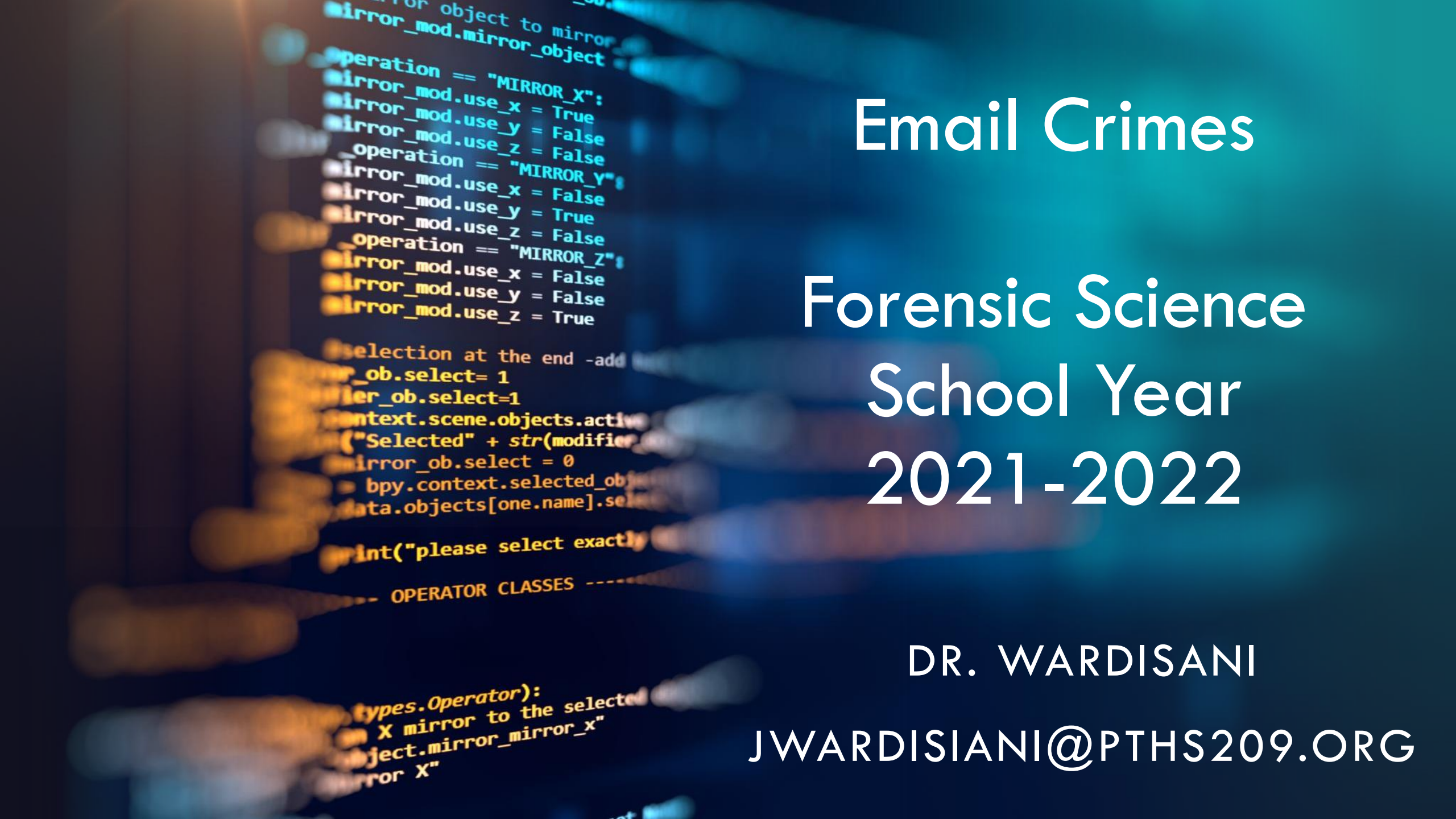


Email Crimes

Forensic Science
School Year
2021-2022

DR. WARDISANI

JWARDISIANI@PTHS209.ORG

Emails

- This section covers some basics that the every day email user can do to trace down an offending email sender.

- Enabled an efficient means of communication, without the limitations of time zones, speed or cost, usually associated with many of the other forms of communication

- Can easily be used for negative purposes as well, making SPAM and virus emails a problem

