# Attribution: Tracking down “whodunnit”

Presented by: Damian Donaldson MSc. CISSP, CISM

# Objectives

- Get the IP address of the person who created the offending profile.
- Get the IP address of the person who created and accessed the email account associated with the offending profile.
- Determine the identity of the individual(s) who committed the offending acts from the IP addresses obtained in the first 2 bullet points above.

# A hunting we will go

- We got the perpetrator's IP addresses from Facebook and the Email Service Provider.
- The IP addresses are registered to a local Internet Service Provider (ISP)
- The ISP indicates that the IP addresses were assigned to 2 organizations during the time the offending profile was created.
- These organizations have private computer networks with several computers connected to it and several persons within those organizations who use those computers to access the Internet.
- The Challenge is to identify which individual(s) within each organization actually committed the offending act.
- It is necessary to go to the organizations and gather evidence in order to investigate and track down the perpetrator.

# Gathering the Evidence

- What evidence do we need?
- Where is the evidence found?
- How do we go about preserving and gathering
- the evidence?
- The Digital Forensics Process will help to answer these questions.

# Gathering the Evidence: Digital Forensics Process

- Digital Forensics is the scientific process of data acquisition, analysis and reporting which supports the investigation of computer technology related incidents.
- Data can come from different sources and devices, hence there are different branches of Digital Forensics – computer forensics, network forensics, mobile device forensics, database forensics etc.

# Gathering the Evidence : Digital Forensics Process

Acquire data – how this is done will depend on the kind of devices/systems being targeted and the kind of data being gathered. However it is key that the acquisition process does not alter the data being gathered or else evidence will be compromised. Once data is gathered chain of custody must be preserved.

# Gathering the Evidence: Digital Forensics Process

Analyze data – examine gathered data to identify evidence which sheds light the incident being investigated. Look for clues to help answer the what, when, where, why and who questions.

# Gathering the Evidence: Digital Forensics Process

Report Findings – The report on findings articulates what the investigation has found. This is key to support building a good case for legal matters.

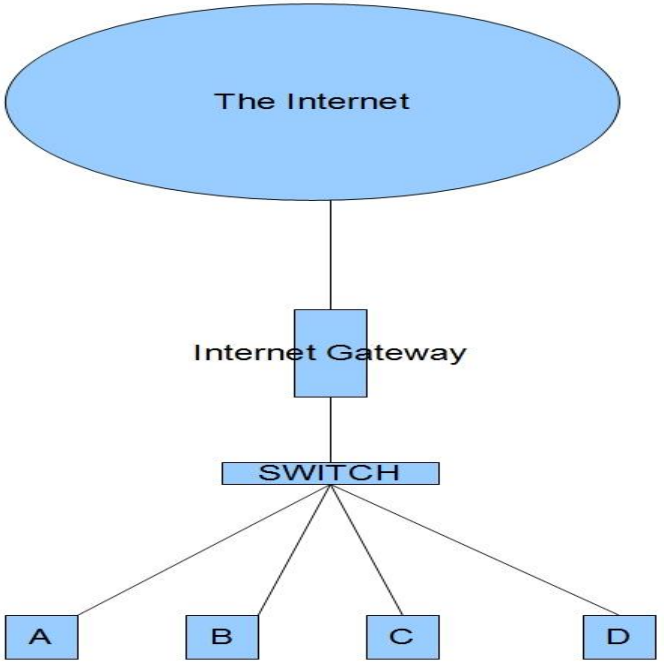
# Gathering the Evidence

- We are looking for anything that can identify who accessed Facebook and created the offending profile.
- We are looking for anything that can identify who created and operated the email account associated with the offending Facebook profile.
- Examples: log file data, images and web pages cached from the sites in question, documents with information tying an individual to the nefarious activities
- Evidence may reside on the actual computer which the perpetrator used to carry out the activities. Evidence may also reside on other computers and/or devices which would have facilitated Internet access to the perpetrator.
- We need to go in, seize computers and equipment, and conduct forensic analysis to obtain and gather the evidence.

# Gathering the Evidence: Considerations

- Which computers/equipment do you seize and search?
- If you don't know which computer(s) were used to commit the offense, you could seize and search everything.
- Seizing and searching everything is very costly and it is very disruptive to the organization.
- Have to find a way to narrow down the search.

# Gathering the Evidence: Typical Corporate LAN



# Gathering the Evidence – The Corporate Internet Gateway

- The Internet Gateway could be a proxy server, firewall, or router.
- In a typical LAN, the Internet Gateway may have logs which tell which users and/or computers have accessed particular sites on the Internet.
- We need to get logs from the Internet Gateway device which show who accessed Facebook at the time the offending profile was created, and who has been accessing and operating the email account associated with the false profile.

