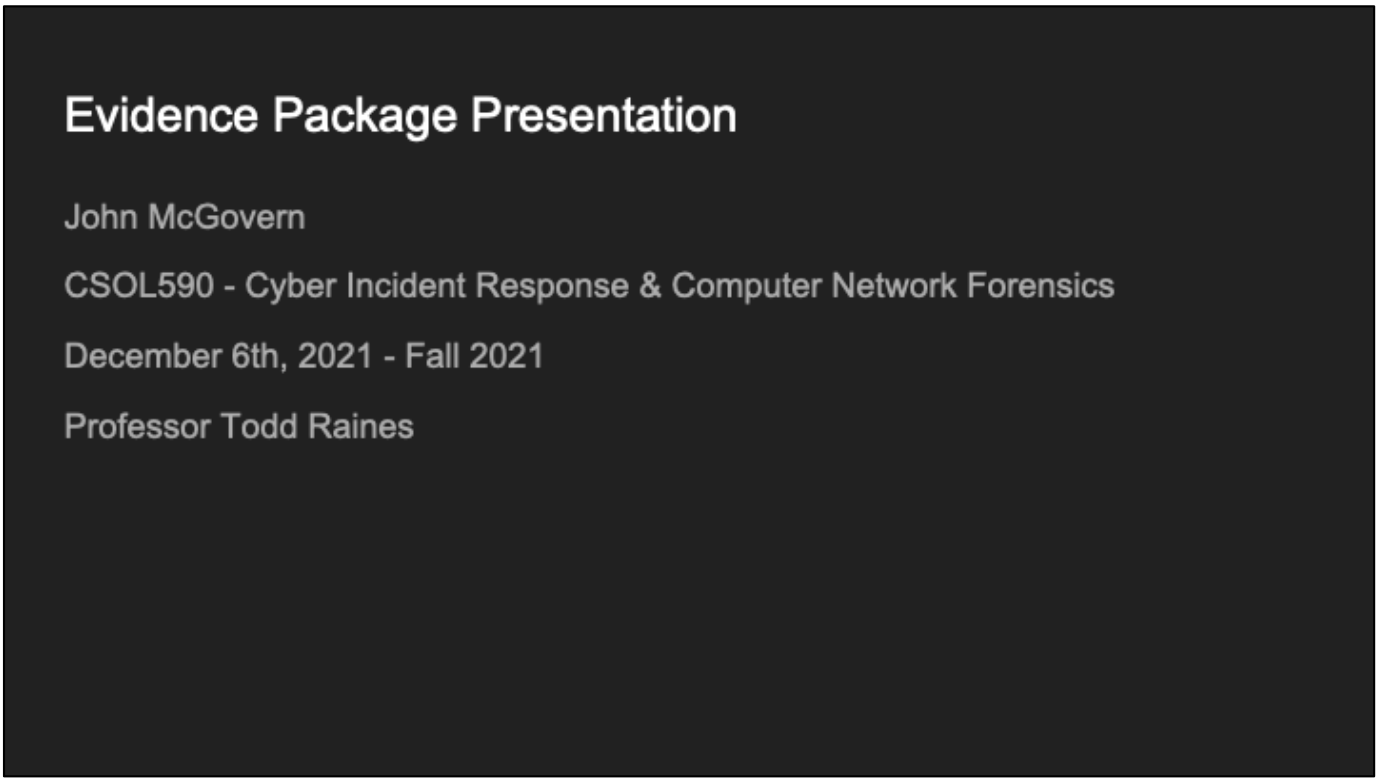
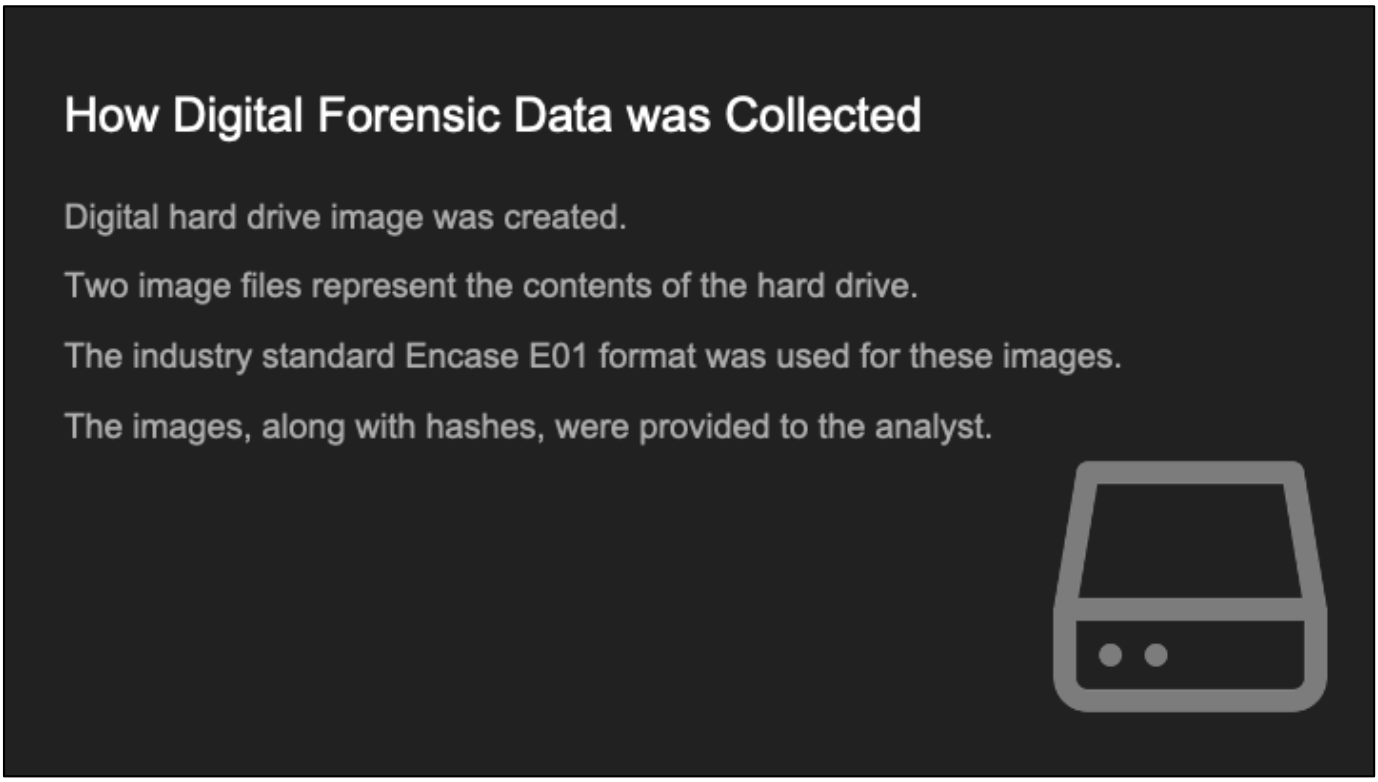


