IBM Security QRadar Incident Forensics
V 7.2.6

用户指南

IBM

备注

使用此信息及其支持的产品前，请阅读第 33 页的『声明』中的信息。

产品信息

本文档适用于 IBM QRadar Security Intelligence Platform V7.2.6 及后续发行版，直到被本文档的更新版本所取代。

目录

IBM Security QRadar Incident Forensics 的使用简介

本指南包含有关通过使用 IBM® Security QRadar® Incident Forensics 调查安全事件的信息。

目标受众

调查者从取证存储库中的网络流量和文档中截取信息。 此信息用于安全事件调查。

技术文档

要在 Web 上查找 IBM Security QRadar 产品文档，包括所有翻译文档，请访问 IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome)。

有关如何在 QRadar 产品库中访问更多技术文档的信息，请参阅访问 IBM Security 文档技术说明 (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)。

与客户支持人员联系

有关与客户支持人员联系的信息，请参阅支持与下载技术说明 (http://www.ibm.com/support/docview.wss?uid=swg21616144)。

有关良好安全实践的声明

IT 系统安全性涉及通过预防、检测和应对企业内外的不当访问来保护系统和信息。不当访问可能会导致信息被篡改、销毁、盗用或滥用，并可能导致系统损坏或者被滥用，包括用于攻击他人。 没有任何 IT 系统或产品应该被认为绝对安全，并且没有任何单一产品、服务或安全措施在预防不当使用或访问方面完全有效。 IBM 的系统、产品和服务设计成合法的综合性安全途径的组成部分，这必定涉及额外的操作过程，并可能需要其他系统、产品或服务才能实现最高效用。 IBM 不保证任何系统、产品或服务不受任何相关方的恶意或非法行为影响，也不保证能够使您的企业不受这些行为影响。

请注意:

此程序的使用可能涉及各种法律或法规，包括与隐私、数据保护、雇佣以及电子通信和存储有关的法律或法规。 IBM Security QRadar 只能用于合法用途并以合法方式使用。客户同意按照适用的法律、法规和政策使用本程序，并承担遵守适用的法律、法规和政策的所有责任。 被许可方表示它将获取或者已经获取允许合法使用 IBM Security QRadar 所需的任何许可或许可证。

备注

IBM Security QRadar Incident Forensics 设计用于帮助公司改善其安全环境和数据。 更具体地说，IBM Security QRadar Incident Forensics 设计用于帮助公司调查和更好地了解网络安全事件中发生了什么。 此工具使公司能够对捕获的网络包数据 (PCAP) 建立索引并进行搜索，并且包含可以将此类数据重建为其原始形式的功能。 此重建功能可以重建数据和文件，包括电子邮件消息、文件和图片附件、VoIP 电话呼叫以及 Web 站点。 与此程序一起提供的手册和其他文档中包含了与此程序的特征和功能以及其配置方式有关的其他信息。 此程序的使用可能涉及各种法律或法规。 包括与隐私、数据保护

、雇佣以及电子通信和存储有关的法律或法规。 IBM Security QRadar Incident Forensics 可能仅用于合法用途并以合法方式使用。 客户同意依据适用的法律、法规和政策使用此程序，并承担遵守适用的法律、法规和政策的所有责任。 被许可方表示它将获取或者已经获取允许合法使用 IBM Security QRadar Incident Forensics 所需的任何许可或许可证。

第 1 章 QRadar Incident Forensics V7.2.6 中的新增功能

IBM Security QRadar Incident Forensics V7.2.6 引入了调查工具，帮助您分析文件和图像是否存在可疑内容或行为。您还可以分析用于显示 Web 页面和协调程序之间的关系或连接的链接。

针对可疑或恶意内容的工件分析

您可以使用工件分析来调查事件，例如，系统如何受到感染以及其他资产是否受到相似影响。

例如，您可以对恢复的包数据使用文件分析功能，以查看所有文件的列表以及这些文件是否包含嵌入文件或脚本。

您可以查看标记为包含可疑内容和嵌入脚本的图像文件。

文件熵分数和分布可以帮助您分辨文件异常，并提供此文件包含遗漏未被检测到的恶意软件的证据，该恶意软件对系统造成影响。

要确定其他可能受到影响的系统，您可以使用链接分析来快速查看之前查看过的所有 Web 站点，以及对受影响 Web 主机的部分访问。

 了解更多...

第 2 章 安全调查

通过 IBM Security QRadar Incident Forensics，您可以检测出现的威胁、确定根源并预防重复发生。 通过使用取证工具，您可以快速将分析聚焦于发起威胁者的身份、其操作方式以及受到破坏的对象。

作为取证调查者，您可以回溯电子犯罪的分布操作，并重构与安全事件相关的原始网络数据。

贵组织首先感知到威胁或潜在安全风险或合规性违规，您设置目标以评估范围、识别所牵涉的实体，并了解动机。

您可以在不同类型的调查（例如，网络安全、内部人员分析、欺诈和滥用以及证据收集）中，根据特定方案使用 IBM Security QRadar Incident Forensics 中的工具。

1. 恢复和重构与 IP 地址的网络会话。
2. 从创建的事件中，您可以查询属性类别以收集证据。

   创建恢复时，会创建事件。
3. 使用搜索过滤器仅检索感兴趣的信息。
4. 根据调查类型，选择为您提供所需证据的取证工具。

可疑内容

您可以使用搜索来查找您了解的攻击者或事件的任何上下文元素或标识。 如果在搜索中使用关键字，会返回可疑内容。某些可疑内容可能与调查相关。

数据透视

数据透视是通过使搜索结果返回的内容显示为热链接来实现的。 例如，如果您搜索“Tom”，那么结果可能包含 Tom 编写的电子邮件、Tom 的聊天记录等上下文信息。 当您单击阅读电子邮件时，每一个资产或实体（例如，附件或 Tom 使用的计算机标识）均显示为链接。 调查者可使用这些链接来快速开展调查。

数字印记

使用“数字印记”来查看数据以及基于频率映射实体（例如，IP 地址、名称和 MAC 地址）之间的关系。 您可以选择一个或多个结果以查看关系的频率和方向。

测试程序

使用测量程序来查看活动时间线，以便您可以回溯攻击。测试程序重构会话并按时间顺序对文档排序。

内容过滤

使用内容过滤来查看内容类别子集（例如，网络邮件、色情内容）以帮助您在搜索时除去干扰或不相关的内容。

网络安全调查

您可以使用 QRadar Incident Forensics 来检测和调查针对关键资产的恶意活动。 您可以使用内建取证工具来帮助补救网络安全违规，并预防再次发生。

使用 QRadar Incident Forensics 调查工具来帮助您发现事件是如何发生的、最大限度降低其影响，并尽一切可能预防再次发生违规。

第一感染源: 识别攻击源

在此方案中，某个组织收到有关可疑违规的警报。 该组织希望寻找到初始攻击点以隔离源头。 该组织必须隔离遭到破坏的实体，预防攻击散播至组织的其他部分。

目标

为解决这些调查中的问题，该组织具有以下目标:

- 确定攻击类型。
- 识别初始威胁入口点。
- 获取有关恶意有效内容的详细信息。
- 了解恶意有效内容如何散播至入口点以外。

调查

使用**取证**选项卡上的工具来帮助您进行调查。

1. 使用自由格式搜索来搜索与恶意有效内容关联的症状属性。
2. 使用内容类别来过滤与调查不相关的内容。
3. 检验产品标记的可疑内容。
4. 使用“数字印记”和“虚拟化”来探索恶意有效内容、犯罪者或目标之间的扩展关系。
5. 使用数据透视，跟踪数据链接，以识别第一感染源。
6. 使用测量程序来查看活动时间线，以便您可以回溯攻击。

遭到安全威胁的系统

在此方案中，某个组织收到警报，其一个或多个系统遭到高级电子攻击技术（例如，水坑式攻击、钓鱼、蛮力攻击或 SQL 注入）的威胁。

目标

为解决这些调查中的问题，该组织具有以下目标:

- 确定组织内遭到破坏的程度。
- 了解每个遭到破坏的系统的操作风险类型。
- 发现初始攻击对规避清理活动和检测执行的任何外围设备操作。

调查

使用**取证**选项卡上的工具来帮助您进行调查。

1. 使用自由格式搜索来搜索恶意有效内容或遭到破坏的资产。
2. 检验产品标记的可疑内容。
3. 使用“数字印记”和“虚拟化”来探索由于系统遭到破坏所导致的实体关系。

4. 使用测量程序来查看活动时间线，以便您可以回溯攻击。
5. 通过使用自由格式搜索、数据透视和可疑内容发现各数据类别之间的不一致或可疑交互。

数据泄漏至未经授权的实体

在此方案中，某个组织收到警报，敏感数据泄漏给组织内部未经授权的实体或者外部各方。

目标

为解决这些调查中的问题，该组织具有以下目标:

- 确定泄漏的数据性质和数据量。
- 了解所采用的技术。
- 发现犯罪者。
- 识别泄漏源。

调查

使用**取证**选项卡上的工具来帮助您进行调查。

1. 使用自由格式搜索来搜索泄漏的数据的标识。
2. 检验产品标记的可疑内容。
3. 通过复审数据重构来复审所有已泄漏或正在泄漏的数据。
4. 使用“数字印记”和可视化来探索所有牵涉的实体关系。
5. 使用测量程序来查看活动时间线，以便您可以回溯攻击。
6. 使用自由格式搜索来发现数据泄漏的动机。
7. 使用数据透视来发现到其他可能已泄漏的数据的链接。