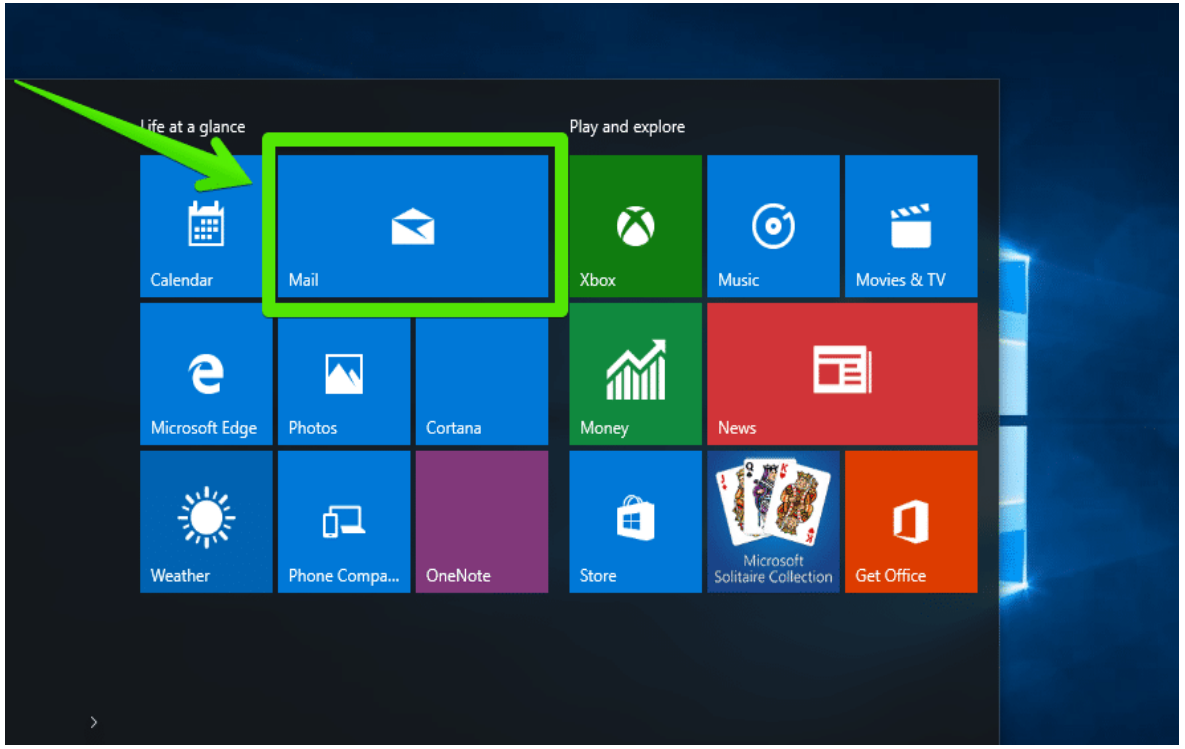
An IP Address

123.456.789.12

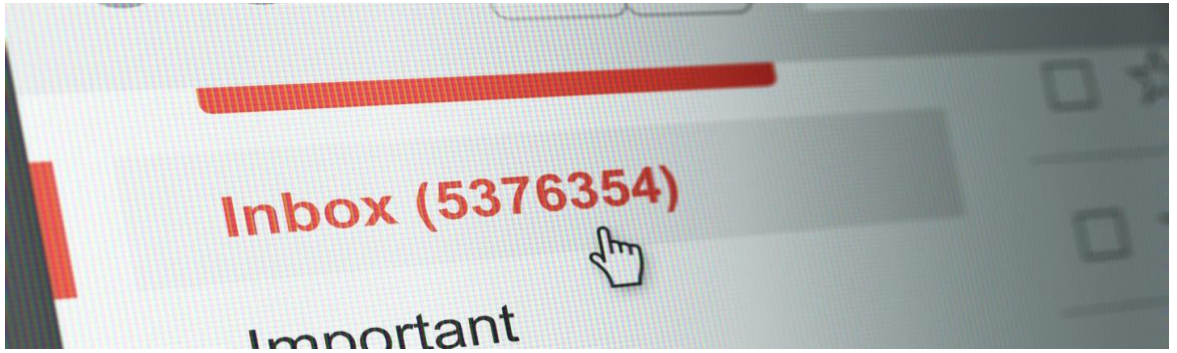
- Used to track down and differentiate between computers.
- Each computer's IP address is unique, composed of 32 bits and grouped into four lots of eight bits.
- The IP address is recorded every time your computer makes contact with a server, including when you first log on with your ISP (internet service provider) to when you access different web pages.
- Different websites have an IP address composed of bits, but for convenience, the long chain of numerals is instead interpreted into an easier to remember word address using a domain name service (DNS).
- During the trace back of an email message, the IP address of the various protocols used to transfer the email from one location to another can be useful.

Email Programs

- There are a variety of email programs used to manage, store and compose emails
- Email programs such as Outlook and Eudora specialize in encoding and decoding received email messages, to make them understandable, not unlike the encryption and decryption process described in the next section, but slightly simpler.
- encoding is mapped to an email standard, a form of coding which holds information for the posting of messages from place to place.
- Some common email standards are MIME (multipurpose internet mail extensions) and uuencode, of which the latter is more often used in attempts to hide information in a message but can be easily decoded by various decoding utilities that come with major operating systems.



Email Logs



- Kept on all email servers as a record of emails which were sent, received, the email addresses involved and the time/date of posting receipt.
- May be a problem if some servers use circular logging where a certain amount of data space is allocated for the storage of log files but once this space is full, the earliest log of files is overwritten and the data is deleted for good.
- The log files are commonly formatted into just plain text and their main use is for identifying the source of the offending emails.
- Different email servers have different forms of email logs, but the information on these files provide are the same.

Email Headers

- Prove information not unlike that of an email log, but details the path the email took in terms of which protocols were used to transfer the messages and thus work backwards
- The return path of the email, the email address to which your email program will send a reply, is not the source of the message when an offender deliberately tries to disguise his/her tracks.
- Each email has a unique message ID, which corresponds to data contained in a message log.
- By default, this information is not shown, but is easily accessible in most email programs.
- For example, Microsoft Outlook displays this information when the property of an email is displayed, and view source is chosen.

Thank You!!! ☺

QUESTIONS AND COMMENTS