# Gathering the Evidence

- Once we get the log files from the Internet Gateway, they can be examined to identify the users/computers that accessed the offending profile and associated email account.
- If the company required users to authenticate with userid before accessing Internet and that information is logged, then we may be able to identify an individual directly from the logs. If they don't, we may just get the IP address of the computer they used to access the sites in question. Regardless, we need to find a computer (or computers) and search.

# Gathering the Evidence

- Once we've gotten the IP addresses of the computer(s) which accessed the sites in question at the times in question, we need to match those IP addresses with physical computers.
- IP addresses are usually leased to computers on the network, expired after a time and renewed. A computer on the network can change IP addresses over time.
- We need to determine which computer(s) held the IP addresses at the times the sites in question were accessed as indicated by the logs.

# Gathering the Evidence: IP address issues

- On a typical corporate network, IP address assignment is handled by a computer called the DHCP Server (DHCP = Dynamic Host Configuration Protocol).
- The DHCP server may have logs recording which IP addresses were assigned to computers.
- The IP addresses are actually associated with MAC Addresses which are hard-coded to the network interfaces inside the computers.
- We need to find which MAC address was assigned the IP address shown in the Internet gateway logs as having accessed the sites in question at the times in question.
- IP addresses can also be statically assigned without the DHCP server. If this was the case, the DHCP server would not have any record of the assignment. We would therefore need to seize and search the computers currently assigned the IP addresses identified in the Internet Gateway logs with the hope that the IP addresses were assigned to those computers during the times in question (no guarantee of this).
- Note that an IP address alone does not provide absolute attribution.

# Gathering the Evidence

- Once the actual computer hardware has been identified either by MAC address or current IP address assignment, actual evidence collection needs to take place.
- To preserve evidence, the users of the computers in question cannot be tipped off about the investigation lest they destroy evidence.
- The computers in question need to be quickly seized, and taken out of service (powered off) so that normal operations do not erase or overwrite the evidence we need.

# Gathering the Evidence: Say Hi to FRED :)


Forensic Recovery of Evidence Device

# Gathering the Evidence

- FRED along with forensic data acquisition software tools (Encase, Forensic Toolkit etc.),allow us to make an exact bit-level digital copy of all the data on the hard drives in the computers we want to forensically analyze (forensic image).
- FRED employs “write blocking” at the hardware level to prevent us from modifying or altering data on the target hard drive while we are in the process of making that bit-level digital copy of the data on it, thus preserving the integrity of the evidence.
- We will use FRED to acquire the data from the target computer(s) in a forensically sound manner for us to analyze for evidence. We will not actually be working with the actual target system for analysis.

# Gathering the Evidence: Chain of Custody

- Now that we've acquired the data, we need to preserve the integrity of the evidence by adhering to strict chain of custody procedures.
- We need to document who has possession of the evidence at all times, and when possession of the evidence is handed over to another custodian.
- We need to ensure that the evidence gathered is securely stored until needed for analysis.
- If chain of custody is broken - evidence is handled by unauthorized persons, evidence is handled in unauthorized manners, or custody cannot be accounted for, then the evidence can no longer be trusted.

# Gathering the Evidence: Analysis

- Now we can search the acquired hard drive data using Digital forensic tools (eg. Encase, or Forensic ToolKit) to see if evidence of visits to the profile in question and email account in question exist.
- This will help to prove the offences were committed from the computer(s) in question.
- We are particularly interested in the contents of the web browser cache which may have downloaded images and web pages from the sites in question.
- We are interested in finding any other files or documents which may evidence the offence.
- Local log files showing who logged into the computer during the time the sites were accessed.

# Gathering the Evidence: Putting it all together

- Once the analysis is complete, and evidence has been identified. It is time to put it all together and report on the findings.
- Were the questions asked answered? Was there evidence to identify who was responsible?
- The steps taken to come to conclusions must be clearly stated in a logical manner so that a proper case can be built and supported for court.

# Gathering the Evidence

- If all goes well, the investigation should reveal who created the malicious facebook profile, who operated the email account associated with the malicious facebook profile and from which computers were these actions perpetrated.
- Findings would be documented in a nicely presentable report which can be understood readily by the court and which supports the case being made.

# Interesting Points

- Just like in the real physical world, in the digital world, there is no guarantee that there will be adequate credible evidence to prove or disprove a particular case.
- Just like in the real physical world, digital evidence can be “lost” - destroyed, corrupted, tampered with, or planted.
- Just like in the real physical world, it may not be enough to rely on “circumstantial evidence” alone. There is need for corroboration of evidence, and often digital evidence needs to be supported by physical evidence (and vice versa) in order to build a strong case.

# The End.

Thank You. :)