内部人员分析调查

使用 QRadar Incident Forensics 来检测共谋、破坏和访问权不当使用。 识别犯罪者、识别共谋者、识别遭到破坏的系统并记录数据丢失。

访问权不当使用

在此方案中，某个组织收到警报，一个或多个员工正在滥用凭证或者被用作为代理，以访问敏感系统和数据，开展未经授权的活动。

目标

为解决这些调查中的问题，该组织具有以下目标:

- 确定用户身份。
- 解决谁或者哪家组织正在采用此身份开展未经授权的活动。
- 了解访问权滥用的目标。
- 评估该实体是否还具有更多可能被滥用的身份。

调查

使用**取证**选项卡上的工具来帮助您进行调查。

1. 使用自由格式搜索来搜索正在访问敏感系统或数据的身份。
2. 通过查看可疑内容、开展自由格式搜索、数据透视和内容过滤，解决其中哪些访问尝试可疑。
3. 查看受到访问的内容的数据重构。
4. 在测量程序中回溯访问的任何模式并评估频率。
5. 使用“数字印记”来显示单一实体使用的别名。

共谋

在此方案中，某个组织收到警报，一个或多个利益主体正在彼此之间或者与外部各方共谋参与对组织有害的活动。

目标

为解决这些调查中的问题，该组织具有以下目标:

- 确定参与共谋的实体。
- 了解勾结者之间交互的性质和模式。
- 发现方案下隐藏的内容。
- 揭示方案持续时间，以了解风险范围。

调查

使用**取证**选项卡上的工具来帮助您进行调查。

1. 使用自由格式搜索来搜索涉及的实体的标识。
2. 检验产品标记的可疑内容。
3. 使用“数字印记”、可视化和内容过滤来标识可能可疑的关系。
4. 使用测量程序来跟踪所牵涉的实体的活动，获取交互的内容。
5. 通过复审重构的文档发现共谋动机。
6. 使用自由格式搜索和数据透视来查找共谋活动的开端。

破坏

在此方案中，某个组织收到警报，一个或多个利益主体正在尝试破坏运营。 此利益主体可能被用作为代理。

目标

为解决这些调查中的问题，该组织具有以下目标:

- 识别破坏者。
- 了解破坏者采用的技术。
- 评估破坏的影响和范围。
- 确定破坏者利用的漏洞

调查

使用**取证**选项卡上的工具来帮助您进行调查。

1. 使用自由格式搜索来了解破坏的症状。
2. 检验产品标记的可疑内容。
3. 使用可视导航、数字印记和内容过滤来探索症状并检测破坏者的标识。
4. 使用测量程序来跟踪破坏者的活动。
5. 使用数据重构来发现破坏者的角色和动机。
6. 使用数据重构来查看破坏者使用的内容。
7. 使用自由格式搜索、测量程序和可疑内容来显示遭到破坏的系统和破坏者启用的过程。

欺诈和滥用调查

使用 QRadar Incident Forensics 来查找未经授权的交易、未经批准的资源分配、协议偏离以及逃避法律控制措施。

未经授权的交易

在此方案中，某个组织收到警报，存在未经授权的交易，导致对业务运营产生负面的财务影响。

目标

为解决这些调查中的问题，该组织具有以下目标:

- 找到未经授权的交易。
- 标识牵涉未经授权的交易并且应该对此类交易负责的实体。
- 了解未经授权的交易的频率和趋势。
- 评估未经授权的交易的风险范围。

调查

使用**取证**选项卡上的工具来帮助您进行调查。

1. 使用自由格式搜索来搜索任何不一致或可疑的交易。
2. 使用自由格式搜索和数据透视来搜索这些交易的重复状况。
3. 使用数据透视和“数字印记”来发现与可疑交易关联的实体。
4. 通过复审重构的文档，揭示交易内容，以显示定量值。

资源分配未经批准

在此方案中，某个组织怀疑资源分配未经批准，导致对业务运营产生负面的财务影响。

目标

为解决这些调查中的问题，该组织具有以下目标:

- 查找资源的错误分配。
- 标识牵涉资源错误分配并且应该对错误分配负责的实体。

- 了解未经批准的资源分配的动机。
- 评估错误分配的资源的大小和范围。

调查

使用**取证**选项卡上的工具来帮助您进行调查。

1. 针对与分配的资源关联的通信使用自由格式。
2. 使用自由格式搜索、数据透视和“数字印记”来查找进行未经授权的资源分配的实体的标识。
3. 通过复审重构的文档和通过使用可视化处理评估动机时所涉及的交互的内容。
4. 使用测量程序来回溯分配活动，了解错误分配的资源的数量。

协议偏差和逃避法律控制措施

在此方案中，某个组织收到警报，其业务、IT 协议和法律控制措施已被避开，导致负面的财务影响。

目标

为解决这些调查中的问题，该组织具有以下目标:

- 评估逃避的协议或法律控制措施。
- 确定参与此行为的实体。
- 了解这些实体的动机。
- 评估此不当行为的普遍性。

调查

使用**取证**选项卡上的工具来帮助您进行调查。

1. 使用自由格式搜索来搜索受协议或控制措施管辖的业务流程。
2. 使用自由格式搜索、数据透视和数据重构与概括协议和法律控制的文档的交叉引用。
3. 使用内容过滤、自由格式搜索来发现逃避协议/控制措施的具体实例。
4. 使用“数字印记”、可视化数据透视和内容过滤来查找关联的实体标识。
5. 使用测量程序来回溯实体活动，探索可能的动机。

证据收集调查

使用 QRadar Incident Forensics 来评估组织内漏洞风险、量化识别威胁或犯罪者的置信度并优化安全实践。

对识别威胁的信心

在此方案中，某个组织收到有关某些威胁、漏洞利用或漏洞的警报。 为调整本可能抢占正常企业运营的补救工作，他们希望量化任何关联风险的置信区间。

目标

为解决这些调查中的问题，该组织具有以下目标:

- 验证安全性风险的敏感性。
- 确定是否存在安全性风险的证据。
- 评估安全性风险的广度和经济影响。
- 了解安全性风险的本质

调查

使用**取证**选项卡上的工具来帮助您进行调查。

1. 使用自由格式搜索、可疑内容和数据透视来通过使用潜在的针对性实体作为起点，搜索威胁、漏洞利用或漏洞。
2. 使用自由格式搜索和数据透视来编译发生的状况。
3. 使用自由格式搜索来交叉引用可提供对影响的参考的文档。
4. 使用“数字印记”和可视化来识别受影响的实体。
5. 使用测量程序来分析与威胁或犯罪者关联的活动。

重新定义安全实践

新行为和存在风险的行为的检测可刺激组织评估现有安全实践是否充分。 在此方案中，某家组织希望针对自身面临的风险，对自己的安全性规则的有效性加以定性。

目标

为解决这些调查中的问题，该组织具有以下目标:

- 识别新行为或存在风险的行为。
- 评估现有安全性规则的有效性。
- 了解由于动态操作导致出现的安全性漏洞。
- 评估建议的安全实践的有效性。

调查

使用**取证**选项卡上的工具来帮助您进行调查。

1. 使用自由格式搜索来通过使用域和组织知识搜索新行为或存在风险的行为，例如移动用户和基于云的服务的行为。
2. 检验可疑内容，使用测试程序将这些行为与现有安全性规则或实践进行交叉引用。
3. 使用自由格式搜索、测试程序、内容重构和可视化来分析来自安全性规则的警报，了解误报的频率。
4. 使用自由格式搜索、测试程序、内容重构、数据透视和可视化来发现现有安全性规则或实践未检测到的误报。

风险评估

在此方案中，一份概括了某些漏洞、漏洞利用或恶意行为的安全公告提示组织采取风险评估。 风险评估确定组织是否易于受到破坏或者已受到破坏。

目标

为解决这些调查中的问题，该组织具有以下目标:

- 评估组织中是否存在已确定的漏洞。
- 检测是否存在恶意的外部各方。
- 发现任何遭到破坏的证据。
- 确定组织是否是遭到漏洞利用的受害者。
- 确定用户身份。

调查

使用**取证**选项卡上的工具来帮助您进行调查。

1. 使用自由格式搜索来搜索安全公告中指定的漏洞、漏洞利用或其他恶意行为的特性。
2. 使用自由格式搜索来将研究或其他数据交叉引用以派生出指标。
3. 使用测量程序来调查可能利用了已识别的漏洞的交互。
4. 检验产品标记的可疑内容。
5. 使用数据重构复审隐藏在存在潜在风险的交互下的内容。
6. 使用测量程序来回溯存在潜在风险的实体的活动。

第 3 章 启动取证调查

要在 IBM Security QRadar Incident Forensics 中启动调查取证，请使用**快速启动**菜单来浏览和过滤取证存储库中的数据。此启动板包含预定义的摘要查询，您可使用这些查询来启动搜索或者获取实体的关系。

要启动调查取证，请遵循以下指导信息:

1. 从**攻击**选项卡上的某个攻击，启动调查恢复或搜索。
   - 如果右键单击攻击或任何 IP 地址，并运行取证恢复，那么取证会从捕获设备检索指定时间范围内的原始捕获数据，抽取并重新构建文档，然后将结果添加到取证存储库。
   - 如果您右键单击某个攻击或任意 IP 地址，然后运行取证搜索，那么会对取证存储库进行过滤并在其中搜索该 IP 地址。然后会在**取证**选项卡上的主窗格中显示结果。您可以通过构建查询来优化搜索。

   当 QRadar Incident Forensics 收到搜索请求时，会处理包捕获数据并恢复为这些数据发送到预期接收方时所采用的格式。例如，会将 Microsoft Word 文档恢复为 Word 文件。IP 语音电话呼叫将恢复为音频文件。然后将使用元数据和文件内容来对恢复后的文件建立索引，从而使这些文件可搜索。
2. 在**取证**选项卡上，单击**快速启动**。

   在您运行恢复或搜索（而不是运行自由格式的搜索并构建您自己的查询）后，可以从**取证**选项卡上的**快速入门**菜单使用预定义的查询来快速启动调查。例如，您可以查看**可疑内容**类别并运行某个查询（例如**实体警报**）。*可疑内容*基于已定义的一组规则，这些规则针对表示可以行为的内容。*实体警报*标示出涉及违反安全策略的可能恶意实体。

   内容分类和过滤功能有助于减少返回的数据量。
3. 从**网格**中选择要查看的文档。

   QRadar Incident Forensics 将返回按优先级排列的搜索结果。与搜索引擎优化对因特网搜索返回的站点划分优先级的方式相似，出现频率最高的文档将显示在列表顶部。

   您可以通过单击连接和搜索与文档关联的元数据以启动对数据的透视。数据透视功能提供了多种不同的搜索视图和数据摘要。
4. 要调查所有操作和安全事件之间的关系，请在文档视图中选择一个链接并右键单击**获取关系**。

   在您调查属性之后，请对通过连接实体而收集到的信息进行过滤。
5. 单击**数字印记**身份线索并获取一组经过汇编的关联项。

   数字印记是元数据的索引，可通过跟踪恶意用户线索来帮助确定可疑攻击或流氓软件。在构建这些关系时，QRadar Incident Forensics 使用来自网络源（例如 IP 地址、MAC 地址以及 TCP 端口和协议）的数据。它能够查找诸如聊天标识之类的信

息，还能够从字处理或电子表格应用程序中读取诸如作者标识之类的信息。数字印记通过将实体的身份与其他用户或实体的标识信息相链接来帮助揭示两者之间的关联。

QRadar Incident Forensics 搜索和书签

调查者使用 IBM Security QRadar Incident Forensics 可从网络流量和文档截取相关数据。

搜索和标记记录

为启用直观的取证活动，QRadar Incident Forensics 会检索包数据并吸取其他内容。 此技术提供由搜索驱动的数据探索、会话重建和法律情报来帮助安全事件调查。

调查者通过粗粒度操作来集中执行其调查，然后继续微调针对相关的最终结果集的调查结果。 简单的高级别方法是首先搜索和标记许多记录。 然后，重点关注已标记的记录以标识最后一组记录。 确定相关材料并微调查询以包含和/或排除项。 使用此材料来验证假设。

在跟踪新线索时，可以通过使用其他方法来跟进这些线索。 您可以使用可视化和分析工具来手动和自动评估相关性结果。 此外，您还可以使用不同查询来获取同一个问题的其他方面。

处理标记的结果

当您找到对调查非常重要的结果后，您可以标记这些结果以便在执行更深入的检查和最终确定。 标记对象不仅仅局限于您认为需要标记的内容。 如果有问题，对其进行标记。 您想要排除不相关的材料并重点关注您认为相关的内容。

对您认为相关的一组结果进行标记后，您可以微调您的检查。

1. 通过可视化和分析工具检查每个已标记的文档。
2. 将案例注释附加到这些文档并最终决定每个文档与案例的相关性。
3. 如果记录不相关，请除去该书签。

   在调查过程中，您确定了存储库中的相关材料，现在您已具有一组相关的已标记的记录。
4. 打印、导出或处理相关记录。

文档搜索和调查

调查者搜索关于安全事件如何发生的线索或假设的相关文档。

搜索

调查者使用取证存储库来截取满足重要特征的文档，而不是手动筛选大量文档，大多数文档与案例无关。 例如，在特定时间段内出现的与重要主题有关的文档，或由可疑攻击者发送或接收的文档。

搜索可以是明确的。 例如，“查找准确的字符串‘Mission Alpha’”是明确的。 搜索也可以是非特有的。 例如，“查找存在于存储库中的所有社会安全号码”是非特有的。

搜索可以是简单的，仅基于一个条件。 复杂搜索结果必须满足多个条件。 例如，查找两个可疑攻击者之间关于特定主题的所有电子邮件，并排除包含附件的电子邮件，属于复杂搜索。 搜索的目的是快速并准确地将记录减少至可管理的工作集。 通过减少调查者检查的文档集数量，文档与案例相关的可能性更高。

对 IP 地址或端口运行恢复

您可以对一个或多个 IP 地址或端口运行恢复。如果不输入 IP 地址或端口，那么将恢复所有 TCP 和 UDP 流量。如果输入多个 IP 地址或端口，必须使用逗号进行分隔。

限制: 通常，您一次可输入约 7 个 IPv4 地址和 7 个端口，或最多约 255 个字符。 **IP 地址**和**端口**字段将与其他短语组合起来以创建过滤器字符串。过滤器字符串的长度不能超过 255 个字符。

取证案例

案例是已导入文档和包捕获文件的集合的逻辑容器。

案例由有权创建案例的管理员或调查者创建。管理员创建并将案例分配给调查者。 当调查者从 IBM Security QRadar 中的 IP 地址检索包捕获数据时，他们可能会创建新的案例。

相关任务:

『将 PCAP 文件和文档从外部系统上载至取证案例』
您可以将外部数据上载至特定案例中。

集合

使用集合可对诸如包捕获 (pcap) 数据文件、PDF 或网络流之类的特定源中的相关数据进行分组。

集合用于标识和管理相关数据组。您可以在完成调查后快速删除集合中的组数据。

集合由管理员或调查者创建。 管理员创建集合以将数据手动装入 IBM Security QRadar Incident Forensics。 管理员还将集合添加到案例。 当调查者从 IBM Security QRadar 中的 IP 地址启动包捕获数据检索时，他们可能会创建新的集合。

请考虑集合和集合名称的以下规则:

- 集合名称必须唯一。
- 案例包含一个或多个集合。
- 集合可以添加到多个案例。
- 调查者拥有具有同一个集合的两个案例时，搜索结果返回重复数据。
- 如果上载新的 pcap 时，集合名称不是唯一的，那么在上载新的 pcap 前删除原来的集合。

将 PCAP 文件和文档从外部系统上载至取证案例

您可以将外部数据上载至特定案例中。

开始之前

管理员必须为希望上载外部文件的用户启用安全的 FTP 许可权。

关于此任务

IBM Security QRadar Incident Forensics 可以吸收来自网络上的任何可访问目录的导入数据。 数据可采用多种格式，包括但不限于以下格式:

- 来自外部数据源的标准 PCAP 格式文件
- 文档，例如，文本文件、PDF 文件、电子表格和演示文稿
- 图像文件
- 来自应用程序的流式数据
- 来自外部 PCAP 数据源的流式数据

您可以将多个文件上载至案例。

限制: 案例名称必须唯一。 您不能创建与现有案例同名的案例。

过程

1. 在 FTP 客户机中，执行以下步骤:
   a. 请确保将传输层安全性 (TLS) 选作为协议。
   b. 添加 QRadar Incident Forensics 主机的 IP 地址。
   c. 创建使用创建的 QRadar Incident Forensics 用户名和密码的登录。
2. 连接至 QRadar Incident Forensics 服务器并创建新目录。
3. 要通过 FTP 传输和存储 PCAP 文件，在为案例创建的目录下，创建名为 `singles` 的目录，并将 PCAP 文件拖到该目录中。
4. 要通过 FTP 传输和存储非 PCAP 文件的其他文件类型，在为案例创建的目录下，创建名为 `import` 的目录，并将文件拖到该目录中。
5. 要重新启动 FTP 服务器，请输入以下命令:

   ```
   etc/init.d/vsftpd restart
   ```

6. 要重新启动服务器以将文件从上载区域移至 QRadar Incident Forensics 目录，请输入以下命令:

结果

您可以在**取证**选项卡上的某个工具中看到自己的案例。

取证存储库查询

调查者指定要从取证数据库检索的文档的特征。 多个查询用于查找一组文档以供调查。

对一小组文档的多个查询和手动检查优先于筛选整个存储库。 后续查询和精确查询的构想通常是在检查不相关文档期间产生的。

查询项的数量增加和特异性导致具有更高关联性的结果集。 您的目标是定义已知的尽可能多的结果并且在可能的情况下高度明确。可向搜索条件输入任何数量的查询项。以

空格或布尔运算符隔开项。 只以空格隔开的项暗示布尔逻辑 OR 运算符。 OR 运算符表示查找任何项都是同样满足需要的。满足大多数搜索项的结果位于列表顶部以指示查询项的匹配程度。