Evidence Package Presentation
John McGovern
CSOL590 - Cyber Incident Response & Computer Network Forensics
December 6th, 2021 - Fall 2021
Professor Todd Raines

M57.Biz
Evidence Package Presentation

John McGovern

December 2021

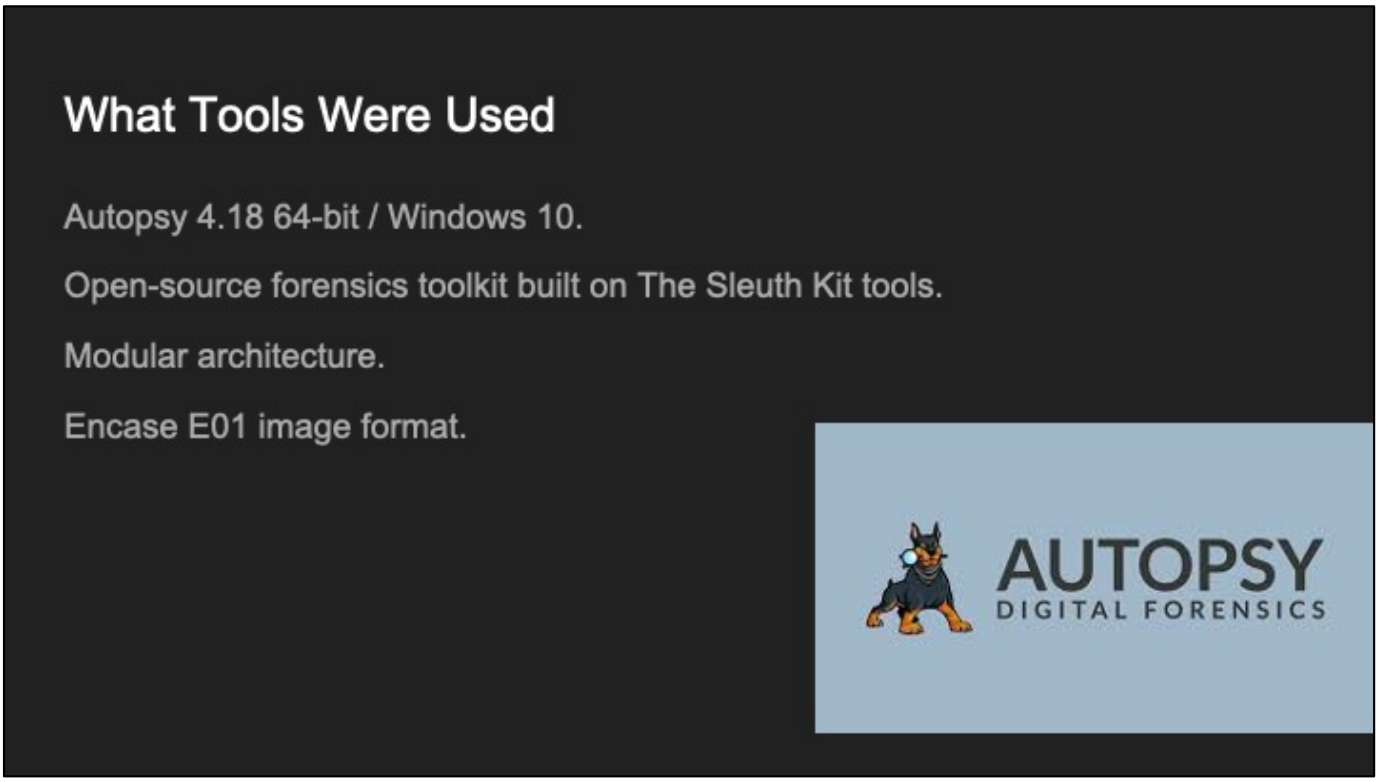


Jean User's PC was forensically imaged.

Two image files: nps-2008-jean.E01 & nps-2008-jean.E02 