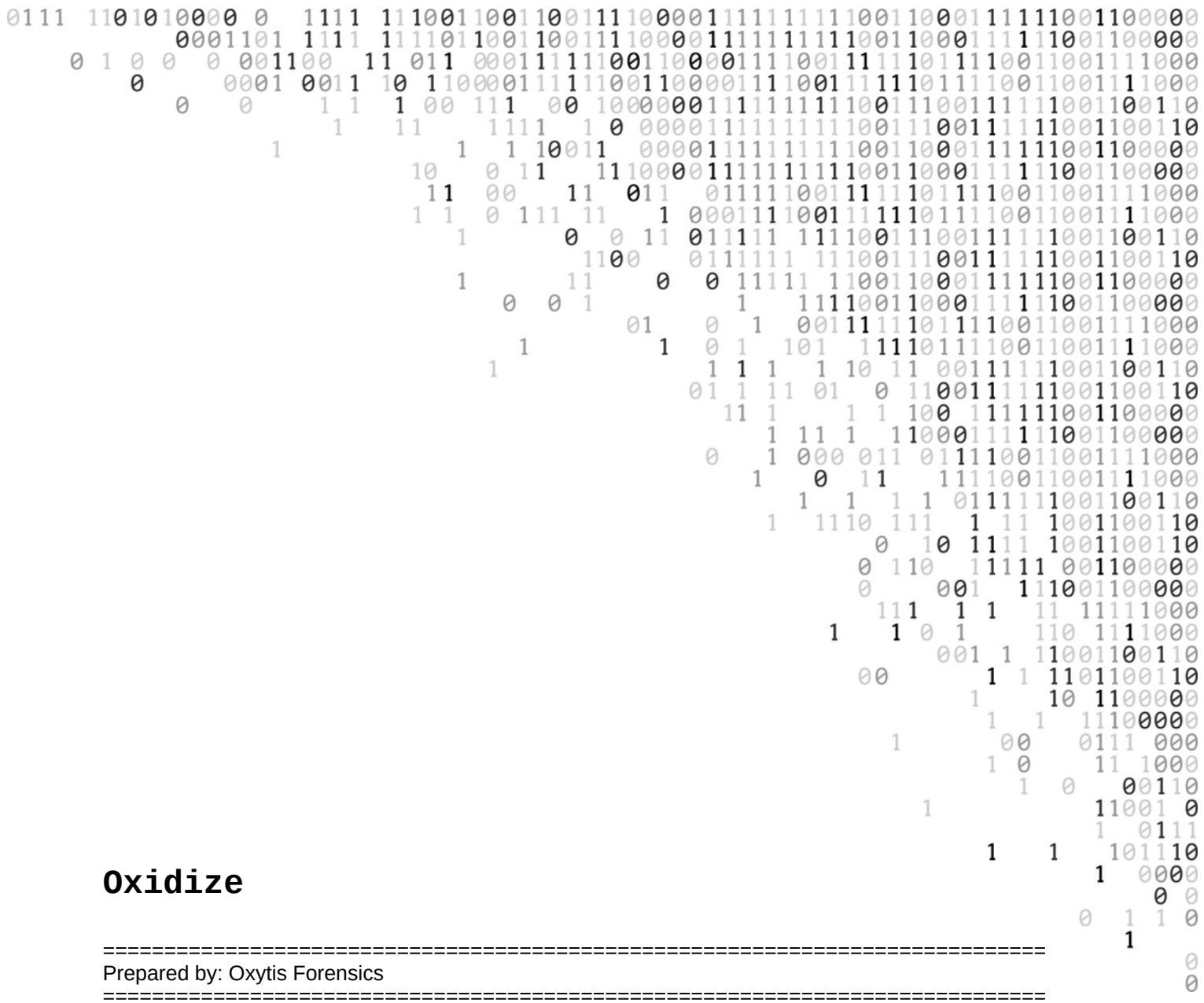


Oxidize

==========
Prepared by: Oxytis Forensics
==========

ACME Incorporated

==========
Date: 11 July 2022
==========

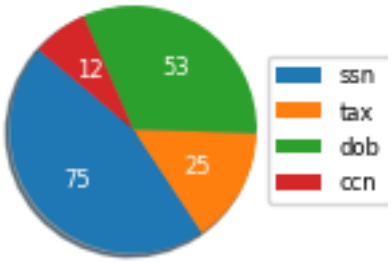
Oxidize

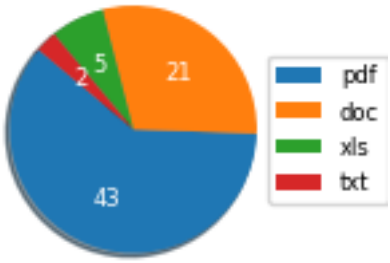
Your request to have a Digital Investigation of Electronically Stored Information (ESI) has been completed. Oxytis Forensics examined objects of digital interest made available by ACME for analysis. These objects were chosen by ACME as a representative sample of suspicious activity and/or impact of malware, or the only objects remaining of forensic interest.

Findings

Oxytis Forensics found 165 total occurrences in 71 unique locations or documents of potential Personally Identifiable Information (PII) information. Alternate searches for numerous data elements and variations of jurisdictional specific PII included (Variations, alternations, colloquial references also searched):

Jurisdiction: US Sectoral; federal and state laws; requirements and pre-emption
State and type business formation: Delaware, LLC
Template: US
Tags: Privacy and Security + Consumer Privacy + Data Security + Identity Theft





Total: 165
Unique: 71

Oxytis Forensics determined the resulting dataset included the [ssn] term or the format of [ssn] as the most discovered PII element.Oxytis Forensics provided a list of all documents including related information on a reasonable basis to believe that the information associated in these documents can be used to identify an individual and is considered individually identifiable information. Some of the information includes direct identifiers that can be uniquely associated to an individual.

Other results may include quasi-identifiers when combined with other quasi-identifiers may also uniquely identify an individual. Quasi-identifying information is often publicly available and can be used with this information, although not publicly available and not considered PII, to uniquely identify an individual. This information can be used for various fraudulent activities from identity theft to tax fraud.

Recommendations

The duty to preserve evidence arises upon the reasonable anticipation of litigation and expands accordingly on receipt of pre-litigation correspondence, service of process and/or subsequently served requests for information. This digital investigation approach corresponds closely to those stages in standard eDiscovery work although the emphasis is subtly different. An eDiscovery seeks to reduce the volume to a manageable amount by using multiple individuals to screen the material and separate the potentially relevant from the irrelevant. However, a digital investigation attempts to find material that will assist the investigation with an understanding of the content of the digital files but also the more obscure contextual information.

Relevant privacy cases

FTC Matter/File Number: 1923133
Flo Health has settled Federal Trade Commission allegations that the company shared health information of its users with outside data analytics providers after promising such information would be kept private.

FTC Matter/File Number: 1923140
SkyMed must put in place a comprehensive information security program as part of a settlement with the FTC over allegations the company failed to take reasonable steps to secure sensitive consumer information such as health records.