单个搜索条件也称作查询项。搜索通常包含多个查询项。 单个搜索的查询项集合也称作查询字符串。 熟练地用公式表示查询需要练习，但是并不难。 它只包含一些查询项以及了解如何创建和否定为您提供所需内容的项组合。 由于查询字符串保存在 QRadar Incident Forensics 中，因此您可以根据对数据的更多了解不断微调您的搜索。

相关任务:

第 25 页的『使关系和关联可视化』
使用“可视化”窗口可查看已恢复文档中的属性之间的关系。例如，您可以检查与特定电子邮件地址通信的电子邮件地址。

自由格式查询项

调查者通过在**取证**选项卡上的搜索条件字段中直接输入查询项来搜索准确的字符串匹配项。 您可以使用单词查询或多词查询。

下表描述了可以使用的搜索查询的类型。

表 1. 自由格式查询的类型

搜索查询的类型	描述	示例
单词查询	在文档中搜索一个项。	puppies
具有通配符的单词查询	为查询项中间或末尾的一个或多个字符搜索匹配项。 **限制**: 在搜索中，通配符不能用作第一个字符。	te?t test* te*t
多词查询	指定按查询项相关性顺序返回的搜索结果。 先列出包含这两个查询项的文档，再列出只包含其中某个查询项的文档。 只包含一个查询项的文档按照单个查询项的发生次数排列。	free puppies
带双引号的多词查询	与准确的字符串匹配。 包含这两个词但是未按照此顺序排列并且非常靠近的文档未作为结果返回。 实际上，双引号将这些两个词转变为单个字符串或查询项。 对于搜索引擎，它们不再被看作两个独立的词。	″free puppies″
使用 AND 运算符的多词查询	指定这两个查询项必须存在于文档中以产生匹配项。 查询项可以使用任何顺序并且相互之间不需要非常靠近。	free AND puppies

元数据标记

已标记公共实体，从而使调查者能够从相关文档快速检索准确的结果集。

根据会话、文档或协议的类型，许多元数据字段可能会用于 Incident Forensic 索引。

指定元数据标记名称时，它必须是准确的并且存在于取证存储库中。

下表列出了元数据标记搜索的类型。

表 2. 元数据标记搜索

元数据标记搜索的类型	格式	示例
标准	MetadataTag:<value>	ApplicationProtocol:http
通配符	MetadataTag:*	CreditCardNumber:*
范围	MetadataTag:[<start value> TO <end value>	Duration:[30 TO 56]

相关概念:

第 18 页的『 文档注释 』
调查者对文档进行标记并将注释添加到文档以跟踪有关其案例中文档的构想和原理阐述。

布尔值组合

使用简单的布尔运算符可将多个查询项捆绑在一起以创建有高度针对性的查询字符串。 通过设置正确的格式，这些查询字符串可以返回与调查者的查找对象完全匹配的结果。

基本布尔运算符为 AND、OR、NOT 和 ()。 AND 运算符指定文档中的两个查询项必须匹配。 OR 运算符指定可在文档中找到任何一个查询项。 NOT 运算符否定或除去与已否定的查询项匹配的结果。 () 运算符对查询项和值进行分组以将函数应用于集合，将多个值应用于单个函数或使语法更加清晰。

布尔运算符必须大写。

下表列出了布尔运算符和查询字符串的示例。

表 3. 查询字符串的布尔运算符

布尔运算符	查询字符串示例	说明示例
AND	TcpPort:80 AND Protocol:http	两个查询项用于查找所有标准 Web 流量。 如果在端口 8080 上发生 Web 测试，那么它将不是匹配项，因为这两个查询项将不为 true。
OR	Collection:yahoo* OR Collection:cnn* OR Collection:msn*	三个查询项用于将结果限制于取证存储库中 Yahoo、CNN 和 MSN 文档集合中的结果。
NOT	ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080 OR 81)	使用非标准端口搜索流量。 第一个查询项查找标准 HTTP 流量，第二个查询项除去使用已接受的 HTTP 端口的所有流量。
()	(ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080)) OR (ApplicationProtocol:pop* AND NOT ServerTcpPort:110) NOT (Collection:yahoo* OR Collection:cnn* OR Collection:msn*)	这些查询有效地使用括号来实现复杂的目的。 如果没有括号，那么要用公式表示并调试，这些查询会更长并且更复杂。

查询构建器工具

使用查询构建器工具可以创建搜索或管理保存的搜索。

查询构建器工具通过示例向调查者生动演示了创建使用查询项分类列表的强大搜索的过程。

表 4. 查询构建器工具的参数

参数	描述
选择类别	过滤**选择字段**列表中提供的元数据标记列表。
选择字段	用于标记取证存储库中的信息的元数据标记。
查询示例	运行**查询输入**字段中的查询并报告结果数。
新建	单击**插入查询**时，将现有查询替换为新的查询。
AND	单击**插入查询**时，将新的查询与现有查询结合。 文档必须与这两个查询项匹配。
OR	单击**插入查询**时，将新的查询与现有查询结合。 文档必须与其中一项匹配。

调查者可以保存并组织文件系统上文件夹中的搜索，允许在调查者之间共享。 调查者将已保存的查询的描述或名称用于引用、管理和理解。

查询选项卡上的**使用查询**功能用于将已保存的查询发送到**搜索条件输入**字段以便执行。

调查者使用先前查询列表来查找先前已运行的查询，并通过选择要运行的查询并单击**插入查询**来重新执行这些查询。

查询过滤工具

查询过滤工具使用活动数据来提供构建持久过滤器的视觉线索。

查询过滤器是可减少查询字符串查询活动文档集的持久的后台过滤器。 通过使用过滤器，您可以在查询字符串未装有过多静态查询项的情况下减少可用文档集。 由此能够更多地控制查询字符串。

由于查询过滤器具有案例依存过滤器类型列表、动态更新和实时结果摘要，因此它是开始调查的好场所。 过滤器类型列表填充了在您的可用案例中找到的所有值。 您可以快速查看自己拥有的案例中包含的数据。 选择或清除过滤器类型列表项会自动更新结果摘要。 您可以快速看到过滤器的有效性，以及使用过滤器时剩余文档集的大小。

不建议微调缺省查询过滤器用于您要复用的查询。 对于要保留的查询，请创建新的查询过滤器。 如果您已经修改缺省查询过滤器，请在完成时将其重置以防止从以后的搜索查询中错误地排除文档。

活动过滤器的结果

调查者在查询过滤器工具上的结果摘要部分中查看活动过滤器的结果。

随着过滤器的更改，摘要进行更新以显示文档总数和可用文档数。 文档总数是在应用过滤器前调查者可用的文档数。 可用文档数是在应用过滤器后可用的文档数。 调查者使用这些计数来判断其过滤器的有效性并在构建时进行适当调整。

对查询过滤器工具搜索过滤器

调查者为其已分配的案例过滤数据。数据按过滤器类型分成组，例如，IP 地址或 MAC 地址。

通过使用逻辑操作切换，调查者可以包含或排除从列表中选择的项。

每个搜索过滤组都具有逻辑操作切换，可以将该切换设置为包含或排除在列表中选择的项。 当设置为包含时，列表中的项使用逻辑 AND 连接，这表示每个可用文档都包含所有选定项。 当设置为排除时，使用逻辑 OR，这表示每个可用文档都不包含任何选定项。

调查者可以使用 **UserQuery** 组来表示要添加到过滤器中的其自己的查询字符串。

限制搜索返回的文档数

可向 IBM Security QRadar Incident Forensics 查询添加过滤器以限制在搜索结果页面中看到的文档数或文档类型。

过程

1. 在**取证**选项卡上，单击**查询过滤器**图标。

   数据将按过滤器类型分组。
2. 在“搜索过滤器”窗口中，单击**包含**或**排除**来为每个过滤器类型选择是否要在搜索结果中包含文档。
3. 要在过滤器中查找某个项，请遵循以下步骤:
   a. 在**过滤器类型**列中，展开某个过滤器组。
   b. 在“搜索”窗口中，选择条件并单击**查找**。

      当您在 **Web 类别**过滤器组中搜索记录时，将显示所有匹配的类别字段。例如，当您搜索 **Web 类别 等于 chat**、**Chat** 和相关类别，那么将显示诸如**即时消息传递**、**Web 邮件/统一消息传递**、**搜索引擎/Web 目录/门户网站**以及**云**之类的类别字段。

文档注释

调查者对文档进行标记并将注释添加到文档以跟踪有关其案例中文档的构想和原理阐述。

可在主要结果屏幕以及按时间顺序排列网格上的测量程序工具中标记文档，该网格显示在交互期间交换的文档的顺序。 由于查询和调查可能比较复杂，因此调查者对所有记录（包括不重要的文档）进行标记。 使用书签可以不需要重新创建复杂查询和调查范围。可在标记记录后创建注释。

在调查期间，您曾经多次想要遵循两个或多个路径。 使用浏览器功能可复制您所处的当前选项卡。 复制选项卡可以帮助您避免需要记得返回并遵循其他路径或者需要记得如何

到达分支点。 您可以根据需要任意次数地复制当前选项卡。 遵循其他选项卡以及与书签有关的文档中的每个不同路径。 您可以添加注释，以指定指向每个已标记文档的路径。

注释是在调查时记录想法的一种方式。 注释只能由管理员除去。 注释标有调查者的用户标识和输入时的时间戳记。 导出文档后，使用重建的文档及其属性输出注释。

相关概念:

第 15 页的『元数据标记』
已标记公共实体，从而使调查者能够从相关文档快速检索准确的结果集。

第 4 章 调查工具

调查者使用测量程序工具、数字印记工具、导出工具和可视化工具以不同方式管理数据。

搜索结果页面是**取证**选项卡上的缺省页面。**网格**选项卡上提供了搜索结果。调查者使用网格上的搜索结果来快速搜索和访问文档。 在**网格**选项卡上，使用测量程序工具、数字印记工具、导出工具和可视化工具来进一步执行调查。

行指示符

行指示符提供结果集中返回的每个文档的唯一标识。 使用行指示符将文档和所有必需的相关文档发送到“重建视图”可视化工具。

行排序

您可以对网格中显示的行进行排序。 由于结果总数可能会大于网格中显示的结果数，因此无法对整个结果集进行排序。

文档查看指示符

文档查看指示符是交替显示红色和绿色的小圆圈，用于指示调查者是否查看了文档。

文档选择

调查者使用显示的文档选择器来选择结果网格中显示的文档数。 您可以使用 SELECT ALL 将文档发送到后续函数并且发送大量文档以供处理或可视化。 使用显示的文档选择器来选择文档时，您将选择所有文档，而不是网格中存在的文档。

网络和文档可视化

调查者使用可视化工具来检测模式，了解特定时间段内网络流量最大和文档拥堵的位置，并查看可疑内容。 例如，调查者可以使网络流量模式可视化，例如，在公司时间后访问的服务器。

VGrid 工具分为时间块。 网格上的红色矩形描述诸如网络流量或文档之类的可疑内容。绿色矩形描述常规内容。 颜色鲜艳的块指示更大流量。 颜色饱和度越高，流量就越大。时间块的鲜艳程度与 VGrid 工具中显示的当前数据有关。 例如，将不同时间块装入更多数据时，颜色鲜艳的时间块变暗。

调查者可以查看网络流量的类型以及包含内容的每个时间块的文档数。

检查时间块中的网络流量和文档

调查者可能想要检查特定时间块中的各个文档、已浏览的 Web 站点或已发送的电子邮件。

过程

1. 在**取证**选项卡上，选择 **VGrid** 选项卡。
2. 使用以下某个选项来检查时间块中的内容:
   - 要查看网络流量类型和文档数，请将光标悬浮在该时间块上。
   - 要搜索时间块中的内容，请选择一个或多个时间块。 右键单击并选择**搜索所选时间块**。
   - 要查看事件的顺序，请选择该时间块，然后选择**测量程序**。
   - 要使内容可视化，请选择时间块，然后选择**可视化**。

测量程序工具

使用测量程序工具可以在安全事件中的一系列事件发生时使其可视化。

调查者使用此工具来查看可疑攻击者的所见内容及其操作。 测量工具在像电影放映一样的可视化器中描述安全事件中活动的时间顺序。 由于测量程序工具以时间为导向，因此从结果屏幕中选择单个文档不显示太多内容。 如果选中的文档数量过少，请在**属性**选项卡中扩大所选文档的时间范围。 通过单击**显示上下文**链接延长时间。

调查者可以按案例时间、协议和 IP 地址过滤其查询。

您可以通过**列表**选项卡来查看已发送和接收的按时间顺序排列的文档列表。 在测量程序工具中描述的交互的逐步重建。

绿色的文档标识号指示由调查者复审文档，带有红色标识号的文档则未复审。

重建的文档视图

视图选项卡显示在“列表”视图中的屏幕左侧选择的文档的重建视图。

左侧强大的序列组合和右侧的重建使您能够查看可疑攻击者在网络上所见的内容以及所执行的操作。 除了遍布网络的可视文档，测量程序还显示已发生的后台计算机到计算机握手和证书交换。

相关任务:

第 31 页的第 5 章，『调查 IP 地址的网络流量』
要获取在安全事件中发生的会话中的相关内容的可视性，您可以恢复并重建与 IP 地址关联的网络流量。 您也可以在与 IP 地址有关的现有案例中进行搜索。

截取的文档内容

文本选项卡显示从文档截取的内容。 文档内容没有格式。

此文本来自搜索引擎索引器。

在 QRadar Incident Forensics 中导出文档

在 IBM Security QRadar Incident Forensics 中，除了导出的 pcap 文档之外，其他所有导出文档都包含重建的文档、文档的原始文本、属性以及附加到文档的注释。

导出 pcap 文档时，不会进行任何重建。例如，当您导出 Web 页面时，将下载主连接已建立期间浏览器所下载的所有内容。通常，大多数文本内容都是在主连接已建立期

间下载的。但是，大多数现代浏览器使用多个连接来下载更多的项（例如样式表和图像），这些项不会导出。当您进行导出时，首先不会重建 pcap 内容。

另一个例子是复杂的协议（例如 FTP 和 VOIP），此类情况下有一个主命令和一个控制连接，另外还有一个数据连接。如果您导出 VOIP 呼叫或 FTP 下载项的 pcap 文件，那么不会重建数据，并且可能得到不期望的结果。

将文档导出为 pcap 文件

您可以从多个 IBM Security QRadar Incident Forensics 和 IBM Security QRadar Packet Capture 设备将文档导出为 pcap 文件。

限制: 导出为 pcap 格式的内容不会重构。

过程

1. 要从所选文档导出数据，请在**取证**选项卡上的恢复网格中，选中文档旁边的复选框，然后单击**导出**。

   最多可以选择 25 个文档导出为 pcap 格式。
2. 从**选择导出类型**列表中，单击 **PCAP**。
3. 在导出 QRadar Incident Forensics 主机的所有文档之后，可以单击**下载**。
4. 如果文档导出失败，请单击**失败**消息再次导出文档。

结果

如果导出单个 pcap 文件，将下载 pcap 文件。如果导出多个 pcap 文件，这些 pcap 文件将合并为一个压缩文件 (.zip)，然后下载该压缩文件。

每个文档都存储 QRadar Incident Forensics 主机的 IP 地址以及该文档最初所来自的 QRadar Packet Capture 设备的 IP 地址。如果除去 QRadar Incident Forensics 主机或者移动 QRadar Packet Capture，那么可能无法进行导出。

数字印记

*数字印记*是标识身份踪迹的一组已编译的关联和关系。 “数字印记”重建网络关系以帮助揭露攻击实体的身份、通信方式以及通信对象。

使用“数字印记”工具可快速回答下列重要问题:

- 哪些是此可疑攻击者、计算机或 IP 地址的已知内容？
- 谁是此可疑攻击者的交谈对象？
- 谁在其联系网络中？
- 可疑攻击者是否尝试隐瞒其身份？

联机标识

诸如电子邮件地址、Skype 地址、MAC 地址、聊天标识、社交媒体标识或 Twitter 标识之类的联机标识用于确定实体或人员。 自动标记网络流量和文档中找到的已知实体和人员。

IBM Security QRadar Incident Forensics 使相互交互的已标记的标识关联以生成数字印记。

数字印记报告中的收集关系表示与攻击者关联的连续收集的电子存在、与网络有关的实体或任何数字印记元数据术语。 调查者可以单击与文档关联的任何已标记的印记标识。 所产生的数字印记报告以表格格式列出并按标识类型组织。

获取关系信息

数字印记报告显示*中心标识*和所有其他标识之间的交互。 *中心标识*是作为安全事件中重要源的联机标识。

许多类别中的顶级标识通常是该标识类型或类别中的中心标识的身份。 例如，如果标识为 MAC 地址，那么交互最多的电子邮件地址很可能属于拥有计算机的可疑攻击者。 但是，如果动态分配 IP 地址，那么您还必须调查在一段时间范围内分配的 IP 地址。

其他类别与中心标识之间的关联通常较弱。 在决定基于数字印记执行操作之前，请使用独立源来验证数据。 使用“数字印记”工具将调查半径范围扩大到更多的可疑攻击者和实体。

调查关系以跟踪身份踪迹。

数字印记重建网络关系以帮助您确定攻击实体以及与其通信的其他实体。

“数字印记”工具显示关联事件的频率分布。 该工具可显示实体之间的关系并对这些关系进行计数。 计数越高，关系越强。 例如，如果您查看电子邮件地址与其他实体之间的关系，那么可以看到通信双方的身份。 您可以查看与此电子邮件地址关联的 IP 地址、嫌疑人访问的 IP 地址，以及与此电子邮件地址关联的其他名称。

在分布式部署中，您可以选择查看组织中的一个节点的关系。

过程

1. 从恢复网格中的文档列表中选择一个结果，然后单击**数字印记**选项卡。
2. 从该列表中，选择要探索的项。

   缺省情况下，数字印记报告以表格格式列出，按标识类型组织。 将显示与中心标识交互的所有标识。交互标识按标识类型组织并按交互频率排序。
3. 如果您看到所需标识，请进行选择。