were produced. They are both part of the same image. The Encase splits the image into multiple 640MB files as needed.

The Encase E01 file format represents and industry standard format that is understood by a variety of forensic imaging tools.

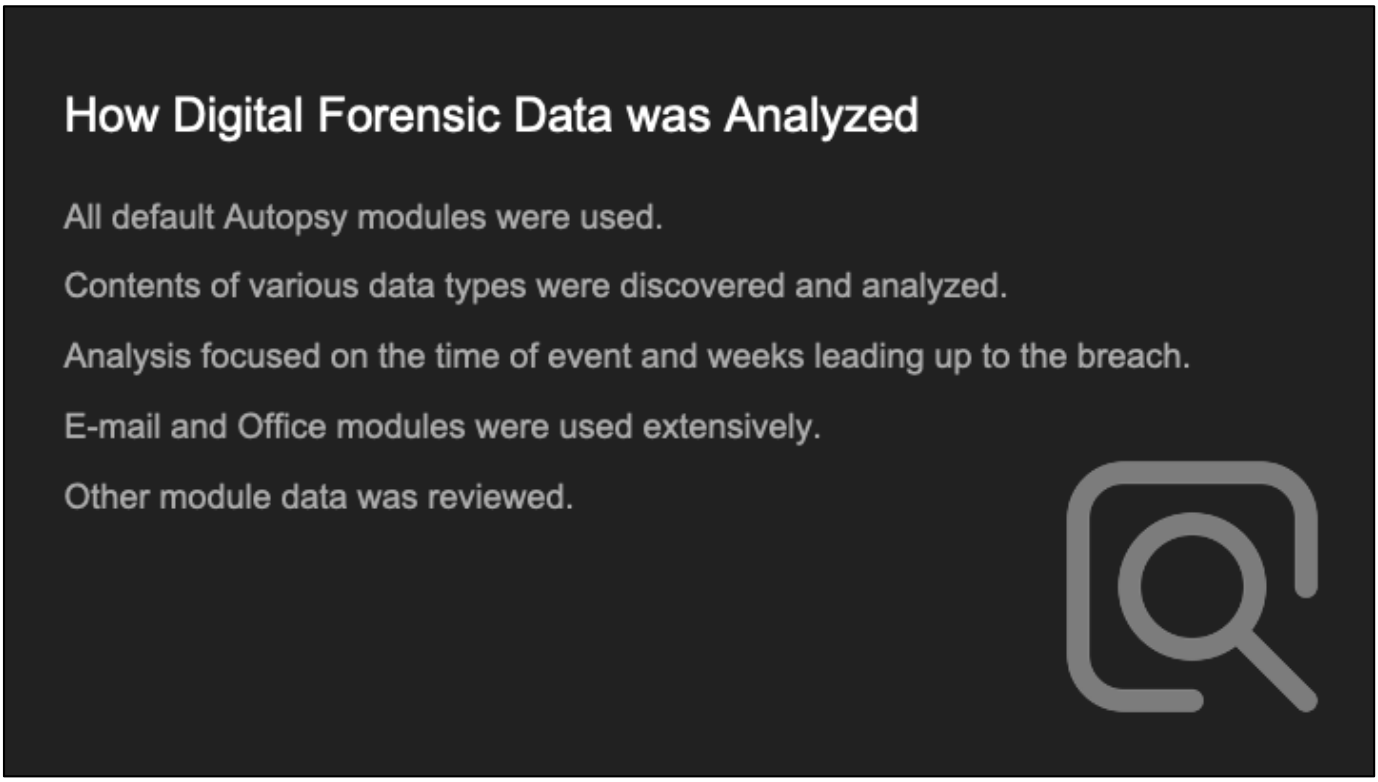
The collected images along with hashes were provided to the analyst for discovery.



