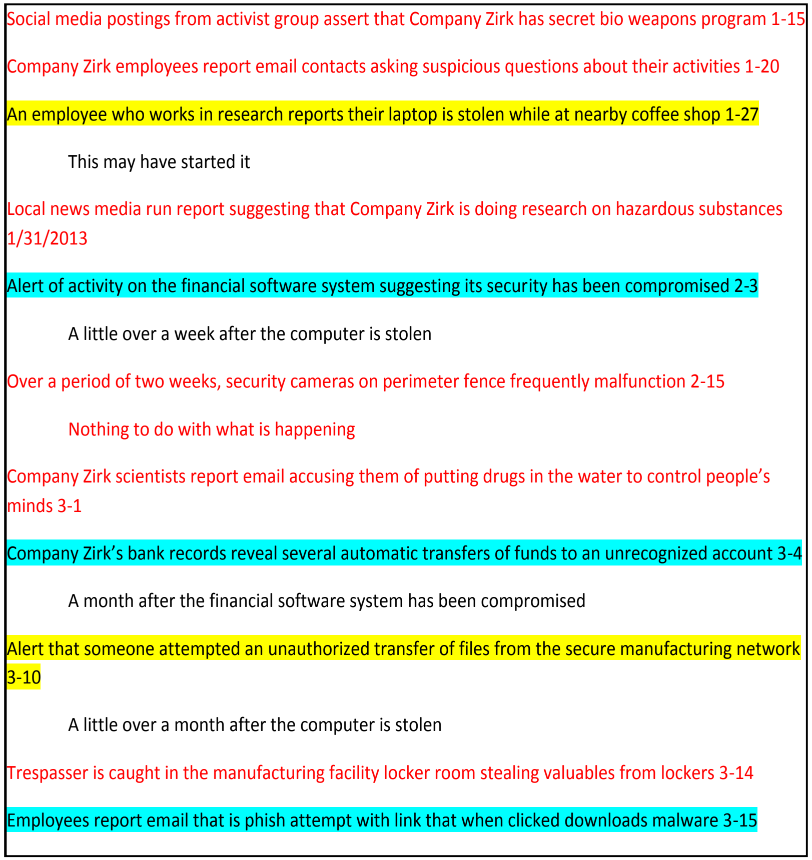
Impoverished had *no visuospatial elements for organizing clues or constructing a narrative*

Excel Spreadsheet with Clues



Event	Date
Local news media run report suggesting that Company Zirk is doing research on hazardous substances	1/31/2013
Media report that Company Zirk’s inventory records raise questions about safety of research activities	4/1/2013
Supplier Q notifies Company Zirk that there has been major compromise of their network security	4/15/2013
Notification of unusual pattern of access to manufacturing facility during off-hours for Employee Bob	3/15/2013
Over a period of two weeks, security cameras on perimeter fence frequently malfunction	2/15/2013
Social media postings from activist group assert that Company Zirk has secret bio weapons program	1/15/2013
Malware allowing a hacker remote access to computers detected on several Company Zirk computers	6/4/2013
Alert of activity on the financial software system suggesting its security has been compromised	2/3/2013
Alert that someone attempted an unauthorized transfer of files from the secure manufacturing network	3/10/2013

Word Document for Making Notes



Social media postings from activist group assert that Company Zirk has secret bio weapons program 1-15

Company Zirk employees report email contacts asking suspicious questions about their activities 1-20

An employee who works in research reports their laptop is stolen while at nearby coffee shop 1-27

This may have started it

Local news media run report suggesting that Company Zirk is doing research on hazardous substances 1/31/2013

Alert of activity on the financial software system suggesting its security has been compromised 2-3

A little over a week after the computer is stolen

Over a period of two weeks, security cameras on perimeter fence frequently malfunction 2-15

Nothing to do with what is happening

Company Zirk scientists report email accusing them of putting drugs in the water to control people’s minds 3-1

Company Zirk’s bank records reveal several automatic transfers of funds to an unrecognized account 3-4