   标识是超链接，您可以将其用作其他报告的中心标识。将创建其他选项卡并显示新的中心标识。 您可以看到与给定的可疑攻击者进行交互的人员以及嫌疑人交互的交互对象。 您可以将调查半径范围扩大到与其交互的更多的可疑攻击者和实体。
4. 要查看其他主机，请从**选择远程主机**列表中选择 IP 地址。

   在分布式安装中，您可以选择 QRadar Incident Forensics 主机，然后查看数字印记。缺省视图为主要主机，但是您可以选择与 QRadar Incident Forensics 主机关联的任何辅助主机。
5. 要查看中心标识与其他标识交互的关联和关系的可视化，请单击**使数据可视化**选项卡。

可视化工具

您可以直观地探索多个属性和数据类别中的关联和关系。

使用“可视化”窗口来查看一个、两个或更多文档的元数据关系图。使用大量文档时，调查者可以全面了解元数据关系和相对频率。 然后，调查者可以按照这些路径来进一步调查安全事件。

通过更改一个或两个关系，可以很容易地使用不同的关系来重建所选文档的可视化。

可视化显示所选文档中包含的每个关系并显示关系的频率。 每个节点都表示所选文档中有关联的一块不同的元数据。 大小表达与其他节点比较的相对频率。 链接显示在若干块不同的元数据之间发现的连接并通过大小表达频率。 调查者可以使用节点来标识进一步调查的可能途径。

使关系和关联可视化

使用“可视化”窗口可查看已恢复文档中的属性之间的关系。例如，您可以检查与特定电子邮件地址通信的电子邮件地址。

过程

1. 在恢复网格中，单击要调查的文档的复选框，然后单击**可视化**。
2. 选择布局、要显示的文档数以及要查看的属性之间的关系，然后单击“刷新”。
3. 使用缩放控件来控制查看图像的详细程度。
4. 要执行新的搜索或修改活动过滤器，请右键单击节点。

   从上下文敏感菜单中，您可以恢复该块元数据以执行新的搜索。 您还可以修改活动过滤器以包含或排除元数据。

   限制: 在一个“可视化”窗口中，您一次最多可查看 9999 个文档。

针对可疑或恶意内容的工件分析

作为安全分析人员，您可以通过分析重构工件（例如文件和图像）来查找逃避了检测的威胁。要了解协调程序和工件之间的连接，您还可以调查与这些文件和图像之间的链接。

示例 - 使用工件分析查找攻击来源（第一感染源）

John 是 Replay Industries 的安全分析人员。虽然所有安全措施均已就位，一些系统仍受到感染。当他确定并隔离这些系统之后，John 需要找出这些系统如何受到感染以及其他资产是否受到相似的损害。

来自 IP 地址的包恢复

从 IP 地址和涉及的大概时间范围着手，John 能够使用 QRadar Incident Forensics 恢复相关包数据。

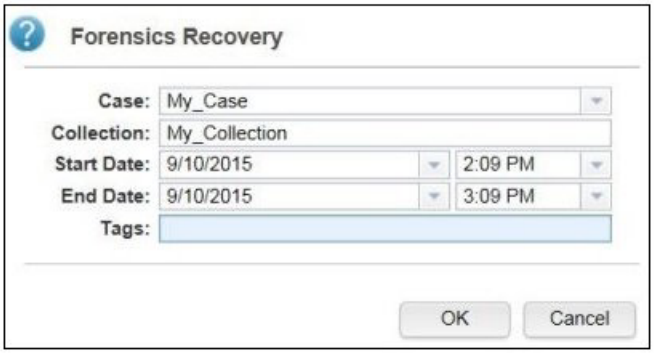


图 1. 从 IP 地址恢复

文件分析

John 首先使用 QRadar Incident Forensics 中包含的文件分析功能查找可执行文件内容。现在，他看到所有文件列表、文件的发送频率、文件是否包含嵌入文件或脚本以及文件熵值。John 迅速看到 QRadar Incident Forensics 标记为可疑内容且包含嵌入脚本的图像文件。

Doc #	File Name	Extension	Description	Protocol	Frequency	Suspect Content	Embedded Script	Embedded Files	File Size (Bytes)	File Hash (SHA-256)	Entropy
1	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	1916	70c6e673cd0150b1ffa89e	4.93731
2	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	163060	dbbb35dcf2e494f068b9d1	5.74523
3	index.php	php	JavaScript	http	1	No Suspect Content	No Embedded Script	0	164112	909a0b9fa48182b58dd85	5.38451

图 2. 文件分析属性

*文件熵分数*测量数据的随机性，用于查找加密的恶意软件，熵分布也明确显示了文件中失去原有内容的部分。进一步分析证明此文件包含新形式的恶意软件，该软件逃避了现有安全措施而未被检测到，对受影响系统负有责任。

在下图中，熵用于指示每字节位数的可变性。由于数据单元中的每个字符都由 1 个字节构成，因此熵值指示字符的变化以及数据单元的可压缩性。文件中的熵值变化可能指示文件中隐藏了可疑内容。例如，高熵值可能指示数据加密存储并压缩，较低值可能指示有效内容在运行时解密并存储在不同的节中。

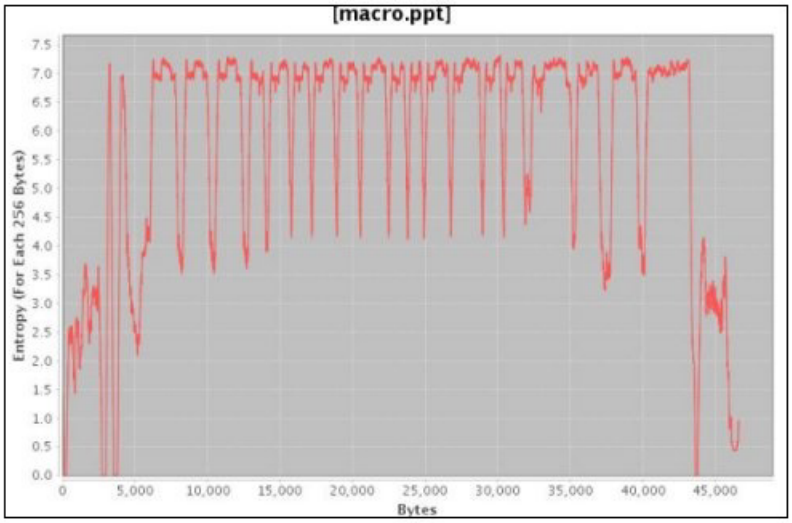


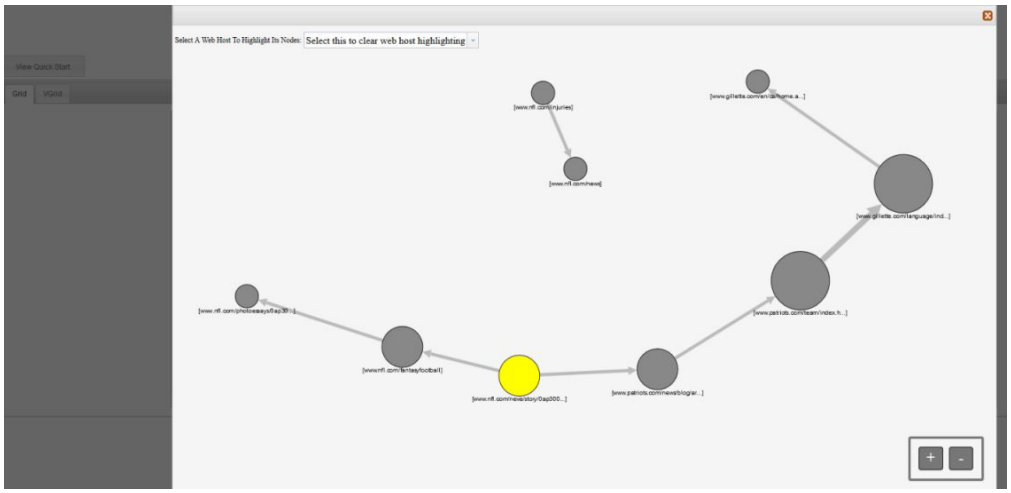
图 3. 显示嵌入脚本的文件熵图形示例

John 现在需要了解此文件来自何处以及还有谁可能拥有此文件。John 使用 QRadar Incident Forensics 快速查找提供了受影响图像文件的 Web 服务器。有问题的 Web 页面广泛用于广播大家都很喜爱的 NFL 团队的最新新闻，该页面受到损害。尽管该 Web 站点包含许多图像，但只有 John 先前使用文件分析发现的那个图像包含嵌入恶意软件。

用于显示 Web 站点通信的链接分析

要确定可能受影响的其他系统，John 使用链接分析快速显示查看过的所有 Web 站点，尽管与 Replay 有业务往来的各个公司的 Web 站点存在大量流量，也可以清楚地看到对受影响 Web 主机的一小部分访问。John 分析这些链接以查看其网络上的哪些其他服务器用于访问此 Web 主机。

在他的调查中，John 使用图形中表示 Web 页面的节点，使用节点间的箭头表示 Web 页面之间的关系或事务，以便快速评估流量模式和查看文档的遍历方式。节点越大，文档在其路径中包含的链接越多，链接箭头越大，链接的使用次数越多。