Autopsy 4.18.0 64-bit running on Windows 10 was used on the analyst's workstation.

Autopsy is an open-source forensics toolkit built on The Sleuth Kit forensic software tools package.

Autopsy's modular architecture allows the analyst to capture and understand a wide variety of data types from the forensic image (Basis Technology, 2016).

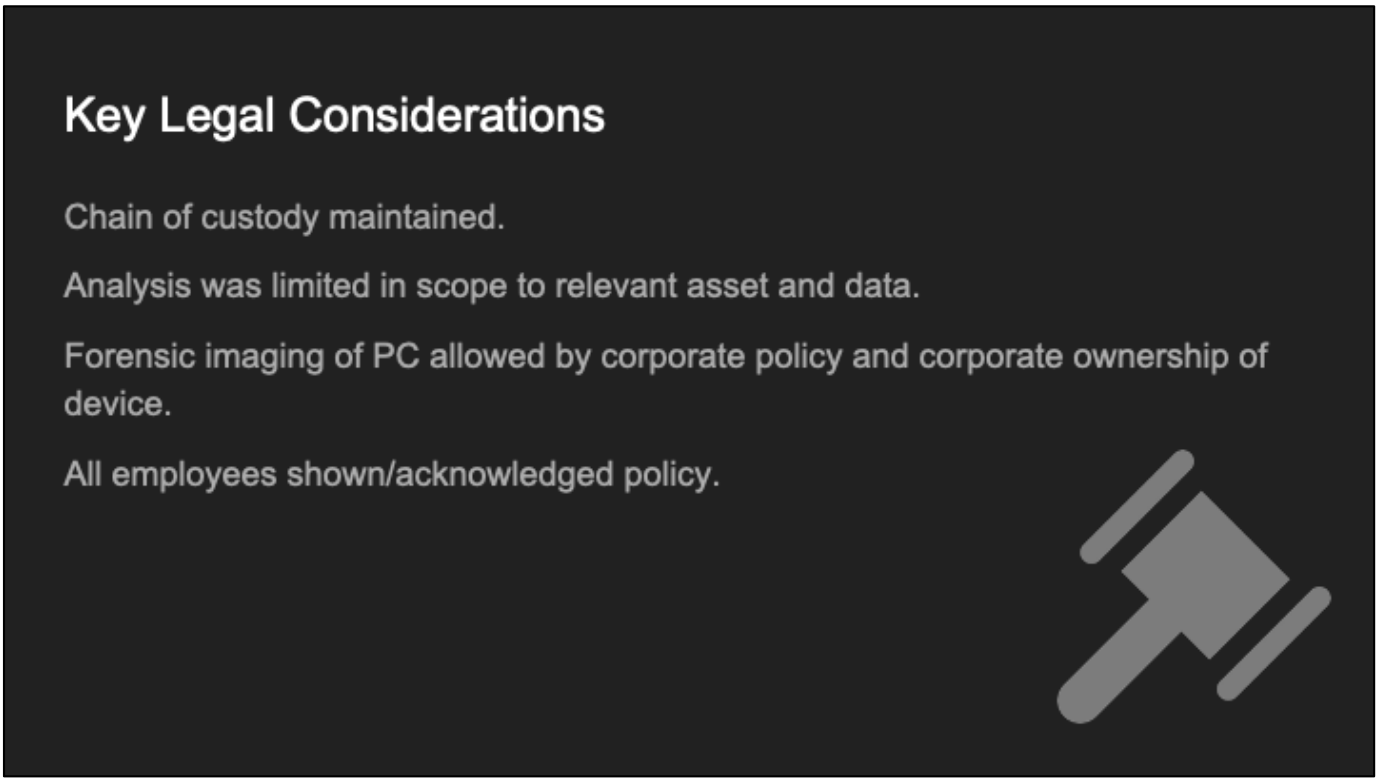


The default set of Autopsy modules were enabled to extract common data formats from a Windows XP system.