A month after the financial software system has been compromised

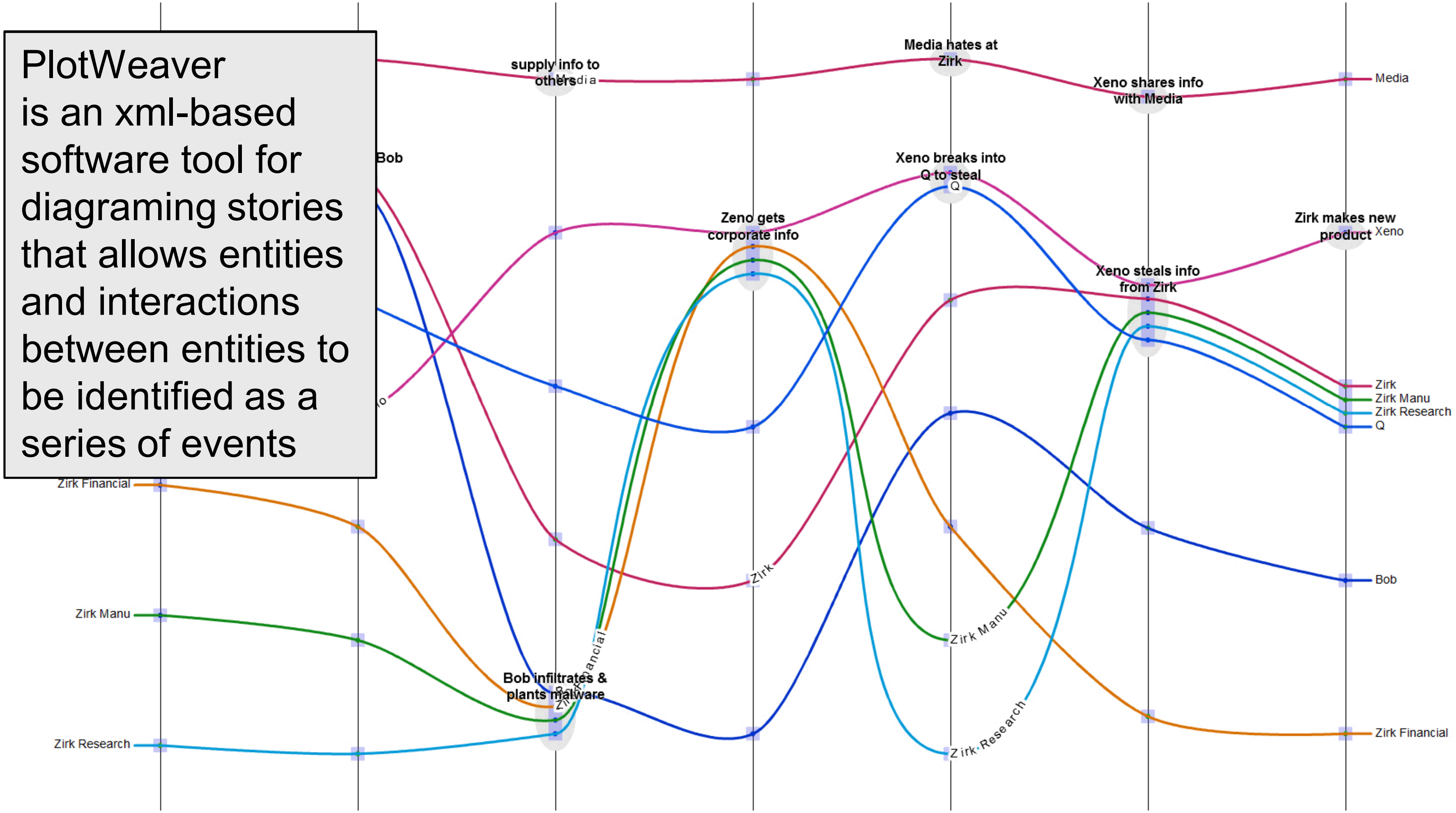
Alert that someone attempted an unauthorized transfer of files from the secure manufacturing network 3-10

A little over a month after the computer is stolen

Trespasser is caught in the manufacturing facility locker room stealing valuables from lockers 3-14

Employees report email that is phish attempt with link that when clicked downloads malware 3-15

After completing their analysis, subjects generated PlotWeaver diagrams



PlotWeaver is an xml-based software tool for diagraming stories that allows entities and interactions between entities to be identified as a series of events

PlotWeaver diagrams provided basis for assessing performance

- Number of clues used in diagrams
    - Number legitimate clues
    - Number red herrings
- Number of connections between clues (i.e., clues in PlotWeaver storyline)
    - Connections between legitimate clues
    - Connections with red herring clues
        - Legitimate x Red Herring
        - Red Herring x Red Herring
- Number of connections within the three threads
    - Hacktivists
    - Criminal
    - Insider

PlotWeaver diagrams provided basis for assessing forensic analysis performance

NOTE: Each "x" indicates that the two clues appeared together within the same PlotWeaver storyline and signifies a "connection"

