Computer Science and Engineering Department, SVNIT, Surat
B.tech.-IV, Semester-VIII
Cyber Law and Forensics - CS402
Final Practical Questions

Odd numbers

(5 Marks each)

1. Identify the applications that will automatically start whenever computer gets started.
2. When the log_tempering.csv was last opened?
3. Identify USB devices attached to the system.
4. Identify the file having manipulated time stamp.

Following is the email header. Analyse the header and identify whether it is legitimate or not. If not, from where it was sent.

Delivered-To: thakarakash@gmail.com
Received: by 2002:a17:907:744:0:0:0:0 with SMTP id xc4csp2849996ejb;
Mon, 12 Sep 2022 22:25:15 -0700 (PDT)
X-Google-Smtp-Source:
AA6agR4y55cusWDge6ym7TZTOuJOLXsiTniRqpIt6alMfXXAP6Co5Elr0Z8HQRALUQFlI1y6BcZ/
X-Received: by 2002:a17:907:1c90:b0:77f:b1ae:9f44 with SMTP id nb16-
20020a1709071c9000b0077fb1ae9f44mr2476003ejc.304.1663046714834;
Mon, 12 Sep 2022 22:25:14 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1663046714; cv=none;
d=google.com; s=arc-20160816;
b=s26SufBTw2ICr8VCFKHKXbnJdJVwGef7D92g8aqjJHSHhLpcSo3XaJfB9256MSfBIc
V3P7lnVYvV57YvipwW845PXCnjVUXl1wmOxW30jSIX1pk/AwdOEpLRjRaiyN0NRuO6ML
5bKfRG+uUv0G365PLn2c18jZuOyfllo99jFNHjSqvwMqpJh/vwSTakQLdTcK2hAoCDPA
nz2OQ+SB7w+hYH7Lt7ucqZShCHHtUX+PH34uxJk2/+eiKwwCyVDMKl/Q0llUqB611Jmb
9+P5u9dfM1mInveI/MM3ESNQlF2RiTbhOZf2FpJIyazpauRxau6YlBOBsKkMFiYqiDR0
/+IQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=content-transfer-encoding:mime-version:message-id:subject:from:to
:date:dkim-signature;
bh=eSSUWZYhACdAdmRQ+rzfXL//rJv96Ucebjxx7sa4V+g=;
b=AM2O9RCT3G6K/p0C+Rh4b50W6l3KTOS9e5Y52ZQ8BTG0dijolCxjgM1wbGF47FADz8
gQaOcYmAX7w9eBFTztObOb5x1S23mRs6aKCoVl8Jk5zTaopKwMkK9P2prGE6dg+hcQXg
lS7FqrUtcMw/oKR2Khrc9t+uCS61d27uc/mZWWdMpPupEYvnaIyY+k7P+tgwX/6axWur
EBqLJBHg9H7QqMAAgDNxLgJJdzGu5TRbirk3JgFgrLWL670XWxLBmXWgfyBZiF+Mju3Y
mg/5Z0fyvX5I3DWwK4+yppMlygeLhnyFQtRQ1R+vp+iivWi3B6x8Zf6ngVqgAM7y1FXQ
i6XQ==
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@s6.eternalimpact.info header.s=mail header.b=tGNPcxog;
spf=pass (google.com: domain of noreply@anonymousemail.me designates 193.46.56.97 as permitted
sender) smtp.mailfrom=noreply@anonymousemail.me;
dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=anonymousemail.me
Return-Path: <noreply@anonymousemail.me>
Received: from s6.eternalimpact.info (s6.eternalimpact.info. [193.46.56.97])
by mx.google.com with ESMTPS id ht21-
20020a170907609500b0078002807b94si35864ejc.80.2022.09.12.22.25.14
for <thakarakash@gmail.com>
(version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
Mon, 12 Sep 2022 22:25:14 -0700 (PDT)
Received-SPF: pass (google.com: domain of noreply@anonymousemail.me designates 193.46.56.97 as
permitted sender) client-ip=193.46.56.97;

Authentication-Results: mx.google.com;
dkim=pass header.i=@s6.eternalimpact.info header.s=mail header.b=tGNPcxog;
spf=pass (google.com: domain of noreply@anonymousemail.me designates 193.46.56.97 as permitted sender) smtp.mailfrom=noreply@anonymousemail.me;
dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=anonymousemail.me
Received: from authenticated-user (s6.eternalimpact.info [193.46.56.97]) (using TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits)) (No client certificate requested) by s6.eternalimpact.info (Postfix) with ESMTPSA id AA60780457 for <thakarakash@gmail.com>; Tue, 13 Sep 2022 05:25:13 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=s6.eternalimpact.info; s=mail; t=1663046713; bh=eSSUWZYhACdAdmRQ+rzfXL//rJv96Ucebjxx7sa4V+g=; h=Date:To:From:Subject:From; b=tGNPcxogsjTCxYpYbaaSUle6bH5slrZZECbPC/aDmTY6Tc+soB7PT2UofMapBr5wj
9CI8l7j7cftgUafCEuNvJ64ZF5bZfu3jNeuK81biAsaMGxoFkfBl2cBxS27Ecm4CVq
CHjB7j7hri9FLW0oR2b0HuZSaJ0/OR8LhMYEt0ycp4VlPXTw2yQdWrDFZAvwL10yRo
tJCbAMt0dBtE8dERLRR+uPOP4rdr15ee8JgnY38CoJUjBXUZN6HMKLY86PdiR5PyaM
fX6l4AbUVorvSCoNG2MuYy/2T+uoTsDB3c8BWS0fmnR1cb4xv+ciN2LjYXJ8ARHqs/
cBQmlOlpGQUMg==
Date: Tue, 13 Sep 2022 05:25:12 +0000
To: thakarakash@gmail.com
From: Anonymousemail <noreply@anonymousemail.me>
Subject: Sample
Message-ID: <155923a0f56c3c42176e910bc72492ad@anonymousemail.me>
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="b1_YzNqVAYlKG3V5yctLfck8peIB0nTiLTdw8Pvucm3s"
Content-Transfer-Encoding: 8bit

--b1_YzNqVAYlKG3V5yctLfck8peIB0nTiLTdw8Pvucm3s
Content-Type: text/plain; charset=us-ascii

This is a sample mail

--b1_YzNqVAYlKG3V5yctLfck8peIB0nTiLTdw8Pvucm3s
Content-Type: text/html; charset=us-ascii

Powered by Anonymousemail → Join Us! This is a sample mail

--b1_YzNqVAYlKG3V5yctLfck8peIB0nTiLTdw8Pvucm3s--