The contents of these data types were organized and presented by the Autopsy software for the analysts review.

Particular attention was paid to the time the breach was suspected and the weeks leading up to it.

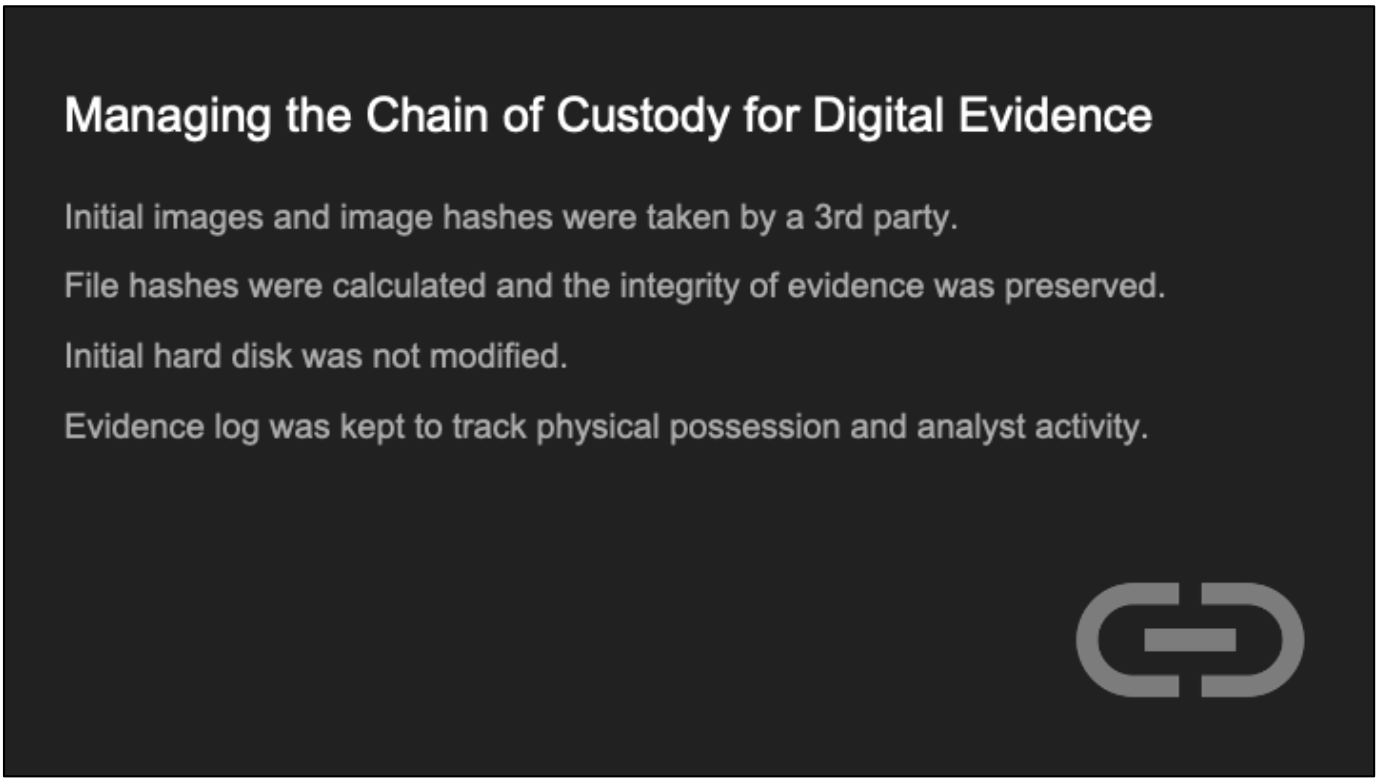
The email and Office document modules were particularly relevant to this case and captured the relevant evidence as discussed in subsequent slides.



The chain of custody of digital evidence was prioritized and maintained throughout the investigation.

The forensic analysis performed was limited in scope to the PC involved in the breach to protect employee data and privacy. No additional forensic images were provided for analysis.

Forensic imaging of the M57.Biz system is allowed as it is a company-owned asset and based on language in the corporate Acceptable Use Policy.