Legitimate Clues

	Quest	Stole Laptop	Media Hazards	Email Phish	Invent Down	Media Safe	Mware Found	Finan Compro	Transfer Funds	Suppler Compro					
Socal media posting				x				x	x	x					
Suspicious questions															
Stolen laptop															
Media hazards															
Email phish								x	x	x					
Inventory dow															
Media safety															
Malware found															
Financial compromised									x	x					
Transfer funds										x	x				x
Supplier compromised											x				x
Invoices unpaid															
Transfer files															
Unusual access															
Flash drive															x
Announce capabilities															

Hacktivist Thread

Criminal Thread

Insider Thread

Red Herrings

	Soc edia	Susp Quest	Stole Laptop	Media Hazards	Email Phish	Invent Down	Media Safe	Mware Found	Finan Compro	Transfer Funds	Suppler Compro	Invoices Unpaid	Transfer Files	Unusual Access	Flash Drive
Drugs in water															
Tresspasser															
Botnet															
Mary gambling															
CD updates w/virus	x				x				x	x	x	x			
Backups corrupted															
External website															

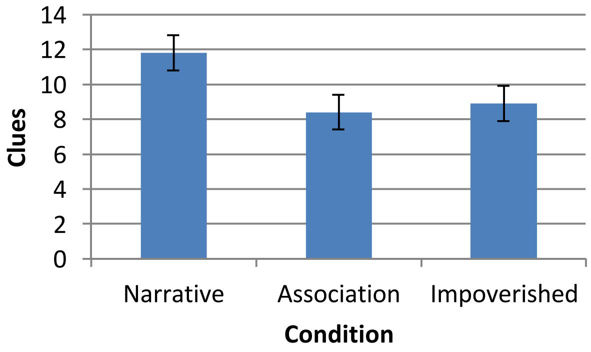
Plots scored through joint deliberation by two experimenters
20% of plots extracted for separate scoring by two experimenters
Interrater reliability = 96%

Subjects Drawn from the Sandia National Laboratories Employee Population

- Subjects
  - 52 subjects
    - 7 removed due to corrupted file for PlotWeaver diagrams
    - 6 removed due to OSPAN working memory scores 1.5 sd below mean
      - Removed OSPAN Scores 0-14;
      - Overall OSPAN Scores; Mean = 42.5 and SD = 19.3
    - Data analysis based on 39 subjects
      - Narrative Condition – N=14
      - Association Condition – N=12
      - Impoverished Condition – N=13

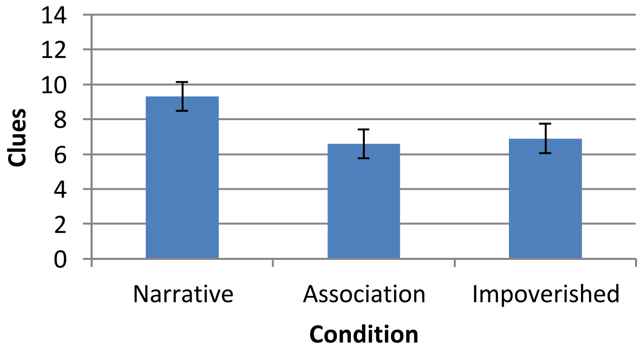
Subjects in Narrative Condition used more clues overall, while ignoring red herrings