作为流行的 NFL 新闻站点，发现一些其他服务器与该 Web 主机联系并可能受到影响并不出奇。

图像分析

为缩小下载了恶意图像文件的服务器的范围，John 切换到图像分析并能够快速查看已发送或收到的所有图像文件。

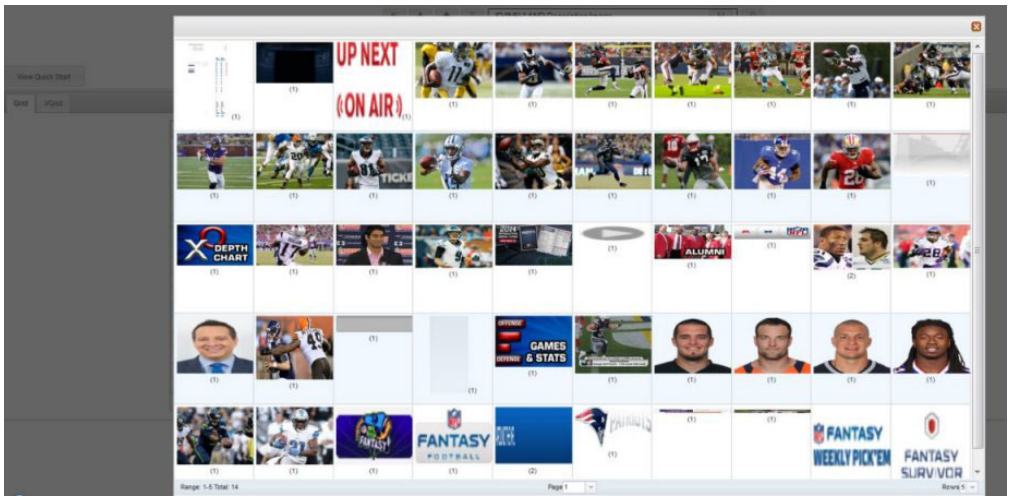


图 4. 图像分析示例

John 快速确认其受影响的所有服务器以及他不知道的 2 个服务器，并具有对受损害图像文件的所有访问权。

John 还确定访问了同一 Web 站点的一些其他服务器没有下载受影响的文件。John 现在已获得隔离这 2 个额外服务器所需的信息，并创建了受影响文件的新文件散列，Replay Industries 可以上载该文件并与 IBM X-Force® Exchange 上的其他用户共享。

分析文件中是否有嵌入内容和恶意活动

要调查文件中是否存在隐藏威胁，可以查看文件熵值，下载嵌入文件和脚本以便进一步分析，并查看文档及其属性。

由于入侵者可能会对容器文件中的二进制文件内容进行模糊处理，因此可以使用 IBM Security QRadar Incident Forensics 中的文件分析检查文件是否包含嵌入脚本或其他二进制内容。

*文件熵*测量文件中数据的随机性，并用于确定文件是否包含隐藏数据或可疑脚本。随机性范围是 0（不随机）到 8（完全随机，如加密文件）。单元的可压缩性越强，熵值越低；单元的可压缩性越弱，熵值越高。

在下图中，熵用于指示每字节位数的可变性。由于数据单元中的每个字符都由 1 个字节构成，因此熵值指示字符的变化以及数据单元的可压缩性。文件中的熵值变化可能指示文件中隐藏了可疑内容。例如，高熵值可能指示数据加密存储并压缩，较低值可能指示有效内容在运行时解密并存储在不同的节中。

过程

1. 在**取证**选项卡上，从**网格**视图选择一个或多个恢复文件。
2. 从网格顶部的调查工具菜单中，单击**文件分析**。

   在结果中，每一行网格包含文档的一项分析数据，例如文件名、描述、是否检测到可疑内容以及熵值。
3. 要按特定属性（例如熵）对文件排序，请单击关联的列标题。
4. 从文件列表中，右键单击文件以便进一步调查

- 要查看文档及其属性，单击**显示文档**。
- 要查看熵图形并检查嵌入文件或脚本是否包含恶意软件，单击**显示熵**。

  您可以使用熵值来指示文件是否包含恶意内容。例如，ASCII 文本文件通常可高度压缩，并具有较低熵值。加密数据通常不可压缩，且普遍具有较高的熵值。恶意软件通常打包和隐藏在这两种文件和图像中。
- 要下载嵌入文件，请单击**抽取嵌入文件**并选择要下载的文件。

  此选项仅可用于包含嵌入文件或脚本的文档。文件将下载到 Web 浏览器的下载位置。请注意不要在未受保护的环境中打开可能有害的脚本。

分析图像中是否有隐藏威胁或可疑活动

查看过的图像按照大小以及与括号中的频率数字的相关性排序。如果员工使用公司资源来查看不合适的、受限的或被禁止的图像，此分析对您来说可能很有用。例如，图像可能与属于安全性违规目标的飞机、某些建筑物或位置有关。

通过图像分析，可以在一个显示屏中查看来自一个或多个包捕获文件中一个或多个文档的最相关图像，而不必被迫打开每个文档并查看图像。

过程

1. 在**取证**选项卡上，从**网格**视图，选择描述中包含图像的一个或多个文档。
2. 从网格顶部的调查工具菜单中，单击**图像分析**。

   在结果中，文档中包含的所有图像的缩略图版本都按照相关性顺序显示。图像旁边括号中的数字指示文档中的图像实例数量。如果将鼠标放在缩略图图像上方，图像会变大。
3. 右键单击图像以获取进一步调查
   - 要查看图像及其属性，单击**显示文档**。
   - 要查看熵图形并检查图像是否包含恶意软件，单击**显示熵**。

     您可以使用熵值来指示文件是否包含恶意内容。例如，位图图像文件和 ASCII 文本文件通常可高度压缩，并具有较低熵值。加密数据通常不可压缩，且普遍具有较高的熵值。恶意软件通常打包和隐藏在这两种文件和图像中。

分析连接和关系的链接

在链接分析中，链接显示查看过的 Web 站点之间的共性。在安全事件调查期间，您可以快速查看是否存在重叠，以及人们之间相互通信的方式。

例如，如果您认为一组犯罪者相互协作但并不确定如何协作，可以查看一些用户的一组文档，并使用链接分析来显示公共 Web 页面。然后，您可以调查特定 Web 站点。

过程

1. 在**取证**选项卡上，从**网格**视图选择一个或多个 Web 页面。
2. 从网格顶部的调查工具菜单中，单击**链接分析**。

   如果 Web 站点之间存在关系，那么 cytoscape 图表会将 Web 页面显示为圆圈（节点），将与 Web 页面之间的链接显示为箭头。节点越大，文档在其路径中包含的链接越多，链接箭头越大，链接的使用次数越多。选中节点为黄色。

3. 要调查来自特定 Web 主机的通信，请从**选择 Web 主机**列表中，选择 Web 主机。

   表示来自所选 Web 主机的 Web 页面的节点突出显示为深灰色圆圈。
4. 要放大或缩小圆圈（节点）和箭头的大小，可使用放大 (+) 或缩小 (-) 控件。

   还可以上下滚动鼠标滚轮以增大或减小节点与箭头的大小。
5. 要移动一个或多个节点，可单击并拖动节点。

   您可以通过单击背景的任意位置，然后按住并拖动来移动整个图形。

从文档的“属性”页面运行恢复

当查看文档的**属性**选项卡时，可以针对 IP 地址或端口运行恢复。

过程

1. 从**取证**选项卡上的“搜索”页面，执行搜索。
2. 从返回的文档列表中，单击以打开文档。
3. 单击**属性**选项卡。
4. 单击 IP 地址或端口。
5. 从菜单中单击**运行恢复的对象**。

第 5 章 调查 IP 地址的网络流量

要获取在安全事件中发生的会话中的相关内容的可视性，您可以恢复并重建与 IP 地址关联的网络流量。 您也可以在与 IP 地址有关的现有案例中进行搜索。

从 IP 地址重建网络流量后，将创建事件。 调查者可以使安全事件中的一系列事件可视化或查看事件中的文档。

IBM Security QRadar Incident Forensics 对每个已恢复文件中的所有可用网络数据、文件数据、元数据和文本字符建立索引。

在分布式部署中，多个捕获设备和 QRadar Incident Forensics 主机捕获并处理数据。 您可以按主机和捕获设备查看聚集的事件恢复结果。

过程

1. 要创建案例并从包捕获设备获取数据，在 QRadar 中，右键单击 IP 地址，然后选择**运行取证恢复** 。
   a. 下表提供了数据恢复参数的指南:

表 5. 数据恢复的参数

参数	描述
案例	用于调查的案例。 **限制**: 案例名称必须唯一。
集合	将恢复的数据分成一个集合并关联到该案例。 **限制**: 集合名称必须唯一。 如果集合名称存在于案例中，那么删除原始集合。
开始日期	数据包捕获的开始日期和时间。
结束日期	数据包捕获的结束日期和时间。
标记	用于从相关文档快速检索准确的结果集的元数据标记。 **限制**: 不允许使用e # 符号。 您可以使用其他特殊字符，例如: $、% 或 *。

   b. 单击**确定**，然后单击**取证**选项卡。

      故障诊断: 如果您看到一条消息，指示您无权恢复数据，请确保您的安全概要文件有权访问 IP 地址。 在某些实例中，如果您在**标记**字段中使用了 # 字符，那么可能会看到此消息。

   c. 单击三角形图标以查看您的事件。
   d. 要使该事件的一系列事件可视化，请单击**跳至测量页面结果**。
   e. 要查看该事件中的文档，请单击**跳至搜索页面结果**。
2. 要搜索 IP 地址的现有案例，在 QRadar 中，右键单击 IP 地址，然后单击**运行取证搜索**。
   a. 在**取证**选项卡上，单击事件（三角形）图标。
   b. 要调查与事件关联的活动聚集，请将光标悬浮在案例上以突出显示该案例，然后单击搜索图标。

c. 要在分布式部署中按 QRadar Incident Forensics 主机和捕获设备调查活动，请展开**案例**条目，然后展开**集合**条目。

d. 要查看事件中按时间顺序排列的交互列表，请将光标悬浮在集合上以突出显示该集合，然后单击测量程序图标。

相关概念:

第 22 页的『重建的文档视图』

视图选项卡显示在“列表”视图中的屏幕左侧选择的文档的重建视图。

声明

此信息为在美国提供的产品和服务而开发。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务的操作，由用户自行负责。

IBM 可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并不意味着授予用户使用这些专利的任何许可。 您可以用书面形式将许可查询寄往:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

有关双字节字符集 (DBCS) 信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

本条款不适用英国或任何这样的条款与当地法律不一致的国家或地区:

International Business Machines Corporation“按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。 某些国家或地区在某些交易中不允许免除明示或暗含的保证。 因此本条款可能不适用于您。

此信息可能包含技术上或印刷上的错误。 将对此信息进行定期的更改；这些更改将编入该出版物的新修订版中。 IBM 可以随时对本资料中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的: (i) 使其能够在独立创建的程序和其它程序（包括本程序）之间进行信息交换，以及 (ii) 使其能够对已经交换的信息进行相互使用，请与下列地址联系:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本资料中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际软件许可协议或任何同等协议中的条款提供。

此处包含的任何性能数据都是在受控环境中测得的。 因此，在其他操作环境中获得的数据可能会有明显的不同。 有些测量可能是在开发级的系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。 此外，有些测量是通过推算而估计的， 实际结果可能会有差异。 本文档的用户应当验证其特定环境的适用数据。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

所有关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

所有 IBM 的价格均是 IBM 当前的建议零售价，可随时更改而不另行通知。 经销商的价格可与此不同。

本信息包含日常业务运作所使用的数据和报表的示例。 为了尽可能完整地说明这些示例，示例中可能会包括个人、公司、品牌和产品的名称。 所有这些名字都是虚构的，如果与实际商业企业使用的名称和地址有任何相似之处，纯属巧合。

如果您正在查看本信息的软拷贝，图片和彩色图例可能无法显示。

商标

IBM、IBM 徽标和 ibm.com® 是 International Business Machines Corp.，在全球许多管辖区域的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。当前 IBM 商标列表可从 Web 站点“版权和商标信息”(www.ibm.com/legal/copytrade.shtml) 获取。

Microsoft、Windows、Windows NT 和 Windows 是 Microsoft Corporation 在美国和/或其他国家或地区的商标。

隐私策略注意事项

IBM 软件产品（包括软件即服务解决方案，以下统称“软件产品”）可能使用 cookie 或其他技术收集产品使用信息、帮助改善最终用户体验、定制与最终用户的交互或用于其他用途。 在许多情况下，软件产品不收集个人可标识信息。 部分软件产品可帮助您收集个人可标识信息。 如果该软件产品使用 cookie 来收集个人可标识信息，那么有关该产品使用 cookie 的具体信息如下所述。

根据部署的配置，“软件产品”可能使用会话 cookie 来收集每个用户的会话 ID，以用于会话管理和认证用途。 可以禁用 cookie，但是这也将删除 cookie 启用的功能。

如果为此软件产品部署的配置提供您以客户身份通过 cookie 或其他技术从最终用户收集个人可标识信息的功能，那么您应该查找关于适用于此类数据收集的所有法律的您自己的合法建议（包括声明和许可）。

有关使用各种技术（包括 cookie）来达到这些目的的更多信息，请参阅 IBM 隐私策略 (http://www.ibm.com/privacy) 和 IBM 在线隐私声明 (http://www.ibm.com/privacy/details) 中标题为“Cookies, Web Beacons and Other Technologies”的部分，以及“IBM Software Products and Software-as-a-Service Privacy Statement”(http://www.ibm.com/software/info/product-privacy)。

词汇表

本词汇表提供 IBM Security QRadar Incident Forensics 软件及产品的术语和定义。

在本词汇表中，使用了下列交叉引用:

- *参见*从非首选术语引用首选术语，或者从缩写引用完整形式。
- *另见*引导您参考相关的或者对立的术语。

要了解其他术语和定义，请参阅 IBM Terminology Web 站点（在新窗口中打开）。

『(A)』 『(B)』 『(C)』 『(D)』 『(G)』 『(H)』 第 38 页的『(J)』 第 38 页的『(L)』 第 38 页的『(M)』 第 38 页的『(Q)』 第 38 页的『(S)』 第 38 页的『(X)』 第 38 页的『(Y)』 第 39 页的『(Z)』

(A)

安全事件 (security incident)
正常网络操作遭到侵犯、破坏或攻击的事件。

案例 (case)
包含在数据库中的有关于特定调查的信息。

(B)

包捕获设备 (packet capture appliance)
拦截和记录交通数据的独立设备。

包捕获信息 (packet capture information)
由捕获设备收集的流量数据信息。

捕获设备 (capture device)
请参阅包捕获设备 (packet capture appliance)。

布尔运算符 (Boolean operator)
内置函数，在评估一组操作时，指定 AND、OR 或 NOT 的逻辑运算。布尔运算符包括 &&、|| 和 !。

(C)

测试程序工具 (surveyor tool)
在可视化器中显示安全事件中活动的时间顺序的工具。

超流 (superflow)
这是由多个具有类似属性的流组成的单个流，旨在通过减少存储约束来增加处理能力。

(D)

对话 (conversation)
在两个或更多个网络端点之间通过取证方式重构的数据流。例如，社交网络对话。

(G)

攻击 (attack)
未经授权的个人对软件程序或网络系统的运行加以破坏的任何尝试。另请参阅攻击者 (attacker)。

攻击 (offense)
这是作为对受监视条件的响应而发送的消息或生成的事件。 例如，攻击将提供有关是否违反了某个策略或网络是否遭受攻击的信息。

攻击者 (attacker)
尝试破坏信息系统或访问并非用于常规访问的信息的用户（人或计算机程序）。另请参阅攻击 (attack)。

(H)

恢复作业 (recovery job)
恢复已查询的捕获数据并将其转发给解封设备以供吸收的过程。

(J)

集合 (collection)
与案例关联的专门指定的一组数据。例如，一组按顺序排列的捕获的网络包。

加密 (encryption)
在计算机安全性领域，这是将数据变换为某种难以理解的格式的过程，此过程使得原始数据不可获取或者只能通过解密过程获取。

假设 (hypothesis)
事件的建议解释，基于案例中收集的可用证据。假设必须可经过测试和证伪。

解封 (decapping)
反编译包捕获数据以使所有吸收的数据生成为结果报告的过程。

(L)

类别 (category)
根据特定描述或分类分组在一起的一组项目。类别可以是某一维度内不同的信息级别。

连续收集的电子存在 (continuously collected electronic presence)
攻击者的联机身份，作为链接的数字印记集合。

流记录 (flow record)
两个主机之间的对话记录。

流量 (traffic)
在数据通信中，传输通过某条路径中特定点的数据量。

漏洞 (vulnerability)
操作系统、系统软件或应用程序软件组件中的安全漏洞。

(M)

面包屑 (breadcrumb)
Web 界面元素，显示用于在站点中的位置。它通常包含一系列超链接，显示在页面顶部或底部。这些链接指示已查看的页面，并支持用户浏览回开始位置。

(Q)

取证调查者 (forensic investigator)
从网络流量中截取相关数据并记录在取证存储库中的用户。

(S)

身份 (identity)
这是来自数据源的属性集合，这些属性表示人员、组织、场所或项。

事件 (incident)
请参阅安全事件 (security incident)。

数字印记 (digital impression)
包含单个案例内彼此关联的标签标识的报告。

数字印记关系 (digital impression relationship)
与案例关联的标签标识之间的关系。

(X)

吸收的网络流量 (ingested network traffic)
捕获的网络流量，已经过取证解封过程的处理。

协议检查程序 (protocol inspector)
专门的检查程序，旨在从网络协议（例如，HTTP 或 FTP）截取取证数据。

(Y)

异常 (anomaly)
这是与网络的预期行为的偏差。

域检验程序 (domain inspector)
专门的检查程序，旨在从特定域 Web 站点（例如，Facebook 或 Gmail）解构并截取取证数据。

元数据 (metadata)
描述数据特征的数据；描述性数据。

元数据关系图 (metadata relational map)
显示来自案例文档的相关元数据的图。

(Z)

中心标识 (centering identifier)

所有其他标识都与之交互的类别项目。中心标识是调查中的中心项目。

踪迹 (trail)

将案例中牵涉的个人连接到案例外的个人的数字印记。

索引