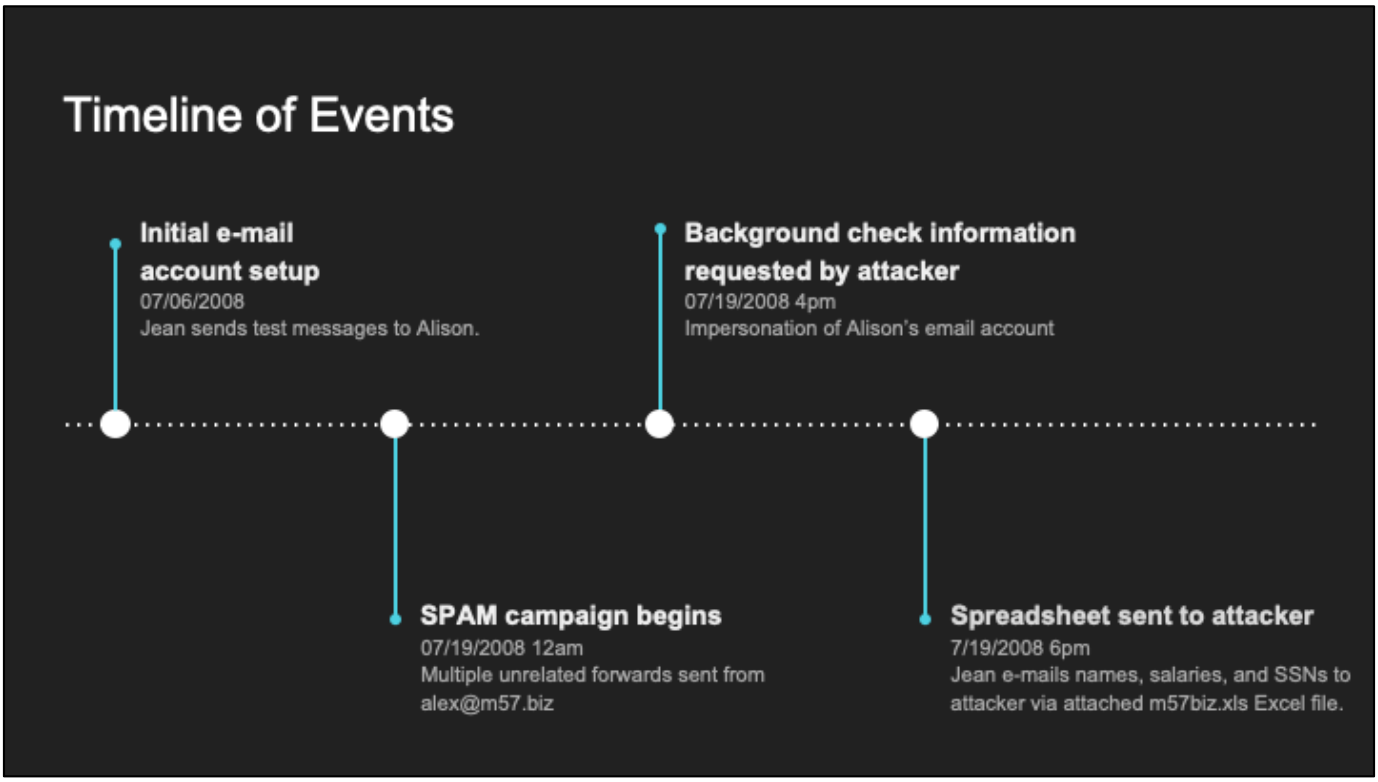


The hard drive image was collected by a 3rd party and provided to the examiner for analysis.

All work was performed on a copy of the forensic data rather than the original drive for the purposes of preserving the original if comparison is needed (Obbayi, 2019).

File hashes of the disk image as a whole and all files applicable to the investigation were taken.

An examiner log was maintained to track physical custody and forensic analyst activity concerning the M57.Biz forensic image. A form based on the NIST provided example was used (NIST, n.d.).



07/06/2008 – Jean's e-mail account was setup and test messages from Jean to Alison were sent to ensure the system was working.

07/19/2008 00:06:31 PDT – SPAM campaign begins from alex@m57.biz address. This was potentially used to cause confusion and distract from other malicious communications.

07/19/2008 16:39:57 PDT – Initial request for background check information was sent from the 3rd party (attacker). An alternate return address was first used in this communication (presumably to capture replies).

7-19-2008 18:28:00 PDT – Jean e-mails m57biz.xls to the 3rd party. This is the message in which the data disclosure occurred.

7-19-2008 22:03:04 PDT – The 3rd party acknowledges receipt of background information spreadsheet.

7-20-16:53:19 PDT – Bob discovers his personal data posted online and informs his colleagues. Subsequent e-mails are sent trying to identify what happened.