Total Clues Used



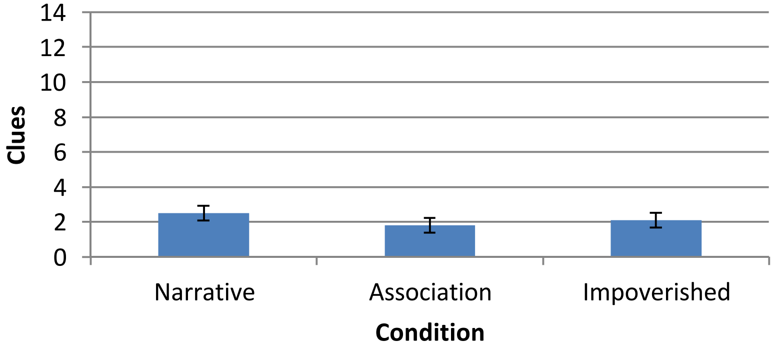
F = 3.49; *p*<0.05

Legitimate Clues Used



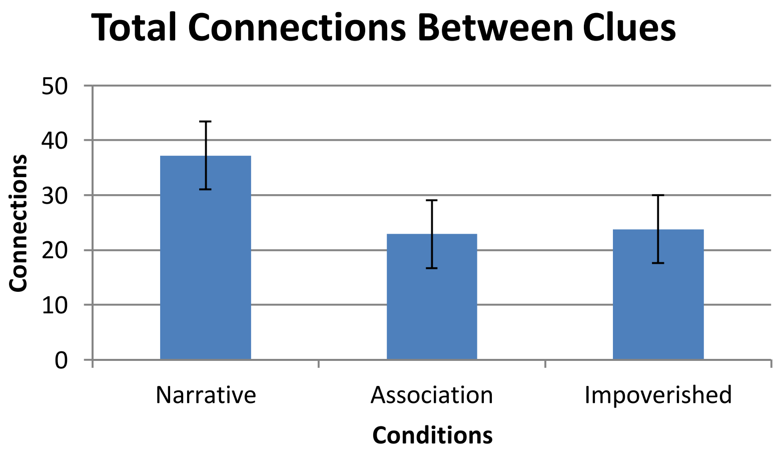
F = 3.37; *p*<0.05

Red Herring Clues Used

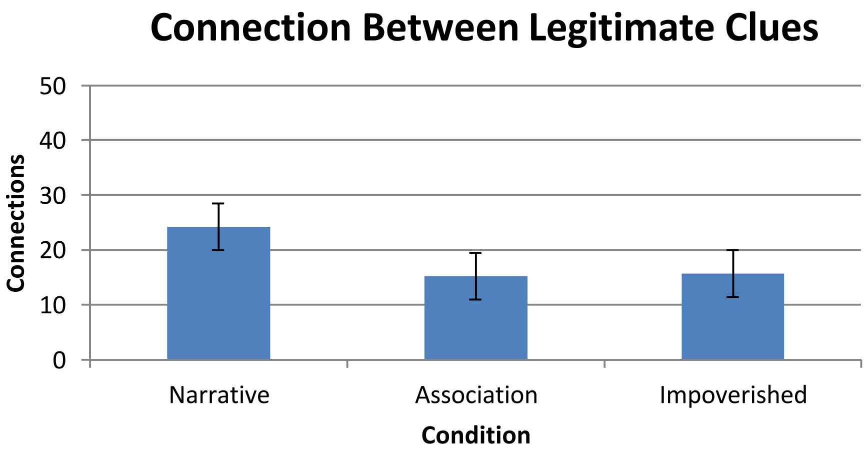


F = 0.55; *NS*

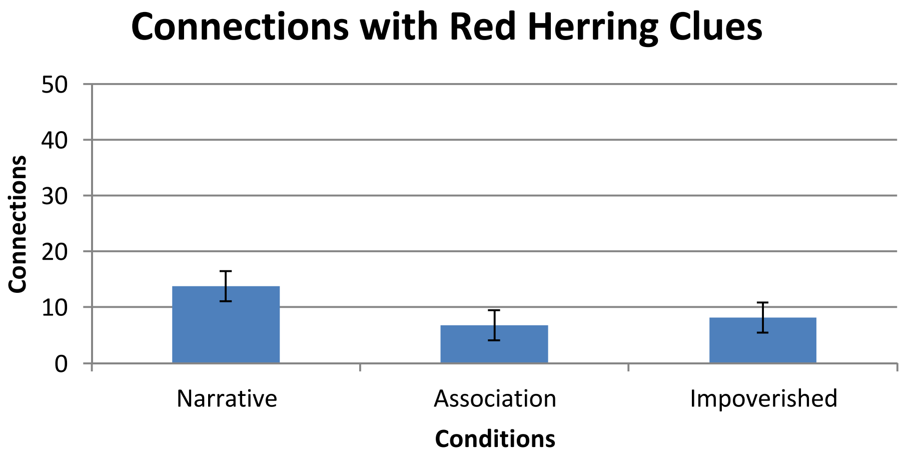
Narrative group made more connections, but the differences were not statistically significant