Summary of Findings

The 3rd party spoofed e-mail information to impersonate Alison.

The 3rd party requested personnel data based on false urgent need.

x57biz.xls spreadsheet was e-mailed to a 3rd party (attacker).

The m57biz.xls spreadsheet was created by Alison, modified by Jean, and sent by Jean.

Multiple successive failures in security controls lead to successful attack.

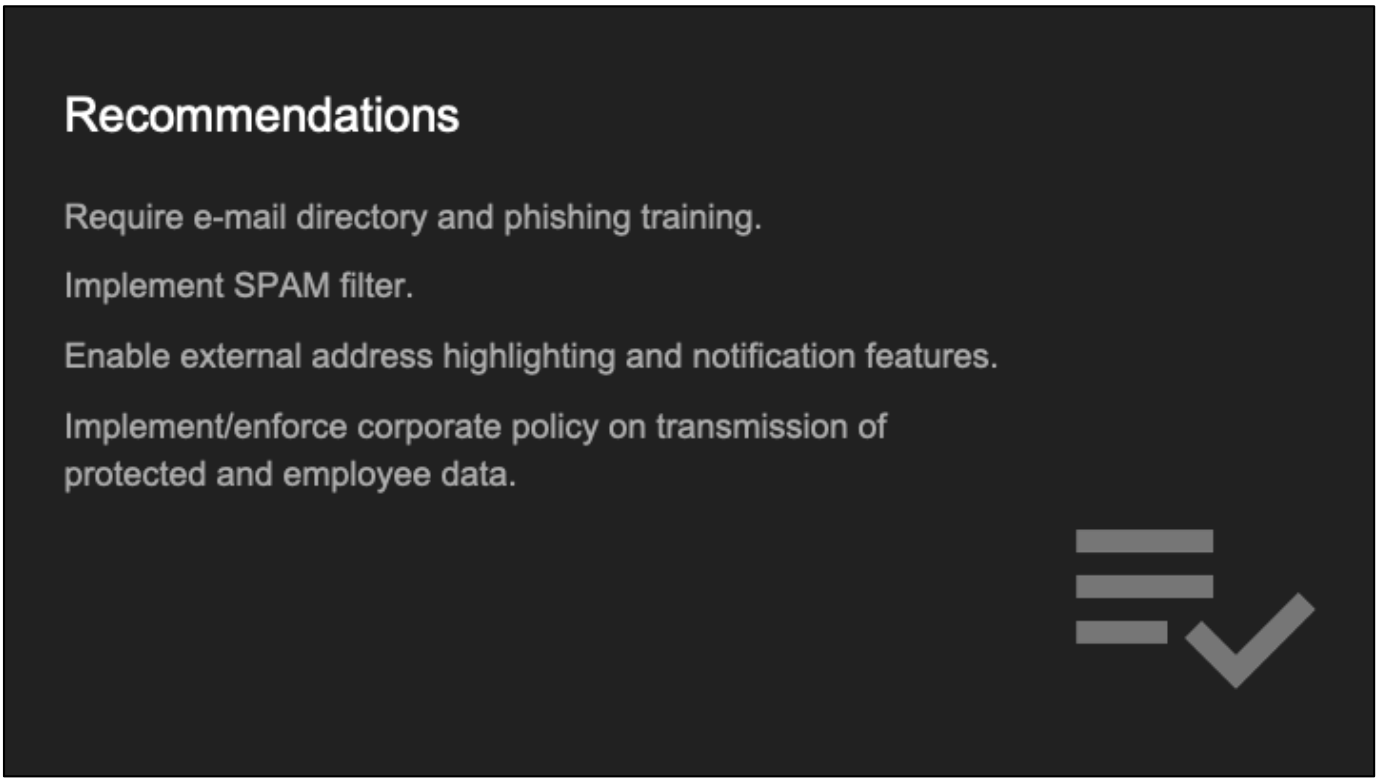
The 3rd party spoofed the e-mail from: address to appear as though they were from Alison and modified return addresses to capture responses.

The 3rd party requested that the employee data be provided based on the claim that venture capital investors were conducting employee background checks.

m57biz.xls Excel spreadsheet was provided via Jean's e-mail account to a third party.

The m57biz.xls Excel spreadsheet was created by Alison. It was modified by Jean before being sent to the 3rd party.

Multiple successive failures in security controls and best practices lead to a successful targeted phishing attack and subsequent disclosure of employee data.

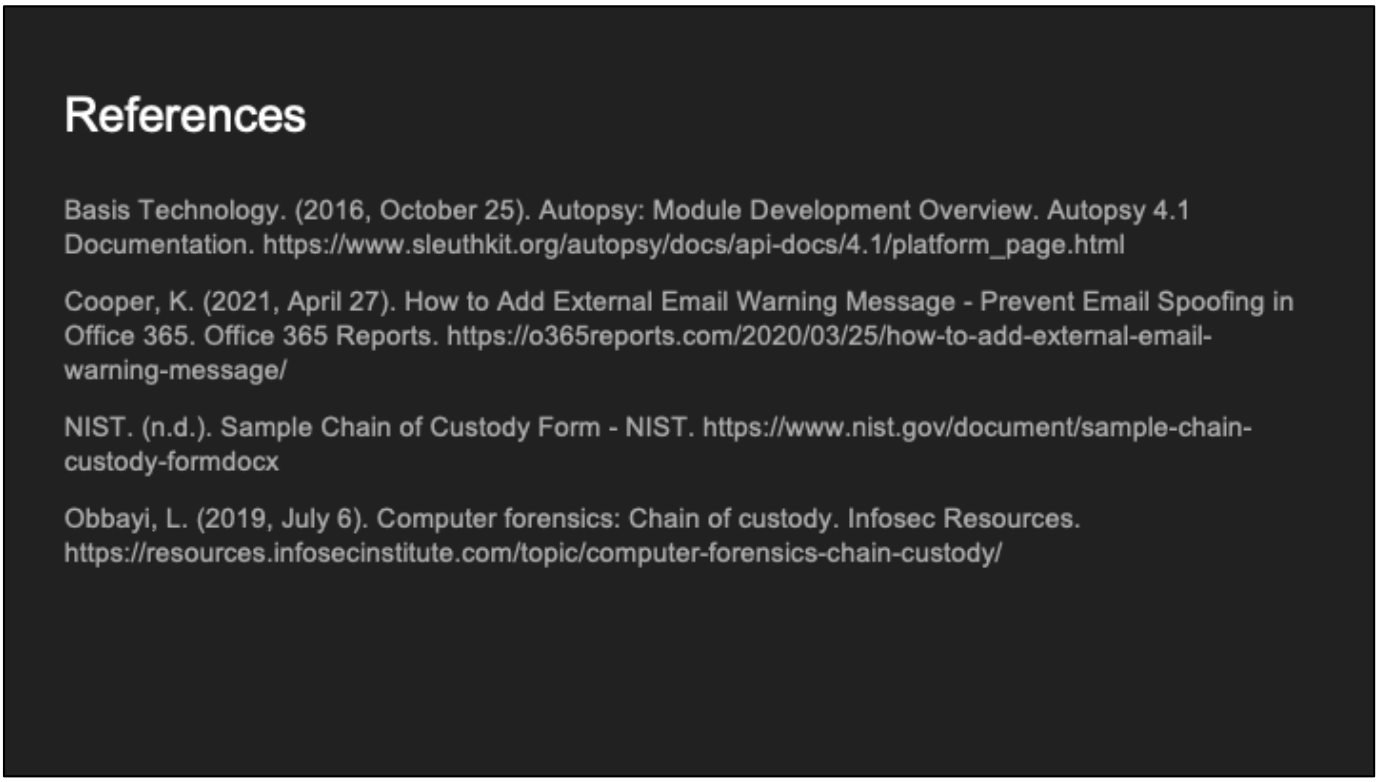


The e-mail setup and addresses in use were confusing for employees. Communications indicated they did not know which address to use for Alison. Corporate e-mail and phishing prevention training should be implemented and required for all employees.

Phishing prevention failed to block the phishing message set. SPAM filtration is highly recommended for the corporate e-mail system.

In-application highlighting, and warnings should be used to indicate when a message will be sent to an external recipient (Cooper, 2021).

Corporate policy should prohibit the use of e-mail to send personnel information such as was provided using the m57biz.xls spreadsheet.



References

Basis Technology. (2016, October 25). Autopsy: Module Development Overview. Autopsy 4.1 Documentation. https://www.sleuthkit.org/autopsy/docs/api-docs/4.1/platform_page.html

Cooper, K. (2021, April 27). How to Add External Email Warning Message - Prevent Email Spoofing in Office 365. Office 365 Reports. https://o365reports.com/2020/03/25/how-to-add-external-email-warning-message/

NIST. (n.d.). Sample Chain of Custody Form - NIST. https://www.nist.gov/document/sample-chain-custody-formdocx

Obbayi, L. (2019, July 6). Computer forensics: Chain of custody. Infosec Resources. https://resources.infosecinstitute.com/topic/computer-forensics-chain-custody/