F = 1.72; NS

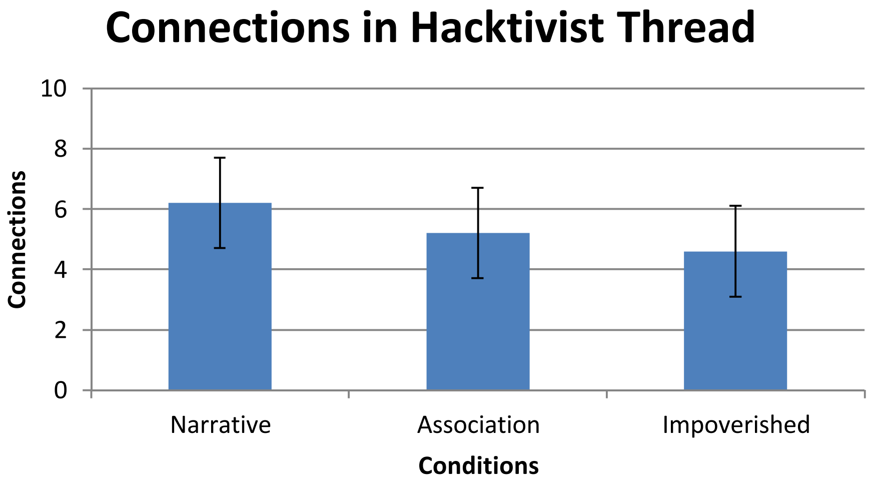


F = 1.44; NS

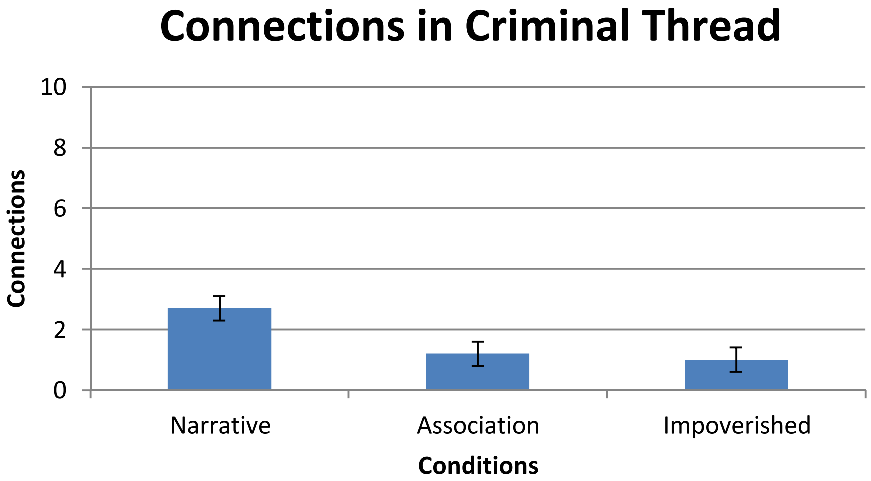


F = 1.63; NS

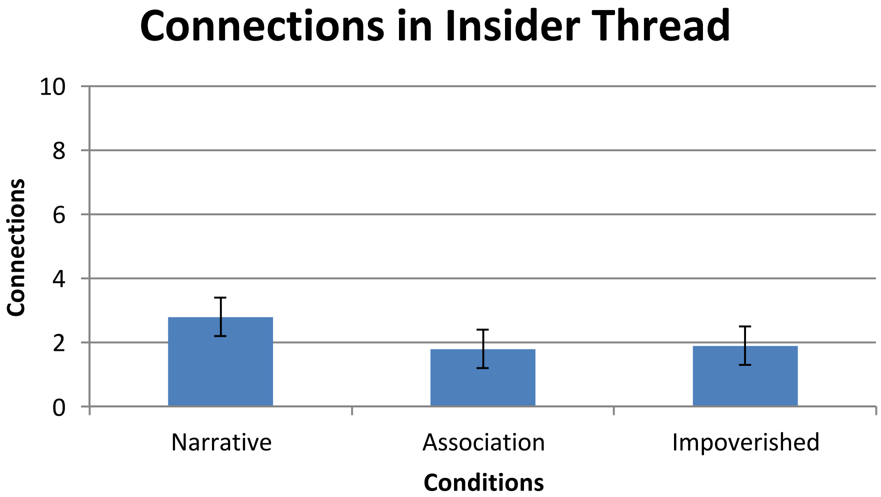
Narrative group made more connections within threads, and notably, the Criminal Thread



F = 0.31; NS



F = 5.68; *p*<0.01



F = 0.97; NS

Conclusion

- Tools facilitating and encouraging construction of a narrative account of events benefit cyber forensic analysis
- This difference may be attributed to two factors
  - 1. Mechanisms for consideration of entities and entity motives
  - 2. Mechanisms for annotating diagrams
- These functions may be incorporated into software tools used by cyber forensic analysts
- Narrative construction may be incorporated into cyber security training